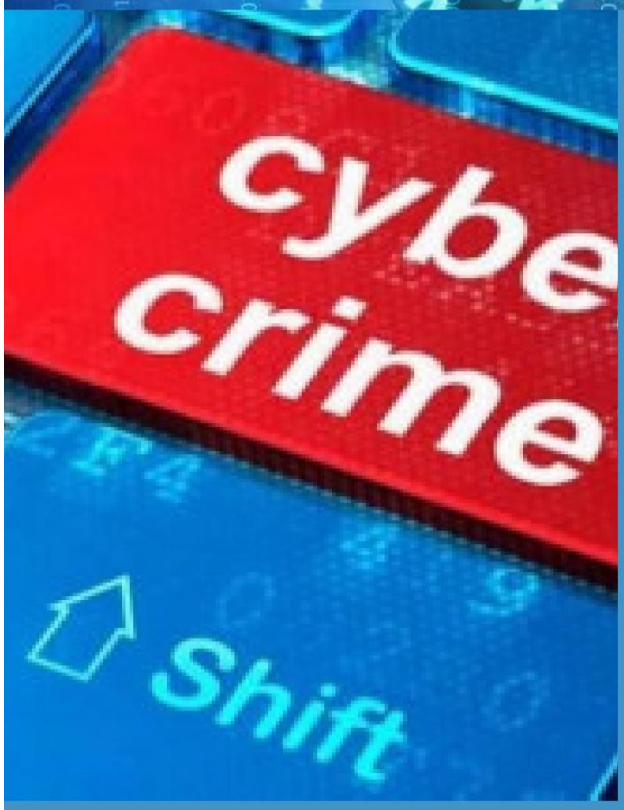


الجرائم الإلكترونية الاقتصادية وتحديات التنمية

الملتقى الوطني عن بعد عبر منصة المودل بتقنية 3B

يوم السبت 24 سبتمبر 2022

مخبر الدراسات القانونية البيئية
كلية الحقوق و العلوم السياسية
جامعة 8 ماي 1945
قالمة

جامعـــة 8 ماي 1945 قالمـــة
كليـــة الحقوق والعلوم السياسيـــة
مخبـــر الدراسات القانونيـــة البيئيـــة

ينظم

الملتقى الوطني عن بعد عبر منصة المودل بتقنية B3 بعنوان :

الجرائم الالكترونية الاقتصادية وتحديات التنمية

يوم السبت 24 سبتمبر 2022

الرئيس الشرفـــــــي: أ.د. صالح العقون رئيس جامعة 8 ماي 1945 قالمة

رئيسة اللجنـة العلميـة : أ.د. شوايدية منية

رئيسة اللجنة التنظيمية: أ.د. العايب سامية

أعضاء اللجنـة العلميـة

أ.د/ سحري فضيلة	عنابة	د/ دريد كمال	أم البواقي	د/ مشري راضية	قالمة
أ.د/ وفاء شيعاوي	الجزائر	د/ سهام عباسي	بريكة	د/ بن بوعبد الله نورة	باتنة
أ.د/ حميدي حميد	عنابة	د/ بولحية شهرة	بريكة	د/ العايب ريمة	قالمة
أ.د/ حسينة شرون	بسكرة	د/ بن عشي حفصية	باتنة	د/ بوشارب إيمان	قالمة
أ.د/ باخويا دريس	أدرار	د/حميداني محمد	قالمة	د/ موشارة حنان	قالمة
أ.د/ العايب سامية	قالمة	د/ بوحجر حسام	قالمة	د/ يلس آسيا	قالمة
د/ بن بوعبد الله منية	سوق اهراس	د/ مقلاتي مونة	قالمة	د/ محمودي سماح	بريكة
د/ ميهوب يزيد	برج بوعريريج	د/ بوقندورة عبد الحفيظ	أم البواقي	د/ قرانة عادل	عنابة

أعضاء اللجنة التنظيمية

الأستاذ فرنان فاروق	الدكتورة موشارة حنان	ط/ لعرابة منال	ط/ نزار بلال
الأستاذ مهيدي كمال	الدكتورة رقطي منيرة	ط/ بن سعادة نبيل	ط/ فراح ربيعة
	ط/ كحل الراس سماح	ط/ حساينية مسعود	

إشكاليـة الملتقى الوطني

يعيش العالم حاليا العديد من المتغيرات الحديثة على الصعيد الدولي أهمها ثورة تكنولوجيا المعلومات والاتصال التي تعتبر من أهم سمات العصر لحديث، حيث برزت تأثيراتها المختلفة على المجال الاقتصادي والاجتماعي والثقافي.

وقد كان من نتاج التطور ظهور أدوات واختراعات وخدمات جديدة فى مختلف المجالات ولقد نتج عن الثورة التكنولوجية تلك، ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التى نعرفها من حيث البيئة التي تتم فيها هذه المعاملات.

يقصد بالمعاملات الإلكترونية كل المعاملات التي تتم عبر عدة أجهزة إلكترونية مثل الهاتف، والفاكس، وأجهزة الحواسب، وشبكة الإنترنت، ومؤخراً عن طريق الهاتف المحمول، وتعتبر جرائم الكمبيوتر والانترنت، أو ما يسمى Cyber Crimes جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل علي المستويات الاقتصادية والاجتماعية والثقافية والأمنية.ولقد أضحت تشكل خطرا محدقا على كل المجتمعات العربية والغربية.

الجرائم الالكترونية قد تمتد للقطاع الاقتصادي، ولكل النشاطات التجارية التقليدية منها والالكترونية ، لذلك يطلق عليها اسم الجرائم الالكترونية الاقتصادية، حيث ترتكب في المجال الاقتصادي بصفة عامة ، ويمكن أن ترتكب في أي مرحلة من مراحل العملية الاقتصادية ، وتحديداً في مرحلة الإنتاج أو التوزيع أو والاتجار بالسلع والخدمات، هذه الجرائم تمس بالاقتصاد

وتعتبر الجريمة الالكترونية الاقتصادية جريمة مستحدثة تُعّرف بنفس أركان الجريمة التقليدية، إلا أنها تغيرت بفعل التقنية المتطورة ، حيث ارتكبت بوسائل مستحدثة، **انطلاقا مما تقدم تتبلور إشكالية الملتقى في ما يلي:**

- **ما هي آثار الجرائم الالكترونية على التنمية الاقتصادية وطنيا ودوليا؟**
- **ما مدى تأثير الجرائم الالكترونية على التنمية الاقتصادية وطنيا ودوليا؟**

محـاور الملتقى الوطني:

المحور الأول: ماهية الجرائم الالكترونية(المفهوم،- الأسباب – الأهداف- الأنواع)

المحور الثاني: صور الجرائم الالكترونية الاقتصادية وآثارها على التنمية الاقتصادية

المحور الثالث: المجرم ألمعلوماتي وأدوات الجريمة الالكترونية الاقتصادية

المحور الرابع: آليات مكافحة الجرائم الالكترونية الاقتصادية وطنيا ودوليا

البرنامج ليوم السبت 24 سبتمبر 2022

الجلسات الثلاث تسير في نفس الوقت بعد الحضور الجماعي للافتتاح الرسمي للملتقى والاستماع للمداخلة الافتتاحية.

مراسيم الافتتاح على الساعة: 09:00 صباحا	**كلمة السيد : مدير الجامعة** **كلمة السيدة : عميدة الكلية / مديرة المخبر** **كلمة السيدة : رئيسة اللجنة العلمية للملتقى أ.د منية شوايدية**

رئيس الجلسة الأولى : الدكتور فنطازي خير الدين

الرقم	المحاضر	عنوان المحاضرة	الجامعة	الصفحة
1	د. مشري راضية	المداخلة الافتتاحية: تحديات إثبات الجريمة الالكترونية	جامعة قالمة	20-1
2	د. بوسنة رابح	ماهية الجريمة الالكترونية (أركان الجريمة الالكترونية)	جامعة قالمة	31-21
3	أ.د نجاح عصام ط/ حيمر زليخة	الجريمة الالكترونية في القانون الجزائري (الدوافع والأنواع)	جامعة قالمة	45-32
4	د.ديب أكرم	الجريمة الإلكترونية "الأسس والمفاهيم "	جامعة باتنة	60-46
5	د/ عطية صورية بن قدور	ماهية الجرائم الالكترونية	جامعة تلمسان	69-61
6	د/ رفاف لخضر د/ معوش فيروز	خصوصية الجريمة الالكترونية	جامعة برج بوعريريج	82-70
7	د/ فنطازي خير الدين	أسباب الجرائم الإلكترونية	جامعة قالمة	104-83
8	د/ بوبرطخ نعيمة	خصوصية المفهوم العام للجريمة الالكترونية	جامعة قسنطينة	115-105
9	د/ بطيحي نسمة	ماهية الجرائم الإلكترونية (دراسة تحليلية في مفهوم الجريمة الالكترونية وخصائصها وأنواعها)	جامعة سطيف2	132-116
10	د/ سلطانة عبد الرحمان زكريا	الجريمة الالكترونية كمفهوم مستحدث	جامعة بشار	146-133
11	د/ بشيخ أم الخير د/ حايطي فاطيمة	الجريمة المعلوماتية في ظل التشريع الجزائري	جامعة تيارت	160-147
12	د/ بلحاج خالدية	ماهية الجرائم الالكترونية الاقتصادية	سيدي بلعباس	170-161
13	د/ زيوش عبد الرؤوف د/ زغيشي مصطفى	الجرائم الالكترونية الاقتصادية: المفهوم والأسباب	جامعة إليزي	179-171
14	أ.د/ شوايدية منية أ/ كحل الراس سماح	القانون الواجب التطبيق على الجرائم الاقتصادية الإلكترونية	جامعة قالمة	191-180

مناقشة عـــــامـــــة، ملخص توصيات الجلسة الأولى

رئيس الجلسة الثانية : الدكتورة فلكاوي مريم				
15	د/ بن دعاس لمياء	خصوصية الجريمة الالكترونية "التعريف –الأنواع– الخصائص	جامعة باتنة 1	202-192
16	د/بن عزوز حاتم أ/شريطي أسامة	معالجة مفاهيمية لصور الجريمة الالكترونية الاقتصادية وانعكاستها على الاقتصاد	جامعة تبسة	212-203
17	أ.د/ باخويا إدريس أ/ مهيدي كمال	الجريمة الالكترونية المنظمة	جامعة أدرار جامعة قالمة	228-213
18	د/ فراقة رمضان د/ رقطي منيرة	جرائم الاحتيال على وسائل الدفع الالكترونية وتأثيره على التجارة الالكترونية والتنمية الاقتصادية	جامعة قالمة	248-229
19	د/ حملاوي نجاة د/ سلالي مصطفى	آثار الجرائم الالكترونية على الجانب الاقتصادي	جامعة إليزي جامعة بسكرة	259-249
20	د/ موشارة حنان	الجرائم الالكترونية الاقتصادية وآثارها على جباية التجارة الالكترونية	جامعة قالمة	272-260
21	د/ مامي هاجر	أشكال الجريمة الإلكترونية الاقتصادية وآثارها على المتعاملين الاقتصاديين	جامعة الجزائر	283-273
22	د/عبد المالك درعي	النظام القانوني للجريمة الالكترونية الماسة بحقوق الملكية الفكرية	جامعة تيزي وزو	295-284
23	د/ بوترفاس حفيظة	القرصنة الالكترونية للعلامات التجارية	جامعة تلمسان	315-296
24	أ.د/عيشوش محمد الحافظ أ/ زاوي عبد السلام	الجرائم الالكترونية كمحفز لتنمية الكفاءات البشرية	جامعة الوادي	330-316
25	د/فلكاوي مريم	خصوصية السلوك الإجرامي للمجرم المعلوماتي	جامعة قالمة	346-331
26	د/فوغالي بسمة	خصوصية المجرم المعلوماتي	جامعة سطيف	357-347
27	د/بوشارب هانية د/شبوعات موسى	دوافع المجرم المعلوماتي	جامعة غرداية	375-358
28	أ/ فرنان فاروق	أدوات المجرم المعلوماتي	جامعة قالمة	388-376

مناقشة عـــــامـــــة، ملخص توصيات الجلسة الثانية

رئيس الجلسة الثالثة : الدكتورة مجدوب لامية				
29	د/ جحايشية نورة د/عزالدين وفاء	الحماية الموضوعية للنظام المعلوماتي في التشريع الجزائري	جامعة قالمة	400-389
30	د/ حساين عومرية	الإطار الإجرائي للجريمة الالكترونية وسبل مكافحتها	المركز الجامعي افلو	418-401
31	أ.د/ بخوش هشام أ/ حندل رشيد	فعالية التشريعات العقابية في مكافحة الجريمة الالكترونية	جامعة سوق هراس	432-419
32	أ/ رزايقية الزهرة	أحكام مكافحة الجريمة الالكترونية في قانون العقوبات الجزائري	جامعة قالمة	444-433
33	د/بن بوعبد الله نورة	تسليم المجرمين كآلية دولية لمكافحة الجرائم الالكترونية الاقتصادية	جامعة باتنة	459-445
34	د/مجدوب لامية	الصعوبات التي تواجه التعاون الدولي في مواجهة الجرائم الالكترونية الاقتصادية وكيفية التصدي لها	جامعة قالمة	467-460
35	د/ حاتم مولود	الأدلة الرقمية آلية لمكافحة الجريمة الالكترونية	جامعة تيزي وزو	478-468
36	د/ العايب ريمة	الحماية الجنائية للمستهلك الالكتروني من الإعلانات المضللة في عقود التجارة الالكترونية	جامعة قالمة	496-479
37	د/ شملال عبد العزيز أ/ حمدي حنان	الآليات المستحدثة لمكافحة الجرائم الالكترونية الاقتصادية في مرحلة البحث والتحري	جامعة أم البواقي	509-497
38	د/ حنان مسكين د/ فاطمة شيخ	الجريمة الالكترونية وآليات التصدي لها في التشريع الجزائري	جامعة سعيدة جامعة مستغانم	522-510
39	د/ بورطال أمينة	استحداث القطب الجزائي لمكافحة الجريمة الالكترونية الاقتصادية في التشريع الجزائري	جامعة عين تموشنت	538-523
40	د/ مقلاتي مونة	إستراتجية مواجهة الجريمة عبر خيار المدن الآمنة	جامعة قالمة	548-539
41	أ.د/ العايب سامية أ/ عرابة منال	قراءة في أحكام غرامة الصلح كآلية لحماية المستهلك الالكتروني على ضوء القانون 05/18	جامعة قالمة	561-549
مناقشة عـــــامـــــة، ملخص توصيات الجلسة الثالثة				

المداخلات

راضية مشري
radiavocat@gmail.com
جامعة 08 ماي 1945 قالمة

المداخلة الافتتاحية: تحديات إثبات الجريمة الإلكترونية

الملخص:

إن الجريمة الإلكترونية باعتبارها من الجرائم المعاصر العابرة للحدود الوطنية، تخضع في إثباتها إلى طرق الإثبات الجرائم العادية سواء التقليدية، وقد استحدث المشرع طرقا حديثة تتلاءم مع طبيعتها من اجل كشف الجرائم والمجرمين، غير أنه نظرا لطبيعة هذه الجريمة باعتبارها تقع في العالم الافتراضي فإنها تثير إشكاليات عديدة، كصعوبة اكتشافها وكذا إثباتها نظرا لغياب الدليل المادي الذي يدين مرتكبيها ولاسيما وان هذا الأخير يتسم بطابع الحيلة والذكاء ويستعمل تقنيات معلوماتية عالية الكفاءة ، مما يؤدي إلى اختراق شبكات وأجهزة الحاسب الآلي المرتبطة بالانترنت، والدخول إلى جهاز الكشف عن محتوياته أو إتلافها والتلاعب بالمعلومات المخزنة فيه من طرف المجرم الإلكتروني بكل يسر وسهولة، هذا من جهة ومن جهة أخرى فإن الدليل المتحصل عليه من طرق الإثبات يخلق تحديات كذلك للقضاة لقبول هذا النوع من الأدلة وبناء عليه قناعته لما يتميز به من مميزات. وعليه سوف تدور هذه المداخلة حول إشكالية التالية **ما هي التحديات التي يواجهها المحققون للبحث عن الجريمة الإلكترونية، وهل يمكن للقاضي الجزائي أن يبني قناعته على الدليل الإلكتروني؟**

مقدمة

لقد غزت المعلوماتية كل مجال من مجالات الحياة، وعادت على الناس بالخير من تيسير وسهولة وسرعة في المعاملات، غير أن البعض استغل هذا الوليد الجديد لاستعمالها لأغراض غير مشروعة وللاعتداء على أموال الناس وعلى مصالحهم، وهذا ما يسمى بالجرائم المعلوماتية أو الإلكترونية.

والجريمة الإلكترونية باعتبارها من الجرائم المعاصر العابرة للحدود الوطنية تثير في مجملها الكثير من الإشكاليات العديدة من عدة نواحي، كصعوبة اكتشافها وكذا إثباتها نظرا لغياب الدليل المادي الذي يدين مرتكبيها ولاسيما وان هذا الأخير يتسم بطابع الحيلة والذكاء ويستعمل تقنيات معلوماتية عالية الكفاءة، مما يؤدي إلى اختراق شبكات وأجهزة الحاسب الآلي المرتبطة بالانترنت، بحيث يتم اختراق نظام الأمن بالشبكة والدخول إلى جهاز الكشف عن محتوياته أو إتلافها والتلاعب بالمعلومات المخزنة فيه من طرف المجرم الإلكتروني بكل يسر وسهولة.

وتبعا لذلك تطلب الأمر جهود دولية لمكافحة الجرائم الناتجة عن هذه التقنيات ووضع حد لها، كما دفع كذلك بالتشريعات الوطنية لأن تكون مواكبة للاستعمالات السلبية للتكنولوجيا وأدوات الاتصال

والمعلوماتية، والمشرّع الجزائري استجابة لهذا التطور السريع وكغيره من التشريعات ومواكبة للتطور على الصعيد التقني استحدث نصوصا تشريعية لمكافحة الجرائم الناتجة عن هذه التقنيات ووضع حدا لها ، إذ أدرج الفصل السابع مكرر من قانون العقوبات بمقتضى تعديله بموجب القانون 04/15 المؤرخ في 10 نوفمبر 2004 ، حيث استحدث بموجبه جرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، وهذا بالإضافة إلى القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وبمقتضاه وسع المشرع من مفهوم الجريمة الإلكترونية لتشمل جانب المساس بأنظمة المعالجة الإلية للمعطيات المحددة في قانون العقوبات ، الجرائم التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية .

وعلاوة على هذه الآليات التي تضمنها القانون 04/09، فقد تضم قانون الإجراءات الجزائية مجموعة من الآليات الخاصة بالتحريات والتحقيقات في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مثل اعتراض المراسلات .

ويبقى من أهم المشاكل التي صاحبت هذا النوع الجديد من الجرائم الذي يقع في العالم الافتراضي هو مسالة الإثبات، إذ يواجه المحققون في هذا الصدد عدة مشاكل تحول دون الحصول على الدليل الكاف ناهيك على الصعوبات التي تعرضهم بسبب المجرم المعلوماتي، ومن ثم تتمثل الإشكالية التي تعمل هذه الورقة على مناقشتها في الصيغة التالية:

ما هي التحديات التي يواجهها المحققون للبحث عن الجريمة الإلكترونية، وهل يمكن للقاضي الجزائي أن يبني قناعته على الدليل الإلكتروني؟

سيتم التعامل مع هذه الإشكالية بإتباع المنهج الوصفي لوصف ظاهرة الجريمة الإلكترونية وأصنافها، كذا طرق الإثبات، وكذا المنهج التحليلي بتحليل نصوص القانونية المتعلقة بالموضوع .

وفقا للخطة المفصلة أدناه.

المبحث الأول: مدى فعالية طرق الإثبات في الجريمة الإلكترونية.

المبحث الثاني: التحديات التي يوجهها المحققون للإثبات الجريمة الإلكترونية.

المبحث الثالث : التحديات الذي يثيرها الدليل الرقمي أمام القاضي الجزائي.

المبحث الأول: مدى فعالية طرق الإثبات في الجريمة الإلكترونية

لقد أصبحت الجريمة الإلكترونية من الظواهر الرائجة حديثا، نظرا لارتباطها بتقنية متطورة هي تكنولوجيا المعلومات والاتصالات، ونظرا لاختلاف الفقهي حول تحديد مفهوم هذا النمط الإجرامي سنحاول تحديد تعريف الجريمة الإلكترونية وخصائصها كما ي شكل الإثبات مسألة مهمة في الكشف عن الجريمة والمجرمين، ولقد نص المشرع على طرق الإثبات بصفة عامة في نصوص قانون الإجراءات الجزائية منها ما هو تقليدي ومنها ما هو حديث ، دون أن يتضمن نصوصا خاصة بالإجرام المعلوماتي، مما يجعل المحقق

يواجه تحديات لإثبات جريمة التقليد، هذا ما يجعلنا نطرح التساؤل التالي: هل يمكن تطبيق طرق الإثبات المنصوص عليها في قانون الإجراءات الجزائية على جريمة الإلكترونية ؟

المطلب الأول: مفهوم الجريمة الإلكترونية:

لفهم الجريمة الإلكترونية من الضروري التطرق إلى تعريفها اذ تعددت وجهات النظر بخصوص هذا النوع المستجد من الجرائم، بحيث لا يوجد إجماع على تعريف الجريمة الإلكترونية؛ من حيث تحديدها والجرائم التي تشملها، كما أن للجريمة الإلكترونية خصائص تميزها عن الجريمة التقليدية تجعل مسألة الإثبات فيها مسالة معقدة .

الفرع الأول: التعريف للجريمة الإلكترونية

أمام مساعي لتصدي لظاهرة الإجرام المعلوماتي، فإنّ المصطلحات التي تناولت هذه الظاهرة، قد اختلفت فيما بينها، حيث لم يتفق الفقه الجنائي على تسمية موحدة للجريمة المعلوماتية، فالبعض أطلق عليها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات، والبعض يسميها جرائم الكمبيوتر والانترنت، وهناك من يطلق عليها الجرائم المستحدثة؛ إضافة إلى عدم الاتفاق على تعريف تشريعي شامل لهذا النوع من الجرائم، وقد ذهب الفقهاء في تعريف الجريمة الإلكترونية مذاهب مختلفة، ونتيجة للتطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات، فإنّ ذلك حال دون وضع تعريف فقهي جامع وشامل، إذ تباينت في هذا السياق الاتجاهات الفقهية، بين موسّع لمفهوم الجريمة الإلكترونية، وبين مضيّق لمفهومه [1] ،وسنحاول إبراز هذين الاتجاهين وفقا لما يلي :

أولا: الاتجاه الضيّق في تعريف الجريمة الإلكترونية:

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وفقا لمعايير متعددة، سواء كانت وفقا لمعيار شخصي من حيث توفر المعرفة والدراية بالتقنية، أو وفقا لمعيار موضوع الجريمة، والمعايير المتعلقة بالبيئة المرتكب فيها الجريمة، وسنسرد في هذا الإطار بعض التعريفات لفقهاء القانون الجنائي، فقد عرفتها ؛ وعرّفها الأستاذ Rosen Blat بأنها: " **كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب، أو التي تُحوّل عن طريقه**[2]؛

يعاب على هذا التعريف أنه يخرج من نطاق الجريمة الإلكترونية، عدد كبير من الأفعال غير المشروعة، والتي يستخدم فيها الحاسب الآلي، كأداة لارتكابها كالاحتيال المعلوماتي، وقد أخذت وزارة العدل الأمريكية بتعريف للجريمة الالكترونية في تقرير صادر عنها عام 1989 المتعلق بجرائم المعلوماتية بكونها:

([1])-نداء نائل فايز المصري، **خصوصية الجرائم المعلوماتية**، مذكرة مقدمة لنيل درجة الماجيستر ، في القانون العام ، بكلية الدراسات العليا في جامعة النجاح الوطنية ، نابلس ، فلسطين ، 2017 ، ص: 03.

([2])-محمد علي قطب، **الجرائم المعلوماتية وطرق مواجهتها** ، مركز الإعلام الأمني ، وزارة الداخلية ، الأكاديمية الملكية للشرطة ، مملكة البحرين ، 2010 ، ص: 09.

"كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الألية بقدر كبير لازم لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى".[3]

يتبيّن لنا من خلال هذا التعريف أنه لا يكف فقط أن تتوافر معرفة تكنولوجيا الحاسبات الألية، بدرجة كبيرة من أجل ارتكاب الجريمة الإلكترونية، ولكن أيضا من أجل ملاحقتها ومتابعتها والتحقيق فيها، بمعنى لابد من توافر قدر كبير من العلم بهذه التكنولوجيا، لدى الجناة والقائمين على معاينة وملاحقة مرتكبيها.

ثانيا: الاتجاه الموسّع في تعريف الجريمة الإلكترونية:

على عكس الاتجاه السابق يرى فريق أخر من الفقهاء، ضرورة التوسّع في مفهوم الجريمة الإلكترونية أو المعلوماتية، وعدم حصرها في الحاسوب وحده، أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية؛ فيعرّفونها بأنّها:

" كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل"؛

كما عرّفتها منظمة التعاون الاقتصادي والتنمية بأنّها:

" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخّل التقنية المعلوماتية[4]**؛**

نستشف من خلال عرضنا للتعاريف الفقهية ، حول مفهوم الجريمة الإلكترونية أنّها اقتصرت على مفاهيم عامة مرتبطة بجهاز الحاسوب من جهة، وبالبيانات من جهة أخرى، فالفقهاء الذين تبنوا الاتجاه الموسع لتعريف الجريمة الإلكترونية، كانوا أكثر حكمة لأنّ هذا العالم الافتراضي سريع التطور، وأي تضييق في مفهوم الجريمة الإلكترونية سوف يقنّن مفهوم الجريمة الإلكترونية،

وعليه يمكن إعطاء تعريف ملخصا لهذه الاتجاهات بأن الجريمة الإلكترونية هو السلوك غير المشروع معاقب عليه القانون صادر عن إرادة إجرامية محله معطيات الكمبيوتر [5].

الفرع الثاني: موقف المشرع الجزائري من الجريمة الإلكترونية:

أدّت الحداثة التي تتميز بها الجريمة الإلكترونية، واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الاتفاق على مصطلح موحد للدلالة عليها، ممّا انجرّ عنه عدم وضع تعريف موحّد لهذه الظاهرة الإجرامية، والمشرّع الجزائري وللدلالة على الجريمة الإلكترونية؛ اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال[6] وكخطوة أولى لمواجهة ما يعرف بجرائم ق بالمساس بأنظمة المعالجة الإلية للمعطيات، وهو ما نصت عليه المواد 394 و394مكرر1 إلى 7 من القسم السابع مكرر، وتراوحت هذه العقوبات من

([3])-سفيانسوير، **جرائم المعلوماتية** ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية ، وعلوم الإجرام ، كلية الحقوق ، جامعة أبو بكر بلقايد تلمسان، الجزائر، 2011، ص:12.

([4])-يزيد بوحليط، **الجرائم الإلكترونية والوقاية منها في القانون الجزائري ، في ضوء الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات ، قانون العقوبات ، ق إ ج ، قوانين خاصة** ، دار الجامعة الجديدة ، الإسكندرية ، 2019 ، ص: 50.

([5]) - المرجع السابق ، ص 53

([6])- أمينة بوشعرة، سهام موساوي، **الإطار القانوني للجريمة الإلكترونية** ، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية، 2018 ، ص12.

شهرين إلى ثلاث سنوات، مع دفع غرامة مالية من 50000دج إلى 5000000 دج، وذلك حسب حجم ودرجة خطورة الجريمة الالكترونية المرتكبة[7]

كما يعدّ قانون 04/09 المتعلق بتكنولوجيات الإعلام والاتصال أول قانون في الجزائر اهتّم بكيفية تبادل المعلومات الرقمية، وتجري فيه كل أنواع المعاملات والخدمات الالكترونية، وقد عرّفت المادة 02 منه الجريمة الالكترونية على أنها:

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية.[8]

توّضح هذه المادة نية المشرع الجزائري في تبنّي مبدأ المرونة في الصياغة التشريعية، للتمكن من استيعاب الأنشطة الاجرامية الالكترونية التي يتعذر حصرها وتحديدها، نظرا لسرعة وتطور أساليبها، تبعا للتطور التقني، وهو ما يتيح للقاضي حرية واسعة في التقدير، وانطلاقا من فحوى هذه المادة، يتبيّن أنّ المشرع الجزائري قسّم هذه الجرائم إلى ثلاثة أنواع:

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛
- جرائم ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية؛
- جرائم ترتكب أو يسهل ارتكابها عن طريق نظام للاتصالات الالكترونية. [9]

يتضح لنا من موقف المشرع الجزائري بشأن تعريف هذه الجريمة، أنّه أعطى لها مفهوما واسعا؛ بالرغم من تحديده لمجالها من خلال كونها متصلة بتكنولوجيات الإعلام والاتصال، إلا أنّه ترك فيما بعد المجال واسعا لتضم إليها أي نوع من الجرائم التي قد يسفر عنها التطور التكنولوجي، خاصة وأنّ هذا الميدان شهد تطورا وتسارعا كبيرين، وقد نصت المادة السابقة على العبارة التالية:

"...**أو أي جريمة أخرى ترتكب، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية**"[10].

من خلال استعمال المشرع الجزائري لمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، للدلالة على الجرائم الالكترونية، فهو يزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة، فالأولى تقوم على استخدام الوسائل التقنية لإدارة وتنظيم ومعالجة البيانات، أما تكنولوجيات الاتصال فتقوم على وسائل تقنية لنقل المعلومات بجميع دلالاتها، ولذلك فقد وُفّق المشرع الجزائري–في نظرنا– باختياره مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي تتوافق مع مصطلح الجرائم الالكترونية

([7])-سعيداني سلامي وطارق طراد، **التجربة الجزائرية لمواجهة الجريمة الالكترونية في ظل البيئة التفاعلية الجديدة: عرض تشريعي قانوني**، مجلة الحقوق والعلوم السياسية، العدد 12، جوان 2019، ص ص245-257.

([8])-قانون 04/09 المؤرخ في 2009/08/05، المتضمن **القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها**، ج ر 74، الصادرة في 2009/08/16.

([9])- يزيد بوحليط، مرجع سابق، ص55.

([10])-محمد السعيد زناتي،" **الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية**"، مجلة إيليزا للبحوث والدراسات، المجلد02، العدد01، ديسمبر 2017، ص ص 28-40.

وعليه فإن تعريف الجريمة الالكترونية الأقرب للصواب هو أنّها تمثّل كل اعتداء يتم باستخدام النظام المعلوماتي، وكان له دور رئيسي في السلوك المجرّم [11].

ا المطلب الثاني : خصائص الجريمة الإلكترونية:

تتميّز الجريمة الالكترونية بـخصائص، تجعلها تختلف عن غيرها من الجرائم؛ وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي، مع ما يتمتع به من تقنية عالية، وهذه الخصائص منها ما هو مشترك مع بعض الجرائم ومنها ما هو مميز لها

أولا: خصائص الجريمة الالكترونية المشتركة مع بعض الجرائم الأخرى

تتسم الجريمة الالكترونية بدرجة من الخطورة البالغة، والحجم الكبير للأضرار التي تنشأ عنها، وهي بذلك تشترك مع بعض الجرائم كالإرهاب والاتجار بالمخدرات، ومن هذه الخصائص يمكن تفصيل ما يلي:

أولا–خطورة الجرائم الالكترونية:

تنطوي الجريمة الالكترونية على قدر كبير من الخطورة، وذلك لوقوعها على الإنسان في فكره وحياته الخاصة، كما تمس المؤسسات في نشاطها الاقتصادي خاصة، ويقع ضررها على أمن البلاد الوطني، مع ما في ذلك من خطر المساس بالمعلومات والأسرار السياسية والعسكرية والاقتصادية، وفي جانب آخر فإنّها جرائم تنتهك حرمة الحياة الخاصة، بلاطلاع على خصوصيات الأفراد يظل جريمة يعاقب عليها القانون، كونها تنتهك حقا أساسيا للأفراد في حماية خصوصياتهم، وهو حق كفلته مختلف التشريعات.

إنّ الاختراقات المتكررة التي تتم لأنظمة الحواسيب في الهيئات الرسمية لعديد الدول، أثبتت كيف أنه مهما بلغ تقدم الدول فإنها تبقى معرّضة لتلك الاختراقات، وهو ما واجهته مثلا وزارة الدفاع الأمريكية من تسريبات للبيانات، واختراق لأنظمتها المعلوماتية وقرصنة لبياناته [(12)]، ولم يسلم من ذلك أرشيف وزارة الخارجية وكذا ملفات المخابرات وهويات العملاء، وأصبح من المعتاد ورود أخبار عن تعرض أعداد كبيرة من الملفات للاختراق والاطلاع والنشر غير القانونيين.

ثانيا–الجرائم الالكترونية باعتبارها جرائم عابرة للحدود

إن الجريمة الالكترونية شكل من الجريمة العابرة للحدود، يستفيد مقترفوها من أثر التقنية في اختزال المسافات، وإخفاء الأثر الالكتروني، وكذا السرعة الزمنية الهائلة في تداول المعلومات والحصول عليها، ووقوع كثير من العمليات الالكترونية في نفس الوقت، ضمن ما يعرف باللحظية المعلوماتية، والعمل عن بعد الذي يعدم التواجد المادي للمجرم المعلوماتي، ويُصعّب عملية البحث بشأنه، ويقتضي تتبع المعاملات الالكترونية التي تتجاوز حدود الدولة الواحد ة، في حرص على الربط بين الفعل والنتيجة الإجرامية له، من خلال المعطيات محل الجريمة.

ثانيا: الخصائص التي تنفرد بها الجريمة الالكترونية عن الجرائم الأخرى:

---

[11] - مقلاتي منى ، مشري راضية ، **الجرائم الإلكترونية دلالة المفهوم وفعالية المعالجة القانونية** ، مجلة ايحاث قانونية وسياسية ، العدد جوان 2021 ، ص 12 .

([12])-محمود أحمد عبابنة ومعمر الرازقي، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر والتوزيع، الأردن: عمّان، 2005 ، ص33.

تنفرد الجريمة الإلكترونية عن سواها من الجرائم الأخرى، بسمات تضفي عليها طابعا مميزا ومنها والتي يمكن إجمالها على النحو التالي:

أ1- يتطلب ارتكابها وجود حاسب ألي ومعرفة تقنية:

يعدّ الكومبيوتر الأداة الأساسية لارتكاب كافة الجرائم الإلكترونية، والمقصود من وجود ه هنا أن يستعان به كوسيلة لتنفيذ هذه الجرائم، ذلك أن الحاسب الآلي وإن كان موضوعا للاعتداء كإتلاف أو سرقة الجهاز نفسه، أو شاشته فلا تثور لدينا أية مشكلة، ذلك لأنّ نصوص قانون العقوبات التقليدية كفيلة بردع الجاني لأن الحاسب هنا لا يتعدى كونه من الأموال المادية المنقولة، ولكن تثور المشكلة عندما يطال الاعتداء على ما يمكن أن يسمى بفن الحاسب الآلي، كتدمير برامجه وسرقتها وتقليدها، أو العبث ببيانات الحاسب أو المعلومات المختزنة، وهذا هو المقصود من جرائم الحاسب الآلي، والتي يصلح فيها الحاسب أن يكون موضوع الاعتداء فيها.[13]

2-: صعوبة اكتشاف الجريمة وإثباتها:

توصف الجرائم الإلكترونية بأنّها خفية ومستترة في أغلبها، بحكم أنّ الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنّه من تنفيذ جريمته بدقة واحترافية، كإرسال فيروسات وسرقة الأموال والبيانات الخاصة، وإتلافها والتجسس وسرقة المكالمات... إلخ [14]، ويمكن رد الأسباب التي تقف وراء صعوبة اكتشافها، إلى عدم تركها لأثار خارجية، كما في الجرائم التقليدية فهي تتم في بيئة افتراضية، كما تُوفّر التقنية المعلوماتية للمجرم إخفاء أثار الجريمة، عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية، وبالتالي محو أثاره مما يخلق صعوبات بالغة لسلطات البحث والتحري في ملاحقته، وضمان عدم إفلاته من العقاب، خاصة وأنّ تنفيذها لا يتطلب وجود الفاعل في مكان الجريمة، بل يمكنه تنفيذ جريمته وفي دولة بعيدة ، كل البعد عن الفاعل [15]، كما أنّ معظم الجرائم الإلكترونية تم اكتشافها بمحض الصدفة، وبعد مرور وقت طويل، إضافة إلى أنه لا يتم في الغالب الإبلاغ عن الجرائم الإلكترونية، إما لعدم اكتشافها من طرف الضحية أو خوفا من التشهير به، لذلك ما يرتكب فعلا من جرائم إلكترونية أكبر بكثير مما يصرح به[16].

3: جرائم هادئة

إن الجرائم الإلكترونية تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم على معرفة تقنية للكومبيوتر، وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغيّر أو تُعدّل، أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، إلا أنّ البعض يشبهها بجرائم العنف؛ مثلما ذهب إليه مكتب

([13])- ، مرجع نفسه ، ص36.
([14])-سعيداني سلامي وطارق طراد، مرجع سابق، ص249.
([15])- يزيد بوحليط، مرجع سابق، ص82.
([16])-المرجع نفسه.

التحقيقات الفيدرالي بالولايات المتحدة الأمريكية، نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف.[17]

المطلب الثاني : طرق إثبات الجريمة الإلكترونية

إذا كانت القواعد العامة في الإثبات تنطبق على جريمة التقليدية،فإن أهم التحديات التي يمكن طرحها في هذا الإطار، والتي تواجه طرق إثبات التعدي على الجريمة الإلكترونية، على أنها لا تتلاءم كليا مع تلك المطبقة في القواعد العامة، وإن كانت الإجراءات هي نفسها التي تتبع وهي فعالة إلى حد ما، لكنها بحاجة إلى تطوير ولو جزئيا بشكل يجعل منها فعالة في هذا النطاق، وأعتقد أن ما يصعب في تطبيق هذه الإجراءات ليس قصورها، لكن طبيعة هذا النوع من الجرائم المركبة خاصة على مستوى الإثبات، كما سبق وأن تم توضيحه، وعليه فإنه يجب الاعتماد على نمط الإثبات الذي ينسجم مع طبيعة هذه الجرائم، وهذا ما جعل الدول تتحرك لإبرام اتفاقيات حول هذا الشأن لعل أهمها اتفاقية بودبست المنعقدة في 23 نوفمبر 2001 وذلك تحت إشراف المجلس الأوربي [18].

ولذا سنقصر دراستنا على أهم طرق الإثبات التي تطرح إشكالا على المستوى المعلوماتي، إذ ستكون الدراسة مطابقة لما سبق دراسته في الإطار التقليدي مع الأخذ في الحسبان تطور مفاهيمه في الوسط الإلكتروني الجديد بطريقة تضمن تطبيبي تلك الإجراءات التقليدية، التي لا تزال فعالة في البيئة التكنولوجية.

الفرع الأول: الطرق التقليدية وتطبيقها في الجريمة الإلكترونية

وتتمثل هذه الطرق فيما يلي :

أولا–المعاينة التقنية في جريمة تقليد المصنفات الإلكترونية:

تعد المعاينة من وسائل الإثبات المهمة التي يستعملها المحقق للكشف عن الجريمة غير أن تطور الإجرام بظهور ثورة المعلوماتية، جعل من القواعد التقليدية غير صالحة للتطبيق على وسائل الإثبات الحديثة، وإذا كانت المعاينة في إطار جريمة التقليية د تتم بالانتقال إلى محل الواقعة الإجرامية كقاعدة عامة، فإنه في إطار المجال المعلوماتي –– يعد من الموضوعات الجديدة، لأن هذه المسألة لا تكون بالضرورة عبر العالم المادي، وإنما تكون عبر العالم الافتراضي فيستطيع عضو سلطة التحقيق أن يقوم بالمعاينة في مكتبه بالمحكمة من خلال الحاسب الآلي الخاص به، كما يمكن أن يلجأ إلى مقهى الأنترنت، أو أن ينتقل إلى مقر مزود بالخدمة والذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة [19]،

عادة ما تستعين سلطات التحقيق، أو جمع الاستدلالات، أو الحكم بالخبراء حين تتعامل مع الجرائم

([17])- رحموني أحمد ، **"خصائص الجريمة الإلكترونية ومجالات استخدامها "**، مجلة الحقيقة ، العدد 41 ، 2018 ، ص ص 432-451.

([18])–دخلت إتفاقية بودابست حيز النفاذ في أول جانفي 2007 بعدما صادقت عليها 30 دولة، بما في ذلك الدول الأربعة غير الأعضاء في المجلس الأوربي وهي كندا، اليابان، جنوب إفريقيا، الولايات المتحدة الأمريكية، وتعد أول معاهدة دولية لمكافحة الجريمة التقنية تعكس الجهود الواسعة للإتحاد الأوربي ولجان الخبراء حول جرائم تقنية المعلومات منذ أكثر من 10 سنوات، لمزيد من المعلومات حول هذه الاتفاقية ارجع إلى النص كاملا من الاتفاقية على الرابط التالي:

http//convention.coe.int/treaty/en/treaties/html/185.htm تاريخ الزيارة 2022/09/20

([19])-ينص المشرع الفرنسي في المادة 17/331 من قانون الملكية الفكرية على فئات خاصة من الموظفين لمعاينة جرائم التعدي على المؤلفات التي تستخدم فيه التقنيات الحديثة وهم موظفي سلطة تنظيم التدابير التقنية.أنظر:

XavrierDaverat**, droit de la propriété littéraire et artistique**, breal, France, aout 2011, p 210.

المتعلقة بالانترنت نظرا للطابع الفني لأساليب ارتكابها والطبيعة غير المادية لمحل الاعتداء، ويتوقف نجاح هذه الجهات في أداء رسالتها على حسن اختيار الخبير وكفائته[20]، ففي فرنسا مثلا نجد فريق من الشرطة التي تقوم بالإشراف على تنفيذ المهمات التي يعهد بها إليه وكلاء النيابة والمحققين وجميعهم تلقو تدريبا متخصصا في مجال التكنولوجيا الحديثة وهم يقومون بمرافقة المحققين أثناء المعاينة، ويستخدمون برامج تستطيع استعادة المعلومات من على أسطوانة صلبة، كما يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات المحمولة [21] وهذا ما حاول إتباعه المشرع الجزائري عندما أنشأ فرقا للشرطة القضائية مختصة بالبحث في الجريمة المعلوماتية، يتلقون تكوينا في الخارج.

ويرى جانب من الفقه[22] أن المعاينة في مجال الكشف عن الجريمة الإلكترونية ، لا تتمتع بالأهمية ذاتها في مجال الجريمة التقليدية، على الرغم من أهميتها الكبيرة، ذلك أنها يمكن أن تكون الدليل الوحيد، ومرد ذلك إلى الاعتبارات الآتية:

-إن جرائم الإلكترونية قلما تترتب عليها آثار مادية، فجميع ما ينتج عن تلك الجرائم من أدلة ما هو إلا بيانات غير مرئية.

-إن عددا كبيرا من الأشخاص قد يترددون على مكان أو مسرح الجريمة خلال الفترة الزمنية التي يتوسط ارتكابها واكتشافها، مما يهيئ الفرصة لحدوث تغيير أو إتلاف بالآثار المادية أو زوال بعضها.

- مشكلة اختفاء الدليل الإلكتروني الذي يمكن تعديله أو تغييره أو محوه في بضع ثوان ، لأن الأمر يتعلق بعملية فنية تقنية، لذا يجوز أن يلتمس طالب المعاينة من القاضي أن يصرح له بتعيين خبير فني [23]، غير أننا نرى أن اتفاقية بودبست أكدت على أهمية المعاينة في إثبات الجريمة المعلوماتية في مادتها السادسة عشر.

الفرع الثاني: الشهادة الإلكترونية في الجريمة الإلكترونية:

تعد الشهادة من وسائل الإثبات الهامة في المسائل الجزائية، غير أن التطور التكنولوجي الهائل، أدى الى ظهور ما يسمى بالشهادة الإلكترونية.

إن الشهادة الإلكترونية مصطلح يطلق على نوع من الشهادة لا يكون فيها الشاهد حاضرا لجلسة التحقيق، وإنما تتم عبر وسائل إلكترونية من خلال استخدام وسائل كهربائية، أو مغناطيسية، أوصوتية، أو إلكترومغناطيسية، أو أي وسائل مشابهة في تبادل المعلومات، وتخزينها أو رقمية من خلال ترجمة معتمدة، أو تحويل أي برنامج إلى نظام أصفار أو آحاد.

ويقصد بالشاهد في مجال جرائم الإلكترونية «الفني صاحب الخبرة والتخصص في تقنية الحاسب،

-([20])-أسامة فرج الله محمود الصباغ،**الحماية الجنائية للمصنفات الإلكترونية**، رسالة لنيل درجة دكتوراه في القانون، جامعة عين شمس،مصر،2011،، ص 202.

([21])-سامة فرج الله محمود الصباغ ،المرجع السابق، ص 204.

([22])-أنظر في ذلك:- حسن محمد إبراهيم، **الحماية الجنائية لحق المؤلف عبر الانترنت**، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق، جامعة عين شمس،1995، ص 155.

- حسين بن سعيد بن يوسف، **السياسة الجنائية في مواجهة جرائم الانترنت** ، رسالة لنيل درجة دكتوراه، كلية الحقوق عين شمس، مصر،2007، ص 354.

([23])-تتم المعاينة عادة من ضباط، سواء كانوا من الباحثين أو المحققين ممن يتوافر فيهم كفاءة علمية وخبرة فنية.

الذي تكون لديه معلومات عن شبكة الانترنت وشبكات الاتصال، وإذا أن مصلحة التحقيق تقتضي البحث عن أدلة الجريمة داخلها" [24]، والشاهد يشمل بهذا المفهوم عدة طوائف أهمها : مستخدمي الحاسب الآلي، وخبراء البرمجة، والمحللون مهندسو الصيانة، والخبراء التقنيين، ومقدمي الخدمات الوسطية.

لم يتضمن قانون الإجراءات الجزائية قواعد خاصة فيما يخص الشهادة الإلكترونية، مما يعني تطبيق القواعد العامة، لكن السؤال المطروح هنا إذا كان يتعين على الشاهد المعلوماتي أن يقوم بطبع ملفات البيانات المخزنة في ذاكرة الحاسب أو الإفصاح عن كلمات المرور السرية، أو الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرنامج أن يقدم إلى سلطة التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في المواقع أو الحسابات بحثا عن أدلة الجريمة، فهل من واجب الشاهد القيام بذلك وفقا للالتزامات التقليدية؟ فالاتجاه الراجح في هذا المقام تؤكد متى كانت مصلحة التحقيق تقتضي اختراقا تنقيبا عن أدلة الجريمة داخله، فيجوز للشاهد الإدلاء ببيانات، ومعلومات جوهرية وهامة.

الفرع الثالث: الخبرة الفنية في الجريمة الإلكترونية:

إذا كانت الاستعانة بخبير في المسائل الفنية البحتة في الجرائم التقليدية أمر واجب على جهة التحقيق والقضاء، فهي كذلك واجبة في مجال استخلاص الدليل التقني لإثبات الجريمة الإلكترونية، خاصة إذا تعلق الأمر بمسائل فنية معقدة، ومحل الجريمة فيها شيء غير مادي والتطور في أساليب ارتكابها سريع ومتلاحق، ولا يكشف غموضها الإ متخصص في مجال المعلوماتية، ولعل هذه الأهمية، هي التي جعلت بعض التشريعات تنظم أعمال الخبرة في مجال الجرائم التقنية بنص خاص مثل القانون البلجيكي الصادر في 2000/12/23 [25]، وتعد الخبرة التقنية في مجال المساعدة القضائية أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات والانترنت، ذلك أنها تؤدي دورا لا يستهان به إزاء نقص المعرفة القضائية الشخصية للعالم الافتراضي، مع العلم أن المشرع الجزائري لم ينص على قواعد خاصة بالخبرة التقنية، مما يفهم أنه تطبق نفس القواعد التقليدية فيما يخص اختيار الخبراء، وحلف اليمين[26]وإيداع التقارير، مع بعض الفرق في طبيعة عمل الخبير التقني.

وتجدر الإشارة أنه بعد انتهاء الخبير من عمله وتقديم رأيه للمحكمة، يعد رأيه استشاريا ولا يلزم المحكمة، لذا فلها أن تأخذ به أو تطرحه، ولها أن تأخذ بعض ما جاء في تقرير الخبرة دون البعض الآخر، أو أن تأخذ بما جاء في تقرير الخبير الذي ندبته سلطة التحقيق الابتدائي، وتطرح تقرير الخبير الذي ندبته أثناء المحاكمة، ويرى جانب من الفقه أن القاضي يظل الخبير الأعلى، حتى ولو كانت المسألة فنية في

([24])-حسن محمد إبراهيم، المرجع السابق، ص 150.

([25])-لقد نصت المادة: 88 من القانون البلجيكي على أنه: " يجوز لقاضي التحقيق والشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام والبحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة والمحمولة أو المنقولة على أن يتم ذلك بالطريقة التي يريدها جهة التحقيق"
مشار إليها في: محمد أبو العلا عقيدة، **التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية**، المرجع السابق، ص 06.

([26])-المادة :145 ق إ ج.

المجال المعلوماتي[27].

الفرع الثاني: الطرق الحديثة في إثبات الجريمة الإلكترونية

استحدث قانون العقوبات في تعديله سنة 2006 إجراءات حديثة تخص جرائم معينة نظرا لخصوصيتها، ومن بينها الجريمة الإلكترونية ، إذ يمكن للضبطية القضائية ممارسة هذه الإجراءات بغرض معاينة الجريمة ومن بين الطرق الحديثة ما يلي :

أولا–الإجراءات المتعلقة بالبيانات المتحركة واعتراض الاتصالات الإلكترونية

الأصل هو حرمة الاتصالات الخاصة فقد أقرت معظم التشريعات على توفير قدر كبير من الحماية الجنائية على سرية الاتصالات الخاصة للأفراد، بحيث عاقب المشرع الجزائري لأول مرة اعتراض الاتصالات السلكية واللاسلكية دون إذن بموجب قانون العقوبات في المادة 303 مكرر منه، ومن ثم فإن اعتراض الاتصالات الإلكترونية يكون بناءا على أذن من السلطة المختصة والذي يعد ضمانة المشروعية الاعتراض طبقا للمادة 65 مكرر ق إ ج بحيث أجازت فيها الاعتراض في جرائم المساس بأنظمة المعالجة الإلية للمعطيات [28].

كما أضافت نص المادة 04 من القانون 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إجراء للوقاية من الجرائم الإلكترونية ،في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني مراقبة الاتصالات الإلكترونية .

ثانيا – التقاط الصور

تعتبر عملية التقاط الصور الفوتوغرافية من الإجراءات الجديدة التي جاء بها المشرع الجزائري لمكافحة الجرائم المستحدثة ومنها لجرائم ، غير أنه لم ينص على تعريفها لا وإنما نص على مجال تطبيقها كما وضح إجراءات القيام بها، ويقوم هذا الإجراء على استخدام الكاميرات أو الأجهزة الخاصة لالتقاط صورة المشتبه فيه على الحالة التي كان عليها وقت التصوير بغرض استخدام هذه الصورة كدليل مادي ، وقد وضع المشرع لهذا الإجراء شروط حتى يحيطها بضمانات وهو ضرورة منح الإذن للقيام بهذه العملية سواء من طرف وكيل الجمهورية أو قاضي التحقيق الإلكترونية ويجب أن يتضمن هذا الإذن على كل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط الصور لم والأماكن المقصودة سواء عامة أو خاصة وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها طبقا لنص المادة 65 مكرر 7 ق إ ج ويسلم الإذن مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد، وتتم عملية التقاط الصور بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة بالجوانب التقنية للعملية طبقا للمادة 65 مكرر 08 ، ما يلتزم ضابط الشرطة القضائية

([27])-عمر أبو بكر بن يونس، **الجرائم الناشئة عن استخدام الأنترنت**، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق،جامعة عين شمس،مصر،2004،ص 103.

غير أن الواقع العملي أثبت أن القاضي يسلم بما خلص إليه الخبير في تقريره، وينبني حكمه على أساسه.

([28]) أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الأولى ، دار هومة ، الجزائر ، 2007، ص 105

المناب بتحرير محضر عن كل عملية التقاط الصور والترتيبات [29].

ثالثا–التسرب:

تعد عملية التسرب ضمن المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته لمكافحة الجرائم المستحدثة، وترجع العلة في استحداث مثل هذه الإجراءات إلى عجز أساليب البحث والتحري التقليدية في الكشف عن جريمة إذ لم تعد كافية وفعالة للكشف عن مثل هذه الجرائم المستحدثة[30]،

لقد عرف المشرع الجزائري التسرب بموجب المادة 65 مكرر 12 ق إ ج، على أنه:

"**يقوم ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية، أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف** "، وقد أجاز المشرع هذا الإجراء في الجرائم الإلكترونية طبقا لنص المادة 65 مكرر 05 ق إ ج(، والتسرب عملية في الغالب عملية معقدة تتطلب أن يتدخل العون المكلف بالعملية في اتصال بالأشخاص المشتبه فيهم ، ويربط معهم علاقات ويحافظ على السر المهني، إلى أن يتحقق الهدف النهائي من عمله[31].

و يعد التسرب أخطر الإجراءات انتهاكا لحرمة الحياة الخاصة، وقد أحاطه المشرع بجملة من الضمانات التي يتعين مراعاتها، وتتمثل هذه الشروط فيما يلي:

– **صدور إذن قضائي مسبب:** ويصدر هذا الإذن إما من وكيل الجمهورية، أو قاضي التحقيق.

–**أن يكون الإذن مكتوبا** : طبقا للمادة 65 مكرر 15 ق إ ج [32]، إذ أن الأصل في العمل الإجرائي الكتابة، ويجب أن يتضمن الإذن بإجراء التسرب على اسم الضابط والمدة المطلوبة لعملية التسرب والتي يجب أن لا تتجاوز أربعة أشهر، ويمكن أن تجدد ضمن نفس الشروط الشكلية والزمانية في نفس الوقت، وقد أجاز القانون للقاضي الذي يرخص بإجرائها أن يأمر في أي وقت بإيقافها قبل انقضاء مدتها المحددة تجدر الإشارة بأن العون المتسرب يمكن أن يواصل نشاطه غير القانوني الوارد في نص المادة 65 مكرر ق إ ج، وهذا إذا كان لم يمكن إيقاف نشاطه داخل المجموعة الإجرامية مع إعفائه من المسؤولية لمدة لا تتجاوز أربعة أشهر على أن يخطر القاضي مصدر الرخصة في أقرب الآجال ، أما إذا لم يتمكن العون المتسرب من إيقاف نشاطه خلال المدة المذكورة في ظروف تضمن أمانه فيمكن للقاضي عندها أن يرخص تمديدها أربعة أشهر أخرى، ويجب على الضباط وكذا أعوان الشرطة القضائية تحرير تقرير مسبق لإطلاع القاضي بشكل تام على ظروف القضية ومتطلباتها.

([29])- يزيد بوحليط ، المرجع السابق ، ص 377

([30])-عائشة بن قارة، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي: في القانون الجزائري والقانون المقارن** ، دار الجامعة الجديدة،الإسكندرية، مصر،2010، ص 119.

([31])-رشيدة بوبكر، المرجع السابق، ص 434.

([32])-تنص المادة :65 مكرر 15 ق إ ج على مايلي:

"يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11، مكتوبا ومسببا وذلك تحت طائلة البطلان.

تذكر في الإذن الجريمة التي تبرر اللجوء الى هذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته.

ويحدد هذا الإذن مدة عملية التسرب، التي لا يمكن أن تتجاوز أربعة (4) أشهر،

ويمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية

ويجوز للقاضي الذي رخص بإجرائها أن يأمر، في أي وقت، بوقفها قبل انقضاء المدة المحددة.

تودع الرخصة في ملف أجراءات بعد الإنتهاء من عملية التسرب."

والملاحظ وان هذه الوسائل الجديدة قد تعترضها إشكالات قانونية عدم توفر النصوص القانونية التي تحدد الوسائل التقنية التكنولوجية للقيام بعملية اعتراض المراسلات والتقاط الصور بالإضافة أن استعمال هذه الإجراءات المستحدثة تتطلب وسائل تقنية عالية وكفاءة بشرية مؤهلة ، ناهيك عن إمكانية التلاعب وإتلاف المرسلات المثبتة على دعامات الكترونية أو مغناطيسية .

المبحث الثاني: الصعوبات الذي يواجهها المحققون للإثبات جريمة الإلكترونية:

أصبح اكتشاف الجاني أمرا صعبا في ظل تطور أساليب ارتكاب الجريمة في هذا المجال،إذ كان يخضع في إثبات الجريمة إلى القواعد التقليدية إلا أن ظهور شبكة الأنترنت وما صاحبها من قضايا، جعلت من مسألة الإثبات تواجه تحديات، وهنا تظهر مشكلة قصور القواعد التقليدية على ملاحقة الظواهر الإجرامية المستحدثة، إذ يصعب على المحقق في كثير من الأحيان العثور على أثر مادي للجريمة والتي لا تنكشف إلا بمحض الصدفة، بالإضافة إلى سهولة محو الدليل في زمن قصير [33].

من أهم الصعوبات التي تعترض كشف جريمة الإلكترونية ، هي نوعية هذه الجرائم، فيما يخص جمع الأدلة بحيث يصعب في أغلب الأحيان تفتيش أنظمة الحاسب الآلي وخاصة في حالة تشفير الأدلة ضف إلى ذلك صعوبة تتعلق بالعنصر البشري، وأخرى متعلقة باكتشاف هذه الجرائم أو تحديد مصدرها، وخاصة في حالة ارتكابها عن بعد من داخل دولة أجنبية، وبناء على ذلك يمكن تقسيم الصعوبات إلى ثلاث كما يلي:

المطلب الأول: التحديات الخاصة بطبيعة جرائم الإلكترونية:

تقع جرائم الإلكترونية في بيئة لا يعتمد فيها التعامل أصلا على الوثائق والمستندات المكتوبة، بل على نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسب، ولا يمكن استخدامها كأدلة ضد الفاعل لأنه يمكن العبث بها في أقل من الثانية أو محوها بالكامل، لذا فإن للمصادفة وسوء الحظ دورا في اكتشافها يفوق دور أساليب التدقيق والرقابة، ووفقا لما لاحظه أحد الخبراء أن معظم مرتكبيها الذين يتم ضبطهم إما أنهم قد تصرفوا بغباء أو أنهم لم يستخدموا الأنظمة المعلوماتية بمهارة [34]، وليس مستحيلا في الكثير من الأحيان إخفاء السلوك المكون لهذه الجرائم وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها وذلك بحكم توافر المعرفة الحاسوبية والخبرة الفنية لدى مرتكبيها.

الفرع الأول–سهولة محو الدليل أو تدميره:

إن الأدلة الإلكترونية هي وسائل لإيجاد الصلة بين الجريمة والجاني، وهي من أهم مقومات الإثبات الجنائي، ومن الصعوبات التي يمكن أن تعترض عملية الإثبات في مجال الجرائم المعلوماتية بصفة عامة

([33]) -جميل عبد الباقي الصغير، **الجوانب الإجرائية للجرائم المتعلقة بالأنترنت**، دار النهضة العربية،القاهرة،2001، ص 11.

([34])-أنظر في ذلك:

John Eaton and j ermysmithers, this **is it Amanagrs guide to information** technology.Philip allam, London 1982, p.263.

- عبد الله حسين علي محمود ،**سرقة المعلومات المخزنة في الحاسب الآلي** ، رسالة لنيل دكتوراه في القانون، كلية حقوق عين شمس، مصر،2001، ص234.

هي سهولة محو الدليل أو تدميره في فترة زمنية متناهية القصر [35]، فضلا عن سهولة تنصل الجاني من هذا العمل بإرجاعه إلى خطأ في نظام الحاسب[36]، فالدليل هنا ليس بالدليل المادي المتمثل في ورقة محصلة من طابعة الحاسب، وإنما هو عبارة عن نبضات إلكترونية يصعب الحصول عليها، لذا فإنه من اليسير على الجاني في ظل التقنيات الحديثة أن يقوم بإخفاء بياناته الشخصية، أو أية أدلة خاصة بجريمته من بعد، وفي أي مكان من العالم[37].

وتعد سهولة محو الأدلة الإلكترونية وتعدد مستخدمي الإنترنت تحت اسم مستعار من أهم الصعوبات التي تواجه أجهزة التحقيق القائمة بهذا العمل في مجال جمع الأدلة [38]، حيث اعتادت سلطات جمع الاستدلالات والتحقيق على أن يكون الإثبات ماديا ملموسا، ولكن في محيط الإنترنت لا يستطيع ضباط الشرطة القضائية أو المحقق تطبيق إجراءات الإثبات التقليدية على المعلومات وهي من طبيعة معنوية، أو كالنبضات الإلكترونية حيث يسهل محو الدليل أو تدميره في لحظات[39]، ولذلك فإن جرائم الإلكترونية غالبا ما تقيد ضد مجهول

الفرع الثاني:–صعوبة الوصول إلى الدليل في جرائم الإلكترونية:

الدليل الإلكتروني هو إحدى الوسائل التي تؤكد نسبة فعل الاعتداء للجاني الذي قام به، ولذلك قد يحيط هذه الأدلة بوسائل فنية لحمايتها، وتكون هذه الوسائل عائقا أمام عمليات البحث والتحري والإطلاع[40].

ويمكن للمجرم المعلوماتي استخدام كلمات السر، أو تقنيات التشغيل لمنع الوصول إلى المصنفات الإلكترونية المقلدة التي قام بالاعتداء عليها، ليزيد من صعوبة عمليات التفتيش التي تباشر الحصول على الأدلة التي تدينه، ولذلك فإن استخدام تقنيات التشغيل لهذا الغرض يعد إحدى العقبات الكبرى التي تعوق رقابة المصنفات المقلدة والمنقولة عبر حدود الدولة ومن تم عمل جهات التحري والتحقيق [41]، كما يتطلب البحث عن معلومات تفيد في كشف أدلة الجريمة المعلوماتية معينة البحث في الكثير من الملفات، والبرامج المخزنة، والتي قد يكون لها ارتباط بمعلومات خاصة بارتكاب الجريمة المعلوماتية داخل الجهاز دليلا،

([35])-جميل عبد الباقي الصغير، **أدلة الإثبات الجنائي والتكنولوجيا الحديثة**، دار النهضة العربية، مصر،2001،ص 04.

([36]) -Sedallain (v), **droit de l'internet réglementation, Responsabilités, contrats**, collection AUL , paris, 1996,p.251.

([37])-سعيد عبد اللطيف، **إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنت: الجرائم الواقعة في مجال تكنولوجية المعلومات** ، دار النهضة العربية، مصر،1999، ص 110.

-([38])Yann Padova":**un aperçu de la lutte contre la cyber criminalité en france**", revue de Science criminelle et droit pénale comparé,n° 4,dalloz, **février,2002,p.**771.

([39])-محي الدين عوض: **"مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)** "، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان "الجرائم الواقعة في في مجال تكنولوجيا المعلومات "، القاهرة 20-27 أكتوبر1994،دار النهضة العربية، 1994،ص 367. مشار إليه في: جميل عبد الباقي الصغير، **الجوانب الإجرائية للجرائم المتعلقة بالانترنت** ، المرجع السابق،ص 05.

([40])-أنظر في ذلك:

-محمد عبد اللطيف فرج: " **مشكلات ملاحظة وتحقيق الجرائم المعلوماتية** "، مجلة مركز البحوث بأكاديمية الشرطة، العدد العاشر،2000، ص 14

([41]) – Berthou Renaud:"**internet et le repect des principes essentiels du droit du fo**r". Date du consultation 22/11/2012 Disponible à l'adresse: http//www. uriscom.net/memoire 12presentation .html.p03.

وتسعى الجهات الأمنية لملاحقته، وهو أمر يتم في ظروف صعبة، إما في الوسائل الفنية الخاصة بطبيعة المعلومات، أو في نقص الخبرة الفنية لجهات البحث والتحري وحتى القضاة[42].

المطلب الثاني: الصعوبات الخاصة بالعنصر البشري:

تتعدد التحديات الخاصة بالعنصر البشري في جرائم الاعتداء على المصنفات الإلكترونية عند إثبات تلك الجرائم، وتتمثل هذه الصعوبات فيما يلي:

الفرع الأول: السمات الخاصة لمرتكبي الجرائم الإلكترونية:

يعتبر المجرم المعلوماتي محور ارتكاب الجريمة، في الجرام الإلكترونية تبعا للدرجة العلمية والمستوى الثقافي والتعليمي في التعامل مع التكنولوجيا الحديثة وتتحدد طبيعة المتهم لارتكابه الجريمة في حدود ما لديه من قدرات تمكنه من ارتكابها، وقد يكون الهدف من ارتكاب جريمة الإلكترونية هو إثبات التفوق العلمي من خلال التحدي الفكري أثناء استخدامه للحاسب الآلي، وإثبات قدرته على اختراق أنظمته و الدخول إليها[43].

ومن أشهر الجرائم التي ارتكبت في الولايات المتحدة الأمريكية جريمة مراهق عمره سبعة عشر عاما يدعى "دينيس موران "وقد اختار لنفسه اسما حركيا هو "كوليو"، والذي قام بشن سلسلة من الهجمات الإلكترونية على مواقع مهمة أنشأتها الحكومة الأمريكية على شبكة الإنترنت، ومنذ نهاية عام 1999 وحتى بداية عام 2000 استطاع "كوليو" أن يحول حياة المسؤولين عن هذه المواقع إلى جحيم، حيث دأب على مهاجمة موقع (DAREORG) المسؤول عن مواجهة مخاطر الإدمان، ونفذ عمليات تخريبية عليه[44].

كما قد يكون الهدف من ارتكاب جرائم التقليد في مجال المعلوماتية هو تحقيق المكاسب المالية، لمن يقوم بنسخ المصنفات وعرضها للبيع بثمن زهيد جدا، وهي المشكلة التي تواجه شركات البرمجية من استنساخ برامجها، وعرضها بالأسواق بأثمان زهيدة جدا، مما يجعل هؤلاء المعتدين يجنون أرباحا خيالية على الرغم من الخسارة الفادحة التي تتعرض لها الشركات المنتجة لهذه البرمجيات.

الفرع الثاني–إحجام المجني عليهم الإبلاغ عن الجرائم الإلكترونية:

ان ضحايا الجرائم الإلكترونية فبدلا من استدعاء الشرطة والإبلاغ عن تلك الجرائم التي تعد ضحية لها، فإنهم يفضلون الصمت وعدم إثارة المشاكل التي من الممكن أن تنال من سمعة شركاتهم، ويلاحظ أن العديد من ضحايا جرائم الحاسب لا يبلغون عن الجريمة، بل يسعون بدلا من ذلك إلى محاولة تجاوز آثارها حتى لو كانت الوسيلة هي مكافأة المجرم.

الفرع الثاني: بعد الجاني عن مسرح ارتكاب الجرائم الإلكترونية:

يتم ارتكاب جرائم الحاسب الآلي عادة عن بعد، بحيث لا يتواجد الفاعل على مسرح الجريمة ومن ثم تتباعد المسافات بين "الفعل" من خلال حاسب الفاعل " والنتيجة " المعطيات محل الاعتداء، وهذه المسافات

([42])-عمر سالم، الحماية **الجنائية للمعلومات غير المعلنة للشركات المقيدة بسوق الأوراق المالية** ، الطبعة الأولى، دون مكان نشر، 1999، ص 13.

([43])-انتصار نور الغريب، **أمن الكمبيوتر والقانون**، دار الراتب الجامعية، بيروت، لبنان،1994، ص 10.

([44])-أسامة فرج الله محمود الصباغ، المرجع السابق، ص 190.

لا تقف عند حدود الدولة بل قد تمتد إلى النطاق الإقليمي لدول أخرى ، مما يضاعف صعوبة كشفها أو ملاحقتها، ويستخدم الجناة عادة أسماء مستعارة أو يدخلون إلى الشبكة من خلال مقاهي الانترنت[45].

الفرع الرابع نقص خبرة الجهات المكلفة بالتحقيق في جرائم ا الإلكترونية:

يتطلب إثبات جرائم الإلكترونية والوصول إلى مرتكبيها وملاحقتهم إتباع إستراتيجيات خاصة تتعلق باكتساب ضباط الشرطة القضائية وجهات التحقيق والمحاكمة مهارات خاصة، تساعدهم على مواجهة تقنيات الحاسب الآلي وشبكاته ، ولقد أوصى المجلس الأوروبي في قرار رقم 1395 في 11 سبتمبر 1995م في شأن مشكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسب وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات [46]، ولكن كثيرا ما تفشل أجهزة الشرطة، وجهات التحقيق في جمع أدلة الجرائم المعلوماتية، بل أن المحقق كما هو الحال أحيانا في بعض الجرائم قد يدمر الدليل بخطأ منه أو إهمال، أو بالتعامل الفني الخاطئ مع تلك الأدلة.

الفرع الرابع : التحديات الخاصة في مجال جمع الأدلة على المستوى الدولي:

تعتبر الجرائم المعلوماتية صورة إجرامية مستحدثة من الجرائم العابرة للحدود الوطنية،إذا تجاوز مرتكبو تلك الجرائم حدود القطر، ومن ثم فإن الصعوبات التي قد تواجه أو تعترض مكافحتها والبحث عن أدلة إثباتها على المستوى الدولي هي كما يلي:

– عدم وجود مفهوم عام مشترك بين الدول حتى الآن حول نماذج النشاط المكون للجريمة المعلوماتية.

–اختلاف مفاهيم الجريمة لاختلاف التقاليد القانونية، وفلسفة النظم القانونية المختلفة.

– ليس هناك مفهوم عام حول تعريف القانون للنشاط الإجرامي المتعلق بهذا النوع من الجرائم.

– عدم التناسق بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحري والتحقيق في الجرائم المتعلقة بالكمبيوتر والإنترنت.

– نقص الخبرة لدى الأجهزة الأمنية وجهات الإدعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت وجمع المعلومات والأدلة عنها[47].

– تعقد المشاكل القانونية والفنية الخاصة بتنفيذ نظام معلوماتي خارج حدود القطر أو ضبط معلومات مخزنة فيه أو الأمر بتسلمها.

– عدم وجود معاهدات للتسليم أو للمساعدة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي أو عدم كفايتها إن كانت موجودة بالفعل لمواجهة المتطلبات الخاصة بالجرائم المعلوماتية وسرعة التحريات فيها [48].

([45])-محي الدين عوض، المرجع السابق، ص 429.نقلا عن جميل عبد الباقي الصغير ، الجوانب الإجرائية المتعلقة بالأنترنت ، المرجع السابق ، ص 10

([46])-أسامة فرج الله محمود الصباغ، المرجع السابق، ص 191.

([47])-عبد الله حسين علي محمود، المرجع السابق، ص 195.

([48])-راجع في ذلك: - أيمن عبد الحفيظ، الاتجاهات **الفنية والأمنية لمواجهة الجرائم المعلوماتية، بدون** دار ومكان نشر،2005، ص**210.**

المبحث الثالث : التحديات الذي يثيرها الدليل الرقمي أمام القاضي الجزائي

يعتبر مبدأ الاقتناع الشخصي للقاضي الجزائي من أهم عناصر الإثبات في الدعوى الجنائية فالقاضي حر بأن يأخذ بالأدلة التي يراها مناسبة للكشف عن الحقيقة وله الحق في أن يستمد اقتناعه وعقيدته من أي مصدر يطمئن إليه وحرية الإقتناع هي حرية خاصة بقاضي من خلالها يعمل سلطته التقديرية ويبسطها على الأدلة الجنائية فبالرغم من أن النيابة العامة عليها أن تقيم الدليل على الإدانة و المتهم عليه أن ينفي هذا الدليل إلا أن التزام القاضي الجنائي بإدراك الحقيقة الواقعية أو المادية استجابة لمقتضيات التجريم جعلت له دورا إيجابيا يدرك بمقتاده الحقيقية ويختلف عن دور القاضي المدني، ومع ظهور الدليل الرقمي للإثبات في الجرائم الإلكترونية اضطر القاضي معه لكشف أنماط جديدة من الجرائم في مقابل نقص الثقافة معلوماتية ، ناهيك عن المشاكل العلمية للدليل الرقمي باعتباره دليل غير مرئي ، مما يؤدي في الأخير إلى إنقاص قيمته ونسبية الاستناد عليه في إثبات الجرائم الإلكترونية [49]وعليه سنتطرق إلى :

المطلب الأول الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الالكتروني :

ان القاضي الجنائي وان تمتع بسلطة واسعة في تقديره للدليل بما في ذلك الدليل الإلكتروني غير أن المشرع وضع له ضوابط وهي بمثابة صمام أمان إزاء إنحراف القاضي عند ممارسة لها كي لا تختل الأحكام

الفرع الأول : الضوابط المتعلقة بمصدر الإقتناع

وتتمثل فيما يلي:

1 -مشروعية الدليل الإلكتروني

يشترط أن يتم الحصول عليه بطرق مشروعة موافقة للقانون، وعليه فإن استخدام الوسائل غير مشروعة للحصول على الأدلة الرقمية يترتب عليه بطلان الإجراءات وعدم صلاحيتها لأن تكون أدلة إدانة في المواد الجزائية ومن هذه الإجراءات استخدام الإكراه المادي أو المعنوي أو الغش [50].

2 -شرط مناقشة الدليل الرقمي

من أهم قواعد الإجراءات أن القاضي لا يبني حكمه إلا على أدلة طرحت إمامه في الجلسة ، ويترتب عن ذلك أن يكون للدليل أصل ثابت في ملف الدعوى وان تمنح للخصوم فرصة الإطلاع عليه ومناقشته وما قضت به المادة 02/212 ق إ ج وهو ما ينطبق كذلك على الدليل الرقمي أي كان شكل ذلك الدليل ، وتقوم مناقشة الدليل على أمرين اثنين أولهما إتاحة الفرصة للخصوم لقع على الدليل الرقمي والرد عليه حتى يتمكن الخصوم من استيفاء حقوق الدفاع ومواجهة هذه الأدلة ، أما الأمر الثاني أن يكون للدليل الرقمي أصل في أوراق الدعوى ، وذلك حتى يكون اقتناع القاضي مبني على أساس [51]

الفرع الثاني :الضوابط المتعلقة بالاقتناع ذاته

([49]) عائشة بن قارة ، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، دار الجامعة الجديدة الإسكندرية ، ص2018 ص 239 .

([50]) الرجع السابق ، ص 236 .

([51]) المادة 02/212 ق إ ج .

يتيح مبدأ الإثبات حرية كبيرة للقاضي في تقدير عناصر الإثبات بما في ذلك الأدلة الرقمية وعليه ، فغن تقدير كفاية أو عدم كفاية الدليل الإلكتروني في إثبات الجريمة الإلكترونية ونسبتها إلى مرتكبيها أمر متروك لقاض ولا رقابة لمحكمة عليا عليه.

وعليه لبلوغ القاضي درجة الاقتناع التام للفصل في القضية، لابد له من شروط تتمثل في

1 –**بلوغ الاقتناع القضائي درجة اليقين :** تقتضي العدالة أن يصدر القاضي حكمه عن اقتناع يقيني بصحة ما ينتهي إليه من وقائع لا مجرد الظن و الاحتمال لأن الشك يفسر لصالح المتهم ، ويقوم اليقين القضائي على عنصرين شخصي يتمثل في ارتياح ضمير القاضي حول إدانة المتهم ، وموضوعي يقوم على أدلة من شأنها أن تؤدي وفقا لمقتضيات العقل والمنطق

2 –**توافق الاقتناع القضائي مع مقتضيات العقل والمنطق**

معنى ذلك أن يكون استخلاص محكمة الموضوع لوقائع الدعوى استخلاصا معقولا سائغا إن معيار معقولية الاقتناع بما ذلك الأدلة الرقمية وهو أن تكون هذه الأدلة مؤدية إلى ما رتبه الحكم عليها من غير تعسف في الاستنتاج [52].

إن المشرع الجزائري وغيرها من التشريعات لم يفرد نصوصا خاصة تحضر على القاضي مقدما قبول أو عدم قبول أي دليل الرقمي وهذا أمر منطقي على اعتبار أن الجزائر تعتمد على مبدأ حرية الإثبات كقاعدة عامة في المواد الجزائية من خلال المواد 212و307من القانون الإجراءات الجزائية 25 و لأن الدليل الرقمي يعتبر من الأدلة العلمية يتطلب دراية خاصة لا يمتلكها القاضي فلا يمكن أن ينزعها في قيمته الإثباتية وذلك لامتيازه بقوة استدلالية من الناحية العلمية .

وحتى أن وقع الشك في المصداقية الدليل بسب إمكانية العبث به وكذا لوجود خطأ في الحصول عليه فالقاضي لا يمكن أن ينفصل فيها باعتبارها مسألة فنية والرأي هنا يعود إلى الخبير فإذا سلم الدليل من العبث و توافره فيه كل الشروط فإن على القاضي القبول هذا الدليل لذلك فإن رفض القاضي لرأي الخبير يكون فيه تعارض مع نفسه وعليه فإن الدليل العلمي ومنه الدليل الرقمي أصبح يقيد حرية القاضي في تقدير الأدلة و يلزمه الحكم حتى ولو لم مقتنعا بصحة الواقعة المطروحة أمامه.

وهناك من يرى خلافا لذلك أن الأدل ة العلمية ليست دليلا مستقلا ، بل هي عبارة قرائن قضائية ليست كافية للإثبات بل هي قرينة تكميلية لا تصلح كدليل وحيد في الإثبات ، بل على القاضي الاستعانة بأهل الخبرة ، إذ حسب هذا الاتجاه فإن الدليل الإلكتروني مهما على شأنه يبقى سلطة قاض ي الجنائي مسيطرة ومن خلالها يمكن للقاضي أن يفسر الشك لصلح المتهم وان يستبعد الأدلة التي تم الحصول عليها بطريقة غير شرعية ، وهذا ما جعل الحقيقة العلمية قضائية [53]

المطلب الثاني : مدى تأثيرات مشكلات الدليل الإلكتروني على مبدأ اقتناع القاضي

([52]) - عائشة بن قارة ، المرجع السابق ، ص 276

[53] - بن طيب مبارك ، رحموني ، **شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية**، مجلة القانون والعلوم السياسية ، المجلد 05 ، العدد 02 ، 2019 ، ص 28 .

إن الدليل الرقمي يثير العديد من إشكالات نظرا لطبيعته التكوينية من جهة ، وإجراءات الحصول عليه من جهة أخرى ،وعليه سنتطرق إلى المشكلات الموضوعية ثم المشكلات الإجرائية للدليل الرقمي.

الفرع الأول: المشكلات الموضوعية للدليل الرقمي

يثير الدليل الرقمي مشكلات موضوعية تتعلق أساسا بالخصائص المنفردة للدليل الرقمي ، مما يشكل صعوبة كبيرة قصد تقديمه للقاضي الجزائي الذي يعمل وفقا لمبدأ الاقتناع الشخصي بحيث يدفعه الأمر لبل جهد إضافي لتقديره مما قد يؤثر سلبا على اقتناعه وهذه المشكلات هي :

أولا–الدليل الرقمي متنوع ومتطور

وتعني هذه الخاصية أنه على رغم من أن الدليل الرقمي في أساسه متحد التكوين بالغة الحوسبة إلا أنه مع ذلك يتخذ أشكالا مختلفة يمكن أن يظهر عليها كأن يكون بيانات غير مقروءة كما هو الشأن في حالة المراقبة عبر الشبكات الآلية كما يمكن أن يكون صورة ثابتة أو متحركة كالأفلام الرقمية أو معدة بنظام التسجيل السمعي البصري أو يكون مخزنا في البريد الإلكتروني(e–mail) التطورات التقنية المذهلة في مجال صناعة الحوسبة والاتصال إذا يرتبط الدليل الرقمي بالطبيعية التي تتمتع بها حركة الاتصال عبر الشبكة الإنترنت والعالم الافتراضي اللذين لا حدود لهما[54]

ثانيا –مشكلة الأصالة في الدليل الرقمي

الأصالة في الدليل الرقمي لها طابع افتراضي لا يرقى إلى مستوى الأصالة في الدليل المادي التقليدي ، فهذه الأخيرة تعبر عن وضعية مادية ملموسة ، في حين الدليل الرقمي عبارة عن تعداد غير محدد من الأرقام الثنائية ، ونظرا لأهمية الأصالة في الدليل الرقمي اعتمد بعد التشريعات منطق افتراض أصالة الدليل الرقمي كالتشريع المريكي [55]

ثالثا :الدليل الرقمي من طبيعة تقنية :

ينبئ الدليل الرقمي عن واقعة علمية شديدة التعقيد ، إذا لا يمكن استخلاصه إلا باستعمال الأساليب العلمية والتقنية. و عليها تتطلب الطبيعة التقنية للدليل الرقمي أن يكون هناك توافق بين الدليل المتحصل عليه والبيئية التي جاء منها، فمثلا لا ينتج عن البيئية الافتراضية سلاح الجريمة أو بصمات المجرم، و إنما ينتج عن تقنية المعلومات هو نبضات الكترونية غير مرئية، مما يجعلنا نستنتج انه ليس هناك دليل الكتروني خارج بيئته الرقمية.

رابعا : صعوبة فهم الدليل المتحصل من الوسائل الإلكترونية

إن الدليل الرقمي قد يكون مضمونه مسائل فنية لا يقوى على فهمها إلا الخبير المتخصص، فهو يستخلص من عمليات فنية معقد عن طريق التلاعب في نبضات و ذبذبات الكترونية و عمليات أخرى ، يكون فهم مضمونها في غاية الصعوبة ، اذ يحتاج الأمر إلى خبرة فنية ومقدرة على المعالجة المعلومات والبيانات بصورة يمكن معها

[54] - يزيد بوحليط ، المرجع السابق ، ص419 .
[55] - عائشة بن قارة ، المرجع السابق ، ص 253

الفرع الثاني المشكلات الإجرائية لدليل الرقمي

لا تقف صعوبة إثبات الجرائم الإلكترونية عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها وإنما تمتد هذه الصعوبة لتشمل إجراءات الصول على هذه الأدلة وهما حالتين

1- ارتفاع تكاليف الحصول على الأدلة الرقمية

3 -نقص المعرفة التقنية لدى جهات البحث والتحري .

الخاتمة:

لقد حاولنا من خلال هذه المداخلة الوقوف على طرق الإثبات المنصوص عليها في قانون الإجراءات الجزائية سواء التقليدية أو الحديثة ومدى انطباقها على الجريمة الإلكترونية باعتبارها جريمة من نوع خاص ترتب في العالم الافتراضي، وقد توصلنا إلى النتائج التالية :

- نظرا للطبيعة الخاصة للجريمة الإلكترونية لا يوجد تعريف موحد، وهي عدة أنواع يخلق معها صعوبة مكافحتها

- أنه يمكن تطبيق الطرق التقليدية للبحث عن الجريمة الإلكترونية.

- أن المشرع استحدث إجراءات وأساليب حديثة لمكافحة الجريمة الإلكترونية .

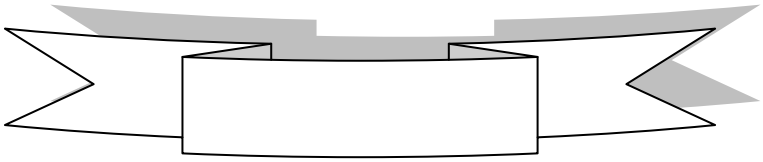
- نظرا لطبيعة الجريمة الإلكترونية يواجه المحققون عدة تحديات منها ما يتعلق بعنصر البشري ومنها ما يتعلق بالجانب التقني.

- إن القاضي الجزائي سيواجه تحديات لاعتماد على الدليل الرقمي، نظرا للمميزات وخصائص هذا النوع من الأدلة ، ومن ثم فإن التعامل معه يجب أن يتماشى مع هذه الطبيعة بحيث يكون الحصول على هذا الدليل إلا بالطرق المشروعة والضوابط القانونية التي حددها المشرع نظرا لسهولة انتهاكها أثناء عمليات البحث والتحصيل الأدلة في هذا النوع من الجرائم .

وعليه نقترح

- توفير الوسائل الحديثة في مجال تكنولوجيات الإعلام والاتصال للسلطات القضائية المكلفة بالبحث والتحري والعمل على تحديثه.

- تكوين الشرطة القضائية وكذا القضاة قصد اكتساب مهارات تقنية اللازمة مع إجراء دورات تكوينية في الخارج للاستفادة من تجارب الدول الرائدة في هذا المجال.



رابح بوسنة
boucennarabah@live.fr
جامعة 8 ماي 1945 –قالمة–

ماهية الجريمة الإلكترونية

مقدمة:

تتنوع الجرائم وتتعدد مظاهرها وصورها من جيل إلى آخر، فهناك دائما توجد جرائم تقليدية وجرائم حديثة، يساهم في نشأتها التطور الحاصل في أساليب ووسائل الحياة، ولعل هذا العصر الذي عرف فيه الإنسان ثورة كبيرة في ميدان العلم والمعرفة، ولاسيما في عالم الرقمنة وتكنولوجيات الإعلام والاتصال، ظهر نوع جديد من الجرائم مرتبط ارتباطا وثيقا بهذا التطور وهو ما اصطلح على تسميته بالجرائم الإلكترونية، وهذه الورقة البحثية جاءت لتجيب عن سؤال جوهري يدور حول ماهية الجريمة الإلكترونية، وفق منهج تحليلي ، نتناول من خلاله نشأة الجريمة الإلكترونية و تعريفها، وأركانها وخصائصها وأنواعها.

1 نشاة الجرائم الإلكترونية.

ظهرت هذه الجريمة بالتزامن مع ظهور أجهزة الحواسيب بأمريكا ، حيث انتقل الفكر الإنساني من طور العد بالحاسبات والتي كان آخرها حاسبة هارفارد مارك سنة 1943، إلى أول كومبيوتر وهو كمبيوتر آنياك(ENIAC) سنة 1946 والذي يعد أول كمبيوتر إلكتروني صنعه (Presper Eckert و John Mauchly)[1]، ثم ظهور شبكة الإنترنت و النقلة النوعية الحاصلة في عالم الاتصالات ، ومع هذا التطور الحاصل في عالم الاتصالات والرقمنة أخذت الجريمة تأخذ صورا وأشكالا جديدة بل و أسماء جديدة، فبعدما سميت في البداية بجرائم الكمبيوتر أو الحاسوب باعتبار أن الحاسوب كان هو محل الجريمة الوحيد أو وسيلتها، أصبحت تسمى فيما بعد بجرائم الإنترنت وهذا بعد شيوع استعمال هذه الشبكات وأصبحت وسيلة للإجرام، وسميت عند آخرينبجرائم المعلوماتية باعتبار أن الجريمة تطال في الأساس المعلومات المخزنة في الحواسيب، أو الجرائم الإلكترونية لأن البيئة التي تعمل فيها الجريمة هي بيئة رقمية إلكترونية، وكل إسم له حظ من دلالة التسمية والفترة التي ظهر فيها، ويكاد يستقر الأمر على التسميتين الأخيرتبن، و لاسيما الجريمة الإلكترونية. ويمكن الوقوف عند المراحل التاريخبة التالية لمعرفة المحطات التي مرت بها الجريمة الإلكترونية:

1 ǂ وقد تم رصد أول عملية قرصنة في العالم سنة 1970حين تم دمج تقنيات الحوسبة في الهواتف لتصبح هدفا للمهاجمين، حيث كان هؤلاء المتسللون المعروفون باسم (Phreakers) يقومون باستغلال النظام عن طريق إدخال تعديلات على الأجهزة والبرامج بهدف سرقة الوقت من الاتصالات التي تجري على مسافات طويلة، عندها أدرك الناس أن أنظمة الكمبيوتر قد تكون

[1]- أنطوان بطرس، موسوعة الكمبيوتر الميسرة، مكتبة لبنان، بيروت، دولة لبنان، ط 2، سنة 1994، ص 30.

عرضة للإجرام، وبدأت التساؤلات والنقاشات تدور حول ما إذا كانت هذه الأنشطة ظواهر عابرة أم جرائم مستحدثة، وإذا كانت تشكل جرائم فهل هي جرائم بالمفهوم القانوني أم مجرد سلوكيات لا أخلاقية، كل هذا كان في ستينيات وسبعينيات القرن الماضي.

- 1-2 وفي الثمانينات من القرن المنصرم طفا على السطح مفهوم جديد لجرائم الكمبيوتر والإنترنت ارتبطت بعمليات اقتحام أنظمة الكمبيوتر عن بعد، و نشر الفيروسات الإلكترونية التي تقوم بتدمير وإتلاف الملفات والبرامج من قبل أشخاص أصطلح على تسميتهم ب(الهاكرز) ومعناها "مقتحمو النظم"، وكان الهدف في البداية هو مجرد إظهار التفوق التقني ، لكنه تحول فيما بعد إلى إجرام حقيقي بدوافع شتى منها الإستيلاء على أموال الغير ومنها التجسس وسرقة البيانات السرية الأمنية والعسكرية وافقتصادية وغيرها...وأخذ الفاعل يومها إسم المجرم المعلوماتي[2].

1 3 في تسعينيات القرن الماضي بدأت أعداد الجرائم الإلكترونية في التنامي ، بدءا من سنة 1990 أين وقعت أول جريمة اشتهرت باسم عملية (**Sundevil**) الشهيرة في عالم الجريمة الإلكترونية [3]، عندها أدرك العالم ضرورة تجريم هذه الأفعال والتصدي لها باعتبارها جرائم خطيرة تمس الأشخاص الطبيعيين والإعتباريين على حد سواء..

عندما تتابعت الدول في تجريم كل الأنشطة الماسة والضارة ذات الصلة بتكنولوجيات الإعلام والإتصال، ومن هذه الدول الجزائر حيث أصدر المشرع عدة نصوص تتعلق بالجريمة الإلكترونية، وهي:

- القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات ،ج.ر .عدد 71. تحت عنوان : "المساس بأنظمة المعالجة الآلية للمعطيات " و يتضمن هذا القسم السابع مكرر ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 8.
- القانون رقم 23/06 المؤرخ في 20 ديسمبر المعدل و المتمم لقانون العقوبات، ج.ر .عدد 84.
- القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47.
- القانون رقم 02/16 المؤرخ في 19 ماي 2016 المعدل و المتمم لقانون العقوبات، ج.ر .عدد 37. مس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- المادة 37 و 45 من القانون رقم 07/17 المؤرخ في 27 مارس 2017 المعدل و المتمم لقانون الإجرات الجزائية ،ج.ر عدد 20.
- قانون رقم 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 ،يتعلق بالتجارة الإلكترونية.

2 مفهوم الجريمة الإلكترونية.

2 1 تعريف الجريمة الإلكترونية باعتباره مركبا إضافيا:

[2]- علاء رضوان، الجريمة الإلكترونية مقال منشور بالموقع https://www.soutalomma اطلع علبه بتاريخ 28-07-2022 على الساعة 09 و45 دقيقة.

[3]- https://cyber-arabs.com/ بتاريخ 287 07-2022 على الساعة 08 و 30 دقيقة.

يتكون هذا المصطلح من مفردتين: "الجريمة" و"الإلكترونية".

- مفردة الجريمة

- لغة : من فعل جَرَمَ، أَيْ كَسَبَ ; لِأَنَّ الَّذِي يَحُوزُهُ فَكَأَنَّهُ اقْتَطَعَهُ. وَفُلَانٌ جَرِيمَةُ أَهْلِهِ، أَيْ كَاسِبُهُمْ ... وَالْجُرْمُ وَالْجَرِيمَةُ: الذَّنْبُ، لِأَنَّهُ كَسْبٌ، وَالْكَسْبُ اقْتِطَاعٌ. وَقَالُوا فِي قَوْلِهِمْ " لَا جَرَمَ ": هُوَ مِنْ قَوْلِهِمْ جَرَمْتُ أَيْ كَسَبْتُ[4]، والمجرم هو المذنب ومنه قولهم (جَرَمَ) وَ (أَجْرَمَ) وَ (اجْتَرَمَ)[5].
- اصطلاحا: الجريمة في الإصطلاح هي سلوك جرمه المشرع بنص ووضع له جزاءا قانونيا ، وعرفها البعض بأنها: السلوك الذي يحظره القانون تحت التهديد بالعقاب عليه[6].

- مفردة الإلكترونية:

- لغة: الإلكترون [مفرد]: ج إلكترونات: (فز) جزء من الذَّرة دقيق جدًّا ذو شحنة كهربائيّة سالبة، وقيل أيضا هو عُنْصُرٌ أَوَّلُ ثَابِتٌ ذُو شِحْنَةٍ كَهْرَبَائِيَّةٍ سَلْبِيَّةٍ، أَسَاسُ الآلِيَّاتِ الإِلِكْتُرونِيَّةِ، وَهُوَ أَحَدُ الْمُكَوِّنَاتِ فِي ذَرَّاتِ الْمَادَّةِ[7].
- أصطلاحا: والإكتروني نسبة إلى الإلكترونيات، أي الذي يستعمل الوسائط أو الأجهزة الرقمية والإلكترونية الحديثة[8].

2 2 تعريف الجريمة الإلكترونية باعتبار.

الجريمة الإلكترونية في تصورنا هي الجريمة التي ترتكب باستعمال وسائل تكنولوجية رقمية حديثة من أجهزة وبرامج وتطبيقات وأنظمة وشبكات اتصال.

و عرفت أيضا على أنها كل عمل غير قانوني يستخدم فيه الحاسب كأداة أو موضوع للجريمة[9].

3 أركان الجريمة وصورها.

كغيرها من الجرائم تقوم الجريمة الإلكترونية على أركان عامة ، ثم إن لكل صورة عناصر تميز ركنها المادي عن غيرما من الصور الأخرى، و فيما يلي نتناول الأركان العامة للجريمة الإلكترونية أولا ثم نتناول صورها ثانيا .

3 1 الأركان العامة للجريمة الإلكترونية:

- الركن المادي:

ويتمثل في: السلوك والنتيجة ورابطة السببية.

---

[4]- أحمد بن فارس بن زكرياء القزويني الرازي، أبو الحسين (ت ٣٩٥هـ)، معجم مقاييس اللغة، دار الفكر، سنة 1979، ج1، ص 446.

[5]- زين الدين أبو عبد الله محمد بن أبي بكر بن عبد القادر الحنفي الرازي (ت ٦٦٦هـ)، مختار الصحاح، المكتبة العصرية ، بيروت – لبنان، الطبعة: الخامسة سنة 1999، ص 56.

[6] - l infraction: Un comportement interdit par la loi, sous la menace [...] d'une peine. » Lombois C., Droit pénal général, 1994, Hachette, coll. « Les fondamentaux », p. 7. Voir : Patrick Kolb Laurence Leturmy, OP cit p 24.

[7]- https://www.arabdict.com/ar تم الولوج إلى الموقع بتاريخ 2022/07/27 على الساعة: 23.00..

[8]- بوسنة رابح، الحماية القانونية للمستهلك في قانون 18-05، مداخلة في الملتقى الوطني حول ضوابط حماية البيئة فيالمعاملات التجاريةالإلكرتونية، من تنظيم قسم الحقوق ، جامعة 8 ماي 1945، شهر ديسمبر2020.

[9]- علاء رضوان ، الجريمة الإلكترونية، مجلة صوت الأمة، على الموقع:https://www.soutalomma.com/ منشور بتاريخ 16 - 11-2018 ، تم الإطلاع عليه بتاريخ 28-07-2022 على الساعة 08 و 45 دقيقة.

- ✓ السلوك المادي الظاهري أو النشاط الإجرامي الإيجابي أو السلبي الذي يأتيه الجاني باستعمال أحد الوسائل الإلكترونية، وهذا يتطلب توفر عنصرين اثنين:
- وجود أجهزة وأدوات إلكترونية [10] رقمية: كالحواسيب والهواتف، التي قد تكون هي بدورها محلا للجرائم الإلكترونية أو وسيلة وأداة لها في نفس الوقت وهو ما يعبر عنه بالبيئة الرقمية.
- أن تكون متصلة بشبكة الإنترنت ، لأن الجريمة الإلكترونية تتم في الغالب عن بعد،إلا إذا قصد الجاني جهاز المجني عليه مباشرة وتصرف فيه بشكل مخالف للقانون، فهذه الصورة قد لا تتطلب وأن تشتمل على برامج وأنظمة وبيانات وتطبيقات، تصلح أن تكون محلا للجريمة أو أداة لها.

وهذا السلوك المادي بهذين العنصرين قد يكون سلوكا إيجابيا (فعل) وهو الغالب مثل سرقة بيانات خاصة وسرية للمجني عليه عن طريق الولوج عبر شبكة الإنترنت واختراقها ، كما قد يكون سلوكا سلبيا (امتناع عن فعل) كامتناع الموظف المختص من حماية معلومات وبيانات الشركة التي يعمل لصالحها.

- ✓ النتيجة ورابطة السببية: ما يميز النتيجة في الجريمة الإلكترونية أنها في الغالب لا تقع في نفس مكان ارتكاب الجريمة (المسرح التقليدي)، بل تقع ضمن نطاق المسرح الإفتراضي للجريمة، وأن رابطة السببية بين النشاط الإجرامي والنتيجة ليست رابطة مادية ملموسة، ولكنها رابطة مادية من نوع خاص أساسها الإتصال الإلكتروني الحاصل بين الحاسب الذي يمتلكه الجاني والحاسب محل الجريمة.

وهذه الخاصية سببها أن البيئة الرقمية بيئة افتراضية من نوع خاص تختلف عن البيئة المادية التي ترتكب فيها الجرائم التقليدية.

3 2 صور الجريمة الكترونية:

هناك عدة اعتبارات يمن على أساسها تقسيم الجريمة الإلكترونية:

أ –فالمعيار الأول يعتمد على تقسيم الجرائم الإلكترونية إلى جرائم حديثة وتقليدية، فالجرائم التقليدية إذا ما ارتكبت باستعمال وسيلة إلكترونية كالحاسوب المتصل بالإنترنت، اعتبرت بهذا العيار جريمة إلكترونية حتى وإن كانت مجرمة في صورتها التقليدية بنصوص أخرى مثل جريمة السرقة والنصب والتجسس والسب والقذف وغير ذلك.

و في المقابل هناك دائما جرائم حديثة ظهرت بظهور الحاسوب والتكنولوجيا الحديثة، وهذه تعتبر جرائم إلكترونية صرفة وخالصة مثل جريمة البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات.

ب المعيارالثاني اعتمد فيه على الجهاز الإلكتروني الذي قد يكون وسيلة للجريمة أو محلا لها. فالحاسوب قد يستعمل كوسيلة فقط لتحقيق غايات غير مشروعة مثل سرقة أموال الغير والتجسس و الأفعال الإباحية وغير ذلك، وقد يكون الحاسوب هو محل الجريمة وهدفها مثل إتلاف المكونات المادية للحاسوب أو الدخول والبقاء في أنظمة المعالجة الآلية للمعطيات، وتدمير وإتلاف البيانات والمعطيات المخزنة، أو التلاعب بها أو تعديلها....إلخ

[10]- حمود بن محسن الدعجاني، الجريمة الإلكترونية، مقال منشور بمجلة الجامعة الإسلامية، العدد 183، الجزء 16، ص 558.

ت المعيار الآخير وهو الأنسب والأصح هو معيار التعداد، أي عد وحصر الجراءم التقليدية التي جاءت النصوص القانونية بصفة حصرية لتجريمها باعتبارها جرائم إلكترونية صرفة، ومن صور هذه الجرائم:

- **جريمة الدخول أو الشروع فيه أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات:** وسواء كان النظام محميا أو غير محمي،وهذه الجريمة نص عليها المشرع الجزائري في المادة 394 مكرر قع، ولها صورتان:

الصورة الأولى : الدخول والبقاء كجريمة بسيطة، وتعتبر الجريمة هنا شكلية أو من جرائم الخطر حيث لم يشترط المشرع وقوع أي نتيجة، فمادام الشخص قد تعمد الدخول في نظام للمعالجة الآلية للمعطيات بغير وجه مشروع، فيعتبر مرتكبا لهذه الجريمة الآنية.

فإن تعمد الفاعل البقاء في النظام بصورة غير مشروعةبعد الدخول فيه، ومهما كانت صفة الدخول، مشروعة أو غير مشروعة، عن عمد أو عن خطإ، فبقاؤه في هذه الحالات كلها يشكل بدوره جريمة مستقلة وهي من الجرائم المستمرة، وهل هي جريمة إيجابية أم سلبية في المسألة رأيان[11].

الجريمة في صورتها المشددة : وهنا تتجول الجريمة من جرائم الخطر إلى جرائم الضرر، فتصبح جريمة مادية تتطلب وقوع ركنها المادي بعنصريه أي السلوك والنتيجة، مع شرط ارتباطهما سببيا، و يتمثل السلوك هنا في:

الحالة الأولى: إذا ترتب على الدخول والبقاء حذف أو تغيير لمعطيات النظام .

الحالة الثانية: إذا ترتب على الدخول أو البقاء تخريب نظام اشتغال المنظومة .

وفي هذين الحالتين شدد المشرع العقوبة فبدل الحبس من 3 اشهر إلى سنة و الغرامة من 50 ألف إلى 100 ألف د ج، تصبح في الحالة الأول الضعف، وفي الحالة الثانية الحبس من 6 أشهر إلى سنتين والغرامة من 50 الف إلى 150 ألف. د ج.

- **جريمة الاعتداء العمدي على البيانات المخزنة في النظام: وجاء النص عليها في المادة 394 مكرر1.**

ويتمثل الركن المادي لهذه الجريمة في الأفعال الثلاثة التالية:

- ✓ الإدخال input:ويحصل ذلك بإضافة معلومات أو بيانات جديدة وغير معتمدةإلى نظام معلومات الحاسوب،أو إدخال برامج ضارة بالحاسب كالفيروسات، وكل ذلك تقوم به الجريمة بغض النظر عن الغاية المقصودة من الفعل، سواء كان بهدف تعديل المعلومات المخزنة أو إتلاف البيانات[12].
- ✓ المحو erasure: ويكون بإزالة و طمس كل أو جزء من المعطيات المخزنة بالنظام، وقد يتعدى مفهوم المحو ليشمل معنى الإتلاف.

[11]- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق ،جامعة الجزائر 1، السنة الجامعية 2009-2010، ص 198.

[12]- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، ط1 ،مكتبة الآلات الحديثة، أسيوط، ، سنة 1992، ص 59. وما بعدها.

✓ التعديل Alteration: وهنا يعمد الجاني إلى تغيير المعطيات المدمجة داخل نظام الحاسوب أو استبدالها بغيرها[13].

وهذه الأفعال الثلاثة تشكل تلاعبا بالمعطيات المخزنة داخل نظام المعالجة الآلية للبيانات، لذلك فهي تعتبر من جرائم الضرر التي تستوجي حصول نتيجة تتمثل في إحداث تغيير في تلك البيانات أو المعطيات والمعلومات عن الحالة التي كانت عليها من قبل.

و لا تتطلب هذه الجريمة سوى القصد الجنائي العام دون القصد الخاص، وبالتالي متى كان الفاعل عالما ومريدا لما أقدم عليه تتحقق الجريمة مكتملة الأركان وتلحق بالجاني عقوبة الحبس من 6 أشهر إلى 3 سنوات، وغرامة تتراوح من 500 ألف إلى 2 مليون د ج.

ث الجريمة المنصوص عليها في المادة 394 مكرر 2، وهذه الجريمة لها صورتان:

- القيام بأحد الأفعال المنصوص عليها في الفقرة الأولى: وهي "تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات محزنة أو معالجة أو مراسلة عن طريقمنظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم أي الجرائم المذكورة آنفا.

فالتصميم كأن بقوم المبرمج بإعداد وتصميم برنامجا حاملا للفيروسات، أو يعد برنامج يصلح لإختراق أنظمة الغير.

البحث رغم أنه في القواعد العامة لا يشكل جريمة لكنه اعتبر جريمة إن كان الغرض البحث عن أدوات لإرتكاب جريمة معلوماتية.

أما التجميع فيتمثل في جمع عدة بيانات ومعلومات تسهل ارتكاب الجريمة

والتوفير يقصد به وضع المعلومات والمعطيات المتحصل عليها تحت تصرف الغير، مما يسمح لهم بالحصول على مزايا مجانية غير مشروعة أو ارتكاب جرائم بواسطتها.

أما النشر وهو قريب المعنى من التوفير، فقط أن الجاني هنا يقوم بوضع المعلومات تحت تصرف عدد غير محدد ولا معلوم من الناس ، بحيث يكون من الممكن استعمال هذه المعطيات في إرتكاب أحد الجرائم السابقة.

أما الإتجار فهو كل عمليات البيع والشراء والإستيراد وكل أعمال التصرف في المعطيات بغرض الحصول على مقابل مالي، مما يجعل إمكانية الحصول على المعطيات من قبل الغير مظنة إرتكاب أحد الجرائم السالفة.

- القيام بأحد الأفعال المنصوص عليها في الفقرة الثانية: وهيحيازة، أو إفشاء، أو نشر، أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في المادة 394 بكل مكرراتها.

فالحيازة تعني الحصول والسيطرة الفعلية على المعطيات و استغلالها والتصرف فيها تصرف المالك لها.

أما النشر فهو بنفس المعنى المذكور آنفا.

[13] - عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة القاهرة، دار النهضةالعربية، 2004، ص 363.

الإستعمال: هو القيام فعليا بأفعال جرمية بعد الحصول على المعطيات ولو لم يتصرف فيها تصرف المالك، مثل استخدام كلمة مرور الغير

وتتطلب هذه الأفعال باعتبارها قصدا جنائيا عاما فهي جرائم عمدية يجب لوقوعها توفر عنصري العلم والإرادة، بالإضافة إلى الفصد الجنائي الخاص، لأن كل جريمة

أما عن العقوبات المرصدة لهذه الجريمة فهي بحسب نص المادة 394 مكرر2 الحبس من شهرين إلى ثلاث سنوات، وغرامة من .دج 5000.000 إلى دج 1000.000 إضافة إلى العقوبات التكميلية التي تمت الإشارة إليها أثناء تناول الأحكام المشتركة لجرائم المعلوماتية[14].

ونشير في نهاية هذه الجرائم إلى بقية النصوص المتبقية في المادة 394، حيث ضاعف المشرع العقوبات في الفقرة 394 مكرر3 إذا كان استهدفت الجريمة الدفاع الوطني والمؤسسات الخاضعة للقانون العام.

كما أشارت المادة 394 مكرر4 إلى عقوبة الشخص المعنوي بغرامة تساوي 5 مرات الغرامة المقررة للشخص الطبيعي.

كما أشارت المادة 394 مكرر 5 إلى معاقبة الإشتراك في الجماعة أنشئت بغرض الإعداد لهذه الجرائم ، شريطة أن تكون الأفعال التحضيريةمجسدة بصورة عملية في فعل أو عدة أفعال.

وأشارت المادة 394 مكرر 6 إلى مصادرة محل الجريمة وإغلاق المحل كعقوبات تكميلية بينما نصت نفس المادة في الفقرة الموالية (مكرر7) إلى المعاقبة على الشروع في الجريمة بنفس عقوية الجريمة التامة.

4 خصائص الجريمة الإلكتورنية.

4 1 من حيث التجريم:

- جريمة حديثة[15] نسبيا: فهي حديثة نسبيا لأنه مر عليها زمن لكن ليس بالطويل، فجذور نشأتها تعود إلى تسعينيات القرن الماضي، ومنذ ذلك الحين بدأت في البروز والظهور والإنتشار، حتى غدت جريمة عالمية وعابرة للحدود.
- مرتكبها مجرم غير اعتيادي:

في الجرائم التقليدية غالبا ما ترتكب الجرائم باستعمال العنف أو لتلبية رغبات وغرائز دنيا ومنحطة، ومن قبل أشخاص غير متعلمين أو أنهم ذوي مستويات تعليمية وثقافية متدنية، ولهم مشاكل نفسية واجتماعية متراكمة، لكن مجرم المعلوماتية أو المجرم الإلكتروني على خلاف كل ما سبق ذكره، فهو شخصية اجتماعية، متوافق في الغالب مع نفسه ومجتمعه، يمتلك مستوى عال من الذكاء والتعليم، ويكتسب مهارات فنية في تخصصه، و غالبا ما تكون له دوافع سامية.

- مساهمة المجني عليه في ارتكاب الجريمة: للضحية سواء كان شخصا طبيعيا أو اعتباريا دور كبير في الجريمة، وهذا من نواح عدة، أهمها عدم اكتسابه للمهارات اللازمة لصد الهجمات الإلكترونية ودفعها،

---

[14] - فايز محمد راجح غلاب، مرجع سابق ، ص 240.

[15]- اخترنا أنها حديثة نسبيا لمرور زمن عليها خلافا للبعض ممن لا يزال يعتبرها حديثة، أنظر على سبيل المثال: محمد أحمد عبدالمحسن بدوي، الجرائم المعلوماتية، مقال منشور في مجلة الأمن والحياة منشورات أكاديمية نايف العربية للعلوم الأمنية، المملكة العربية السعودية، سنة 2010، مج 29، ع 335، ص. 66 و 67.

والثقة الزائدة في منح الغير الأسرار والمعلومات الشخصية وعدم تأمينها، وأيضا عدم امتلاك الأفراد والمؤسسات تكنولوجيات متطورة لمجابهة هجمات مخترقي الأنظمة (HACKERS).

- ضف إلى ذلك عدم رغبة المجني عليهم في التبليغ عن هذه الجرائم وهذا مرده إلى أسباب كثيرة، منها خشية التشهير بالمجني عليه نفسه.

4 2 من حيث العقاب:

كانت العقوبات في بداية ظهور الجريمة متساهلة وبسيطة لبساطة الأضرار المترتبة على الجريمة ، ولكن كلما أزدادت خطورتها لا سيما في بعض القطاعات الحساسة، كلما زادت العقوبات قساوة وشدة، حتى اعتبرت في بعض النصوص القانونية من الجرائم الإرهابية.

4 3 من حيث الجسامة:

- فهي متفاوتة الخطورة حيق قد تبلغ شدة هذه الجرائم من حيث الجسامة أن تترتب عليها أضرار شديدة الخطورة، سواء على الأموال واقتصاديات الدول بالنسبة للجرائم الواقعة على المؤسسات المالية، أو على أمن وسلامة الدول وسيادتها، إذا تعلق الأمر باختراق مؤسسات أمنية وعسكرية... وقد يعتبرها المشره في صور أخرى جرائم بسيطة تستحق عقوبات الغرامة فقط كما هو الحال في المخالفات المتعلقة بالتجارة الإلكترونية.

4 4 من حيث الإختصاص المكاني:

- هذه الجرائم كما قد ترتكب داخل نفس الدولة التي يحمل الجاني والمجني عليه جنسيتها، فإنها أيضا قد ترتكب خارج الإقليم ، بل و في أكثر من إقليم، مما يجعل الإختصاص القضائي ينعقد لأكثر من دولة، وهذا كله لكون هذه الجريمة عابرة للحدود الدولية والقارية.

4 5 من حيث الإثبات

- **لها قواعد إثبات خاصة** : حتى وإن كانت الجريمة الإلكترونية تخضع للقاعدة العامة المتمثلة في حرية الإثبات في المادة الجزائية، وحرية القاضي الجزائي في الإقتناع، غير أن الجريمة المعلوماتية تتجاوز الأدلة التقليدية، ذلك كونها جريمة علمية تستعمل تكنولوجيات وتقنيات حديثة مما بتطلب أن على جهات التحقيق استعمال أدوات وتقنيات حديثة وأن تكون لهم خبرات ومهارات علمية وفنية عالية المستوى، حتى يتمكنوا من امتلاك الأدلة العلمية القاطعة والدالة على ارتكاب الجريمة ،وهذا ما يسمى بالإدلة العلمية في الإثبات، ومن الأمثلة على ذلك:

- أن الشاهد المعلوماتي يختلف عن الشاهد التقليدي، فالأول تصح شهادته إذا كان خبيرا وعارفا بعالم تكنولوجيات الإعلام والإتصال، مثل مشغلوا الحواسيب والمحللون والمبرمجون ومهندسوا الصيانة والإتصالات وغيرهم من أهل الإختصاص.

- أن القرائن المعلوماتية ذات صبغة علمية بحتة مثل الرقم التسلسلي لبطاقة الشبكة (MAC ADDRESS)، عنوان البروتوكول (IP ADDRESS) والبريد الإلكتروني [16] وغير ذلك من القرائن العلمية الأخرى.
- أما الخبرة الفنية فهي دائما ذات صبغة علمية سواء في الجرائم التقليدية أو الحديثة، فقط يجب أن يكون الخبير الفني مختصا في مجال المعلوماتية،

- **صعوبة الإثبات.**

رغم تطور الرصيد المعرفي لدى المحققين في محال المعلوماتية مقارنة بفترات سابقة، فإن الجريمة الإلكترونية ظلت عصية على جهات التحقيق من حيث إثباتها، ولاسيما في الدول التي لا تمتلك تقنيات وتكنولوجيات متطورة في هذه الميادبن، وذلك كون هذه الجريمة تتم بعيدة عن الأنظار، ولا يمكن معاينتها في الحال، وغالبا لا يترك مرتكبها أي أثر يدل عليها، وها ما يفسر قلة الجرائم المحالة على المحاكم الجنائية.

ويترتب على ما سبق أن أدلة الإدانة تكون في الغالب غير كافية لأن الجناة يعمدون إلى طمس معالم الجريمة وعدم ترك أي أثر يدل عليها ويسمح بتتبع مرتكبيها.

خاتمة

بعد هذه الجولة التي تعرضنا فيها إلى نشأة ومفهوم الجريمة الإلكترونية وبيان خصائصها وأنواعها، حيث اتضح لنا بأن الجريمة الإلكترونية تشكل بحق جريمة خاصة ومتميزة تحتاج إلى قواعد خاصة تخالف نلك التي ألفناها في الجرائم التقليدية.

فمن ناحية المصطلح لا يوجد اتفاق بشأنه فكل يسمي الجريمة باسم مختلف عن البقية، وهذا بحسب نظرة كل مشرع، وهذا بطبيعة الحال ينطبق حتى بالنسبة لصور هذه الجريمة التي تنطوي تحتها.

وهذا يستدعي من الفقه ثم التشريع تبعا له من المسارعة في توحيد مصطلحات هذا النوع من الجرائم وضبط مفاهيمه بالاستعانة بطبيعة الحال بالخبراء والمختصين في الإعلام الآلي.

كما أن هذا النوع من الجرائم بحاجة إلى التحيين المستمر فالجرائم المعلوماتية ذات وتيرة متسارعة، فكلما حصل تطور تقني برز نوع جديد من الجرائم، وهذا يحتم على المشرع المبادرة إلى وضع نصوص جديدة لتجريم هذه الأفعال.

و هذا بدوره يدعو المشرع إلى المتابعة المستمرة للتطورات الحاصلة في ميدان تكنولوجيات الإعلام والاتصال ، وكذا متابعة تشريعات الدول التي سبقتنا في هذه الميادين للاستفادة منهم في عملية التقنين للنصوص العقابية.

يبدو ان المشرع أحيانا يتساهل في وضع العقوبات والاكتفاء في كثير من الأحيان بالغرامة ، وربما هذه السياسة كانت نتيجة أن الفاعلين ليسوا مجرمين بالمفهوم التقليدي للمجرم ، بل هو مجرم من نوع خاص يكفي لإصلاحه شيئ من العقوبات المخففة، بل ويمكن الاستفادة منه في مجال اختصاصه.

[16]- حمود بن محسن الدعجاني، مرجع سابق، ص 583.

قائمة المصادر والمراجع.

أولا: النصوص القانونية.

5 القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات ،ج.ر .عدد 71. تحت عنوان : "المساس بأنظمة المعالجة الآلية للمعطيات "

6 القانون رقم 23/06 المؤرخ في 20 ديسمبر المعدل و المتمم لقانون العقوبات، ج.ر .عدد 84.

7 القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47.

8 القانون رقم 02/16 المؤرخ في 19 ماي 2016 المعدل و المتمم لقانون العقوبات، ج.ر .عدد 37.

9 القانون رقم 07/17 المؤرخ في 27 مارس 2017 المعدل و المتمم لقانون الإجراتالجزائية ،ج.ر عدد 20.

10 قانون رقم 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 ،يتعلق بالتجارة الإلكترونية.

ثانيا : المؤلفات:

1 -الكتب

- أحمد بن فارس بن زكرياء القزويني الرازي، أبو الحسين (ت ٣٩٥هـ)، معجم مقاييس اللغة، دار الفكر، سنة 1979، ج1، ص 446.

- أنطوان بطرس، موسوعة الكمبيوتر الميسرة، مكتبة لبنان، بيروت، دولة لبنان، ط 2، سنة 1994، ص 30.

- زين الدين أبو عبد الله محمد بن أبي بكر بن عبد القادر الحنفي الرازي (ت ٦٦٦هـ) ، مختار الصحاح، المكتبة العصرية ، بيروت – لبنان، الطبعة: الخامسة سنة 1999، ص 56.

- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، ط 1 ،مكتبة الآلات الحديثة، أسيوط، سنة 1992.

2 -الرسائل العلمية

- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق ،جامعة الجزائر 1، السنة الجامعية 2009-2010.

- عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة القاهرة، دار النهضةالعربية، 2004.

3 -المداخلات و المقالات

- بوسنة رابح، الحماية القانونية للمستهلك في قانون 18-05، مداخلة في الملتقى الوطني حول ضوابط حماية البيئة في المعاملات التجارية الإلكترونية، من تنظيم قسم الحقوق ، جامعة 8 ماي 1945، شهر ديسمبر 2020.
- حمود بن محسن الدعجاني، الجريمة الإلكترونية، مقال منشور بمجلة الجامعة الإسلامية، العدد 183، الجزء 16.
- علاء رضوان، الجريمة الإلكترونية مقال منشور بمجلة صوت الأمة بالموقع https://www.soutalomma منشور بتاريخ 16 -11-2018.
محمد أحمد عبدالمحسن بدوي، الجرائم المعلوماتية، مقال منشور في مجلة الأمن والحياة منشورات أكاديمية نايف العربية للعلوم الأمنية، المملكة العربية السعودية، سنة 2010، مج 29، ع 335.

4 -المواقع الإلكترونية

- https://cyber-arabs.com/ بتاريخ 287 07-2022 على الساعة 08 و 30 دقيقة.
- https://www.arabdict.com/ar تم الولوج إلى الموقع بتاريخ 2022/07/27 على الساعة: 23.00..

5 -المراجع الأجنبية:

- Lombois C., Droit pénal général, 1994, Hachette, coll. « Les fondamentaux », p. 7.

نجاح عصام
جامعة 8 ماي 1945 –قالمة–
nedjah25@yahoo.fr

حيمر زوليخة
جامعة 8 ماي 1945 –قالمة–
z.himeur10@gmail.com

الجريمة الإلكترونية في القانون الجزائري –الدوافع والأنواع–

ملخص:

شهد العالم في القرن الحالي ثروة معلوماتية وإلكترونية ضخمة لا حدود لها، حيث سعت الجزائر على غرار باقي دول العالم السير بخطى حثيثة نحو عصرنة ورقمنة كافة أجهزة الدولة ومرافقها بغية تطوير الحياة وتسهيلها عن طريق استعمال الحاسب الآلي والانترنت إلا أن هذا التطور المتواتر في وسائل الاتصال الإلكتروني صاحبه تطور في الجرائم والتي تخالف الجانب التقليدي لها والتي أصطلح عليها بالجرائم الالكترونية أو المعلوماتية التي تتم بواسطة استخدام خطوط وشبكات الاتصالات ذات التقنية العالية وعن بعد،مما يستدعي الأمر إلى الإسراع في ضبط مفهوم هذه الجريمة ونطاقها لنستطيع التحكم فيها أو تلافي آثارها.

***الكلمات المفتاحية*:** الجريمة الإلكترونية، المعلوماتية، الإنترنت، وسائل الاتصال.

***Summary*:**

In the present century, the world has witnessed a huge and limitless information and electronic wealth, as Algeria, like the rest of the world, has sought to move rapidly towards modernizing and digitizing all state agencies and facilities in order to develop and facilitate life through the use of computers and the Internet, but this frequent development in the means of electronic communication It is accompanied by a development in crimes that contradict the traditional aspect of it, which is termed as electronic or information crimes that are carried out through the use of high-tech and remote communication lines and networks, which calls for expediting the control of the concept and scope of this crime so that we can control it or avoid its effects.

Keywords: electronic crime, informatics, the Internet, means of communication**.**

مقدمة:

يعرف العالم طفرة نوعية وثورة متميزة في مجال تكنولوجيا المعلومات والاتصالات الحديثة، أصطلح عليها بالثورة المعلوماتية وقد سارت هذه الأخيرة بخطى حثيثة وحققت درجة متقدمة في تطوير سبل الحياة وانعكست على كل جوانبها وأصبحت قوة لا يستهان في أيدي الأفراد والدول.

ومما لاشك فيه أن الثروة المعلوماتية التي تقوم على استخدام الحاسب الآلي والانترنت والشبكات المعلوماتية التي تربط بينهما قد خلفت آثار إيجابية وقفزة حضارية في الحياة المعاصرة، وذلك لاتسامها

بالسرعة والدقة في تجميع المعلومات وإستخدمها ومعالجتها وتبادلها بين جهات مختلفة– أفراد أو مؤسسات– وعبر دول متعددة فهي لا تعتد بقيد الزمان والمكان من جهة.

ومن جهة أخرى أصبحت تشكل الذاكرة الحية المركزة لأسرار الدول الأمنية والعسكرية والاقتصادية وعلى الرغم من أهمية الوسائل التكنولوجية وإيجابيات استعمالها قابله العديد من الانعكاسات السلبية التي أفرزتها هذه التقنية المعلوماتية عن طريق الإساءة في إستخدام الأنظمة المعلوماتية وإستغلالها بشكل غير مشروع يضر بمصالح الافراد والمجتمع بأكمله حيث أدى هذا التطور المذهل الى ظهور نمط مستحدث من الجرائم أصطلح عليه بالجريمة الالكترونية.

وبتامي معدلات الجريمة الالكترونية وتعدد مجالات إرتكابها والذي شكل خطورة تمس بحياة الافراد وتهدد الأمن والسيادة الوطنية للدول بات لازما بتدخل السياسة التشريعية عموما ولاسيما السياسة الجنائية لمجابهة الاستخدام غير مشروع للأنظمة المعلوماتية وهذا لا يتأتى إلا من خلال ضبط وحصر هذه الجريمة وتحديد نطاقها.

فما مدى إستيعاب المشرع الجزائري للجريمة الالكترونية، وفيما يتحدد نطاقها؟

للإجابة عن هذا عن هذه الإشكالية، إرتأينا تقسيم الدراسة إلى محورين، حيث تناولنا في المحور الأول مفهوم الجريمة الإلكترونية.

أما المحور الثاني فقد خصص لدراسة نطاق إرتكاب الجريمة الإلكترونية.

المبحث الأول: مفهوم الجريمة الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة في عالم الإجرام وذلك لارتباطها بوسائل التقنيات الحديثة عن شبكات الإنترنت والمواقع الإلكترونية وأجهزة الكمبيوتر، ونظرا لحداثتها وسرعة تطورها وإنتشارها خلف ذلك إنعكاسات خطيرة تمس الجوانب السياسية والإقتصادية والإجتماعية للدول، تقتضي منا المسألة توضيح مفهوم الجريمة الإلكترونية ومميزاتها التي جعلتها تنمو بنحو متزايد من خلال ضبط تعريف الجريمة الإلكترونية في المطلب الأول، ومن ثمة التعرض إلى سمات وخصائص الجريمة الإلكترونية والمدرجة في المطلب الثاني.

المطلب الأول: تعريف الجريمة الإلكترونية

تتباين تعريفات الجريمة عموما بين الفقهاء القانونيين [1] إلا أنها تتفق في أن الجريمة بأنها بيان سلوك والسلوك غير المشروع وفق القانون.

وفي موضوع بحثنا هذا سنحاول الغوص في خصوصية الجريمة الإلكترونية على خلاف الجريمة التقليدية التي تقع في الواقع الملموس وذلك من خلال تناول رأي الفقه القانوني ثم استعراض رأي التشريعات المقارنة وفق الفرعين التاليين:

[1]- والتي يمكن حصرها في إتجاهين اتجاه شكلي: يربط تعريف الجريمة بين العلاقة الشكلية الواقعة والمرتكبة وبين القاعدة القانونية أي فعل مجرم بنص القانون أما الإتجاه الموضوعي يحاول إبراز جوهر الجريمة باعتبارها إعتداء على مصلحة اجتماعية أي جريمة هي واقعة ضارة لكيان المجتمع وأمنه؛ أنظر في ذلك: عبد الله سليمان، شرح قانون العقوبات الجزائري، الجزء الأول، الجريمة، (د، ط)، ديوان المطبوعات الجامعية، الجزائر 1996، ص58.

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية.

الفرع الثاني: التعريف القانوني للجريمة الإلكترونية.

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الإلكترونية، فهناك عدة تسميات لها منها الجريمة المعلوماتية، جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال، جرائم الكمبيوتر والإنترنت، الجرائم المستحدثة[1]، الجريمة الناعمة، إجرام ذوي الياقات البيضاء[2].

ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية، وتعرف الجرائم الإلكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.

وهنا ارتكز الباحثين والمختصين على ثلاثة معايير أساسية في تعريفهم للجريمة الإلكترونية، أولهما حاول تعريفها بالارتكاز على الوسائل المستخدمة للجرم وتم تعريفها بأنها "كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية المتمثلة في الحاسوب الآلي الرقمي وشبكة الإنترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف، وأما المعيار الثاني فيقوم على مستوى المعرفة بالتقنيات الحديثة وحينئذ عرفت بأنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى"[3]. أما المعيار الثالث فيستند في تعريفه للجريمة الإلكترونية على حسب موضوعها أو محلها ومنه فإن "الجرائم الإلكترونية هي الجرائم التي ترتكب ضد الأنظمة الإلكترونية والشبكات المعلوماتية"، والبعض الآخر في ذات الجزئية ذهب إلى القول بأنها "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب الإلكتروني أو التي تحول عن طريقه"[4].

وقد انقسم الفقهاء إلى اتجاهين، منهم من ينظر إلى الجريمة الإلكترونية بمفهوم ضيق، ومنهم من ينظر إليها بمفهوم واسع وهذا ما سيتم بيانه كما يلي:

أولا: الإتجاه المضيق لتعريف الجريمة الإلكترونية

يرى أنصار هذا الاتجاه أن الجريمة الإلكترونية بأنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي، أو الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية" كما يرى

---

[1]- وتجدر الإشارة إلى أن جرائم الكمبيوتر هي الإستخدام الأكثر شيوعا، أنظر في ذلك: ذياب موسى البداينة، الجرائم الإلكترونية، المفهوم والأسباب، الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة 2-2014/09/4، عمان، الأردن، ص5.

[2]- جرائم ذوي الياقات البيضاء مصطلح يطلق على الجرائم غير العنيفة والمرتكبة لدوافع مالية من قبل رجال الأعمال وأصحاب النفوذ في علم الجريمة وعرّفها إدوين سذرلاند المتخصص بعلم الاجتماع لأول مرة في عام 1939 بأنه «جريمة يرتكبها فرد من ذوي الطبقات الاجتماعية العليا وله مكانة مرموقة في نطاق مهنته» نقلا عن الموقع:

بتاريخ (2022/07/24 على الساعة10:21) -جرائم- ذوي- الياقات –البيضاء/ https://ar.wikipedia.org/wiki

[3]- فرج الحسين، الجريمة الإلكترونية وتداعيتها على أمن الوطن والمواطن بين المكافحة القانونية وأجهزة الكشف والتحري، مجلة الإدارة العامة والقانون والتنمية، المجلد الثالث، العدد الأول، 2022، ص74.

[4]- أشرف جمال محمود عبد العاطي، الإدارة الإلكترونية للمرافق العامة، (د، ط)، دار النهضة العربية، القاهرة، مصر، د.ت.ن، ص04.

الأستاذ Tredman أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات[1].

ويعاب على أنصار هذا الاتجاه أن نطاق الجريمة الإلكترونية من وجهة نظرهم ينقسم إلى عدة أفعال إجرامية غير مشروعة، وانتقد كذلك لأنه يحصر الجريمة في ضرورة توفر قدر عالي من التحكم في التقنية[2].

ثانيا: الإتجاه الموسع من تعريف الجريمة الإلكترونية

على عكس الإتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاما حاسو بيا، أو شبكة حاسوبية، للوصول إلى البيانات، والبرامج بغية نسخها، أو تغييرها، أو حذفها، أو تزويرها، أو تخريبها، أو جعلها غير صالحة، أو حيازتها، أو توزيعها بصورة غير مشروعة [3]. أما اتفاقية كومنولث الدول المستقلة (Agreement The Commonwealth of Indépendant States) من دون استخدام مصطلح "جرائم الإلكترونية" فعرفت الجريمة المتص لة بمعلومات الحاسوب بأنها العمل الإجرامي الذي يستهدف معلومات الحاسوب[4]. أي أن الاتفاقية قامت بتحديد تعريفها بشكل سهل ومبسط.

وبناء على ذلك فإن الجريمة الإلكترونية وفق ما سبق ذكره عموما هي كل سلوك إجرامي يرتكب باستخدام الحاسوب[5].

الفرع الثاني: التعريف القانوني للجريمة الإلكترونية

إصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها بموجب أحكام المادة 02 من القانون رقم 09-04[6] على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكا بها عن طريق منظومة معلوماتية، أو نظام للإتصالات الإلكترونية".

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما بينها في قانون العقوبات [7] من المادة 394 مكرر إلى 394 مكرر 07، وترك المجال واسع لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

---

[1]- نقلا عن حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، السنة الجامعية 2011-2012، ص14.

[2]- عبد الحكيم مولاي إبراهيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، العدد 23، جامعة زيان عاشور 2015، ص213.

[3]- كامل فريد السالك، الجريمة المعلوماتية، مداخلة في ندوة التنمية ومجتمع المعلوماتية، حلب، 21 و 23 أكتوبر، سوريا 2000.

[4]- ذياب موسى البداينة، المرجع السابق، ص6.

[5]- عبد الحكيم مولاي إبراهيم، المرجع السابق، ص213.

[6]- القانون رقم 09-04، المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها (الجريدة الرسمية العدد 47 الصادرة في 16 غشت 2009).

[7]- القانون رقم 04-15، الصادر في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 156/66، الصادر في 08 يونيو 1966، المتضمن قانون العقوبات، (الجريدة الرسمية العدد 71 الصادرة في 10 نوفمبر 2004).

والجدير بالذكر أن المشرع الجزائري قد وسع موقفه من تحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكا بها عن طريق منظومة معلوماتية، أو نظام الإتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الإتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية[1] ومن أمثلة الجريمة الإلكترونية المرتكبة في الجزائر، تسرب أسئلة البكالوريا لسنة 2016[2]، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطة الفيدرالية الأمريكية[3].

ومنه نخلص إلى :

- أن المشرع الجزائري قد إعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الإتصالات الالكترونية، وثانيها معيار موضوع الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات
- كذلك حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل إرتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الإلكترونية في القانون الجزائري[4].

المطلب الثاني: خصائص الجريمة الإلكترونية

بما أن الجريمة الإلكترونية هي وليدة التطورات العلمية التكنولوجية وبالتالي فهي تنفرد بجملة الخصائص والسمات التي تميزها عن الجريمة التقليدية التي ترتكب في الواقع المادي لا الإفتراضي سواء تلك المتعلقة بالجريمة ذاتها أو الخاصة بمرتكب الجريمة وهو ما سيتم بيانه من خلال الفرعين التاليين.

الفرع الأول: السمات الخاصة بالجريمة ذاتها

نظرا للطبيعة المميزة للجريمة الإلكترونية باعتبارها تمس المعلومات هذا ما جعلها تتميز عن نظير تها التقليدية بمجموعة من الخصائص أو السمات، والتي نوجزها فيما يلي:

- **خفاء الجريمة وسرعة التطور في إرتكابها**، حيث تتسم بأنها خفية ومستترة في أغلبها لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على شبكة الإتصالات، لأن الجاني يتمتع بقدرات فنية

---

[1]- سفيان سوير، جرائم المعلوماتية، رسالة ماجستير، فرع العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2010-2011، ص ص14-16.

[2]- للمزيد في التفاصيل تصفح في ذلك: https://radioalgerie.dz/news/ar/article/20160605/79589.html بتاريخ: (2022/07/24 على الساعة 12:35)

[3]- وهذا ما أكده مكتب التحقيقات الفيدرالي "أف بي آي" حيث نشر بعض التهم الموجهة لابن دلاج، من قبيل أنه سطى على حسابات 217 بنكا وحوّل من حساباتها ثروة تقدر بنحو 3.4 مليارات دولار، وتسبب بإفلاس شركات، وإخترق مواقع لقنصليات أوروبية ومؤسسات إسرائيلية وحتى بنوك ماليزية وقام بغلق أكثر من ثمانية آلاف موقع فرنسي؛ منشور على الموقع:
https://www.aljazeera.net/encyclopedia/icons/2015/8/30/حمزة-بن-دلاج-هاكر-بين-الحقيقة
بتاريخ: (2022/07/24 على الساعة 12:29).

[4]- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص52.

تمكنه من إرتكاب جريمته بدقة، مثلا عند إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم.

- **الجريمة الإلكترونية ذات بعد دولي :** أي أنها عابرة الحدود، فهي قد تتجاوز الحدود الجغرافية بسبب أن تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية، كما ينتج عنه صعوبات سياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية[1].
- **الجريمة الالكترونية صعبة الاكتشاف والإثبات:** تتسم الجريمة الإلكترونية بصعوبة بالغة في كشفها، وإن تم كشفها فهي من محض الصدفة، بسبب عدم ترك مرتكبيها في غالب أي أثر خارجي مرئي، أو قيام الجاني بتدمير الدلائل في ثواني معدودة[2].
- **أنها تتطلب وجود علم كافي بالجوانب الفنية كالتقنية لإستخدام الحاسوب والإنترنت،** وتعتبر العلاقة بين مدى الدراية بالجوانب الفنية والتقنية للحاسوب وبين الجريمة الإلكترونية علاقة طردية، فكلما زادت الخبرة لدى الأفراد بمعرفة تقنية الحاسوب، زاد إحتمال استخدام خبرتهم بشكل غير مشروع والعكس صحيح.

وبالتالي فأسلوب ارتكاب الجريمة الإلكترونية يختلف عن الجرائم التقليدية بكثير، فإذا كان متعارف عليه أن الجرائم التقليدية تستدعي للقيام بها نوع من الجهد العضلي في صور مختلف مثل السرقة والتعدي والاختطاف والعنف، فإن الجرائم الإلكترونية تحتاج إلى ذكاء وحنكة واستطاعة على التعامل مع جهاز الحاسوب في مستويات تقنية توظف لفعل غير مشروع[3].

الفرع الثاني: خصائص المجرم الإلكتروني

يتميز مرتكب الجريمة الالكترونية بمميزات خاصة تميزه من غيره من مرتكبي الجرائم الأخرى التقليدية، وسنوضحه فيما يلي:

- **المجرم الالكتروني شخص ذكي ومتخصص:** مرتكب الجريمة الإلكترونية في الغالب يكون شخص متميز بالذكاء، والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب وكيفية تشغيله، وكيفية تخزين المعلومات والحصول عليها، في حين أن مرتكب الجريمة التقليدية في الغالب شخص أمي[4].
- فضلا على أنه يتمتع بـللقيام بالتخطيط والتنظيم، ففي عالم الشبكات الإلكترونية، كما هو الحال في العالم الحقيقي، يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة حيث ترتكب أغلب الجرائم من مجموعة متكونة من عدة أشخاص يحدد لكل شخص دور معين، ويتم العمل بينهم وفقا لتخطيط

[1]- إسمهان بوضياف، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد الحادي عشر، سبتمبر 2018، ص355.
[2]- فرج الحسين، المرجع السابق، ص76.
[3]- إسمهان بوضياف، المرجع السابق، ص356.
[4]- إسمهان بوضياف، المرجع السابق، ص356.

وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمنا فيها متخصص في الحاسب الآلي يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب ولتحويل المكاسب إليه[1].

- **المجرم الإلكتروني شخص سوي واجتماعي:** عادة ما يتميز المجرم الإلكتروني بسلوك حسن وسط المجتمع، ولا يضع نفسه وسط عداء مجتمعي، غير أنه مقابل ذلك أو بدافع اللهو أحيانا أو بدافع الحصول على الأموال والإنتقام أحيانا أخرى يصبح مجرم الكترونيا [2] وهذا ما سيتم تناوله في محور الدراسة التالية.

المبحث الثاني: نطاق إرتكاب الجريمة الإلكترونية

تتفق الجريمة الإلكترونية مع الجرائم التقليدية من حيث قيامها على ثلاثة أركان وهي الركن الشرعي وتتمثل في الصفة غير المشروعة للفعل أي قاعدة التجريم والعقاب وما تضمنه القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، أما الركن المادي يتمثل في السلوك الإجرامي والنتيجة والعلاقة السببية بينهما، على العلم بأن الركن المادي قد يتحقق دون تحقق النتيجة[3]، فضلا عن الركن المعنوي وهو توفر الإرادة على الفعل بقصد أو بدون قصد[4].

وإن كان هذا التوافق يقوم على الأركان العامة للجريمة إلا أن طبيعة الجريمة الإلكترونية والمجرم الإلكتروني يقتضي هنا البحث عن أسباب الجريمة الإلكترونية والتي تختلف بحسب أنواعها وكل هذا بهدف ردع الجاني أو على الأقل تلافي وقوعها وسنعرض إلى تحديد أهم الأسباب والدوافع التي تسهم في إرتكاب الجريمة الإلكترونية (المطلب الأول) لنصل لتحديد أنواع الجرائم الإلكترونية في(المطلب الثاني).

المطلب الأول: دوافع إرتكاب الجريمة الإلكترونية

من الطبيعي أن نجد إختلاف في الأسباب والعوامل التي تدفع إلى إرتكاب الفعل غير المشروع، فالدافع (الباعث)، الغرض، الغاية، كلها مفاهيم لها دلالات في الفقه الجنائي، تتصل بما يعرف بالقصد الجنائي في الجريمة وهي مسألة تتمايز بين الجريمة لأنها قوة نفسية ذاتية تدفع الإرادة إلى إرتكاب الجريمة لتحقيق غاية معينة كالمحبة، الشفقة والبغضاء والإنتقام، كما أن الغاية فهي الهدف الذي يسعى الجاني لتحقيقه من وراء إرتكاب الجريمة كسلب المال، الإنتقام وأهم هذه الأسباب التي تختلف وفق أهداف المحترفين يمكن تبيانها كمايلي:

الفرع الأول: الدوافع الشخصية

هنا يظهر تأثير العنصر المادي لتحقيق الربح في إرتكاب الجريمة وتصنف إلى دوافع مادية وذهنية.

---

[1]- عائشة نايري، الجريمة الالكترونية في التشريع الجزائري، مذكرة ماستر، تخصص القانون الاداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، السنة الجامعية 2016-2017، ص 19.

[2]- محمد رحموني، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة للعلوم الإنسانية والإجتماعية، جامعة أحمد دراية، أدرار، المجلد 16، العدد 03، 2017، ص444.

[3]- مثلا إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة كما قد يكون الركن المادي في الجريمة كصورة فعل إيجابي كجريمة الغش الإلكتروني وتغيير في المحررات الإلكترونية، أنظر في ذلك: فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر (الجرائم الإلكترونية)، طرابلس، 24 و 25 مارس 2017، ص112.

[4]- فرج الحسين، المرجع السابق، ص78.

أولا: الدوافع المادية

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الإلكتروني إلى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الإحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الآلية لها من خلال اكتشافه لفجوا تها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه، أو لحساب شركائه، أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة[1].

والجدير بالذكر أن نجاح المجرم الإلكتروني في إرتكاب جريمته فإن ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة إقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الإلكترونية، حيث تبين أن 85 %من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة للأنظمة المعلوماتية، وأن 64% لحقت بهم خسائر مادية جراء هذه الإعتداءات[2].

ثانيا: الدوافع الذهنية لارتكاب الجريمة الإلكترونية

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي و إثبات الذات ، وقد تكون هذه الدوافع مجرد شغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد الوسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه[3].

الفرع الثاني: الدوافع الموضوعية لإرتكاب الجريمة الإلكترونية

أحيانا يتأثر المجرم الإلكتروني ببعض المواقف تدفعه لإرتكاب الجريمة ولا يسعى في ذلك لا للمتعة أو التسلية أو كسب المال ولكن إلى دافع الإنحراف وخرق القانون، فضلا عن التعاون بين خبراء ومختصين في الأنظمة المعلوماتية لإرتكابهم هذا المشروع الإجرامي ويمكن حصرها في:

أولا: دافع الإنتقام وإلحاق الضرر برب العمل

يعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى إرتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، وغالبا ما يكون هذا

---

[1]- عائشة نايري، المرجع السابق، ص11.

[2]- نعيم سرعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، تخصص العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012-2013، ص ص60-61.

[3]- تجدر الإشارة إلى أن أغلب هذه الجرائم يرتكبها شباب طائش وصغير السن وذلك من باب التحدي والظهور في الإعلام للمزيد من التفاصيل، أنظر في ذلك: ذياب موسى البدانية، المرجع السابق، ص10.

الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المجرم الإلكتروني الرغبة في الإنتقام من رب العمل، ومثال ذلك أن الإنتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه[1].

ثانيا: دافع التعاون والتواطؤ

هذا النوع يتكرر كثيرا في الجرائم الإلكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم[2].

المطلب الثاني: أنواع الجرائم الإلكترونية

تعد الجريمة الإلكترونية من الجرائم المستحدثة والتي لا يمكن حصرها نتيجة التطور السريع لها من حين إلى آخر، فهي متغيرة ومتجددة ومرتبطة إرتباطا وثيقا بوسائل إستخدام الحاسوب الآلي والإنترنت وقد قسم المشرع الجزائري الجريمة الإلكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي فقد نص عليها ولم يحددها، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والإتصال.

أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي والتي حددها قانون العقوبات.

وهذا ما سيتم إدراجها وفق الفرعين التاليين:

الفرع الأول: الجريمة الإلكترونية واقعة بواسطة النظام المعلوماتي

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، ومنها الجريمة الواقعة على الأشخاص، الواقعة على الأموال، الجريمة الواقعة على أمن الدولة.

أولا: الجرائم الواقعة على الأشخاص

لقد أضحت حياة الأشخاص في ظل التطور العلمي والتكنولوجي في خطورة نتيجة حالات السطو والإطلاع على أدق تفاصيلهم وإستعمال السلبي ضدهم كما سنوضحه فيما يلي:

1 -التهديد: بمعنى المضايقة وزرع في نفس الأفراد أضرار تمسهم شخصيا أو من تحت رعايتهم أو من تربطهم صلة بهم، لاسيما خلال إرسال المجرم الإلكتروني رسائل تنطوي على تخويف وتهديد بغية ابتزاز الضحية أو رغبة في تحكم فيه.

[1]- هناك من أطلق عليها تسمية الضغوط العامة وإرجاعها إلى العوامل الاجتماعية والإقتصادية كانخفاض الأجور، توظيف متعاقدين من الخارج لما تخلق من مشاعر سلبية في زيادة إرتكاب جريمة الكترونية، أنظر في ذلك: ذياب موسى البدانية، المرجع نفسه، ص12.

[2]- نعيم سعيداني، المرجع السابق، ص62.

2 -إنتحال الشخصية: من خلال قيام المجرم الإلكتروني باستغلال شخصية فرد من أفراد لأجل الإستفادة من سلطته أو سمعته أو ماله ويجد هذا المجال انتشارا في الميدان التجاري.

3 -ترويج الإباحة: من خلال إرسال أو نشر أي نشاط إباحي أو إعداده أو طبعه أو نشره وترويجه لصور جنسية فاضحة التي تستهدف الأطفال والشباب عموما كونهم أقل تحصينا[1].

ثانيا: الجرائم الواقعة على الأموال

وهي من أبرز القضايا المنتشرة في شبكات الإنترنت بعد أن باتت أغلب المعاملات المالية التجارية تتم عبر الإنترنت وأبرز مجالاتها ما يلي:

1 -بطاقات الإئتمان والتحويلات المالية الإلكترونية: حيث يتم كسر الكلمة السرية للبطاقات الإلكترونية أو من خلال فك شفرة الصراف الآلي وقيام بتحويلات مالية من المصدر إلى رصيده أو رصيد متعامل آخر أو الحصول من خلالها على سلع وخدمات من بطاقات مثل ماستر كارد[2].

2 -سرقة البنوك: والذي يتم من خلال استغلال المجرم الإلكتروني الحاسوب للدخول عبر الشبكة لنظام معلومات البنوك أو المؤسسات المالية ويباشر القيام بتحويلات من حساب العملاء إلى حسابات أخرى من خلال كميات قليلة حتى لا يتم اكتشافه أو دفعة واحدة.

3 -غسيل الأموال [3]: تشير إحصائيات الأمم المتحدة وصندوق البنك الدولي أن ما قيمته 30 مليار أمريكي من الأموال تغسل سنويا عبر شبكة الإنترنت، مخترقة ما يقرب 76 دولة، تتولاه شبكات منظمة على درجة عالية من التخطيط والتنسيق بينها[4].

ثالثا: الجرائم الواقعة على أمن الدولة

إستغلت الكثير من الجماعات المتطرفة الطبعة الإتصالية للإنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدي عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا معنى آخر في إستعمال الإنترنت، التي سمحت لهم في إرتكاب جرائم غاية الخطورة في حق المجتمعات والدول، بل الأخطر من ذلك آتاحت الإنترنت لكثير من الدول ممارسة التجسس على دول آخرى، وذلك بالإطلاع على مختلف الأسرار السياسية و العسكرية والاقتصادية لهذه الأخيرة خاصة فيما يتعلق بالدول التي يكون فيها نزاعات، ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر

---

[1]- فرج الحسين، المرجع السابق، ص77.

[2]- تعرف بطاقات الماستر كارد بأنها بطاقات دفع مصرفية عالمية، وتشمل هذه البطاقات عدة علامات تجارية وهي (MasterCard) (Cirrus) (Maestro) (PayPass)، وتقوم هذه العلامات التجارية على أساس التعاون مع المؤسسات المالية والبنوك التي تصدر هذه البطاقات وأيضاً مع التجار الذي يقبلون التعامل مع هذه البطاقات، ويوجد أكثر من 28 مليون موقع يقبل التعامل والدفع من خلال بطاقات الماستر كارد، ومن الجدير بالذكر بأنّ شبكة الماستر كارد لا تقوم بإصدار البطاقات ولا تفرض أية رسوم سنوية لحاملي البطاقة ولا تطلب من التجار قبول بطاقاتها، لكنّها بالمقابل تضع سياسات خاصّة تتعلّق بالدفع وإعادة الشحن. للمزيد من التفاصيل تصفح في ذلك: https://www.creditcards.com/glossary/term-mastercard ;DV(25/07/2022, 10H43).

[3]- هي أي عملية من شأنها إخفاء المصدر غير المشروع الذي اكتسبت منه الأموال؛ وللمزيد من التفاصيل :راجع نص المادة الثانية من القانون رقم 05-01 المؤرخ في 06 فيفري 2005 المتضمن قانون الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما،(الجريدة الرسمية، العدد 11 الصادرة في 09 فيفري 2005).

[4]- محمد حجازي، جرائم الحاسبات والانترنت (الجرائم المعلوماتية)، (د، ط)، المركز المصري للملكية الفكرية، القاهرة، مصر، 2005، ص21.

الإنترنت، حيث تعطي الإنترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات وأمم بأكملها مما يسهل خلق الفوضى[1].

الفرع الثاني: الجريمة الإلكترونية الواقعة على النظام المعلوماتي

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 04-15 المتضمن قانون العقوبات بتجريم كل أنواع الإعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد السالفة الذكر(394 مكرر إلى 394 مكرر 07)، وتأخذ صور الإعتداء في المجال الالكتروني صورتين هما : الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش وهو ما سنتناوله تباعا وكالاتي:

أولا: جريمتي الدخول والبقاء غير المشروعان في المنظومة المعلوماتية

تنص المادة 394 مكرر من قانون العقوبات الجزائري على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فإن العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام[2].

1. **فعل الدخول غير المشروع:** لا نعني هنا الدخول بالمعنى المادي، أي الدخول إلى مكان معين كمنزل أو غيره، وإنما ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات، وتقع هذه الجريمة من كل إنسان أيا كانت صفته سواء كان شخص يعمل في مجال المعلوماتية أو لا يعمل، وسواء كان يستطيع أن يستفيد من الدخول أم لا، فيكفي أن يكون الجاني ممن ليس له الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط.
2. **فعل البقاء غير المشروع:** يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول في النظام وقد يجتمعان، ويكون البقاء معاقبا عليه إستقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ، وهنا يجب على المتدخل

[1]- وبالتالي فالجرائم الالكترونية الواقعة على أمن الدولة يمكن اجمالها في جرائم الارهاب وجرائم التجسس والجريمة المنظمة للمزيد من التفاصيل أنظر في ذلك: محمد رحموني، المرجع السابق، ص ص 448-449.

[2]- تنص المادة 394 مكرر من القانون رقم 15/04 المتضمن قانون العقوبات الجزائري المعدل والمتمم على أنه : "يعاقب بالحبس من ثلاثة أشهر(3) الى ستة (6) وبغرامة من 50.000 دج إلى 100000 دج لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.....".

أن يقتطع وجوده داخل النظام وينسحب، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع[1].

ثانيا: جريمة المساس بمنظومة معلوماتية

نص المشرع الجزائري في قانون العقوبات على معاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش. هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي[2].

ثالثا: أفعال إجرامية أخرى

جرم المشرع الجزائري في قانون العقوبات السابق الذكر الأعمال الآتية: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السابقة الذكر [3]، ويقصد بتصميم المعطيات هنا الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في إرتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية، أو المعطيات المعلوماتية في حد ذاتها، كما جرم المشرع كذلك أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لأي غرض[4].

الخاتمة:

وختاما لما سبق، وعلى مدار هذه الدراسة يتضح لنا أن الجريمة الالكترونية ذات طبيعة خاصة ومتميزة فهي جريمة ناعمة حال إرتكابها بأيدي بيضاء لاتصل إلى حد قسوة وخشونة الجرائم التقليدية، لأنها تقع في ثواني معدودة بمجرد ملامسة المجرم الالكتروني زر لوحة مفاتيح الحاسب الآلي، ودون إلتقاء بينها وبين الضحية في مسرح الجريمة ويمكننا إستخلاص النتائج التالية:

أولا: عدم إجماع الفقه القانوني على تعريف موحد للجريمة الالكترونية خاصة الاتجاه الموسع – وقد تبنى هذا الاتجاه المشرع الجزائري في القانون رقم 09-04 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها – الذي وسع واعتبر كل فعل غير مشروع يكون للحاسب الآلي دورا في إرتكاب الجريمة الأمر الذي صعب من مهمة المشرع في ضبطها وإعطاء

---

[1]- حمزة بن عقون، المرجع السابق، ص ص 182-183.

[2]- عملا بأحكام المادة 394 مكرر1 من القانون رقم 15/04 المتضمن قانون العقوبات الجزائري المعدل والمتمم على أنه: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500000 دج الى 2000000 دج لكل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطرق الغش المعطيات التي يتضمنها".

[3]- المادة 394 مكرر2 من القانون 2 العقوبات الجزائري السالف ذكره على أنه: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 500000 دج إلى 2000000 دج كل من يقوم عمدا وعن طرق الغش بما يأتي....".

[4]- الجدير بالذكر أن من أخطر الفيروسات الحالية هو فيروس الفدية هو نوع خبيث من البرامج يقفل أجهزة الحاسوب الشخصي أو اللوحي أو الهواتف الذكية – أو يضع تشفيرا على الملفات ثم يطلب فدية مقابل إعادتها إليك في حالة سليمة و هناك نوعان أساسيان منه فيروس التشفير وفيروس الحجب، تصفح في ذلك الموقع:

https://noransom.kaspersky.com/ar/faq/ DV:(25/07/2022,11H44)

تعريف مانع جامع للجريمة الالكترونية أو حصر نطاقها، والسبب في ذلك يعود إلى أن الوسائط الالكترونية في تطور مستمر – عصر التكنولوجيا–.

ثانيا: أن الجريمة الالكترونية التي تستهدف الجانب البرمجي للنظم المعلوماتية تتعدد أنماطها وتتنوع دوافع إرتكابها، مما خلف أثار سلبية تهدد إمن الأشخاص و الاموال والدول.

وعلى ضوء ذلك يمكننا التوصل إلى المقترحات التالية:

1/ ضرورة تدخل المشرع الجزائري في ضبط هذه الجريمة المستحدثة و إستدراك النقص الموجود في القانون رقم 09-04 على المستوى الموضوعي و الإجرائي لضبط الجريمة الالكترونية بشكل دقيق.

2/ تنسيق الجهود الدولية لسن قانون دولي يتناسب مع حجم ظاهرة الجريمة الالكترونية العابرة للحدود.

3/ مواكبة التطور المتواتر في مجال الاتصالات الحديثة وضرورة إعادة النظر في المناهج المتبعة في كليات الحقوق وتدريس مقاييس لها علاقة بالجريمة الالكترونية، المحكمة الالكترونية.

قائمة المراجع

أولا: القوانين

– القانون رقم 04-15، الصادر في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 156/66، الصادر في 08 يونيو 1966، المتضمن قانون العقوبات، (الجريدة الرسمية العدد 71 الصادرة في 10 نوفمبر 2004).

– القانون رقم 05-01 المؤرخ في 06 فيفري 2005 المتضمن قانون الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، (الجريدة الرسمية، العدد 11 الصادرة في 09 فيفري 2005).

– القانون رقم 09-04، المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها (الجريدة الرسمية العدد 47 الصادرة في 16 غشت 2009).

ثانيا: الكتب

– عبد الله سليمان، شرح قانون العقوبات الجزائري، الجزء الأول، الجريمة، (د، ط)، ديوان المطبوعات الجامعية، الجزائر 1996.

– أشرف جمال محمود عبد العاطي، الإدارة الإلكترونية للمرافق العامة، (د، ط)، دار النهضة العربية، القاهرة، مصر، د.ت.ن.

– نهلا عبد القادر المومني، الجرائم المعلوماتية ، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008.

– محمد حجازي، جرائم الحاسبات والانترنت (الجرائم المعلوماتية)، (د، ط)، المركز المصري للملكية الفكرية، القاهرة، مصر، 2005.

ثالثا : الرسائل والمذكرات الجامعية

– حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، السنة الجامعية 2011-2012.

– سفيان سوير، جرائم المعلوماتية، رسالة ماجستير، فرع العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، السنة الجامعية 2010–2011.

– نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، تخصص العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012–2013.

– عائشة نايري، الجريمة الالكترونية في التشريع الجزائري، مذكرة ماستر، تخصص القانون الاداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، السنة الجامعية 2016–2017.

رابعا: المقالات

– فرج الحسين، الجريمة الإلكترونية وتداعيتها على أمن الوطن والمواطن بين المكافحة القانونية وأجهزة الكشف والتحري، مجلة الإدارة العامة والقانون والتنمية، المجلد الثالث، العدد الأول، 2022.

– عبد الحكيم مولاي إبراهيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، العدد 23، جامعة زيان عاشور، 2015.

– إسمهان بوضياف، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد الحادي عشر، سبتمبر 2018.

– محمد رحموني، خصائص الجريمة الإلكترونية ومجالات است خدامها، مجلة الحقيقة للعلوم الإنسانية والإجتماعية، جامعة أحمد دراية، أدرار، المجلد 16، العدد 03، 2017.

خامسا: الملتقيات

– ذياب موسى البداينة، الجرائم الإلكترونية، المفهوم والأسباب، الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة 2–2014/09/4، عمان، الأردن.

– كامل فريد السالك، الجريمة المعلوماتية، مداخلة في ندوة التنمية ومجتمع المعلوماتية، حلب، 21 و 23 أكتوبر، سوريا 2000.

– فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر (الجرائم الإلكترونية)، طرابلس، 24 و 25 مارس 2017.

خامسا: المواقع الالكترونية

https://ar.wikipedia.org/wiki/جرائم_ذوي_الياقات_البيضاء/

https://radioalgerie.dz/news/ar/article/20160605/79589.html

https://www.aljazeera.net/encyclopedia/icons/2015/8/30/حمزة-بن-دلاج-هاكر-بين-الحقيقة

https://www.creditcards.com/glossary/term-mastercard

https://noransom.kaspersky.com/ar/faq/–

ديب أكرم
akram.dib@univ-batna.dz
جامعة الحاج لخضر باتنة 1
مخبر الحوكمة والقانون الاقتصادي

الجريمة الإلكترونية " الأسس و المفاهيم "

Cybercrime "Foundations and Concepts"

ملخص:

أدى التطور التكنولوجي و التقنيو التغيرات التي عرفها العالم بأسره لاسيما الثروة المعلوماتية الهائلة والتحرر الاقتصادي في إطار العولمة ، إلى انتشار واسع للشبكات الالكترونية و بروز وسائل التكنولوجيا و الاتصال الحديثة التي فرضت نفسها في جميع مناحي الحياة، و صاحب هذا التطور ظهور أنماط جديدة من الإجرام المستحدث تختلف من حيث طبيعتها و مرتكبيها و أساليب ارتكابها عن الجرائم التقليدية، و أضحت الجريمة الالكترونية تشغل حيزا لا يستهان به ضمن حقل العلوم الجنائية و الدراسات الأكاديمية، حيث يكتنف هذه الجرائم سلوكيات إجرامية خطيرة و متطورة بالتزامن مع التطور الذي تشهده مختلف الميادين و الاستخدام الواسع للشبكة العنكبوتية التي أتاحت للأفراد تبادل و تداول المعلومات في البيئة الافتراضية، و هو ما انجر عنه المساس بمصالح الأفراد و المؤسسات و مصالح أساسية محمية قانونا.

وأمام التحولات التي تشهدها الجريمة كظاهرة اجتماعية انتقلت من البيئة الواقعية إلى البيئة الافتراضية دون أن تعرف حدودا مكانية أو زمانية، تأتي هذه الدراسة بهدف تسليط الضوء على الجريمة الالكترونية للتعرف عليها وبيان خصوصيتها والبحث في الدوافع التي ساهمت في استفحالها، بالإضافة إلى الخوض في أنواعها وتصنيفاتها.

الكلمات المفتاحية: الجريمة الالكترونية _ الإجرام المستحدث _ البيئة الافتراضية _ الثورة المعلوماتية_ وسائل التكنولوجيا والاتصال الحديثة.

Abstract:

Led technological development and technical And the changes that the whole world has known, especially the huge information wealth and economic liberalization in the context of globalization, To the wide spread of electronic networks and the emergence of modern means of technology and communication that imposed itself in all aspects of life, and this development was accompanied by the emergence of new patterns of newly created crime that differ in terms of their nature, perpetrators and methods of committing them from traditional crimes, and cybercrime has become a space not It is insignificant within the field of forensic sciences and academic studies, where these crimes are surrounded by dangerous and sophisticated criminal behaviors in conjunction with the development witnessed in various fields and the widespread use of the Internet that allowed individuals to exchange and circulate information in the virtual environment, which

resulted in prejudice to the interests of individuals Institutions and basic interests are legally protected.

In the face of the transformations witnessed by crime as a social phenomenon that moved from the real environment to the virtual environment without knowing spatial or temporal limits, comes this study with a goal Highlight Electronic crime to identify it, clarify its privacy and research the motives that contributed to its exacerbation, in addition to delving into its types and classifications.

key words: *cyber crime, newly created crime, virtual environment, The information revolution, the means of modern technology and communication.*

مقدمة:

حقق العالم قفزة نوعية في مجال التكنولوجيا بفضل التطور النوعي الذي كان نتاج الثورة المعلوماتية و التقنية تجلت ملامحها في بروز النظام العالمي الجديد و التحول إلى التعاملات الالكترونية باستخدام الشبكة العالمية العنكبوتية (الإنترنت) في كافة الميادين، و هو ما أثر إيجابا على نمط حياة الأفراد و المجتمعات نظرا للخدمات و التسهيلات التي تقدمها الشبكات الالكترونية في وقت قياسي و التي جعلت من العالم قرية صغيرة يتم تداول المعلومات فيه على نطاق واسع دون قيود أو احتكار للمعلومة أو التقنية.

الجانب الإيجابي لهذه التطورات و التغيرات في العالم نتج عنه انعكاسات سلبية لسوء استخدام وسائل التكنولوجيا و الاتصال الحديثة، برزت في شكل سلوكيات مادية ترقى إلى جرائم خطيرة تهدف للأضرار بالمصالح الأساسية للمجتمع و أفراده و مؤسساته، من خلال استغلال الأنظمة المعلوماتية في نشاطات غير مشروعة، و هو ما اصطلح عليه بالجرائم الالكترونية كظاهرة إجرامية مستحدثة اقترنت بثورة المعلومات و التكنولوجيا، اتخذت من الفضاء الافتراضي منشأ لها و التي يتم اقترافها من طرف مجرمين معروفين بالدهاء و الذكاء و الدقة في التخطيط و الإلمام بأدوات المعرفة التقنية.

و لا شك أن النمط الجديد من الإجرام المستحدث له انعكاسات وخيمة على المجتمع و أفراده سواء على الصعيد الاقتصادي، الاجتماعي، الثقافي، السياسي، و هو ما استلزم ضرورة تكثيف الجهود للإلمام بهذه الظاهرة الإجرامية بداية من تحديد تعريف موحد لها و بيان خصائصها مرورا بالبحث عن أسباب ارتكابها و الدوافع التي يرمي إليها مرتكبيها، وصولا إلى تنصيفها حسب طبيعتها، و كل ذلك تمهيدا لمواجهة تشريعية تعمل على احتوائها و الحد منها، وتأسيسا على ما سبق فإن دراسة هذا الموضوع كانت من منطق إشكالية رئيسية مفادها:

إلى أي مدى وفقت الجهود الدولية والإقليمية وكذا المحلية في الإحاطة بالجانب المفاهيمي للجريمة الالكترونية؟

وللإجابة على الإشكالية الرئيسية قسمنا موضوع دراستنا إلى مطلبين، الأول يتعلق بمفهوم الجريمة الالكترونية،والثاني نتطرق لتصنيفات الجرائم الالكترونية، ونختم هذه الدراسة بأبرز النتائج والتوصيات.

المطلب الأول: مفهوم الجريمة الالكترونية

تعتبر الجريمة الإلكترونية من الجرائم العصرية المستحدثة اقترنت بالثورة التكنولوجية و المعلوماتية التي شهدها العالم بأسره و بروز معالم النظام العالمي الجديد و ما صاحبه من انفتاح اقتصادي و تغيرات

و تطورات في شتى الميادين ، و قد باتت هذه الطائفة من الجرائم من اكثر الجرائم استفحالا في الوقت الراهن، اتخذت من البيئة الالكترونية أو الافتراضية مرتعا لها، و لم تعد تعرف حدودا مكانية أو زمانية، ناهيك عن أنها تختلف من حيث طبيعتها و مضمونها و أساليبها عن الجرائم التقليدية، و هو ما يستلزم ضرورة تحديد تعريفا لها و بيان خصائصها و دوافع ارتكابها و الأهداف التي ترمي إليها، حيث نتناول في هذا المطلب تعريف الجريمة الالكترونية في **الفرع الأول** ، ثم نتطرق بالدراسة إلى بيان أسباب و أهداف الجريمة الالكترونية في **الفرع الثاني** .

الفرع الأول: تعريف الجريمة الالكترونية

عرف مصطلح الجريمة الإلكترونية استخداما واسعا في السنوات الأخيرة، ممّا أحدث تغيرات جذرية في المفاهيم القانونية بمختلف فروع القانون، وهو ما استلزم حتمية تحديد مدلول الجريمة الإلكترونية سواء في الجانب الفقهي أو القانوني وبيان خصائصها باعتبارها من الجرائم المستحدثة التي استفحلت بشكل غير مسبوق في الأونة الأخيرة، وعليه لابد من تحديد المقصود بالجريمة الالكترونية **أولا**، ثم نتطرق لخصائصها وسماتها **ثانيا**.

أولا: المقصود بالجريمة الالكترونية

تناول العديد من المفكرين والباحثين تعريفات عديدة للجريمة الالكترونية، كما برزت جهود لمنظمات دولية وتشريعات وطنية لتحديد تعريف شامل لهذه الظاهرة الإجرامية

1 -التعريفات الفقهية للجريمة الالكترونية

قبل الشروع في تعريف الجريمة الالكترونية لابد من إعطاء تعريف للجريمة في حد ذاتها حسب المفاهيم المتعارف عليها، حيث ينظر للجريمة بالمفهوم القانوني كل مخالفة لقواعد القانون الوضعي المعمول به سواء كانت هذه القواعد متعلقة بالقانون الجنائي أو غيره من القوانين [1]، و ينصرف هذا التعريف للمفهوم الواسع للجريمة أي كل مخالفة تقع على قاعدة قانونية مهما كان نوعها جنائية، مدنية أو إدارية.

ويذهب الدكتور محمود نجيب حسني إلى القول بأن الجريمة هي" كل فعل غير مشروع صادر عن إرادة جنائية، ويقرر له القانون عقوبة أو تدبير أمن من التدابير الأمنية" [2]، والجريمة في أبسط معانيها هي كل سلوك أو امتناع مخالف للقانون يعرض مرتكبه للعقوبة أو الجزاء الجنائي كما هو مقرر في قانون العقوبات والقوانين المكملة له.

ويذهب الدكتور عبد الفتاح مراد إلى تعريف الجريمة الالكترونية بأنها: " جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسط الحاسب الآلي من خلال شبكة الإنترنت وهي تتطلب إلماما خاصا بتقنيات

[1] _ حسين عبد الكريم يونس، خليل يوسف الجندي، الابتزاز الالكتروني و الجرائم الالكترونية المفهوم و الأسباب، الطبعة الأولى، دار كفاءة المعرفة، عمان، الأردن ، سنة 2021، ص 63.

[2] _ سعيد بوعلي، شرح قانون العقوبات الجزائري القسم العام، دار بلقيس للنشر، الجزائر، سنة 2017، ص44.

الحاسب الآلي ونظم المعلومات سواء لارتكابها أو للتحقيق فيها ويقصد بها أيضا أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الإنترنت مثل مواقع الإنترنت وغرف المحادثة أو البريد الالكتروني"[3].

بيد أنه يأخذ على التعريفات السابقة أنها تناولت تعريف الجريمة الالكترونية بالنظر إلى الوسيلة المستعملة في ارتكابها، و حصرت هذه الوسيلة في الحاسب الآلي أو الكمبيوتر ، و الواقع أن الجرائم الالكترونية يمكن أن ترتكب بوسائل التكنولوجيا و الاتصال الحديثة الأخرى غير الحاسب الآلي، كالهواتف الذكية و اللوحات الالكترونية و غيرها، خصوصا فيما يتعلق بالجرائم الواقعة على مواقع التواصل الاجتماعي كجريمة الابتزاز الالكتروني و القذف و التشهير الالكترونيين، و جرائم الإرهاب الالكتروني ، فمثل هاته الجرائم تتخذ عدة وسائل كأداة لارتكابها، و من ثم فالتعريفات السابقة جاءت بقصور في إعطاء تعريف شامل و جامع للجرائم الالكترونية.

وتداركا لذلك يرى بعض المفكرين والباحثين أن الجريمة الالكترونية هي: " كل فعل أو نشاط أو سلوك غير مشروع يقع على الشبكة الالكترونية أو على أجهزة أو وسائل تكنولوجيا المعلومات بشكل عام، أو كل فعل أو نشاط غير مشروع يقع من خلال الشبكة الالكترونية أو إحدى وسائل تكنولوجيا المعلومات[4].

2 -الجريمة الالكترونية في المواثيق الدولية والتشريعات الوطنية:

الجريمة الالكترونية باعتبارها صورة مستحدثة للجريمة في مفهومها التقليدي، فقد تباينت التعريفات بشأنها نتيجة للتطور المستمر والمتسارع لتكنولوجيا المعلومات والاتصال الحديثة، فعرفها مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة **2000**، بأنها: " أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوب، وهذه الجريمة تشمل الجرائم التي يمكن ارتكابها في بيئة الكترونية"[5].

عرف مكتب تقييم التقنية في الولايات المتحدة الأمريكية الجريمة الإلكترونية من خلال تعريف الحاسب الآلي بأنها: " الجرائم التي تقوم فيها بيانات الحاسب الآلي و البرامج المعلوماتية بدور رئيسي" [6]، و في ذات النسق تعتبر منظمة التعاون و التنمية الاقتصادية **OCDE** من السباقين لوضع تعريف للجريمة الالكترونية و الغش المعلوماتي و التي ذهبت إلى القول بأنها :

« Est considère comme crime informatique tout comportement illégale ou contraire à l'éthique, ou non autorisé qui concerne un traitement automatique de données ou de transmissions de données »[7].

---

[3] محمد الشبلي العتوم، جرائم تكنولوجيا المعلومات، النظرية العامة للجرائم الالكترونية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، الأردن، سنة 2021، ص190.

[4] عبد الله ذيب محمود، أسامة إسماعيل دراج، الوجيز في الجرائم الالكترونية القواعد الموضوعية و الإجرائية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، الأردن، سنة 2022، ص 20.

[5] المرجع نفسه،ص 19.

[6] صراع كريمة، دقيش جمال، الأبعاد الاقتصادية للجريمة الإلكترونية، مجلة الدراسات التسويقية و إدارة الأعمال، المجلد 2، العدد 1، الجزائر، جانفي2018، ص37.

[7] دمان ذبيح عماد، بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق و العلوم السياسية، العدد13، الجزائر، جانفي 2020، ص 141.

و من ثم فالجريمة الالكترونية هي : " كل جريمة أو سلوك غير مشروع يستخدم بالحاسب الآلي أو محاولة نسخ أو حذف أو إتلاف لبرامج الحاسب الآلي أو أي جريمة يكون لتنفيذها صلة بالقواعد و العلوم المعلوماتية أو أي سلوك غير مشروع متعلق بالمعالجة الآلية للبيانات"[8].

و تطرقت الاتفاقية العربية و اتفاقية بودابست والاتحاد الدولي للاتصالات لتعريف موحد للجريمة الالكترونية على أنها: " كل جناية أو جنحة ترتكب ضد فرد أو جماعة بدافع جرمي و نية الإساءة لسمعة الضحية أو جسده أو فكره أو ماله أو حياته، سواء كان ذلك بطريقة مباشرة أم بطريقة غير مباشرة باستخدام وسائل الاتصالات الحديثة و الإنترنت"[9].

في حين أغفلت غالبية التشريعات التطرق لتعريف الإجرام الالكتروني و اقتصرت على تجريم الأفعال المادية المرتبطة بالجريمة الالكترونية، بيد أن المشرع الإماراتي وضع تعريفا لها من خلال قانون مكافحة جرائم تقنية المعلومات، حيث عرفها بأنها: " كل فعل عمدي بقصد اختراق موقع مؤمن نتج عن ذلك إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات حكومية كانت أو شخصية "[10].

وتبنى المشرع الجزائري للدلالة على الجريمة الالكترونية مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، حيث جرم الأفعال الماسة بالمنظومة المعلوماتية وبأنظمة الحاسب الآلي من خلال تعديل قانون العقوبات بموجب القانون رقم **04-15** المؤرخ في **10** نوفمبر **2004**، و اعتبر المشرع الجزائري النظام المعلوماتي في حذ ذاته و ما يحتويه من مكونات غير مادية محلا للجريمة [11]، و لم يتطرق المشرع إلى تعريف الجريمة الالكترونية و إنما حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات بموجب نص المادة **394مكرر1** من قانون **04-15** المتضمن قانون العقوبات.

ثانيا: سمات الجريمة الالكترونية

تنفرد الجريمة الالكترونية بمجموعة من الخصائص لا تتوافر في الجرائم العادية، وذلك نظرا لطبيعتها الخاصة والوسيلة المستعملة في ارتكابها، ويمكن إجمال خصائصها فيمايلي:

1 -الجريمة الالكترونية جريمة مستحدثة:

تعتبر الجرائم الالكترونية سواء التي تتعرض لها أجهزة الحاسوب والشبكات الالكترونية وأجهزة تكنولوجيا المعلومات المختلفة من الجرائم المستحدثة التي لم يألفها المجتمع من قبل، فالتقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة [12]. و صاحب هذا التطور ظهور أنماط جديدة من الجرائم من بينها الجرائم الإلكترونية التي تختلف من حيث طبيعتها و مرتكبيها و أساليب ارتكابها عن الجرائم التقليدية.

---

[8] _ المرجع نفسه، ص141.

[9] _ فريدة ناشف، الطاهر ياكر، المواجهة الأمنية و الجزائية للجرائم الالكترونية، مجلة الحقيقة للعلوم الاجتماعية و الإنسانية، المجلد 21، العدد01، الجزائر، سنة 2022،ص64.

[10] _ جاسم محمد جندل، الجرائم الالكترونية، الطبعة الأولى، دار المعتز للنشر و التوزيع، عمان، الأردن، سنة 2022، ص37.

[11] _ القانون رقم 04-15 مؤرخ في 01 نوفمبر 2004، يعدل و يتمم الأمر رقم 66-156، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، جريدة رسمية، عدد71، مؤرخة في 10 نوفمبر2004.

[12] _ عبد الله ذيب محمود، أسامة إسماعيل دراج، المرجع السابق،ص26.

2 جرائم ترتكب في بيئة رقمية:

من المعروف أن مثل هاته الجرائم ترتكب في بيئة رقمية أو الكترونية، الأمر الذي يتطلب أن يتوافر لدى الجاني إلمام ومعرفة فنية بتقنيات الحاسوب ونظم المعلومات والتي تمكنه من ارتكابها، إضافة إلى توافر الأدوات اللازمة لديه كالحواسيب ومختلف أجهزة الاتصال الحديثة وشبكات الإنترنت وبعض المهارات الأخرى اللازمة لارتكاب هذا النوع من الجرائم[13].

3 جرائم عابرة للحدود الوطنية وعالمية:

بمعنى أنها تتعدى الحدود الجغرافية للدول، فانتشار شبكة الاتصالات العالمية والإنترنت أمكن من ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة، وأضحى من السهل ارتكاب الجرائم عن بعد دون اعتراف بالحدود الجغرافية للدول، إذ يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر[14].

4 جرائم ناعمة:

بحيث يمكن أن يقوم بالجريمة الالكترونية طفل أو فتاة أو رجل كبير بالسن، فهي لا تحتاج إلى قوة بدنية أو عنف بقدر ما تحتاج إلى قوة ذهنية و استخدام البرمجيات الرقمية و التحكم فيها، حيث ترتكب عن بعد بواسطة الوسائل الالكترونية المختلفة، و بالتالي يكون مسرح الجريمة هو الفضاء الالكتروني[15].

5 جرائم سهلة الارتكاب وصعبة الإثبات:

إذ إن ما يميز هذا النوع من الجرائم أنها جرائم سريعة التنفيذ لا تحتاج إلى وقت أو جهد وغالبا ما تتم بكبسة معينة في جهاز الحاسوب ممّا يجعلها مغرية للجناة لسهولة تحقيق المنافع والمكاسب المادية دون أدنى مجهود جسدي و غياب الرقابة الأمنية و لذلك يطلق عليها الفقه مصطلح " جرائم ذوي الياقات البيضاء"[16].

كما يصعب إثبات الجريمة الالكترونية بحيث يصعب تتبعها و اكتشافها، فهي لا تترك أثرا يقتفى، و إنما مجرد أرقام و معظم الجرائم الالكترونية تم اكتشافها بالصدفة و بعد وقت طويل من ارتكابها، و هذا يجعلها أيضا تفتقر للدليل المادي[17].

الفرع الثاني: دوافع ارتكاب الجريمة الالكترونية وأهدافها

ترتبط الجرائم الالكترونية بدوافع أو أسباب يسعى المجرم الالكتروني لتحقيقها من وراء اقترافه لمثل هذا النوع من الجرائم، كما أن التطور التكنولوجي ساهم بشكل أساسي ومباشر في استفحال الجرائم الالكترونية، وعليه نتناول **أولا** أسباب ارتكاب الجريمة الالكترونية، ثم نتطرق لأهداف الجريمة الالكترونية **ثانيا**.

أولا: أسباب ارتكاب الجريمة الإلكترونية

---

[13] محمد الشبلي العتوم، المرجع السابق، ص26.

[14] لامية طالة، كهينة سلام، الجريمة الالكترونية، بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد06، العدد02، الجزائر، سنة 2020، ص 75.

[15] عبد الله ذيب محمود، أسامة إسماعيل دراج، المرجع السابق، ص28.

[16] محمد الشبلي العتوم، المرجع السابق، ص27.

[17] نعيمة دوادي، الجريمة الالكترونية، خصائصها و مجالات استخدامها و أهم سبل مكافحتها، مجلة مهد اللغات، المجلد 2، العدد 1، الجزائر، سنة 2020،ص 49.

توجد العديد من الأسباب المؤدية إلى ارتكاب الجريمة الإلكترونية حسب نوعها و صفة المجني عليه فيها ، و يمكن تقسيم أسبابها إلى أسباب تتعلق بالمجرم الالكتروني في حد ذاته، و منها ما يرتبط بالتطور التكنولوجي.

1 -الأسباب المتعلقة بالمجرم الالكتروني:

يسعى المجرم الالكتروني إلى تحقيق دوافع مادية أو انتقامية أو السعي لإثبات الذات.

أ -دوافع مادية:

أي السعي للحصول على الأموال وتحقيق الثراء، فالكثير من الجرائم الالكترونية يكون الدافع من ورائها تحقيق الكسب المادي وهو دافع تشترك فيه الجريمة الالكترونية مع بعض أصناف نظريتها الجريمة التقليدية [18]، و يندرج ضمن هذا الدافع البطالة التي تكثر بين فئة الشباب المكتسبين للمعرفة و الحاصلين على مستوى تعليمي عال، إذ أن الانعكاسات السلبية للبطالة توجههم لتوظيف معارفهم التقنية و الفنية في نشاطات إجرامية الكترونية، كالنصب و الاحتيال الالكتروني و اختراق بطاقات الائتمان و غيرها من أصناف الجرائم الالكترونية.

ب -دوافع انتقامية:

و هذه الدوافع قد تستهدف أشخاصا طبيعيين أو معنويين، فقد يعبث المجرم الالكتروني بالنظام المعلوماتي للجهة المستهدفة و ذلك انتقاما منها على تصرف ما بدر منها، و كذلك الحالة التي يقوم فيها رب العمل باتخاذ إجراءات عقابية ضد الموظف أو أن يقوم بتسريحة من العمل، كما قد يكون الانتقام كرد فعل على تعرضه لتصرف مهين من شخص ما[19].

ت -السعي لإثبات الذات:

تكثر هذه الدوافع لدى الشباب المراهق، حيث يسعى البعض من الشباب لإثبات ذاته و البحث عن التقدير في محيطه و مجتمعه و لفت الانتباه، و من ثم يجد غايته في ذلك من خلال ارتكاب جرائم الكترونية كالابتزاز الالكتروني، و تطوير مهاراته في التقنيات و البرمجيات و يتطور به الأمر لاختراق منظومات معلوماتية لوسائط اجتماعية و حسابات افتراضية لأشخاص من معارفه أو وسطه الاجتماعي.

2 -الأسباب المتعلقة بالتطور التكنولوجي:

تعد التغيرات والتطورات التي عرفها العالم في شتى الميادين، لاسيما التحول إلى العالم الرقمي والانفجار المعلوماتي الهائل والانفتاح الاقتصادي في عصر العولمة، من أهم الدوافع التي أدت إلى استفحال الجرائم الالكتروني بشتى صورها، ويمكن إجمال هذه الأسباب فيما يلي:

أ -التحول للمجتمع الرقمي:

التغيرات الكمية في مقدار المعلومات المتدفقة و نوعيها بفعل تكنولوجيا الاتصالات و المواصلات ساهم بشكل مباشرة في عملية التحول إلى المجتمع الرقمي، حيث أضحى تداول و تبادل المعلومات و الصور عبر البريد الالكتروني أو مختلف وسائط التواصل الاجتماعي متاح للجميع، و ظهر ما يسمى بالعلاقات

[18] _ بن يحي إسماعيل، التحقيق الجنائي في الجرائم الالكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، جامعة أبي بكر بلقايد تلمسان، كلية الحقوق، الجزائر، سنة 2021/2020، ص33.

[19] _ المرجع نفسه، ص33.

الاجتماعية الافتراضية[20]، و هذا التحول الرقمي صاحبه ظهور أنماط جديدة من الأفعال الإجرامية ترتكب الكترونيا و بسهولة و دون عناء، فمستخدمي الشبكات الالكترونية يقضون أوقاتا زمنية متفاوتة في الفضاء الالكتروني و هذا في حد ذاته يمكنهم من اكتساب المعارف التقنية و الفنية لهذا العالم الرقمي.

ب العولمة:

إن التدفقات المعرفية التي يشهدها العالم بفضل العولمة، ساهمت في دفع التطور التكنولوجي والتأثير الإيجابي على اقتصادات السوق والتحرر الاقتصادي من جهة، ومن جهة ثانية ساهمت في استفحال أصناف جديدة من الجرائم بفعل الترابط الكوني الذي حققته العولمة في فضاء الإنترنت، فالتحرر الاقتصادي على سبيل المثال لا الحصر صاحبه جرائم واقعة على التجارة الإلكترونية ونظم المعلومات.

ت التنفيذ عن بعد:

لا تتطلب الجرائم الالكترونية في تنفيذ أفعالها المادية تواجد الفاعل في مسرح الجريمة باعتبار هذا الأخير افتراضي، و إنما بإمكان الفاعل ارتكاب الجريمة و هو في مكان بعيد عن محل الجريمة، و ذلك بمجرد الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب [21]، و يعد هذا الدافع من أهم أسباب ارتكاب و استفحال الجرائم الالكترونية نظرا للسهولة و المرونة التي تتسم بها هذه الجرائم من حيث التنفيذ و تجنب المخاطرة بالتواجد في مكان الجريمة.

ثانيا: أهداف الجريمة الإلكترونية

إن أي جريمة ترتكب في العالم لابد من وجود باعث للقيام بها، فمن غير الممكن أن يقدم شخص على سلوك إجرامي معين إلا وكان يهدف من وراءه لتحقيق غاية ما، وعليه تتمثل أهداف الجريمة الالكترونية أساسا في الأهداف التالية:

_ التمكن من الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يخدم مصالح المجرم أو مصالح الأشخاص الذين يعمل معهم.

_ التمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها.

_ الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات و البنوك و الجهات الحكومية و الأفراد و ابتزازهم بواسطتها.

_ الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات الاختراق و هدم المواقع على الشبكة العنكبوتية و تزوير بطاقات الائتمان و سرقة الحسابات المصرفية[22].

---

[20] _ جاسم محمد جندل، المراجع السابق، ص139.

[21] _ إسمهان بن مالك، خصائص الجريمة المعلوماتية و أسباب ارتكابها، مجلة البيبان للدراسات القانونية و السياسية، المجلد 4، العدد 1، الجزائر، سنة 2019، ص119.

[22] _ إسراء جبريل رشاد مرعي، الجرائم الالكترونية " الأهداف-الأسباب – طرق الجريمة و معالجتها"، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018، ص428.

_ تحقيق مصالح سياسية تتمثل في إسقاط الأنظمة السياسية وابتزاز الشخصيات السياسية و العامة في المجتمع عن طريق تجنيد أشخاص تعمل على التجسس و التصيد الالكتروني و تجنيد الأشخاص في إطار الإرهاب الالكتروني الماس بأمن الدولة و استقرارها.

المطلب الثاني: تصنيفات الجرائم الالكترونية

باعتبار الجرائم الالكترونية جرائم مستحدثة فهي تتطور و تتغير بوتيرة متسارعة بفعل ما تشهده التكنولوجيا من تغيرات في شتى الميادين ، و من ثم قد تظهر أصناف جديدة من الجرائم بظهور وسائل تكنولوجية جديدة تستخدم كأداة في ارتكابها، و هو الأمر الذي يصعب من عملية تصنيف الجرائم الالكترونية في نسق متكامل و منظم، ناهيك عن أن الجرائم الالكترونية تختلف من مجتمع لأخره من حيث تطوره، و عليه نتناول في هذا المطلب الجرائم الالكترونية الماسة بأمن الدولة و أنظمتها المعلوماتية في **الفرع الأول**، ثم نتطرق للجرائم الماسة بالأشخاص و الأموال في **الفرع الثاني**.

الفرع الأول: الجرائم الالكترونية الماسة بأمن الدولة وأنظمتها المعلوماتية

تعتبر طائفة الجرائم الماسة بأمن الدولة من أكثر الجرائم استفحالا في البيئة الرقمية، سواء كان مساسا بأمن الدولة الداخلي أو الخارجي، وأضحت هذه الجرائم التي ترتكب من طرف أفراد أو كيانات تشكل خطرا حقيقيا على أمن الدولة واستقرارها، وعليه نتناول في هذا الفرع الجرائم الماسة بأمن الدولة الداخلي في البيئة الافتراضية **أولا**، ثم نتطرق للجرائم الماسة بأمن الدولة الخارجي في الفضاء الرقمي **ثانيا**.

أولا: الجرائم الماسة بأمن الدولة الخارجي في الفضاء الرقمي

تكون الجرائم ماسة بأمن الدولة الداخلي عندما ترتكب ضد الدولة بصفتها شخصا من أشخاص القانون العام الداخلي، وتستهدف إلحاق الضرر بها بصفتها سلطة عليا، أو تستهدف السيطرة عليها، وتغيير أحكام الدستور أو تعديلها بصفتها غير شرعية، أو إثارة العصيان المسلح ضد السلطات القائمة و منعها من ممارسة وظائفها، أو غصب أو الشروع في غصب سلطة سياسية أو مدنية أو قيادة عسكرية[23].

و نتيجة للتطور التكنولوجي الذي عرفه العالم و ظهور وسائل التكنولوجيا و الاتصال الحديثة أصبحت هذه الجرائم ترتكب في الفضاء الالكتروني بوسائل الكترونية عن طريق اختراق المنظومات المعلوماتية و القرصنة و التجسس الالكتروني و إثارة الفتن و تغليط الرأي العام عبر الشبكات الاجتماعية و غيرها من الصور التي تعد من صميم الجرائم الإلكترونية الماسة بأمن الدولة الداخلي و التي سنتناول تطبيقات منها تباعا.

1 جرائم التجسس الالكتروني:

يعتمد هذا النوع من الجرائم على تقنيات عالية التقدم حيث لم يعد يقتصر التجسس على ما يتعلق بالمعلومات العسكرية أو السياسية بل تعداه إلى المجال الاقتصادي والتجاري والثقافي، ومن الأساليب المعتمدة أسلوب إخفاء المعلومات داخل المعلومات بحيث يتم إخفاء تلك المعلومات المهمة والمستهدفة داخل معلومات

[23] _ هروال هبة نبيلة، جرائم الأنترنت، أطروحة دكتوراه، جامعة أبي بكر بلقايد تلمسان، كلية الحقوق و العلوم السياسية، الجزائر، سنة 2013-2014، ص311.

عادية في جهاز الحاسب الآلي، و من ثم يتم تهريبها باستعمال أساليب متطورة لا يتم اكتشافها، و أبرز مثال لهذه الجريمة ما قامت به الشبكة الدولية الضخمة للتجسس الالكتروني التابعة لوكالة الأمن القومية الأمريكية بالتعاون مع أجهزة استخبارات كندية و بريطانية لرصد المكالمات الهاتفية بهدف التعامل مع الأهداف غير العسكرية[24].

2 -جرائم الإرهاب الالكتروني:

هي اختراقات للأنظمة الأمنية الحيوية على مواقع الإنترنت تكون جزءا من مجهود منظم لمجموعة من الإرهابيين الالكترونيين أو وكالات مخابرات دولية أو أي جماعات تسعى للاستفادة من ثغرات هذه المواقع والأنظمة والوصول للمواقع المشفرة والمحجوبة[25].

ويندرج ضمن الأفعال المادية لجرائم الإرهاب الالكتروني استغلال الفضاء الالكتروني كوسيلة للتدريب والتجنيد الالكتروني، بما في ذلك نشر إرشادات التدريب و التخطيط و التنفيذ.

3 -الجريمة المنظمة:

غني عن البيان أن أعضاء الجريمة المنظمة يستفيدون من التطور التكنولوجي في مجال المعلومات الإلكترونية، وذلك من خلال استغلال الإمكانات المتاحة الكترونيا في التخطيط والتوجيه وتنفيذ المخططات الإجرامية بسهولة، مخترقة بذلك حدود الدول بأقل تكلفة ممكنة ودون مخاطرة[26].

ثانيا: الجرائم الماسة بأمن الدولة الداخلي في البيئة الافتراضية

تستهدف هذه الطائفة من الجرائم أمن الدولة الداخلي وزعزعة استقرارهاو إحداث شرخ كبير داخل المجتمع و وحدته، و من شأنها الإضرار بمصالح محمية قانونا، و قد اتخذت هذه الجرائم مؤخرا البيئة الرقمية مرتعا لها، و تعد جرائم إثارة الفتنة و التمييز و نشر خطاب الكراهية من أبرز صور الجرائم الماسة بأمن الدولة الداخلي الواقعة في البيئة الإلكترونية ، ذلك أن المصالح المحمية في هذه الصورة من الجرائم تمثل مصالح عليا للدولة، و هي من الركائز الأساسية لأمن الدولة الداخلي و السلم الاجتماعي، و قد أضحت البيئة الالكترونية بؤرة لاستفحال و انتشار هذا النوع من الجرائم، التي تستهدف العرق و الجنس و المذهب و الإيديولوجيا، محدثة بذلك تمزقات في المجتمع و أفراده، حيث يعد السلم الاجتماعي صمام أمان للوحدة الوطنية و الاستقرار [27]، و هو ما دفع العديد من التشريعات لتجريم أفعالها المادية و تصنيفها ضمن الجرائم الالكترونية الماسة بالمصلحة العامة و أمن الدولة الداخلي.

الفرع الثاني: الجرائم الماسة بالأشخاص والأموال

يتسع نطاق الجريمة الالكترونية ليشمل جميع مناحي حياة المجتمع وأفراده، بداية من التدخل في حياته الخاصة وصولا لأمنه، فنطاق الجريمة الالكترونية تمس أمن الدولة وسلامتها، وتطال أبضا حياة الأشخاص

[24] ـ ليندة شرابشة، السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات و أبحاث، المجلد01، العدد01، سنة 2009، ص242.

[25] ـ جاسم محمد جندل، المرجع السابق، ص121.

[26] ـ نعيمة دوادي، المرجع السابق، ص51.

[27] ـ سيف مجيد العاني، مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل الاجتماعي، دراسة مقارنة، دروب المعرفة للنشر و التوزيع، الإسكندرية، مصر، سنة 2022،ص94.

الخاصة وأموال الأفراد والمؤسسات[28]، وهو ما سنعالجه بالدراسة في هذا الفرع، حيث نتطرق للجرائم الالكترونية الواقعة على الأشخاص **أولا**، ثم نعرج للجرائم الواقعة على الأموال **ثانيا**.

أولا: الجرائم الالكترونية الواقعة على الأشخاص

الجرائم الواقعة على الأشخاص أو الجرائم ضد النفس _بوجه عام_ هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع الشخصي البحت [29]، ومع تطور شبكة الإنترنت وبروز وسائل الاتصال والتكنولوجيا الحديثة أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما جعلها عرضة للانتهاك والاستعمال من طرف المجرمين الالكترونيين وجعلت سمعة وشرف الأفراد مستباحة [30]، ومن أبرز صورها الابتزاز الالكتروني وانتحال الشخصية و و القذف و التشهير بالأشخاص.

1 -الابتزاز الالكتروني:

تبرز جريمة الابتزاز الالكتروني كإحدى الجرائم الالكترونية المستحدثة التي ظهرت مؤخرا، و التي أثرت على المجتمع بشكل كبير، إذ تعد نتاج الاستخدام السلبي لثورة التكنولوجيا و التي لحقت بالعالم مطلع القرن العشرين، و من الآثار غير المرغوبة لهذا التطور، تمكين المجرم الالكتروني من إنشاء صفحات و حسابات شخصية بأسماء وهمية و يختبئ خلف الشاشة و يمارس عملا إجراميا ينتهك به مصلحة يحميها القانون، باعتماد أسلوب الابتزاز الالكتروني كوسيلة للضغط و الإكراه[31] عن طريق التهديد و الوعيد بنشر معلومات و صور أو مقاطع مرئية للمجني عليه على قدر من الخصوصية لا يرغب هذا الأخير في إظهارها، مقابل تحقيق منفعة شخصية يطلبها الجاني قد تكون مادية أو جنسية أو غيرها.

2 -انتحال الشخصية:

يتم ذلك من خلال استخدام المجرم الالكتروني لشخصية الضحية أو المجني عليه بغرض الاستفادة من سمعته أو سلطته أو ماله أو غيره من الأسباب، ويكثر استخدام هذا النمط في الوسط التجاري، و تستهدف هذه الجريمة استدراج الضحايا بداية من تكوين صداقة عبر الشبكة العنكبوتية[32].

3 -التشهير بالأشخاص:

تتحقق هذه الصورة من صور السلوك الإجرامي الالكتروني، بقيام المجرم الالكتروني بتشويه سمعة الأشخاص عن طريق نشر جوانب من حياتهم الخاصة، أو بث أخبار غير صحيحة تستهدفهم، أو التعرض لأسرهم أو طبيعة عملهم، و تكثر هذه الجرائم على وسائل التواصل الاجتماعي كنوع من الانتقام من المجني عليه[33].

4 -القذف والسب:

يعد حق الإنسان في شرفه و اعتباره من الحقوق اللصيقة بالشخصية القانونية و المتفرعة عنها أيا كانت المكانة الاجتماعية التي يحتلها في المجتمع، و نظرا لإساءة استخدام التكنولوجيا عموما و وسائل التواصل

[28] نعيمة دوادي، المرجع السابق،ص49.
[29] حسين عبد الكريم يونس، خليل يوسف الجندي، المرجع السابق، ص36.
[30] جاسم محمد جندل، المرجع السابق،ص124.
[31] سيف مجيد العاني، المرجع السابق،ص111.
[32] نعيمة دوادي، المرجع السابق،ص49.
[33] سيف مجيد العاني، المرجع السابق،ص116.

الاجتماعي بالأخص استفحلت سلوكيات مادية تضم ألفاظ السب التي تخدش شرف و اعتبار الغير باستعمال الميزات التي أتاحتها الإنترنت من خدمات للتعبير عن الرأي كالنشر و التعليق و إعادة المشاركة للمحتوى و غيرها [34]، و تعاني معظم المجتمعات المتقدمة منها و النامية من هذه الظاهرة الإجرامية التي تستهدف الأشخاص طبيعيين كانوا أو معنويين.

ثانيا: الجرائم الالكترونية الواقعة على الأموال

من المعلوم أنه باتت الكثير من المعاملات المالية في وقتنا الحاضر تتم بواسطة الشبكات الالكترونية، مما زاد من تطور وسائل الدفع الالكتروني، مما أدى إلى تطور الجريمة الالكترونية بغاية الحصول على الأموال بأقل تكلفة ممكنة [35]، من أبرز صور الجرائم الالكترونية التي تطال الأموال جريمة الاحتيال الالكتروني وغسيل الأموال الالكتروني والسطو على أرقام بطاقات الائتمان والتحويل الالكتروني غير المشروع.

1 الاحتيال الالكتروني:

الاحتيال الالكتروني هو أي سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي، أي التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، وكل ذلك من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير[36].

2 السطو على بطاقات الائتمان:

يعتبر السطو على بطاقات الائتمان نمط إجرامي تقني مستحدث يتم من خلال الاستيلاء غير المشروع على الأرقام والمعلومات الخاصة بالبطاقات الائتمانية المملوكة للغير من خلال الاعتماد على تقنية شبكة الإنترنت بهدف الحصول على أثمن السلع والخدمات من المواقع التجارية المنتشرة عبر الشبكة العنكبوتية والتي يقبل عليها الوفاء بالبطاقات الممغنطة، بحيث يتم خصم قيمة السلع من العملاء الشرعيين لهذه البطاقات، ويتم ذلك السطو إما عن طريق سرقتها والاستيلاء عليها أو عن طريق النصب و الاحتيال[37].

3 غسيل الأموال الالكتروني:

في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات الالكترونية و ما انجر عنه من تطور في وسائل الدفع و التحويلات المصرفية و في خضم التداول المالي عبر الإنترنت أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم، حيث يحتاج أصحاب الأموال الضخمة الغير شرعية إلى غسلها قبل إنفاقها أو استثمارها، و وجدوا سبيلا في ذلك من خلال الغسيل الالكتروني كصورة مستحدثة لغسيل الأموال في صورته التقليدية المعروفة، و يتم ذلك عن طريق مراسلات بين البنوك و المصارف تسمى بالتحويلات المصرفية و التي يصعب مراقبتها نتيجة لعددها الكبير[38].

---

[34] المرجع نفسه،ص118.

[35] نعيمة دوادي، المرجع السابق،ص50.

[36] بولحية شهيرة، سويح دنيا زاد، الاحتيال الالكتروني، مجلة الدراسات القانونية و الاقتصادية، المركز الجامعي سي الحواس-بريكة، العدد 04، الجزائر، ديسمبر، سنة2019،ص39.

[37] هروال هبة نبيلة، المرجع السابق، ص287.

[38] جاسم محمد جندل، المرجع السابق، ص117 و ما بعدها.

خاتمة:

في ختام هذه الدراسة يمكن القولأنالجريمة الالكترونية تعتبر من جرائم العصر التي شغلت اهتمام الباحثين باختلاف تخصصاتهم العلمية، و هو ما أدى إلى التباين من منظور المفاهيم المرتبطة بها، و اختلافها من حيث طبيعتها و خصائصها عن الجرائم التقليدية، و إلى جانب كونها جرائم ناعمة و متطورة و لا تعرف حدودا جغرافية فهي كذلك سهلة الارتكاب و صعبة الإثبات نظرا للبيئة الافتراضية التي تنشأ فيها و شخصية مرتكبيها المبنية على الذكاء و الدقة في التعامل مع مكونات الحاسب الآلي و مختلف وسائل الاتصال و التكنولوجيا الحديثة، حيث يهدف مرتكبيها لتحقيق غايات مادية و انتقامية و إثبات ذواتهم، و من الدوافع التي ساعدتهم في ارتكاب مثل هاته الأفعال المادية الميزات و التسهيلات التي يوفرها الفضاء الرقمي من أدوات و سهولة إيجاد الضحايا، ناهيك عن أن التنفيذ عن بعد لهذه الجرائم يعد دافعا قويا لارتكابها على اعتبار تجنب التواجد في مسرح الجريمة الواقعي و تجنب عنصر المخاطرة.

ونظرا للتطور المتسارع التي تشهده الجرائم الالكترونية فإن ذلك جعل المنظمات الدولية والإقليمية و التشريعات القانونية تأخذ بتصنيفات عديدة لها حسب الوسيلة المستعملة في ارتكابها و صفة المجني عليه فيها، فعندما تمس الجرائم الالكترونية بالمصلحة العامة للمجتمع تكون بذلك جرائم ماسة بأمن الدولة، كما تجد تطبيقاتها عند مساسها بمصالح أساسية محمية قانونا، سواء كان مساسا بالأشخاص أو الأموال.

وبناء على ما تقدم، خلصت دراستنا إلى جملة من النتائج تعد بمثابة حجر الأساس للتوصيات القابلة للنظر والتجسيد:

1 النتائج:

_ الجريمة الالكترونية من أخطر الظواهر الإجرامية التي تهدد أمن المجتمع و أفراده، و هي تمثل أي سلوك إجرامي يرتكب عبر شبكة الاتصال الدولي " الإنترنت" باستخدام الحاسب الآلي أو وسائل التكنولوجيا و الاتصال الحديثة في ذلك.

_ الجرائم الالكترونية جرائم مستحدثة و ناعمة لا يقتصر ارتكابها على فئة معينة من المجرمين، و هي جرائم لا تعرف حدودا جغرافية و ترتكب في بيئة افتراضية تحاكي البيئة الواقعية مما يصعب من عملية اكتشافها.

_ يعد الانفتاح الاقتصادي في إطار عصر العولمة و التحول إلى العالم الرقمي من أهم الأسباب والدوافع المؤدية الى ارتكاب الجرائم الالكترونية من طرف المجرمين الالكترونيين الذين يسعون بدورهم لتحقيق دوافع مادية و انتقامية و البحث عن الثراء و إثبات الذات.

_ الجرائم الالكترونية تتطور تبعا للتطورات و التغيرات التي يشهدها العالم، و هي بذلك تتنوع و تتعدد إلى عدة أصناف جرمية، منها ما يمس بالمصلحة العامة و السلم الاجتماعي و أمن الدولة سواء الداخلي أو الخارجي، ومنها ما يمس باعتبار الأشخاص ومصالحهم، وإلى جانب ذلك تطال الجرائم الالكترونية المعاملات المالية فيما يعرف بالجرائم الالكترونية الواقعة على الأموال.

2 التوصيات:

_ ضرورة تعزيز الجهود الدولية و الإقليمية و المحلية للإحاطة بمختلف جوانب الجريمة الالكترونية مواكبة للتطورات التي يشهدها عالم الجريمة، من بروز أنماط جديدة من الإجرام المستحدث خاصة الواقعة عبر وسائل التواصل الاجتماعي كجرائم البث المباشر و التشجيع على الفسق و إثارة الغرائز الجنسية عبر التطبيقات الهاتفية.

_ التكثيف من إنشاء المراكز المتخصصة للدراسات و الأبحاث تعنى بدراسة الظواهر الإجرامية المستحدثة و تبحث في أسباب ارتكابها و اقتراح الاستراتيجية الكفيلة لاحتوائها و التصدي لها.

_ إشراك المجتمع المدني و المؤسسات التربوية و الجامعية و الأفراد في السياسة الوقائية من الجرائم الالكترونية، عن طريق التوعية و التحسيس بخطورتها و إضرارها بمصالح المجتمع و أفراده، و نشر ثقافة التبليغ عن هذه الجرائم الخطيرة.

_ استحداث مرصد وطني لمراقبة و ضبط السلوكيات الواقعة في البيئة الرقمية و الافتراضية، لاسيما تلك التي ترتكب عبر الشبكات الالكترونية و وسائل التواصل الاجتماعي و تطبيقات الهواتف الذكية، و منح هذا المرصد صلاحيات الحظر و الحد من ولوج بعض التطبيقات أو الشبكات الالكترونية في حالة ارتكاب إحدى أصناف الجرائم الالكترونية.

_ إدراج محتوى علمي مضمونه الأمن الالكتروني أو المعلوماتي ضمن المقررات التعليمية لمختلف الأطوار بما فيها مؤسسات التعليم العالي، نظرا للأسس التي يحتويها الأمن الالكتروني في حماية الخصوصية.

قائمة المصادر و المراجع:

1 القوانين:

- القانون رقم 04-15 مؤرخ في 01 نوفمبر 2004، يعدل و يتمم الأمر رقم 66-156، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، جريدة رسمية، عدد71، مؤرخة في 10 نوفمبر2004.

2 الكتب:

1 حسين عبد الكريم يونس، خليل يوسف الجندي، الابتزاز الالكتروني و الجرائم الالكترونية المفهوم و الأسباب، الطبعة الأولى، دار كفاءة المعرفة، عمان، الأردن ، سنة 2021.

2 _ سعيد بوعلي، شرح قانون العقوبات الجزائري القسم العام، دار بلقيس للنشر، الجزائر، سنة 2017.

3 –محمد الشبلي العتوم، جرائم تكنولوجيا المعلومات، النظرية العامة للجرائم الالكترونية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، الأردن، سنة 2021.

4 –عبد الله ذيب محمود، أسامة إسماعيل دراج، الوجيز في الجرائم الالكترونية القواعد الموضوعية و الإجرائية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، الأردن، سنة 2022.

5 جاسم محمد جندل، الجرائم الالكترونية، الطبعة 1، دار المعتز للنشر والتوزيع، عمان،الأردن، 2022.

6 سيف مجيد العاني، مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل الاجتماعي، دراسة مقارنة، دروب المعرفة للنشر و التوزيع، الإسكندرية، مصر، سنة 2022.

3 -أطروحات الدكتوراه:

1 -بن يحي إسماعيل، التحقيق الجنائي في الجرائم الالكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، جامعة أبي بكر بلقايد تلمسان، كلية الحقوق، الجزائر، سنة 2021/2020.

2 -هروال هبة نبيلة، جرائم الأنترنت، أطروحة دكتوراه، جامعة أبي بكر بلقايد تلمسان، كلية الحقوق و العلوم السياسية، الجزائر، سنة 2013-2014.

3 -المقالات العلمية:

1 -صراع كريمة، دقيش جمال، الأبعاد الاقتصادية للجريمة الإلكترونية، مجلة الدراسات التسويقية و إدارة الأعمال، المجلد2، العدد1، الجزائر، جانفي2018.

2 -دمان ذبيح عماد، بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، العدد13، الجزائر، جانفي 2020.

3 -فريدة ناشف، الطاهر ياكر، المواجهة الأمنية والجزائية للجرائم الالكترونية، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، المجلد21، العدد01، الجزائر، سنة 2022.

4 -لامية طالة، كهينة سلام، الجريمة الالكترونية، بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد06، العدد02، الجزائر، سنة 2020.

5 -نعيمة دوادي، الجريمة الالكترونية، خصائصها و مجالات استخدامها و أهم سبل مكافحتها، مجلة مهد اللغات، المجلد 2، العدد 1، الجزائر، سنة 2020.

6 -إسمهان بن مالك، خصائص الجريمة المعلوماتية و أسباب ارتكابها، مجلة البيبان للدراسات القانونية و السياسية، المجلد4، العدد1، الجزائر، سنة 2019.

7 -إسراء جبريل رشاد مرعي، الجرائم الالكترونية " الأهداف-الأسباب – طرق الجريمة و معالجتها"، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018.

8 -ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات و أبحاث، المجلد01، العدد01، سنة 2009.

9 -بولحية شهيرة، سويح دنيا زاد، الاحتيال الالكتروني، مجلة الدراسات القانونية و الاقتصادية، المركز الجامعي سي الحواس-بريكة، العدد 04، الجزائر، ديسمبر، سنة2019.

قدور بن عطية صورية
souriakaddour@gmail.com
جامعة أبو بكر بلقايد تلمسان

الجريمة الإلكترونية
Cyber crime

الملخص

تعتبر الجريمة الإلكترونية من إفرازات الثورة المعلوماتية فهي نتاج التطور التكنولوجي و الاستخدام الهائل لتـــقنيات وسائل الإعلام والاتصال، وقد أدى هذا الاستخدام إلى بروز نمط جديد من الجريمة يشترك مع الجريمة التـــــقليدية في أركانها و يخـــتلف عنها في البيئة الذي تقوم عليها الجريمة و الذي يكون عبر الفضاء الإلكتروني .

و اختلف العـــــلماء و الباحثين في تعريف الجريمة الالكترونية وشرح مفهومها و تسميتها و من ابرز مسمايتها " الجريمة الإلكترومعلوماتية " .

و الـــجزائر كسائر الدول الذي ازدادت الجريمة الالكترونية فيها بسبب الاستخدام الهائل للأنترنت حيت سجـلت مصالح الدرك و الشرطة قرابة 8 ألاف جريمة الإلكترونية خلال سنة 2020 و سجلت المديرية الـــــعامة للأمن الوطني ارتفاعا قياسيا أي من 500 جريمة سنة 2015 إلى 5200 جريمة خلال سنة 2020.

Abstract:

Cybercrime is one of the consequences of the information revolution, it is the product of technological development and the massive lack of media and communication technologies, and this intelligence has led to the emergence of a new pattern of crime that shares with traditional crime in its pillars and differs from the environment on which crime is based, which is through cyberspace. Scientists and researchers differed in defining cybercrime and explaining its concept and name, one of its most prominent names being "electroinformatic crime." Algeria, like all other countries where cybercrime has increased due to the massive internet takeover, has recorded nearly 8,000 cybercrimes by the gendarmerie and police in 2020, and the Directorate General of National Security recorded a record high of 500 crimes in 2015 to 5,200 in 2020.

مقدمة

رغم الإيجابيات التي أحدثتها الثورة التكنولوجية و دورها الفعال في تسريع وتيرة العمل في مختلف الإدارات و المؤسسات خاصـــة في الأونة الأخيرة مع أزمة جائحة كورونا "كوفيد 19 " و الإغلاق التام الذي فرضته هذه الازمة أدى إلى ضرورة الإنتقال من إلى الإدارة الإلكترونية لـــضمان استمرارية العمل و الحياة

العادية و قد أدت أيضا لظهور هاجس الجريمة الإلكترونية الذي اصبح يرعب العديد من الأفراد نظرا لخطورتها حيث انها ترتكب في هدوء تام دون بذل أي جهد عضلي كما انها لا تقتصر على منطقة أو دولة معينة و إنما هي مشكلة عالمية و دولية .

و تـكمن خطورة الدرائم الإلكترونية في ان العالم اصبح يعتمد على الفضاء الإلكتروني بكثرة لاسيما في البنى التحتية المعلوماتية المصرفية و الحكومية و العسكرية و أيـــــضا المؤسسات و الشركات العامة و الخاصة .

ووفقا لإحصاءات الانترنت فقد إجتازت الشبكة العنكبوتية 1.83 مليار موقع إلكتروني حول العالم لعام 2021 و تستقطب حوالي 4.803.660.196 مستخذم .

<u>أسباب إختيار الموضوع :</u>

* غموض الجريمة الإلكترونية و حداثتها .
* الإستعمال الهائل للحاسوب و الأنظمة المعلوماتية .
* سهولة إرتكاب الجريمة الإلكترونية .

<u>أهمية الموضوع :</u>

* ضرورة التصدي للجرائم الإلكترونية ووضح حدا لها .
* نقص كفاءة السلطات على التعامل مع الجرائم الإلكترونية .
* دور الأنظمة المعلوماتية في شتى المجالات .

و مما سبق تتبلور الإشكالية فيما يلي :

ماهية الجريمة الإلكترونية و ماهي أنواعها و أسبابها

و لتحـــــليل هذه الإشـــــكالية اتبعنا خطة مـــنهجية ثنائية الفصول، خصصنا المبحث الأول منها ماهية الجريمة الإلكـــــــــترونية متطرقين في ذلك إلى مفـــهومها في المطلب الأول مفهوم الجريمة الإلكترونية من خلال تعريفها و تسمياتها و كذا أنواعها و خصائصها في المطلب الثاني .

أما المبحث الثاني حيـــــت تناولنا فيه أسبابها و أهداف الجريمة الإلكترونية حيث تطرقنا إلى أسباب الجرائم الإلكترونية في المطلب الأول و أهداف الجريمة الالكترونية في المطلب الثاني .

<u>المبحث الأول: ماهية الجريمة الإلكترونية</u>

لقد أحاط بـتعريف الجريمة الإلكترونية الكثير من الغموض حيت تعددت الأراء حول مفهومها و لم يتفق على مـــفهوم موحدا و شاملا و بغياب تعريف موحدا لها نجد أنفسنا أمام مشكلة مواجهة هاته الجريمة و بتعذر علينا محاربتها و مكافحتها .

<u>المطلب الأول مفهوم الجريمة الإلكترونية :</u>

هي كل فعل غير مشروع صادر عن إرادة أثمة يقرر لها القانون عقوبة أو تدبير إحترازي .

ينقسم تعريف الجريمة الإلكترونية إلى عدة إتجاهات تقوم على أسس مختلفة نذكر منها :

<u>1*على أساس وسيلة إرتكاب الجريمة</u> :كل الجرائم المرتبطة بالحاسوب او إحدى الوسائل التقنية .

المفهوم :هي كـــــــل فعل غير مشروع مرتكب بواسطة الكمبيوتر أو انترنت أو أي وسيلة إلكترونية أو بالأحرى كل نشاط إجرامي تستخدم فيه تقنية الحاسب الالي بطريقة مباشرة أو غير مباشرة .

إنتقادته :تعرض هذا المفهوم لعدة إنتقادات أهمها إتسامه بالعمومية و الاتساع .

2* على أساس موضوع الجريمة : كل معالجة ألية للبيانات أي كل تعريف أو تـــعديل أو نقل أونسخ غير مشروع حيت عرفت كذلك أنها غش معلوماتي .

المفهوم : هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة و إساءة إستخذام المخرجات، إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية متل تعديل الكمبوتر .

إنتقادته : ما يميز الـــــجريمة الإلكترونية انها تتم في وسط إفتراضي و تمس بمعطيات الحاسوب الألي

3* على أساس توفر المعرفة بتقنية المعلومات : يرتكز هذا التعريف على معيار شخصي أي مدى معرفة الجاني بتقنية المعلومات و إتقانها .

المفهوم :جريمة يتطلب القيام بها ان يتوافر لدى فاعلها معرفة بتقنية الحاسوب .

إنتقادته :حـصر و ربط شخصــية الفاعل في تعريفها و هذا لا يكفي لأنه يمكن لأي شخص عادي حتى و لم يكن مؤهل بتقنيات الحاسب الألي إرتكاب جريمة الغش المعلوماتي أو السرقة المعلوماتية .

4* على أساس الجمع بين عدة معايير : هي الإعتماد على عدة معايير لتعريف الجريمة الإلكترونية .

المفهوم : هي الجريمة التي يستخذم فيها الحاسوب الألي كوسيلة أو أداة لإرتكابها او الجريمة التي يكون الحاسوب نفسه صحيتها .

إنتقادته : يعاب عليه أنه جمع بين عدة تعاريف لتعريف جرائم الانترنت إلا انه يعد الناجح و الراجح من الناحية العملية .

5* على أساس الإتساع و التضيق :

التعريف الواسع : هي كل فعل أو إمتناع عمدي ينشأ عن الإستخذام غير المشروع للتقنية المعلوماتية بهدف الإعتداء على الأموال أو الأشياء المعنوية .

التعريف الضيق : هي كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الألية كبير لازما لإرتكابه من ناحية و لملاحقته و تحقيقه من ناحية أخرى .

التعريف اللغوي للجريمة الإلكترونية :

مصطلح الـــجريمة الإلكترونية من شأنه ان يدخل في مفهومه جرائم الحاسوب و غيرها من الجرائم التي يسميها البعض بالجرائم المـعلوماتية و الغش المعلوماتي أو جرائم الإعتماد على معطيات الحاسب الألي و جرائم الانترنت .

تعريف المشرع الجزائري للجريمة الإلكترونية :

سوف نتطرق لتعـــــــريف الجريمة الإلكترونية في القانون الجزائري تعريفا فقهيا و أكديميا و قانونيا .

التعريف الفقهي : هي جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ، أو داخل نظام حاسوب و تتمثل من الناحية المبدئية جميع الجرائم التي يمكن إرتكابهافي بيئة إلكترونية .

التعريف الأكاديمي : كل فعل إجرامي متعمد يترتب عنه خسارة تلتحق بالضحية أو مكسب يحققه الجاني

التـــــــــعريف القانوني :حسب القانون 09-04 المتضمن القواعد الـــــخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها مسميا أياه : "المنظومة المعلوماتية "

هي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض او مرتبطة يقوم واحد منها أو أكثر معالجة الألية للمعطيات ، تنفيذا لبرنامج معين .

تعريف منظمة التعاون الاقتصادي و التنمية في أوروبا :كل فـــــعل أو إمتـــناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية

تعريف الفقيه الفرنسي ماس Mass:

بأنها : الإعتداءات القانونية التي يمكن ان ترتكب بواسطة المعلوماتية بغرض تحقيق الربح .

تعريف الخبير الأمريكي باركر parker :

هي كل فـــــعل إجرامي معتمد أيا كانت صلته بالمعلوماتية و ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل .

تعريف الفقيه Michel: مــن أنها ســـــوء إستخدام الحاسب أو جريمة الحاسب تشمل إستخذام الحاسب كأداة لإرتكاب الجريمة .

تعريف الفقيه تردمان :الجـــــريمة الإلكترونية هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بإستخذام الحاسب الألي .

تعريف الفقيه دول :كل فعل إجرامي يستخدم الحاسب الآلي لإتمامه .

تعريف الفقيه المصري :فهناك من يرى ان الجريمة المعلوماتية هي " كل فعل او إمتناع عمدي ، ينشأ عن الإستخذام غير المشروع لتقنية المعلوماتية و يهدف إلى الاعتداء على الأموالأو المعنوية ".

و فريق أخر يرى ان الجريمة المعلوماتية هي : " عمل أو إمتناع يأتيه اضرار بمكونات الحاسب و شبكات الاتصال الخاصة به ،التي يحميها قانون العقوبات و يفرض لها عقابا .

للجريمة الإلكترونية عدة مسميات نذكر منها :

* جرائم الحاسوب و الانترنت .
*جرائم التقنية العالية .
* الجريمة الإلكترونية .

* الجريمة السايبرية .
* جرائم أصحاب الياقات البيضاء .
* الجرائم الإلكترومعلوماتية .
* جرائم إساءة إستخذام تكنولوجيا المعلومات و الاتصال .

الفرق بين الجريمة التقليدية و الجريمة الإلكترونية :

الجريمة التقليدية	الجريمة الالكترونية
الإحتيال	الإحتيال على الشبكة ، الاحتيال بالمزاد الالكتروني .....إلخ
السطو	القرصنة على الانترنت ، الحرمان من الخدمة ، الفيروسات
جرائم الأطفال الجنسية	استمالة الأطفال على النت ،المواقع الإباحية .
غسيل الاموال	أنظمة الدفع على الشبكة
السرقة	جرائم الهوية و سرقة الملكية

المطلب الثاني : أنواع و خصائص الجريمة الإلكترونية

**** أنواع الجريمة الإلكترونية :*** للجريمة الإلكترونية عدة أنواع و هي كالتالي :

1/الجرائم الأنترنت الشخصية : هي جرائم تستهدف الأفراد و تقتضي الحصول بطريقة غير شرعية على هويتهم الإلكترونية "البريد الإلكتروني–حساباتهم الاجتماعية – كلمات السر الخاصة بهم ".
كما تدخل في هذه الجريمة عمليات : سرقة الصور الشخصية و الملفات المهمة من أجهزة الضحايا ".

2/ الجريمة الإلكترونية التي تستهدف الحكومات : و هي الهجمات التي يشنها القراصنة على المواقع الرسمية الحكومية و تدميرها و سرقة البيانات و المعلومات منها و في الغالب تكون هذه الجريمة ذات غاية سياسية .

3/ جريمةالإعتداء على البريد الإلكتروني :

* مجرد الدخول إلى موقع البريد الالكتروني و الاطلاع على رسائله بدون إذن من صاحبه ، يعد جريمة إنتهاك سرية المراسلات المكفولة بنصوص الدستور .

4/الجرائم السياسية الإلكترونية : تستهدف المواقع العسكرية و سرقة المعلومات المتعلقة بأمن الدولة .

5/جرائم السب و الشتم و القذف على الانترنت: تعد من أكثر الجرائم إنتشارا أصبحت الشغل الشاغل لكثير من الناس ،فهي و إن كان البعض يراها إبداء رأي خاصة في حال التعليق على منشور معين ، قد يراها الطرف الاخر ضرارا و إساءة و قذفا أو حتى تنمرا .

6/جرائم الفيروسات : وتعتبر من أكثر الوسائل إنتشارا و من هذه الفيروسات الضارة حصان طروادة .

7/الإرهاب الإلكتروني : هو دعم الجماعات المتطرفة أو المساهمة في نشر أفكارهم.

8/الجرائم الجنسية الإلكترونية : التسويق للمحتويات الإباحية .

9/ جرائم التجارة الإلكترونية : عمليات السطو و القرصنة على البيانات الشخصية عبر الانترنت

10/ جريمة التزوير الالكتروني : هو تغيير الحقيقة في المستندات المعالجة أليا و المستندات المعلوماتية و ذلك بغية إستعماله و ينحصر نشاطها الاجرامي في افعال الادخال و المحو و التعديل على المحررات و الوثائق الالكترونية .

2 خصائص الجريمة الإلكترونية :

1- الجريمة الإلكترونية جريمة عالمية الحدود : هي جريمة تتخطى الحدود الجغرافية للدول فهي تتجاوز الحدود الجغرافية بإعتبار تنفيذها يتم عبر الشبكة المعلوماتية .

2- الجريمة الإلكترونية سريعة التنفيد :تنفيذها لا يتطلب الوقت الكثير فبضغطة واحدة على لوحة المفاتيح يمكن ان تنتقل ملايين الدولارات من مكان إلى أخر فهي لا تتطلب الإعداد قبل التنفيذ .

3- الجريمة الإلكترونية صعوبة إثباتها : جريمة لا تترك أي اثار جانبية لما بعد إرتكابها لأنها تقع في بنية إلكترونية يتم فيها نقل المعلومات و تداولها بالنبضات الإلكترونية غير مرئية و صعوبة الإحتفاظ بها

4- مرتكبو الجريمة الإلكترونية ذو صفات خاصة : يتميز المجرم المعلوماتي عن غيره من المجرمين العاديين حسب باركر فيمايلي :

-مجرم متخصص و محترم في تنفيذ جريمته .

- مجرم ذكي يتمتع بالمهارة او معرفة بدرجة عالمية من الثقافة .

5/ قلة الإبلاغ عن وقوع الجريمة الإلكترونية : إمتناع الضحايا عن التبليغ السلطات المختصة خوفا على سمعتهم و مكانتهم و هذا ما يؤدي إلى عدم معاقبة المجرمون .

6/الجريمة الإلكترونية جريمة مستحدتة : تعتبر من الجرائم الحديتة الظهور و التي كان نتاج العولمة و ثورة المجتمع الإلكتروني .

7/ الجريمة الالكترونية جريمة ناعمة : تعتمد هذه الجرائم على المجهود الذهني المحكم و التفكير المدروس و المهارة العالية لتقنية الحاسب الألي .

8/ عدم كفاية التعاون الدولي في مجال الجرائم الإلكتروني :

عدم وجود معاهدات دولية كافية للتسليم او للمعاونة التنائية او الجماعية بين الدول تسمح بالتعاون الدولي .

*خصائص الجريمة الإلكترونية حسب **الباحثة إسراء جبريل رشاد مرعي** في كتابها الجرائم الإلكترونية :

1 تتسم بسهولة الوقوع في فخها بسبب غياب الرقابة الأمنية .

*2*الضرر الناجم عن الجرائم الالكترونية غير قابل للقياس إذا انها تلحق أضرار و جسيمة .

3 صعوبة الكشف عن مرتكبها إلا بأساليب أمنية و تقنية عالمية .

4 سلوك خارج عن المألوف و غير أخلاقي مجتمعيا .

5 ذات عنف و جهد أقل من الجرائم التقليدية .

أركان الجريمة الإلكترونية :و هي ثلاثة أركان

الركن الشرعي : هو الصفة غير المشروعة للفعل .

الركن المادي : هي ماديات الجريمة التي تبرز به إلى العالم الخارجي .

الركن المعنوي : الإدارة التي يقترن بها الفعل سواءا في صورة القصد او الخطأ .

المبحث الثاني : أسباب و اهداف الجريمة الالكترونية

المطلب الأول : أسباب و دوافع الجريمة الالكترونية

***1* أسباب و دوافع الجريمة :**

أولا :الدوافع الشخصية:يمـــيل المجرم المعلوماتي إلى إظهار تـــــــفوقه و مستوى برعاته اكثر من شهوة الحـــــصول على الربح حـــــيث لديه شغف الالة و يحاول كسر حواجز الامن لأنظمة الكمبيوتر و شبكات المعلومات و إظهار تفوقهم على الوسائل التكنولوجيا .

1 : حب التعلم : حب التعلم و الإستطلاع من الأسباب الرئيسية التي تدفع إلى إرتكاب الجريمة الإلكترونية .

2 : المنفعة المادية : محاولات الكسب السريع و جني الأرباح الطائلة دون تعب و لا رأس المال من أسباب التي تدفع الى إختراق أنظمة إلكترونية .

3 : التسلية و اللهو: يعتبر البعض من مخترقي الأنظمة هذه وسيلة للمرح و التسلية و تقضية اكبر وقت ممكن في أنظمة و حواسيب اخرين .

ثانيا : الدوافع الخارجية : يتأثر الانسان من بعض الموافق تجعله في حالة إستلام تام لكثيرين من المؤثرات و الدوافع الخارجية التي تدفعه إلى إرتكاب بعض الجرائم الالكترونية و ذلك نتيجة لوجوده في بيئة المعالجة الالية للمعلومات و مع توفر هذه المؤثرات فإن الامرحتما سوف يؤدي الى إرتكاب الجريمة الالكترونية .

ثالثا : دافع الانتقام و الحاق الضرر برب العمل :قد يكون الانتقام مؤثر في إرتكاب الجريمة الالكترونية ،قد يقوم مثلا العامل بدافع الانتقام من منشأة او رب العمل من إرتكاب جرائم الحاسوب .

1:دافع عقائدي :تتمتل في تلك القوى الداخلية المحركة لأشخاص حيت يبرر الكثير محاولاتهم لإختراق أجهزة الغير بحجة انهم على مذاهب او طوائف دينية معادية لمذاهبهم او بحجة تفكيرهم و فضح اسرارهم 2:دافع عنصري : من أجل تميز بين عرق و اخر او قبيلة و أخرى.

3: دافع سياسي و إيديولوجي : الدافع الذي يلعب فيه الإرهاب الدور الرئيسي من خلال لجوئه للأنترنت من أجل إستخذام المتفجرات .

أدوات الجريمة الإلكترونية :

* الإتصال بشبكة الانترنت : و تعتبر أداة رئيسية لتنفيذ الجريمة .

*توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخذم على جهاز الحاسوب .

*وسائل التجسيس و منها ربط الكاميرات بخطوط اتصال الهاتفي .

*الباركود و هي عبارة عن أدوات تستخدم لمسح الترميز الرقمي و فك الشفيرة الرموز .

*طابلات –هواتف رقمية و نقالة – برامج ضارة .

المطلب الثاني : اهداف الجريمة الإلكترونية

عندما نتحدث عن أهداف الجرائم الإلكترونية فنحن نتحدث عن مجموعة من الأهداف المختلفة نذكر أهمها :

*1*السعي للحصول على المعلومات السرية بطرق غير مشروعة لسرقتها او مجرد الاطلاع عليها و أحيانا حذفها .

*2*غزو أجهزة الخوادم التي توفر المعلومات التي تهم الهاكر من خلال شبكةالانترنت و التلاعب بها و تعطيلها.

*3*استقطاب معلومات غير مسموح الإطلاع عليها مخزنة على خوادم جهات تعتمد على التكنولوجيا في تخزين بياناتها السرية كالبنوك ، الحكومات و المؤسسات و إســتخذامها كوسيلة للتهديد و الحصول على هدف ماديا أو معنويا أو سياسيا.

4 السعي لكسب غير مشروع و الذي يكون ماديا او معنويا أو سياسيا كسرقة أرقام حسابات عملاء البنوك و هي منشرة بشكل أوسع .

الخاتمة :

من خلال كل ما تطرقنا إليه نجد ان الجريمة الإلكترونية لا تختلف كثيرا عن التقليدية فكلهما يشتركان في اركان الـــــــجريمة و يختلفان في وسيلة ارتكابها حيث ان الجريمة الالكترونية ترتبط بالنظام المعلوماتي و شبكة الانترنت .

رغم إنتــشار هذه الظاهرة بشكل كبير في العالم بصفة عامة و الجزائر بصفة خاصة إلا انه لم يتم تحديد تعريف موحدا و شـــــــــــاملا لها و نظرا لما تتميز به من خصائص حالت دون إيجاد حلول و طرق لمواجهتها و مكافحتها من بينها انها تقع في العالم الإفتراضي على خلاف الجريمة التقليدية التي تقع في الواقع الملموس .

و بناءا على ماسبق توصلنا إلى **النتائج الآتية :**

– الجريمة الالكترونية ظاهرة حديثة و بالتاي من المحتمل ظهور أنواع أخرى من الجرائم المعلوماتية .

–الجريمة الالكترونية لا تتصف بالعنف في حدوتها .

–دوافع إرتكاب الجريمة الالكترونية هو الربح بالدرجة الأولى .

–جهاز الحاسوب الالي هو الأساس في ارتكاب الجريمة الالكترونية .

و نخلص إلى بعض **التوصيات الآتية :**

–العمل على إيجاد تعريف موحدا و شاملا للجريمة الالكترونية .

–هذا النوع من الجرائم له جوانب سلبية خطيرة تهدد امن و سلامة الفرد و المجتمع .

-إن الجريمة الالكترونية تتسم بالغموض حيث يصعب إثباتها و التحقيق فيها .

المراجع :

- محمد أمين أحـــــمد الشوابكة ،جرائم الحاسوب و الانترنت ، " الجريمة المعلوماتية "، مكتب دار الثقافة للنشر و التوزيع ، عمان الاردن ، 2004 ، الطبعة الاولى .
- علي كـــــحلوش، جرائم الحاسوب و أساليب مواجهتها ،مجلة الشرطة ، المديرية العامة الامن الوطني ،عدد 84،13 جويلية 2007.
-نهلة عبد القادر المومني ، الجرائم المعلوماتية ، ماجيستير في القانون الجنائي المعلوماتي ، دار الثقافة للنشر و التوزيع 1429 هـ 2008 م ،الطبعة الاولى ، الاصدار الاول ،2008-ص 20.
- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية و الانترنت "الجرائم الإلكترونية "، دراسة مقارنة ،منشورات الحلبي الحقوقية ، بيروت ،2007 ، الطبعة الاولى .
- خالد ممدوح إبراهيم ، الجرائم الإلكترونية، الطبعة الاولى الإسكندرية : دار الفكر الجامعي ، 2008.
- جلال محمد الزغبي ، اسامة احمد المناعسة ، جرائم تقنية نظم المعلومات الالكترونية ، دراسة مقارنة ، دار التقافة للنشر و التوزيع ، عمان ، 2010، الطبعة الاولى .
- محمود إبراهيم الغازي ، الحماية الجنائية للخصوصية و التجارة الالكترونية ، مكتب الوفاء القانونية ، الاسكندرية ، الطبعة الاولى ، 2014 .
-غنية باطلي ، الجريمة الإلكترونية ، دراسة مقارنة ، الدار الجزائرية لنشر و التوزيع ،الجزائر ، 2015 .
- ادهم باسم نمر بغدادي ، وسائل البحث و التحري عن الجرائم الالكترونية ، اطروحة بدرجة ماجيستير في القانون العام بكلية الدراسات العليا ، جامعة النجاح الوطنية ، نابلس ، فلسطين 2018 .

رفاف لخضر
جامعة محمد البشير الإبراهيمي – برج بوعريريج
reffaf.lakhdar@gmail.com

معوش فيروز
جامعة محمد البشير الإبراهيمي – برج بوعريريج
fairouz.maouche@univ-bba.dz

خصوصية الجريمة الإلكترونية

الملخص:

تعد الجريمة الإلكترونية ظاهرة إجرامية حديثة أفرزتها الثورة المعلوماتية نتيجة الاستغلال السيئ لتقنياتها إذ أصبح اقتران الحاسب مع الإنترنت وسطا ملائما لارتكاب هذا النوع من الجرائم يمثل انتهاكا وتهديدا حقيقيا للأفراد والدول، تتجاوز أحيانا خطورة الجرائم التقليدية ويزداد الأمر تعقيدا للطابع الخاص الذي تتسم به من عدة جوانب بدء بخصائصها وفاعلها والأركان القائمة عليها، الأمر الذي دفع المشرع في إطار الحماية الجنائية من مخاطر هذه الجريمة تخصيص مجموعة من النصوص القانونية التي تقر بتجريمها والمعاقبة عليها.

الكلمات المفتاحية: الجريمة الإلكترونية، المجرم المعلوماتي، الأنظمة المعلوماتية، الحاسب الآلي، الأنترنت.

Abstract:

Cybercrime is a modern criminal phenomenon produced by the information revolution as a result of the bad exploitation of its technologies, The association of the computer with the Internet has become an appropriate medium for committing this type of crime. It represents a violation and a real threat to individuals and countries, sometimes exceeding the danger of traditional crimes. With its characteristics, perpetrator and the pillars based on it, which prompted the legislator within the framework of criminal protection from the dangers of this crime to allocate a set of legal texts that recognize its criminalization and punishment.

***Keywords** : electronic crime, information criminal, information systems, computer, the Internet.*

مقدمة:

شكلت الثورة المعلوماتية قفزة نوعية وحضارية في حياة الأفراد والدول نتيجة لما جاءت به من تقنيات متطورة متمثلة أساسا في تكنولوجيات الحواسيب والأجهزة الذكية واقترانها بالشبكة العنكبوتية التي أصبحت ضرورة حتمية تفرض وجودها على الدول في ظل عصر الرقمنة إذ أصبح الوعي بأهميتها مظهرا من مظاهر تقدم ورقي الشعوب والأمم، فتزايد الاعتماد عليها بشكل أساسي في تسيير المجتمعات ضمنمختلف القطاعاتلامتيازاتها وإيجابيتها الكبيرة كالسرعة والدقة في تجميع المعلومات و تخزينها

ومعالجتها خاصة وأن الطرق التقليدية أصبحت غير كافية لتلبية حاجيات المستفيدين، إلا أن الاستغلال والاستعمال السيئ لهذه التقنيات والأنظمة المعلوماتية في غير الغرض التي وجدت من أجله أدى إلى خلق نوعا جديد من الجرائم يشكل تهديدا ومساسا غير مشروع بحقوق الأشخاص وحرياتهم ناهيك عما يسببه من انتهاكات خطيرة على الصعيد الدولي والوطني،وهو ما يعرف بالجريمة الإلكترونية مما يجعلها تنفرد بطبيعة خاصة مختلفة عن الجرائم التقليدية تنعكس في عدة جوانب خاصة ما تعلق بجانبها الموضوعي، الأمر الذي يدفعنا لطرح التساؤل الآتي: **ما مدى خصوصية الجريمة الإلكترونية من الناحية الموضوعية؟.**

في محاولتنا للإجابة على الإشكالية المطروحة اعتمدنا على المنهج الوصفي التحليلي نظرا لطبيعة الموضوع وخصوصيته من أجل محاولة تحديد أهم الخصوصيات التي تتميز بها الجريمة الإلكترونية، ولدراسة هذا الموضوع ومحاولة الإلمام به ارتأينا تقسيمه إلى ثلاثة أجزاء، يتناول الجزء الأول خصائص الجريمة الإلكترونية، أما الجزء الثاني فيعالج الطابع الخصوصي لمرتكبي الجريمة الإلكترونية، و الجزء الثالث يتعلق بخصوصية أركان الجريمة الإلكترونية.

أولا: خصائص الجريمة الإلكترونية

نظرا لارتباط الجريمة الإلكترونية بالمجال المعلوماتي جعلها تنفرد بمجموعة من الخصائص تميزها عن الجريمة التقليدية المتمثلة أساسا في:

01/ الجريمة الإلكترونية من الجرائم الهادئة الواقعة في بيئة معلوماتية:

تقع الجرائم الإلكترونية أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات أو أثناء مرحلة المعالجة أو مرحلة إخراج المعلومات [1]، وهذا لا يتم إلا في حضور وسيلتين مهمتين ألا وهما الحاسب الآلي وشبكة الأنترنت إذ يمثل هذا النظام الشرط الأساسي لتوفر وتحقق الجريمة المعلوماتية، وتبعا لذلك يجعلها تتسم بالطبيعة الهادئة لأن ارتكابها لا يحتاج إلى قوة عضلية كما هو الحال في الجرائم التقليدية، بحيث يطلق عليها"soft crime" إذ لا تحتاج إلى العنف فكل ما تحتاج إليه هو القدرة والتعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة[2].

02/ الجريمة الإلكترونية عابرة للحدود الوطنية:

جعلت الإنترنت العالم قرية صغيرة من خلال خلق ما يسمى بالمجتمع المعلوماتي الافتراضي إذ به تختصر المسافات بين مختلف دول العالم حيث لا وجود لقيود زمنية أو مكانية تقف أمام نقل

[1] عبد الله دغش العجمي، **المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة**، مذكرة لنيل شهادة الماجستير، تخصص قانون عام، جامعة الشرق الأوسط، 2014، ص24.

[2] نهلا عبد القادر،**الجرائم المعلوماتية**، الطبعة الأولى، دار الثقافة للنشر و التوزيع، الأردن، 2008،ص58.

المعلومات، لذلك فمن السهولة أن يكون المجرم في بلد والمجنى عليه مقيما في بلد آخر مما يعني أن مساحة مسرح الجريمة الإلكترونية لم تعد محلية وإنما أصبحت عالمية حيث يتم ارتكابها عبر المسافات لا يتواجد فيها الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد، و بالتالي يكون هناك تباعد مكاني بين الفعل الإجرامي والنتيجة [1]، وهنا تظهر الحاجة إلى وجود تنظيم دولي وداخلي متلائم معه لمكافحة هذا النوع من الجرائم و ضبط فاعليتها[2]،كما أن هذه الخاصية تثير العديد من المشكلات القانونية بما أنها تخرج عن الحدود الوطنية كمشكلة السيادة و الاختصاص القضائي ، تحديد القانون الواجب التطبيق و الإشكالية المتعلقة بإجراءات الملاحقة القضائية[3].

02/الجرائم الإلكترونية صعبة الاكتشاف والإثبات:

يصعب اكتشاف الجريمة الإلكترونية نظرا للطبيعة الغير المادية التي تتسم بها، فهي جريمة يسهل إخفاء معالمها وأدواتها بالإضافة إلى نقص خبرة الشرطة وجهات القضاء والإدعاء ضمن الميدان المعلوماتي في الكشف عنها [4]،خاصة وأن المجرم يستطيع محو وإزالة الدلائل بشكل كامل في ظرف وجيزهذا من جهة، ومن جهة أخرى فالجاني يرتكب هذه الجرائم في دول أخرى مختلفة عن بلد المجنى عليه، كما أن هذا الأخير قديساهم في صعوبة اكتشاف الجريمة المعلوماتية من خلال اتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعته أو مكانته أو هز الثقة في كفاءتها[5]، وبالتالي فإن اكتشافها في معظم الأحيان يكون بمحض الصدفة.

وإذا تم اكتشاف الجريمة المعلوماتية فإن إثباتها يكون صعبا نظرا للطبيعة الخاصة للدليل المثبت لها فهو ليس بدليل مرئي ملموس حيث يصعب الوقوف عليه والتمكن من الإحاطة به [6]، فضلا عن إمكانية تدمير كل ما يستخدم كدليل للإثبات في دقائق معدودة، إضافة إلا أن عدم ملائمة الأدلة التقليدية في القانون الجنائي في إثباتها ومن ثم يلزم البحث عن أدلة جديدة حديثة ناتجة عن ذات الحاسب ومن هنا تبدأ صعوبات البحث عن الدليل، وتبدأ مشكلات قبوله إن وجد، ومدى موثوقيته ومصداقيته على إثبات وقائع الجريمة[7].

03/الجرائم الإلكترونية مغرية تتسبب في أضرار فادحة

إذا كانت بعض الجرائم التقليدية تحتاج من مرتكبيها قوة عضلية فإن الجرائم المعلوماتية لا تحتاج إلى مثل تلك القوة العضلية لتنفيذها وإنما إلى قوة علمية وقدر من الذكاء ومهارة في توظيف

---

[1]فتيحة رصاع، **الحماية الجنائية للمعلومات على شبكة الأنترنت**، مذكرة لنيل شهادة الماجستير، تخصص قانون العام ، كلية الحقوق و العلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2012/2011، ص43.

[2]عبد الله دعش العجمي،المرجع السابق، ص20.

[3]ريمة بن عميروش، **عن خصوصية الجريمة المعلوماتية**، مجلة الفقه القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة تيارت، المجلد02، العدد02، 2021/10/23، ص78.

[4]كريمة برني، احمد بولمكاحل، **خصوصية الجريمة المعلوماتية بين التجريم والعقاب**، مجلة القانون و العلوم السياسية، المجلد 07، العدد02، 2021، ص85.

[5]فتيحة رصاع، المرجع السابق، ص45.

[6]ريمة بن عميروش، المرجع السابق ، ص85.

[7] فتيحة رصاع، المرجع السابق، ص 45.

ذلك،كما أن الجاني في سبيل تنفيذها لا يحتاج من الوقت إلا ثوان أو دقائق معدودات [1]، بالإضافة إلى صعوبة اكتشافها وإثباتها وما يمكن أن تدره من أموال وأرباح طائلة يجعلها مصدر إغراء لتنفيذها مما يؤدي إلى خسائر فادحة إذ من شأنها المساس بالمركز الحسابي والإداري وتنقلات الأموال والاستثمارات سواء في المنشآت العامة أو الخاصة وتهديد قدسية وسرية الحياة الخاصة والحرية السياسية بالمساس بالمعلومات الشخصية لمختلف فئات الأشخاص أو إذا تعلقت بالمعلومات الخاصة بإدارة الدولة وعمل الحكومة خاصة ضمن المجال الأمني[2].

فقد أثبتت العديد من الدراسات أن الأضرار الناجمة عن الجرائم المعلوماتية تفوق بكثير عن تلك الناجمة عن الجرائم التقليدية من بينها الأبحاث التي أجرتها شركة "مكافي" للأمن السيبيراني عن مدى الضرر المالي الذي أحدثته جرائم الإنترنت على مستوى العالم الذي بلغ سنة 2018 تريليون دولار أي ما يعادل 1في المئة من الناتج المحلي الإجمالي العالمي [3]، و كشفت شركة "آي بي أم سكيروتز" في دراسة حديثة عن زيادة الهجمات الإلكترونية بنسبة 93 في المئة خلال النصف الأول من عام 2021 حيث كان الاستهداف يشمل بكثرة الشركات حيث تقع اليوم شركة ضحية للاعتداءات الإلكترونية كل 11 ثانية[4].

ثانيا: الطابع الخصوصي لمرتكب الجريمة الإلكترونية

إن ارتباط الجريمة الإلكترونية بتكنولوجيا المعلومات أدت إلى ظهور فئة جديدة من المجرمين يعرفون باسم مجرمي المعلوماتية تختلف عن فئة المجرمين العادين من عدة جوانب يستدعي تحديدها إلى الوقوف عند مفهوم هذا النوع الخاص والجديد من المجرمين من خلال التطرق إلى تعريفه وخصائصه، وتحديد أصنافه ودوافع ارتكابه لمثل هذه الجرائم.

01/ تعريف المجرم المعلوماتي :

يصطلح على الجاني في الجريمة الإلكترونية ضمن المجال المعلوماتي بإسم الهاكر تبعا لخبراء المعلوماتية الإلكترونية فهو الذي يقوم بعمليات الاختراق والتخريب عبر شبكة الأنترنت أما ضمن المجال القانوني فيصطلح عليه بالمجرم المعلوماتي أو الإلكتروني، ويقصد به الشخص الذي يخترق الحاسب الآلي ويجد متعة في فحص واستكشاف عن كثب نظام قابل للبرمجة ويسعى إلى توسيع معارفه في هذا المجال إلى أقصى حد [5]، وهناك من يعرفه بأنه كل شخص سواء كان طفل أو رجل أو أنثى يأتي بأفعال إرادية تشكل سلوكا إيجابيا أو سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالاعتداء على حق

[1] محمد خليفة، **خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها** مجلة الدراسات والأبحاث، جامعة زيان عاشور، المجلد 1، العدد1، الجلفة، 2009، ص 375.

[2] عادل يوسف عبد النبي الشكري، **الجريمة المعلوماتية وأزمة الشرعية الجزائية**، مجلة مركز الدراسات، الكوفة، العراق، المجلد 5، العدد السابع، 2008، ص116.

[3] http//m-youm7.com, ،اطلع عليه بتاريخ 2022/07/15 ، الساعة 22:00.

[4] http/www.idependentarabia.com، اطلع عليه بتاريخ 28 جوان 2022، الساعة12 :16.

[5] بشرى غريبي، **خصوصية المجرم المعلوماتي و دوافعه**، مجلة نوميروس الأكاديمية، جامعة أو بكر بلقايد، المجلد الثاني، العدد الثاني، 2021، ص103.

أو مصلحة[1]، أو هو المجرم الإلكتروني الرقمي الذي لديه القدرة بواسطة خبراته العالية في الإعلام الآلي على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني الرقمي وملحقاته ووسلائل الاتصال الرقمية بأداء فعل أو الامتناع عنه مما يحدث اضطرابات في المجتمع الدولي أو المحلي لمخالفته قواعد الضبط الاجتماعي محليا ودوليا [2]، ونظرا للتعريفات المختلفة للمجرم المعلوماتي يمكن القول أن القيام بعمل أو الامتناع عن عمل يتم ارتكابه في ظل استخدامات تكنولوجيا الإنترنت وتقنياتوأنظمة المعلوماتية قد حظره المشرع يطلق على مرتكبه تسمية المجرم الإلكتروني.

02/ خصائص المجرم المعلوماتي

أ/المجرم المعلوماتي يتمتع بالذكاء والخبرة والمهارة:

يتميز المجرم المعلوماتي بالذكاء والاحترافية والمهارة في المجال المعلوماتي نظرا لأن ارتكاب الجريمة الإلكترونية يتطلب قدرا كبيرا من الذكاء لاتصالها بأكثر الميادين تطورا وحاجة إلى مقدرة عقلية وذهنية، فالمجرم يستخدم قوته العقلية المتمثلة في الذكاء ولا يلجأ إلى استخدام القوة العضلية كالعنف والإتلاف المادي وبالتالي يمكن القول أن الإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف [3]، حيث أن اكتسابه للذكاء والمهارة والاحترافية قد يكون عن طريق الدراسة المتخصصة أو الخبرة المكتسبة في مجال المعلوماتية، فشخصية المجرم المعلوماتي لطالما ارتبطت بصورة الشخص المهووس بتقنية المعلوماتية الذي يتميز بالقدرة على اختراق النظم المعلوماتية والتلاعب بها وبالتالي يتمكن من الوصول إلى طرق وأساليب جديدة ومبتكرة لتنفيذ مبتغاه.

ب/المجرم المعلوماتي شخص اجتماعي:

نتيجة لتميز المجرم المعلوماتي بالذكاء فإنه يساعده على عملية التكيف مع مجتمعه فيعتبر شخصا اجتماعيا بطبعه يعيش ويمارس حياته وعمله بتوافق مع الأشخاص المحيطين به،إلا أن هذا التكيف الإجتماعي مع شخصيته الإجرامية يؤدي إلى زيادة خطورته بسبب شعوره أنه محل ثقة من مجتمعه وأنه خارج إطار الشبهات مما قد يدفعه إلى التمادي في ارتكاب الجرائم التي قد لا تكتشف [4]، ونتيجة لاندماجه في المجتمع يعتبر حذرا لكشف أمره مما يجعله حرصا وعلى حذر دائم في اتباع أسلوب تدمير ومحو لكل البيانات الناتجة عن فعله[5].

ج/المجرم المعلوماتي يتمتع بالسلطة تجاه النظام المعلوماتي

---

[1]رضا عسال، عماد عبد الرزاق، **الجريمة الإلكترونية و المجرم المعلوماتي: مقاربة مفاهيمية**، بيليوفيليا لدراسات المكتبات والمعلومات، جامعة العربي تبسي، تبسة، العدد 05، 2020/03/30، ص155.

[2]خالد ممدوح ابراهيم، **جرائم المعلوماتية**، دار الفكر الجامعي، الاسكندرية، مصر، 2009 ،ص26.

[3]نهلا عبد القادر المومني، **المرجع السابق**، ص78.

[4]نهلا عبد القادر، المرجع السابق،ص 79.

[5]حسين ربيعي، **المجرم المعلوماتي: شخصيتهوأصنافه**، مجلة العلوم الإنسانية، جامعة محمد خيضر، بسكرة، العدد40، جوان 2015، ص290.

استغلال المجرم المعلوماتي للخبرة و المهارات والذكاء التي يتميز بها تمكنه من السيطرة الفعلية على النظام المعلوماتي وتسهل عليه ارتكاب جريمته تبعا للمعلومات و البيانات المتوفرة له، كالرقم السري الخاص للنظام معين، أو فتح ملفات وقراءتها ..

03/أصناف المجرم الإلكتروني

إن اختلاف الأسباب و الوسائل المؤدية إلى ارتكاب الجريمة الإلكترونية يؤدي إلى وجود أصناف عدة لمجرمي المعلوماتية اختلف الفقهاء والعلماء في تصنيفهم تبعا لاختلاف الزاوية التي ينظر منها إليه إذ يمكن إجمالهم فيما يلي:

أ/ صنفي مجرمي المعلوماتية الهواة :

يندرج ضمن فئة مجرمي المعلوماتية الهواة كل من العابثون والقراصنة الهواة، فالبنسبة لصنف العابثون أو مايسمى بصغار نوابغ المعلوماتية هم الشباب والمراهقون المهتمين والمهوسين بالمعلوماتية إذ يرتكبون أفعال إجرامية في الغالب تكون من أجل إبراز قدراتهم في التمكن من عالم المعلوماتيةحبا للاكتشاف، وقد عرفهم دون باركر" بأنهم تلك الطائفة التي ترتكب أفعالها بغرض التسلية فهم لا يهدفون إلى تعطيل أو سرقة الأنظمة المعلوماتية وإنما هدفهم الرئيسي هو اللعب من أجل التسلية".

أما بالنسبة لفئة القراصنة الهواة ويصطلح عليهم بالهاكرز ويقابله في اللغة العربية بالقراصنة أو المخترق حيث ظهر هذا الصنف في الستينيات من القرن العشرين إذ كان يقتصر على طلبة الحاسوب والاتصال[1]، تتفوق هذه الفئة على العابثون علما ومعرفة وخبرة في مجال المعلوماتية وهم في العادة مختصين ضمن مجال المعلوماتية، فهم متطفلون يتحدون إجراءات أمن النظم والشبكات ولا تتوفر لديهم في الغالب الأعم دوافع حاقدة أوتخريبية [2]، وتنقسم هذه الفئة بدورها إلى أربعة أصناف تتمثل في القبعات البيضاء ويكون هدفهم كشف الثغرات الامنية ونقاط الضعف الأنظمة المعلوماتية وإبلاغ المسؤولين لتصحيحها، والقبعات الرمادية التي تستغل وتستفيد من نقاط الضعف الأنظمة المعلوماتية، والقبعات السوداء هم فئة غايتهم خرق الأنظمة المعلوماتية من أجل تحقيق الربح بصفة غير مشروعة[3].

ب/ صنف مجرمي المعلوماتية المحترفين:

ويشمل هذا الصنف كل من القراصنة المحترفون، المجرمون المعلوماتين المحترفون في إطار الجريمة المنظمة، المجرمون المعلوماتيون المتطفلون، الموظفون العاملون في مجال الأنظمة المعلوماتية.

– بالنسبة للقراصنة المحترفون أو الكراكز يعتبرون من أخطر مجرمي المعلوماتية الذين تتجاوز أعمارهم 25 سنة لهم قدرات وخبرات عالية في مجال الحاسب الآلي، يمثلون تهديدا كبيرا للأنظمة والتقنيات

[1]سهام خليلي، **خصوصية المجرم المعلوماتي**، مجلة المفكر، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، العدد 15، جوان 2017،ص 406.

[2]صالح بن منصور، كوش أنيسة، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة لنيل شهادة الماستر، تخصص القانون الخاص و العلوم الجنائية، كلية الحقوق و العلوم السياسية، جامعة عبد الرحمان لن ميرة، بجاية، 2015/2014، ص36.

[3]حسين ربيعي، المرجع السابق، ص296.

المعلوماتية لوصولهم إلى مرحلة كبيرة من التوغل ضمن عالم المعلوماتية والهيمنة والسيطرة الكاملة على تقنيات الحاسوب والشبكة المعلوماتية، تعكس اعتداءاتهم ميولا إجرامية خطرة تنبئ عن رغبتها في إحداث التخريب[1]. وقد أصبحت في الوقت الحالي مسألة إعداد البرامج المعلوماتية الخبيثة ومواجهة كل ماهو محظور بهدف الكسب المادي من المهام الرئيسية التي تتولاه هذه الفئة[2].

– المجرمون المعلوماتيون المحترفون في إطار الجريمة المنظمة فيقصد بهم الجماعات الإجرامية كالمافيا والعصابات المختصة التي يكون هدفها الربح المادي بطرق غير شرعية باستغلال شبكة الأنترنت وتقنيات المعلوماتية في ارتكاب الجرائم المنظمة من أجل تحقيق الأرباح الطائلة كنهب الأموال وتحويلها بطرق غير مشروعة لحساباتهم أو غسيل الأموال، اختراق شبكات المعلومات الخاصة بالدول والمؤسسات المالية الكبرى..إلخ.

– المجرمون المعلوماتيون المتطرفون فهم مجموعة الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية يدافعون عنها ويرغبون في فرضها باللجوء إلى ارتكاب أفعال خطيرة ضد الأنظمة المعلوماتية دون أن يكون الهدف الربح المادي.

– الموظفون العاملون في مجال الأنظمة المعلوماتية هم الموظفون الذين يكون النظام المعلوماتي مجال عملهم ونظرا للمهارات والمعرفة التقنية ومعرفتهم التي يتمتعون بها فإنهم يقترفون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية [3]، وبالتالي نظرا للإرتباط الوطيد بوظيفتهم يجعلهم محل ائتمان وثقة مما يسهل عليهم عملية ارتكاب الجرائم.

04/دوافع ارتكاب المجرم المعلوماتي للجريمة الإلكترونية:

الدافع هو العامل المحرك للإرادة إذ هو قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة بغية تحقيق غاية معينة تختلف من مجرم لآخر [4]، فنظرا لتعدد أصناف مجرمي المعلوماتية فإن دوافع وبواعث ارتكابها تختلف من مجرم لآخر إذ منها ما يتعلق بالدوافع الشخصية والبعض الآخر يرجع إلى دوافع داخلية.

أ/الدوافع الشخصية:

يقصد بالدوافع الشخصية تلك العوامل اللصيقة بشخصية المجرم المعلوماتي والتي تدفعه لارتكاب الجريمة المعلوماتية[5]، إذ تتعدد وتختلف من مجرم لآخر يمكن حصرها فيما يلي:

– الرغبة في تحقيق الربح المادي: إذ يعتبر السبب الأول لانتشار الإجرام الإلكتروني، إذ هو الدافع الأول والحافز للمجرم المعلوماتي من أجل تحقيق الكسب المالي السريع والطائل عن طريق التلاعب

[1] نهلا عبد القادر، المرجع السابق،ص84.
[2] حسين ربيعي، المرجع السابقن ص 297.
[3] نهلا عبد القادر مومني، المرجع السابق، ص 86.
[4] حمزة عقون، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة لنيل شهادة الماجستير، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012/2011، ص46.
[5] بشرى غريبي، المرجع السابق، ص109.

بالأنظمة المعلوماتية للمؤسسات المالية، فقد أشارت الدراسات إلى أن المحرك الأساسي لأنشطة احتيال الكمبيوتر وفيما بعد احتيال الإنترنت هو تحقيق الكسب المالي تبعا لدراسة قديمة أجراها الفقيه باركر[1].

- الرغبة في قهر النظام المعلوماتي وإثبات الذات: يقوم مجرمي المعلوماتية من أجل استظهار قدراتهم والحصول على الاعتراف الاجتماعي بكفاءتهم وإثبات الذات بارتكاب أفعال محظورة لايدركون بخطورتها ضمن المجال المعلوماتي تمثل لهم انتصار على تقنية الأنظمة المعلوماتية، كما أن اختراق الأنظمة المعلوماتية وكسر الحواجز الأمنية يشكل متعة كبيرة وتسلية لهم يؤدي ذلك إلى الرغبة في تحقيق الذات وقهر النظام المعلوماتي[2]، يتوفر هذا الدافع عادة لدى فئة مجرمي المعلوماتية الهواة.
- الرغبة في التعلم :قد يكون الغرض من ارتكاب الجريمة المعلوماتية الحصول على الجديد من المعلومات من خلال البحث والاكتشاف والعمل ضمن مجموعة والتعلم من بعضهم البعض[3].

ب/دوافع خارجية:

تتوفر هذه الدوافع عادة لدى فئة مجرمي المعلوماتية المحترفين وتتمثل في كل من دافع الانتقام وإلحاق الضرر والدافع السياسي:

-دافع الانتقام وإلحاق الضرر الذي يتجسد لدى فئة الموظفون العاملون في مجال الأنظمة المعلوماتية نتيجة للضغوطات ومشكلات متعلقة بوظيفتهم يدفعهم الأمر لارتكاب مثل هذه الأفعال بدافع الانتقام من رب العمل أو من المؤسسة إذ يكونون في وضعية مناسبة من خلال استغلال وظيفتهم لتنفيذ مبتغاهم.

-الدافع السياسي: حيث يكون القصد من ارتكاب هذه الجرائم لأغراض سياسية تظهر في شكل اعتداءات إلكترونية تسعى إلى تعطيل المواقع التي تدعو إلى العنصرية أو الدفاع عن مبادئ الحرية الإنسانية، وقد يتحول الدافع السياسي إلى دافع إرهابي من خلال التحريض على القتل والتمرد والعصيان المدني[4].

ثالثا: خصوصيةأركان الجريمة الإلكترونية

غيرت الجريمة الإلكترونية العديد من المبادئ القانونية في القانون الجنائي باعتبارها جريمة مستحدثة تتخذ صورا عديدة نظرا للتطورات السريعة في الميدان المعلوماتي التي أدت إلى وجود تقنيات وأساليب جديدة للاختراق والقرصنة صعب مجاراته من طرف السلطة التشريعية بحيث أصبحنا نعيش فيما يمكن تسميته الطوفان الرقمي[5]، إذ يصعب حصر صور الجرائم الإلكترونية الأمر الذي يؤدي إلى توسيع مضامين الأركان العامة للجريمة المعلوماتية المتمثلة أساسا في الركن الشرعي والمادي والمعنوي.

01/ الركن الشرعي للجريمة الإلكترونية

[1]سمير شعبان، **الجريمة الإلكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم**، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، المجلد01، العدد01، 2009، ص128.
[2]بشرى غريبي، المرجع السابق،ص 110.
[3]نهلا عبد القادر، المرجع السابق، ص90.
[4]حسين ربيعي، المرجع السابق،ص 293، 294.
[5]أنيس العذار، **مكافحة الجريمة الإلكترونية**، المجلة الأكاديمية للبحث القانوني، المجلد 17، العدد01، 2018، ص730.

يمثل الركن الشرعي النص الذي يجرم الفعل ويحدد عقوبته قبل وقوعه تبعا لأحكام المادة الأولى من قانون العقوبات[1] التي تقضي بقولها:"لاجريمة ولاعقوبة أو تدابير أمن إلا بنص"، والجريمة الإلكترونية كغيرها من الجرائم التقليدية نظرا لمخاطرها تحتاج إلى ركن شرعي من خلال إقرار وتبني نصوص عقابية خاصة لمواجهتها والحد من ارتكابها إلا أن ذلك يثير عدة مشكلات تتمثل في تحديد الطائفة التي يندرج ضمنها هذا النوع من الجرائم، بالإضافة إلى إشكالية المصطلحات نظرا لغموض مفهومها باعتبارها غريبة عن لغة القانون [2]، وبناء على ذلك اختلفت الدول في وضع النمط التشريعي المنظم للجريمة الإلكترونية،فنجد المشرع الجزائريوضع مجموعة من التنظيمات القانونية المتعلقة بالجريمة الإلكترونية في كل من القانون رقم 04-15 المتضمن قانون العقوبات[3] ضمن القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 إلى 394 مكرر 7، وضمن القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال [4] ومكافحتها ضمن 19 مادة، ونتيجة لهذا التدخل التشريعي فإن القاضي يمنع من قياس فعل لم يرد النص على تجريمه على فعل ورد نص بتجريمه[5]،إلا أن هناك من يرى عكس ذلكنظرا لأن النصوص القانونية للجريمةالإلكترونية تحتوي على مصطلحات فضفاضة خاصة وأنها لا تمت صلة بلغة القانون إذ يمكن أن تشمل عدة جرائم وبالتالي تحتوي على أوجه تفسير عديدة حيث يكون للقاضي سلطة أكبر في إسقاط عدد أكبر من هذه الجرائم[6].

02/ الركن المادي للجريمة الإلكترونية

يتمثل الركن المادي للجرائم المعلوماتية في الاعتداء على أنظمة المعالجة الآلية للمعطيات من خلال الدخول أو البقاء عن طريق الغش إلى هذه الأنظمة تبعا لأحكام المادة 394 مكرر من قانون العقوبات، فالبنسبة لفعل الدخول يتحقق بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبه لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أويسمح بالدخول لكن مقابل نفقات[7]،فالدخول الغير المشروع إلى نظم وقواعد معالجة البيانات دون اشتراط وجود تلاعب بهذه البيانات من عدمه يعد سلوكا إجراميا وبالتالي فمجرد الدخول بأي شكل أو وسيلة غير مشروعة للمواقع الإلكترونية أو الأنظمة الحسابية يجعل النشاط الإجرامي في هذه الحالة محققا [8]،أما بالنسبة لفعل البقاء فهو التواجد

[1]الامر رقم 66-15 المؤرخ في 10 جوان 1966، يتضمن قانون العقوبات، ج ر ج ، العدد 49، الصادرة في 11 جوان 1966.
[2]آمال قارة، **الجريمة المعلوماتية**، مذكرة لنيل شهادة الماجستير، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2002/2001، ص38،37.
[3] القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004المتمم لقانون العقوبات، ج ر ج، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.
[4]القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ج ر، العدد 47، الصادرة بتاريخ 16 أوت 2009.
[5]حمزة خضري، حمزة عشاش، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، مجلة الدراسات القانونية في التشريع الجزائري، جامعة عمار ثليجي، الأغواط، المجلد 06، العدد 2، جوان 2020، ص173.
[6]نداء نائل فايز المصري، **خصوصية الجرائم المعلوماتية**، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الدراسات العليا ، جامعة النجاح الوطنية، نابلس، فلسطين، 2017، ص13.
[7]حمزة خضري، حمزة عشاش،المرجع السابق، ص174.
[8]كريمة برني، احمد بولمكاحل، المرجع السابق، ص85.

داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، أو يتجاوز المدة المسموح له بالبقاء فيها، أو عدم الانسحاب فورا وقطع وجوده في نظام البيانات أو يطبع معلومات حين يسمح له بالرؤية فقط [1]، فتتمثل الصورة البسيطة في مجرد الدخول أو البقاء غير المشروع بينما الصورة المشددة تتحقق بتوافر الظرف المشدد لها وهو يكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغير في المعطيات الموجودة في النظام[2].

03/ الركن المعنوي:

يمثل الركن المعنوي عموما الجانب النفسي الذي يرتبط بالفعل فلا يكفي لقيام الجريمة وقوع الفعل بل يلزم أن يقع بموجب إرادة حرة وواعية [3]،فتوافره في الجرائم الإلكترونية يعد من الأمور الهامة من أجل تحديد نوع الجريمة المرتكبة ومنه يتحدد النص الواجب التطبيق،إذ يختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلا أخرى خاصة وأنه يعتبر مقياسا لتقسيم الجرائم إلى عمدية وغير عمدية.

فالمقصود بالركن المعنوي في الجرائم المعلوماتية هو اتجاه إرادة الجاني إلى إحداث النتيجة الجرمية وارتكاب إحدى الجرائم المعلوماتية المنصوص عليها بالتشريعات المختلفة [4]، فتكتسب إرادة الجاني طابع التجريم من الفعل الإجرامي المرتكب النابع عن ارتكابها مع توافر علمه بالآثار المترتبة عنه[5]، وتبعا لما جاء في المواد المنظمة في المواد من 394 مكرر إلى المادة 394 مكرر 5 ما احتوته من عبارات "كالغش"، "العمد"،يظهرأن الجريمة المعلوماتية جريمة عمدية بامتياز ولا يفترض فيها عنصر الخطأ[6].

خاتمة:

في ختام دراستنا يمكن القول أن الجريمة الإلكترونية تعد نمطا حديثا ظهر وتطور وانتشر في ضوء التسهيلات والامتيازات التي تقدمها الثورة المعلوماتية التي تشكل مساسا بالحياة الخاصة للأفراد وتهديدا للأمن القومي والسيادة، تنفرد بمجموعة من الخصائص التيتميزها عن الجرائم التقليدية تجعلها أكثر خطورة منها، مما جعل المشرع الجزائري كغيره من التشريعات المقارنة التدخل لإقرار مجموعة من التنظيمات القانونية للحد والتصدي لها تتحدد من خلالها أركانها العامة، ما يأخذنا إلى عرض أهم النتائج المتوصل لها :

- السمة المميزة للكثير من الجرائم الإلكترونية هي أنها جريمة عابرة للحدود الوطنية لاتقتصر على إقليم الدولة، وإنما يكون هناك بعد مكاني بين وجود الجاني ومكان المجنى عليه الأمر الذي يخلق عدة مشكلات متعلقة بالسيادة .

[1] آمال قارة، المرجع السابق، 44.
[2] المرجع نفسه، ص42
[3] عبد الرحمان خلفي، **القانون الجنائي العام**، الطبعة الرابعة، دار بلقيس للنشر والتوزيع، الجزائر، 2019، ص71.
[4] نداء نائل فايز المصري، المرجع السابق، ص19.
[5] كريمة برني، احمد بولمكاحل، المرجع السابق، ص86.
[6] حمزة خضري، حمزة عشاش، المرجع السابق، ص175.

- تحتاج الجرائم الإلكترونية لتحققها إلى مستوى علمي ومعرفي ضمن المجال المعلوماتيعلى خلاف الجرائم التقليدية، إذ يتميز مرتكبها المعروف بالمجرم المعلوماتي أو الإلكترونيبمهارات عملية متطورة بالتقنيات والأنظمة المعلوماتية الأمر الذي يجعل الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية، كما يصعب وقد يستحيل اكتشافها وإثباتها نظرالسرعة وذكاء المجرمين المعلوماتين في إخفاء نشاطه وسهولة تدمير الدليل جعلتهم دائما يفلتون من العقاب في ظل غياب الدليل المثبت للجريمة.
- في إطار مواجهة مخاطر هذه الجرائم حاول المشرع الجزائري كغيره من التشريعات المقارنة وضع وسن مجموعة من النصوص القانونية التي تقر بتجريمها وتحديد العقوبات اللازمة لها مع تعداد صورها ضمن القانون04-15 المتضمن قانون العقوبات، والقانون رقم09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بعد التعديل في قانون العقوبات، إلا أن ذلك يبدو غير كافيا إذ يصعب حصر الجرائم الإلكترونية نظرا للتطورات السريعة في المجال المعلوماتي إذ يجد المجرم المعلوماتي أساليب وطرق جديدة للاختراق والقرصنة، خاصة مع حظر القياس في المواد الجنائية مما يمكن العديد من المجرمين الإفلات من العقوبة.

إذ يمكننا في هذا السياق الوقوف على بعضا لاقتراحات المتمثلة في:

- جمع وتوحيد الأحكام والنصوص المتعلقة بالجرائم الإلكترونية في تقنين موحد وتوسيع مضامينها لتشمل وتواكب التطور المستمر لهذه الجرائم وتتناسب مع خصوصيتها مع تشديد العقوبات على مرتكبي هذه الجرائم، وإنشاء أجهزة وهيئات متخصصة من الخبراء في المجال المعلوماتي لمكافحة الجرائم الإلكترونية.
- تدريب وتأهيل الجهات الأمنية والقضائية في المجال المعلوماتي لرفع مستوى الكفاءة،والتعاون والتنسيق مع الشركات المتخصصة والاستعانة بالخبرات والتجارب الأجنبية الناجحة في سبيل مكافحة الجرائم الإلكترونية.

قائمة المراجع والمصادر:

أ/ النصوص القانونية:

1. الأمر رقم 66-15 المؤرخ في 10 جوان 1966، يتضمن قانون العقوبات، ج ر ج ، العدد 49، الصادرة في 11 جوان 1966.
2. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004المتمم لقانون العقوبات، ج ر ج، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

3. القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ج ر، العدد 47، الصادرة بتاريخ 16 أوت 2009.

ب/ الكتب:

1. عبد الرحمان خلفي، **القانون الجنائي العام**، الطبعة الرابعة، دار بلقيس للنشر والتوزيع، الجزائر، 2019.
2. خالد ممدوح ابراهيم، **جرائم المعلوماتية**، دار الفكر الجامعي، الاسكندرية، مصر، 2009.
3. نهلا عبد القادر، **الجرائم المعلوماتية** ، الطبعة الأولى، دار الثقافة للنشر و التوزيع، الأردن، 2008.

ج/ الرسائل الجامعية :

1. آمال قارة، **الجريمة المعلوماتية**، مذكرة لنيل شهادة الماجستير، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر01، 2002/2001.
2. حمزة عقون، **السلوك الإجرامي للمجرم المعلوماتي** ، مذكرة لنيل شهادة الماجستير، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012/2011.
3. عبد الله دغش العجمي، **المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة** ، مذكرة لنيل شهادة الماجستير، تخصص قانون عام، جامعة الشرق الأوسط، 2014.
4. فتيحة رصاع، **الحماية الجنائية للمعلومات على شبكة الأنترنت** ، مذكرة لنيل شهادة الماجستير، تخصص قانون العام ، كلية الحقوق و العلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2012/2011.
5. نداء نائل فايز المصري، **خصوصية الجرائم المعلوماتية**، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الدراسات العليا ، جامعة النجاح الوطنية، نابلس، فلسطين، 2017.
6. صالح بن منصور، كوش أنيسة، **السلوك الإجرامي للمجرم المعلوماتي** ، مذكرة لنيل شهادة الماستر، تخصص القانون الخاص و العلوم الجنائية، كلية الحقوق و العلوم السياسية، جامعة عبد الرحمان لن ميرة، بجاية، 2015/2014.

ج/ المقالات العلمية:

1. أنيس العذار، **مكافحة الجريمة الإلكترونية** ، المجلة الأكاديمية للبحث القانوني، المجلد 17، العدد01، 2018.
2. بشرى غريبي، **خصوصية المجرم المعلوماتي و دوافعه**، مجلة نوميروس الأكاديمية، جامعة أو بكر بلقايد، المجلد الثاني، العدد الثاني، 2021.

3. حسين ربيعي، **المجرم المعلوماتي: شخصيته وأصنافه** ، مجلة العلوم الإنسانية، جامعة محمد خيضر، بسكرة، العدد40، جوان 2015.
4. حمزة خضري، حمزة عشاش، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري** ، مجلة الدراسات القانونية في التشريع الجزائري، جامعة عمار ثليجي، الأغواط، المجلد 06، العدد 2، جوان 2020.
5. رضا عسال، عماد عبد الرزاق ، **الجريمة الإلكترونية و المجرم المعلوماتي: مقاربة مفاهيمية** ، بيليوفيليا لدراسات المكتبات والمعلومات، جامعة العربي تبسي، تبسة، العدد 05، 2020/03/30.
6. ريمة بن عميروش ، **عن خصوصية الجريمة المعلوماتية** ، مجلة الفقه القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة تيارت، المجلد02، العدد02، 2021/10/23.
7. سمير شعبان، **الجريمة الإلكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم** ، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، المجلد01، العدد01، 2009.
8. سهام خليلي، **خصوصية المجرم المعلوماتي** ، مجلة المفكر، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، العدد 15، جوان 2017.
9. عادل يوسف عبد النبي الشكري، **الجريمة المعلوماتية وأزمة الشرعية الجزائية** ، مجلة مركز الدراسات، الكوفة، العراق، المجلد 5، العدد السابع، 2008.
10. كريمة برني، احمد بولمكاحل، **خصوصية الجريمة المعلوماتية بين التجريم والعقاب** ، مجلة القانون و العلوم السياسية، المجلد 07، العدد02، 2021.
11. محمد خليفة، **خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها** ، مجلة الدراسات والأبحاث، جامعة زيان عاشور، المجلد 1، العدد1، الجلفة، 2009.

د/المواقع الإكترونية:

1. http//m-youm7.com ،اطلع عليه بتاريخ 2022/07/15 ، الساعة 22:00.
2. http/www.idependentarabia.com، اطلع عليه بتاريخ 2022/07/15،الساعة 22:00.

فنطازي خيرالدين
fantazi.kheireddine@univ-guelma.dz
جامعة 8 ماي 1945 قالمة

أسباب الجرائم الإلكترونية

مقدمة

إن الجريمة هي إفراز للمجتمع و مظهر من مظاهره, و من ثم تعكس كافة ما تموج به المجتمعات من ظروف و أسباب ,حيث أن ذلك مرجعه إلى ما يحويه السلوك الإنساني في علاقاته المتشابكة من جمع لعنصري الخير و الشر و تصارعهما بصفة دائمة في دورة الحياة اليومية ,وبالتالي يستحيل إمكان تصور خلو الحياة دون اجتماع مظهريهما.[1] و من الثابت ان الجريمة و النشاط المعادي للمجتمع قد اقتحمه نوع جديد من المجرمين إلى جانب ا الجرم التقليدي الذي عهدناه في الماضي و الذي كانت تقتصر جرائمه على أبعادها الفردية و الاجتماعية فهي أبعاد تقليدية.

و قد تميز القرن العشرين باختراعات هائلة على المستوى التقني و لعل من أهمها و أكثرها توسعا وفائدة ظهور الحاسبات الآلية التي أصبحت لها قيمة لما تحتوي عليه من معلومات يمكن تخزينها واسترجاعها في ثوان معدودات، فقد أصبح النظام الالكتروني في نهاية القرن الماضي من لوازم الحياة الضرورية و المتطورة على المستوى العام و الخاص و الدور الذي تؤديه في مختلف مجالات النشاط حيث تؤثر في الإنسان كيانا و نشاطا ، و لا يخفى أن كل تطور تقني تكون له انعكاساته على المستوى القانوني بصفة عامة و في إطار القانون الجنائي بصفة خاصة فكل المخترعات الحديثة تثير بعض المصالح و الحقوق التي تحتاج إلى الحماية الجنائية لها سواء في إطار النصوص التقليدية أو باستحداث النصوص الملائمة لطبيعتها.

ولقد تطورت الظاهرة الإجرامية في الآونة الأخيرة تطورا مذهلا سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها ،و الذي يتمثل في استعمال آخر ما توصل إليه العلم و تطويعه في خدمة الجريمة [2]، فقد أصبحت المعلومات تجوب العالم في سرعة كبيرة فشبكات المعلومات التي تربط بين الحاسبات الآلية في مختلف أنحاء العالم جعلت اعتماد المعاملات المالية بشكل أساسي على هذه الحاسبات الآلية التي أصبحت مستودع أسرار الأشخاص، سواء تلك المتعلقة بحياتهم الخاصة أو أموالهم أو نشاطهم الاقتصادي ؛ و لهذا لم تتطرق التشريعات العربية إلى جرائم الحاسب الآلي إلا فيما ندر، و لعل السبب في ذلك أن ثورة الحاسب الآلي في البلدان العربية قد بدأت منذ نهاية العقد الأخير في القرن الماضي، و على العكس من ذلك فالبلدان الأوروبية و كندا و الولايات المتحدة الأمريكية يعتمدون على الحاسب الآلي منذ عقدين من الزمن أو أكثر و لذلك بدأت هذه البلدان في تنظيم تشريعاتها لمواجهة هذا النمط الجديد من الجرائم و الذي ظهر مصاحبا لاستخدام الحاسب الآلي و هي الجرائم المسماة "بالجرائم الالكترونية" وإن ثمة تباين كبير بشأن الاصطلاحات

[1] سيد عويس "ظاهرة الجريمة في مجتمعنا المتغير مجلة الأمن العام 1986 العدد 100 ص 27
[2] أحمد ضياء الدين خليل - الظاهرة الإجرامية بين الفهم و التحليل - دار الطويعي للطاعة طبعة 1992/1 ص 256

المستخدمة للدلالة على الظاهرة الجرمية الناشئة في بيئة الحاسب الآلي أو ما يعرف بالكمبيوتر و فيما بعد بيئة الشبكات ؛و هو تباين رافق مسيرة نشأة و تطور ظاهرة الإجرام المتصلة بتقنية المعلومات فابتداء من اصطلاح إساءة استخدام الكمبيوتر مرورا باصطلاح احتيال الكمبيوتر، جرائم الكمبيوتر فاصطلاحات الجريمة المرتبطة بالكمبيوتر جرائم التقنية العالية إلى جرائم الحاسوب أو الاختراقات و جرائم الانترنت و جرائم الكمبيوتر و الانترنت فالجريمة الالكترونية و أخيرا السيبر جرائم.

غير ان اختيار الاصطلاح يتعين أن يزاوج بين البعدين التقني و القانوني فإذا عدنا للحقيقة الأولى المتصلة بولادة و تطور تقنية المعلومات نجد أنها تشمل فرعين جرى بحكم التطور تقاربهما و اندماجهما الحوسبة و الاتصال، أما الحوسبة فتقوم على استخدام وسائل التقنية لإدارة و تنظيم و معالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب و المنطق أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها الدارجة. ومع تزاوج و اندماج وسائل كلا الميدانيين (الحوسبة و الاتصال) ساد التدليل على هذا الاندماج بالتقنية العالية أو بتقنية المعلومات Information Technology و التي تعرفها منظمة اليونسكو UNESCO من بين أشمل تعريفها بأنها "الفروع العلمية و التقنية و الهندسية و أساليب الإدارة الفنية المستخدمة في تداول و معالجة المعلومات، و في تطبيقاتها و المتعلقة بالحواسب و تفاعلها مع الإنسان و الآلات، و ما يرتبط بذلك من أمور اجتماعية و اقتصادية و ثقافية"

أما المنطلق الثاني لدقة اختيار الاصطلاح فيتعين أن ينطلق من أهمية التمييز بين الاصطلاحات المنتمية لما يعرف بأخلاقيات التقنية أو أخلاقيات الكمبيوتر و الانترنت، و بين ما يعرف بإجرام التقنية أو الجرائم الالكترونية ؛ و هو ما يجيب عن التساؤل الرئيسي بشأن الحدود التي ينتهي عندها العبث ,و تلك التي تبدأ عندها المسؤولية عن الأفعال الجنائية ؛ لهذا نجد مثلا أن اصطلاح : إساءة استخدام الكمبيوتر ينتمي لطائفة الاصطلاحات ذات المحتوى الأخلاقي[1].

والمنطلق الثالث الهام برأينا هو أن يكون الاصطلاح قادرا على أن يعبر بقدر الإمكان عن حدود محله فيكون شاملا لما يعبر عنه فلا يعبر عن الجزء ليعني الكل ؛أو يكون العكس مائع الحدود يطال ما لا ينطوي تحت نطاقه . و من هنا فكل اصطلاح وصف الظاهرة بدلالة إحدى جرائم الكمبيوتر كان قاصرا على الإحاطة الشمولية بالمعبر عنه ؛ كاصطلاح احتيال الكمبيوتر أو؛ غش الكمبيوتر أو جرائم التقنية العالية الذي يقصد منها التعبير عن جرائم الكمبيوتر قبل و بعد ولادة و اتساع استخدام الانترنت, و عليه فهي تعابير واسعة الدلالة تحيط بأكثر ما تحتوي عليه ظاهرة الجريمة الالكترونية, أو تلك التي غلبت الطابع الإعلامي على الطابع اللآكاديمي للمصطلح كمصطلح جرائم الياقات البيضاء White collar crime، و لأن الدقة العلمية تقتضي انطباق الوصف على الموصوف، و لأن جرائم الياقات البيضاء تتسع لتشمل أكثر من الجرائم الالكترونية فإنه يتعين معه استبعاد هذا المصطلح ،و كذا المصطلحات التي استخدمت اصطلاح جرائم الكمبيوتر أو الجرائم المرتبطة بالكمبيوتر و شبكة الانترنت للدلالة على التوالي على الأفعال التي يكون الكمبيوتر فيها هدفا للجريمة أو وسيلة لارتكابها.

[1] هدى قشقوش –جرائم الحاسب الالكتروني في التشريع المقارن- الطبعة الأولى دار النهضة العربية القاهرة 1992 ص15

وعليه و تبعا لما تقدم أعلاه فإنه يتضح جليا أن أكثر المصطلحات دلالة على الظاهرة الجرمية ؛و الأكثر شمولية لها هو مصطلح الجريمة أو الجرائم الالكترونية أو ما يعرف ب Cyber crime ؛كي يدرك المتلقي أن كافة الجرائم التي تقع على المعلومات متضمنة في التعبير بمعنى : أنها تشمل جرائم الكمبيوتر بصورها السابقة على ولادة شبكات المعلومات العملاقة التي تجسد الانترنت أكثرها شعبية و شيوعا؛ و كذا بصورها اللاحقة على ولادتها ، و هو المصطلح المستخدم في النطاق الأوروبي عموما و انتشر خارجه ، حيث اعتبر هذا المصطلح شاملا لجرائم الكمبيوتر و جرائم الشبكات ، باعتبار أن كلمة سابير Cyber تستخدم لدى الأكثرية بمعنى الانترنت ذاتها أو العالم الافتراضي ؛في حين أنها أخذت معنى عالم أو عصر الالكترونية بالنسبة للباحثين ، و لم يعد ثمة تمييز كبير في نطاقها بين الكمبيوتر أو الانترنت لما بينهما من وحدة دمج في بيئة معالجة و تبادل المعطيات.

إذا ثمة مقبولية و مبررات لاستخدام اصطلاح الجريمة الالكترونية Cyber crime .والذي تنقسم في نطاقه الجرائم إلى طوائف بحيث تشمل الجرائم التي تستهدف النظم و المعلومات كهدف (المعنى الضيق لجرائم الكمبيوتر) و الجرائم التي تستخدم الكمبيوتر وسيلة لارتكابها أو الجرائم المتعلقة بمحتوى مواقع الالكترونية و بيئتها (جرائم الانترنت حصرا أو السيبر Cyber بالمعنى الضيق).

أهمية موضوع البحث:

يرجع اختيارنا لهذا الموضوع للتعريف بظاهرة جديدة هي "الجريمة الالكترونية" التي بدأت في الظهور و الانتشار ؛وارتبطت بتكنولوجيا متطورة هي تكنولوجيا الحاسبات الآلية ، مما أسفر عن تميزها بمجموعة من الخصائص تختلف عن غيرها من الجرائم ؛مما يستتبع ضرورة التعامل معها بما يتلاءم مع هذه الخصوصية.

ولما كانت هذه الجرائم ترتبط بتقدم المجتمعات فكلما ازداد اعتماد المجتمع على الحاسبات الآلية كلما كان ذلك إيذانا بزيادة معدل جرائم الالكترونية، كان لزاما أن يواكب هذا التقدم فهما كاملا للجريمة الالكترونية و كيفية مواجهتها سواء من الناحية التقنية و هو عمل المتخصصين في مجال تكنولوجيا المعلومات، أو من الناحية القانونية و هي مهمة المشتغلين بالقانون.

ولقد زاد من أهمية البحث صعوبة تطبيق النصوص التقليدية على هذه الجرائم ، وهو ما دفع العديد من الدول إلى التدخل التشريعي لمواجهة الجريمة الالكترونية ؛لذا فإن إدراك ماهية هته الجريمة و الطبيعة الموضوعية لها و استظهار موضوعها و خصائصها و مخاطرها و حجم الخسائر الناجمة عنها و سمات مرتكبيها و دوافعهم و أنواعها و جزاءاتها يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة.

وإذا كان مجتمعنا الجزائري لم يتأثر بعد بشكل ملموس فعلا بمخاطر هذا النمط المستجد من الإجرام؛ فإن خطر الجريمة الالكترونية المحتمل في بيئتنا يمكن أن يكون كبيرا باعتبار أن الجاهزية التقنية و التشريعية و اللآدائية (استراتيجيات حماية الالكترونية) لمواجهتها ليست بالمستوى المطلوب إن لم تكن غائبة تماما.

وفيما يخص **الإشكالية الأساسية** فتتمثل في إبراز الأسباب الحقيقية التي ظهرت بظهور الالكترونية في نطاق القانون الجنائي وقانون الإجراءات الجزائية ؛ خاصة فيما تعلق منها بطبيعة المال الالكتروني، باعتباره

مالا معنويا؛ في حين أن الحماية الجزائية للمعلوماتية يقتصر في أغلب الدول على المال المادي، إضافة إلى تكييف المنقول فيما يخص المعلومات، وقصور قواعد الإجراءات الجزائية في مواجهة الإجرام الإلكتروني خاصة ما تعلق منها بالأعمال المصرفية و ما مدى كفاية النصوص القانونية الحالية لمنع الجريمة الالكترونية وردع مرتكبيها ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهـــرة.ثم من جهة أخرى هل تفي نصوص الإجراءات الجزائية في تحقيق غايتها؟

أم يلزم تعديل هذه النصوص بما يتلاءم مع التطور التقني للمعلوماتية؟. وعلى الرغم مما يكتف هذا الموضوع من صعوبات تتمثل أساسا في حداثته و اتصاله بتكنولوجيا المعلومات و الحاسبات الآلية و ندرة المراجع في المكتبة العربية و نقص التطبيقات القضائية الجزائرية فإنه تم اختيارنا له إذ حاولنا تعويض هذه النقائص بما توصلنا إليه من مراجع باللغات الأجنبية – الانجليزية و الفرنسية و التشريعات و التطبيقات القضائية في دول أخرى ذاع فيها استعمال الحاسبات الآلية و تقنية المعلومات، وبالتالي فنحن لا ندعي أننا سوف نحيط بكافة أسباب وجوانب وعناصر هذه الظاهرة ولا أننا سوف ندرس تفاصيل كل ما سنتعرض إليه من موضوعات. غير أننا سنحاول إبراز أهم عناصر هذا الموضوع وذلك بأسلوب ومنهج تحليلي نبدأ فيه بتعريف الجريمة الالكترونية وتبيان ميزاتها الأساسية و دوافع ارتكابها لنصل إلى نظريات و أسس تصنيف طوائف و أنواع الجرائم الإلكترونية أحاط بالجريمة الإلكترونية شأنها في ذلك شأن كل ظاهرة جديدة الكثير من التساؤلات التي تتعلق بتحديد مفهومها، وخصائصها و التمييز بينها و بين ما يقترب منها من ظواهر ، و بتحديد حجم هذه الظاهرة و معرفة العوامل المختلفة التي تتدخل في هذا التحديد ؛و الحقيقة أن تحديد مفهوم الجريمة الالكترونية و تحديد حجمها هو خطوة أولى للتعرف على هذه الظاهرة من جميع جوانبها القانونية.

وسوف نحاول من خلال هذهالمداخلة إلقاء الضوء على تعريف الجريمة الالكترونية و كذا خصائصها و ذلك في المبحث الأول لنتطرق في المبحث الثاني إلى أسباب ودوافع ارتكابها لنصل أخيرا إلى نظريات وأسس تصنيف طوائف وأنواع الجرائم الالكترونية وهو الأمر الذي سنتناوله بالدراسة.

المبحث الأول : تعريف الجريمة الالكترونية و خصائصها

تعددت تعريفات الجريمة الالكترونية و تباينت فيما بينها ضيقا و اتساعا و قد أسفر ذلك عن تعذر إيجاد فهم مشترك لظاهرة الجريمة الالكترونية، وما يستتبع ذلك من تسهيل التوصل إلى الحلول المناسبة لمواجهتها. و سوف نحاول من خلال هذا المبحث الوصول إلى تعريف يتلاءم مع طبيعة الجريمة الالكترونية لننتقل بعد ذلك إلى خصائص هذه الجريمة.

المطلب الأول : تعريف الجريمة الالكترونية

تعرف **الجريمة** عموما في نطاق القانون الجنائي العام بأنها سلوك الفرد عملا كان أو امتناعا يواجهه المجتمع بتطبيق عقوبة جزائية ،و ذلك بسبب الاضطرابات التي يحدثه في النظام الاجتماعي [1]؛و هو التعريف الذي يستند على عناصر الجريمة إلى جانب بيانه لأثرها (السلوك، و السلوك غير المشروع وفق القانون الإرادة الجنائية و أثرها. العقوبة أو التدبير الذي يفرضه القانون) ؛و هي الأوصاف التي تميز بين الجريمة عموما ،و بين الأفعال المستهجنة في نطاق الأخلاق أو الجرائم المدنية أو التأديبية.

أما مصطلح **الالكترونية** فهو مشتق من كلمة المعلومات (Informatique)، و هي الكلمة التي شاع استعمالها منذ خمسينات القرن الماضي في مجالات مختلفة و سياقات شتى مما جعل لها في الاستعمال الدارج مفاهيم متنوعة[2] .

فالمعلومة لغويا مشتقة من كلمة "علم" ،و دلالتها فيها و تدور بوجه عام حول المعرفة التي يمكن نقلها أو اكتسابها [3]،و قريب من ذلك إشارتها في اللغة الفرنسية إلى فحوى عمليات الاتصال التي تستهدف نقل و توصيل إشارة أو رسالة أو الإعلام عنها و اتخاذ وظيفتها في نقل المعارف.

والمعلومات في اللغة الانجليزية و الألمانية و الروسية تعني كلمة (Information) اللاتينية الدالة بحسب الأصل على شيء للابلاغ و التوضيح ،أو على عملية " Process " الابلاغ أو النقل أو التوصيل و هو نفس ما يعنيه لفظ " Xinxi " المقابل لها في اللغة الصينية[4].

أما اصطلاحا فهناك المئات من التعريفات التي أدلى بها باحثون من تخصصات و ثقافات مختلفة لفهم و إدراك المعنى المراد بمصطلح "المعلومات" إذا ما استخدم الاتصال العلمي بغير تحديد.

ولا يوجد إلى يومنا هذا نص قانوني يعطي تعريفا جامعا مانعا للمعلومة ؛غير أن القانون الفرنسي الصادر في 29 يوليو 1982 الخاص بالاتصالات السمعية و البصرية أشار إلى تعريف عام للمعلومة حيث ينظر إليها بوصفها "رنين أو صور أو وثائق أو بيانات أو رسائل من أي نوع " Sons, images, documents, données ou messages de toute nature" ،و يعرف الأستاذ Catala المعلومة بأنها "رسالة ما معبر عنها بشكل يجعلها قابلة للنقل أو الإبلاغ للغير" [5]، و يعرفها البعض الأخر بأنها "رمز أو مجموعة رموز تنطوي على إمكانية الإفضاء إلى معنى"[6].

وسيتخلص مما ذك رأعلاه من تعريفات أن المعلومة هي "مجموعة رموز يستخلص منها معنى معين في مجال محدد ،و تتمتع بالتحديد ،و الابتكار ،و السرية ،و الاستئثار". و بالنظر إلى المعلومة باعتبارها نتاج نشاط

---

[1] أحسن بوسقيعة – الوجيز في القانون الجزائي العام – الطبعة الثالثة 2006 ، دار هومه ص 3 عن
g .stéfani ;g.levasseur ;b.bouloc : droit général DALLOZ ;17éme édition P.5 .

[2] عزة محمود أحمد خليل –مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي- دراسة مقارنة في القانون المدني و الشريعة الاسلامية – رسالة دكتورا- مقدمة لكلية الحقوق 1994 ص18 .

[3] المعجم الوسيط "أعلم فلان بالخبر :أخبره به.....و أعلم فلانا الأمر؛جعله يعلمه ،و في لسان العرب العلم يفيض الجهل و علمت الشيءأعلمه علما عرفته وفي مختار الصحاح علم الشيء عرفه.....(استعمله) الخبر (أعلمه) اياه .

[4] أحمد خليفة الملط – الجرائم المعلوماتية –دار الفكر الجامعي – الطبعة الثانية 2006 ص72 .

[5] Piérre CATALA « la propriété de l'information » Cité par f.Toubal ;le logiciel- analyse juridique FUDUL .L.G.D.J.1986 P 126-127 .

[6] هشام فريد رستم –جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة- بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة و معاملة المجرمين –مجلة الأمن العام العدد 151-1995 ص24 .

إنساني فإنه يجب أن يتوفر فيها عنصران أساسيان **أولهما** التحديد و الابتكار و **ثانيهما** السرية و الاستئثار، إذ أن المعلومة المحددة هي التي يمكن فقط حصرها في دائرة خاصة بها؛ و أن الاعتداء على القيم يفترض دائما أن يقع على شيء محدد يكون محلا لحق محدد، و يجب أن تكون المعلومة مبتكرة و سرية كون السرية صفة لازمة تحصر حركة الرسالة و تحمل المعلومة في دائرة محددة من الأشخاص ، فلا يمكن تصور الجرائم الخاصة بالسرقة و النصب و خيانة الأمانة إذا انعدم هذا الحصر لأن المعلومة غير السرية تقبل التداول، و من ثم تكون بمنأى من أي حيازة ،أما الاستئثار فهو أمر ضروري لأنه في جميع الجرائم التي تنطوي على اعتداء قانوني على القيم سيتأثر الفاعل سلطة تخص الغير وعلى نحو مطلق[1].

ففي أول السبعينات ازدهرت صناعة جديدة أطلق عليها **صناعة المعلومات**، و أصبحت مصدرا للثروة و تتصف بعظمة التعقيد التقني و ضخامة ما يستثمر فيها من أموال، و أصبحت مقياسا لتقدم الأمم [2]، و مصدرا للقوة الاقتصادية و السياسية و العسكرية ،و موردا لا يقل و لا ينصب ،تتزايد دوما و لا تتناقص بالاستخدام، و لا تستهلك ،و ترتبط بالزمان و المكان ،و تتفاعل مع التطور ،و هي في الحقبة المعاصرة مفتاح للموارد الأخرى و سلعة و خدمة تباع و تشتري ،و مصدر قوة اقتصادية و سياسية لمن يحسن جمعها و تنسيقها و استخدامها لارتباطها بمختلف مجالات النشاط الإنساني و تداخلها في كل جوانب الحياة المعاصرة، و أصبح توفيرها و حسن استغلالها من الأسس الضرورية لدفع عجلة التقدم في الأمم و المجتمعات ،و صار تدفقها و انسيابها بمثابة النبض و العصب لجهود التنمية و التحديث و الرقي المعرفي و الحضاري و بات الوعي بأهميتها مظهرا و مقياسا لتقدم الدول[23].

وتماشيا مع ما ذكر أعلاه فإن **الالكترونية "هي علم المعالجة العقلية للمعلومات باستخدام آلات تعمل ذاتيا".**

ولعل المشكلة الأولى و الأساسية التي تعترض ظاهرة الجريمة الالكترونية هي عدم وجود تعريف مجمع عليه لهذه الجريمة، و إن بذلت من أجل ذلك عدة محاولات اتجهت بعضها إلى التضييق من مفهوم هذه الجريمة ؛بتقليل الحالات التي يمكن أن يتصف النشاط الإجرامي بها، و البعض الآخر ذهب إلى التوسيع من مفهوم الجريمة الالكترونية حتى أنه يمكن القول أنه يدخل في عدادها في كثير من الأحيان أفعال لا يمكن أن تعد من قبيل جرائم الحاسب الآلي.

فمصطلح الجريمة الالكترونية مزيج بين مصطلحي " **الجريمة و الالكترونية** " و لعل **تعريف منظمة التعاون الاقتصادي و التنمية الخاص باستبيان الغش الالكتروني** عام 1982 و الذي أوردته بلجيكا في تقريرها بأن الجرائم الالكترونية هي " " ***كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية و المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الالكترونية*** "[4]إذ أن هذا التعريف يتسم بالوضوح؛ هذا فضلا عن تحديده لماهية السلوك الإجرامي للجريمة التي قد تقع به، إذ شمل كلا من الفعل الإيجابي و السلوك السلبي المتمثل في الامتناع ؛و ربط أيضا بين موضوع مذكرة تخرجنا المتعلقة بالاعتداء على المال المعنوي

[1] أحمد خليفة الملط – المرجع السابق – ص76 .
[2] هشام فريد رستم - المرجع السابق - ص23 .
[3] هشام فريد رستم- المرجع السابق - ص33 .
[4] نائلة عادل محمد فريد قورة -جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية- منشورات الحاتي الحقوقية 2005 ص32.

(المال الالكتروني) عن طريق استخدام الأنظمة الالكترونية و المعلومات و هو تعريف أكثر شمولا مما سبقه من تعريفات إذ أنه راعى عدة اعتبارات أهمها :

1) تلاؤم هذا التعريف مع فكرة عالمية المعلومات و الاتصالات ؛إذ أنه تعريف مقبول و مفهوم على المستوى العالمي.
2) مراعاة التعريف للتطور المتلاحق لتكنولوجيا الحاسبات الآلية بصفة خاصة ،بحيث لا يقتصر على التكنولوجيا الراهنة ،بل يسمح باستيعاب ما قد يجد من صور للجريمة الالكترونية نتيجة تطور المعلومات.
3) و أخيرا لما كانت الجريمة الالكترونية يمكن أن تنطوي على أشكال مختلفة للسلوك الإجرامي ابتداء من القتل إلى الاعتداء على حرمة الحياة الخاصة فيجب أن يوضح التعريف خصوصية الجريمة الالكترونية ؛بحيث يبدو واضحا الدور الذي يقوم به الحاسب الآلي و المعلومات في ارتكاب الجريمة[1].

المطلب الثاني : خصائص الجريمة الالكترونية

تتميز الجريمة الالكترونية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية؛ و ذلك نتيجة ارتباطها بتقنية المعلومات و الحاسب الآلي مع ما يتمتع به من تقنية عالية ،و قد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات و الحقائق؛ و التي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف **بالمجرم الالكتروني** لتميزه أيضا عن المجرم التقليدي ،و قد كان لظهور شبكة المعلومات و تطورها إلى الصورة التي أصبحت عليها الآن فيما يعرف بالانترنت أثره في إعطاء شكل جديد للجريمة الالكترونية؛ و لعل أهم ما أضفته شبكة المعلومات على الجريمة الالكترونية هو الطبيعة الدولية أو متعددة الحدود. و سوف نحاول فيما يلي التطرق إلى بعض السمات الخاصة بالجريمة الالكترونية ثم سنتناول بالدراسة أهم السمات التي تميز المجرم الالكتروني.

الفرع الأول : السمات الخاصة بالجريمة الالكترونية

تتميز الجريمة الالكترونية بصفة عامة عن الجريمة التقليدية في عدة نواح، سواء كان هذا التمييز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة.

أولا : خصوصية الجريمة الالكترونية : تتسم الجريمة الالكترونية بصعوبة اكتشافها و إثباتها ؛و يرجع ذلك إلى عدة أسباب من بينها :

- وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد. بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقد ثقة عملائهم؛ فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة [2]. فعلى سبيل المثال أحصت وزارة الداخلية في فرنسا عام 1986 حوالي 1200 جريمة معلوماتية في حين كان هناك حوالي 53600 جريمة ضد الأشخاص و 18900 جريمة تندرج تحت وصف جرائم الآداب و 3 مليون جريمة ضد

[1] هشام فريد رستم –المرجع السابق- ص 33 .
[2] نائلة عادل محمد فريد قورة- المرجع السابق- ص49

الأموال، و في أحدث تقارير مركز شكاوى احتيال الانترنت (IFFC) الأمريكي أظهر التحليل الشامل للشكاوى التي قدمت للمركز خلال سنة 2004 قد بلغت 6348 شكوى من ضمنها 5273 حالة تتعلق باختراق الكمبيوتر عبر الانترنت و 814 تتعلق بوسائل الدخول و الاقتحام الأخرى كالدخول عبر الهاتف أو الدخول المباشر إلى النظام بشكل مادي؛ مع الإشارة إلى أن هذه الحالات هي فقط التي تم الإبلاغ عنها و لا تمثل الأرقام الحقيقية لعدد حالات الاحتيال الفعلي[1].

- وفي مقابل انخفاض نسبة جرائم الالكترونية في مواجهة الجرائم التقليدية ؛ترتفع الخسارة الناجمة عن الجرائم الالكترونية بصورة كبيرة بالمقارنة بغيرها من الجرائم، فعلى سبيل المثال كانت الخسارة الناجمة عن 8000 حالة سرقة بالإكراه في فرنسا عام 1986 حوالي 561 مليونا من الفرنكات الفرنسية FF ؛في حين يتضاعف هذا الرقم في حالة الجرائم الالكترونية على الرغم من انخفاضها نسبة 8 مرات عن حالات السرقة بالإكراه؛و في الولايات المتحدة الأمريكية توصل مكتب التحقيقات الفيدرالية F.B.I. إلى أن متوسط الخسائر التي تحققها الجريمة الالكترونية يبلغ حوالي 500.000 دولار $ في حين لا تزيد الخسائر التي تخلفها جرائم السرقة العادية عن 3500 $[2].
- وفي المقابل فانه وعلى غرار الآراء التي تتجه إلى القول بأن الجريمة الالكترونية لا يوجد شعور حقيقي بعدم الأمان في مواجهتها ،أو أنه لا يوجد شعور عام بعدم أخلاقية هذه الأفعال ؛فإننا لا نتفق مع هته الآراء إذ أن الجريمة الالكترونية لا تختلف عن غيرها من الجرائم من حيث اعتدائها على مصالح لها أهميتها لدى أفراد المجتمع ؛و من ثم تستحق الحماية القانونية كون أن مساس هذه الأفعال بهذه المصالح هو الذي يبرر تجريمها.

ثانيا : الطبيعة المتعدية الحدود(الدولية) للجريمة الالكترونية :

يمكن القول أن من أهم الخصائص التي تميز الجريمة الالكترونية هي تخطيها للحدود الجغرافية ،و من اكتسابها طبيعة دولية ،أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعددة الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل و تبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال ؛قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة الالكترونية الواحدة في آن واحد ،كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة الالكترونية و حجم المعلومات و الأموال المستهدفة و المسافة التي قد تفصل الجاني عن هذه المعلومات و الأموال، قد ميزت الجريمة الالكترونية عن الجريمة التقليدية بصورة كبيرة[1].

ولقد أثارت الطبيعة الدولية للجرائم الالكترونية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي ؛أم تلك التي توجد بها المعلومات محل الجريمة؛ أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب ،كما أثارت هذه الطبيعة أيضا الشكوك حول مدى

[1] هدى قشقوش -جرائم الحاسب الالكتروني في التشريع المقارن -الطبعة الأولى دار النهضة العربية القاهرة 1992 ص53
[2] نائلة عادل محمد فريد قورة المرجع السابق ص50

[1]P83 Related crime on computer Recommandation N R89 – 9 The

فاعلية القوانين القائمة في التعامل مع الجريمة الالكترونية و بصفة خاصة فيما يتعلق بجمع و قبول اللأدلة [1] ؛و لذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم الالكترونية و العمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم ،فيجب أن يشمل هذا التعاون تبادل المعلومات ، تسليم المجرمين ،و ضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى ،كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة الالكترونية ،و هو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، و تعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "**إبرام الاتفاقيات الدولية**".

وتعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي الالكترونية و تجنب خلق ما يسمى "بجنة جرائم الالكترونية" Computer Crime Havens ، إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي بطبيعة الحال التنسيق بين قوانين الدول المختلفة لضمان تحقق "مبدأ ازدواجية التجريم" فيما يتعلق بجرائم الالكترونية.

ونجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم. و إن كان مشرعنا قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون 15/04 المعدل و المتمم للأمر 156/66 المتضمن قانون العقوبات. و الذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة الالكترونية في المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.

ونخلص مما سبق إلى أنه في سبيل مكافحة الجريمة الالكترونية يجب أن تتحرك الدول المختلفة في محورين :

- **الأول : داخلي** بحيث تتلاءم تشريعاتها الداخلية مع هذا النمط الجديد من الجرائم.
- **الثاني : دولي** عن طريق عقد الاتفاقيات الدولية، حيث لا يستفيد مجرمو الالكترونية عن عجز التشريعات الداخلية من ناحية ،و غياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم من ناحية أخرى.

الفرع الثاني : السمات الخاصة بالمجرم الالكتروني

لم يكن لارتباط الجريمة الالكترونية بالحاسب الآلي أثره على تمييز الجريمة الالكترونية عن غيرها من الجرائم التقليدية فحسب ،و إنما كان له أثره أيضا على تمييز المجرم الالكتروني عن غيره من المجرمين.و لقد اختلف الباحثون في تحديد هذه السمات، و يعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا بالجريمة الالكترونية بصفة عامة ؛و بالمجرم الالكتروني بصفة خاصة. إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه. فكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء. و إن كانت – في رأيه– لا تتطابق معها.

فالمجرم الالكتروني من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه على درجة من العلم و المعرفة (و إن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو

[1] نائلة عادل محمد فريد قورة -المرجع السابق- ص54.

الحال في جرائم ذوي الياقات البيضاء [1]) . كما يتفق مجرمو الالكترونية مع ذوي الياقات البيضاء في أن الفاعل في الحالتين يبرر جريمته ، بل إنه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق.

ويتميز المجرم الالكتروني كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين و يرمز إليها الأستاذ Parker بكلمة S.K.R.A.M و هي تعني :

- المهارة Skills،
- المعرفة Knowledge،
- الوسيلة Resources،
- السلطة Anthority،
- و أخيرا الباعث Motives [2].

وتعد **المهارة :** المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم الالكتروني، و التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال ،أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات ،أو بمجرد التفاعل الاجتماعي مع الآخرين. إلا أن ذلك لا يعني ضرورة أن يكون المجرم الالكتروني على قدر كبير من العلم في هذا المجال. بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي الالكترونية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أما **المعرفة:** فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها و إمكانيات نجاحها واحتمالات فشلها. إذ أن المجرم الالكتروني باستطاعته أن يكون تصورا كاملا لجريمته. كون المسرح الذي تمارس فيه الجريمة الالكترونية هو نظام الحاسب الآلي. فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها و ذلك قبل تنفيذ جريمته.

أما **الوسيلة:** فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم الالكتروني فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة و بسهولة الحصول عليها.

أما **السلطة:** فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم الالكتروني و التي تمكنه من ارتكاب جريمته ؛قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات و التي تعطي الفاعل مزايا متعددة كفتح الملفات و محو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها. وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات. وقد تكون هذه السلطة

[1] Suthreland (Eduin H) "White collar criminality " Gers (Gilbert) in white collar criminal The offender in business the professions atherton press 1968

[2] Parker (Donn B) Figding computer crime A neur Framework for protecting information 1998/P 114

في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات. و قد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

وأخيرا يأتي **الباعث** وراء ارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى ،فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة الالكترونية[1] ، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب و تخطي حواجز الحماية المضروبة حوله، و أخيرا الانتقام من رب العمل أو أحد الزملاء, حيث يفرق مرتكبي هذه الجرائم بين الأضرار بالأشخاص الأمر الذي يعدونه غاية اللاأخلاقية ،و بين الاضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم، و هو ما يطلق عليه أعراض روبن هود The Roben Hood Syndrome [2].

المبحث الثاني : أسباب ارتكاب الجريمة الالكترونية

الدافع الباعث الغرض أو الغاية تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي. تتصل بما يعرف بالقصد الخاص في الجريمة ، وللجريمة الالكترونية عدة دوافع على ارتكابها فبعضها يرجع إلى دافع شخصي و منها ما يرجع إلى دافع خارجي و منها ما يكون خاصا بالمنشأة. و كل هذه الدوافع قد تكون مصدرها هو الرغبة الإجرامية؛ و سنتعرض لكل دافع في مطلب على حدى.

المطلب الأول : الدوافع الشخصية

منذ بداية الظاهرة فإن الدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر و فيما بعد احتيال الإنترنت هو تحقيق الكسب المالي، ففي دراسة الفقيه Parker الصادرة في إحدى مجلات المتخصصة بخصوص موضوع الأمن الالكتروني تبين أن[3] :

1- 34% من جرائم الغش الالكتروني من أجل اختلاس الأموال.

2- 23% من أجل سرقة المعلومات.

3- 19% من أجل الإتلاف.

4- 15% من أجل سرقة وقت الحاسوب لأغراض شخصية .

وإذا انتقلنا للدراسات الحديثة، فسنجد أن هذا الدافع يسود على غيره و يعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية، و في مقدمة هذه الدراسات المسحية و الإحصائية الدراسات و التقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية N.F.I.C.

وهناك فئة من مرتكبي الجرائم الالكترونية يرجع ارتكابهم لها إلى الديون الناتجة من المشاكل العائلية و الخسائر الضخمة من ألعاب القمار أو إدمان المخدرات، فقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه الحالات، فالغاية تبرر الوسيلة[4].

---

[1] و يرى البعض أن أغلب مجرمي المعلوماتية ليس لديهم أطماع مادية بقدر ما يحاولون حل مشكلات مادية تواجههم لا يستطيعون حلها باللجوء إلى الجرائم الأخرى أنظر précédent p142 Parker (DonnB)ouvrage

[2] هشام محمد فريد رستم- المرجع السابق- ص38

[3] G.Delmare, sécurité informatique Ressource informatique N° 1 juill

[4] أحمد خليفة ملط -المرجع السابق -ص 89

الفرع الثاني : الدوافع الذهنية أو النمطية

غالبا ما يكون الدافع لدى مرتكب الجرائم الالكترونية هو الرغبة في إثبات الذات و تحقيق انتصار على تقنية الأنظمة الالكترونية دون أن يكون لهم نوايا آثمة، و يرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام الالكتروني لارتكاب تلك الجرائم.و عليه فإنه يرى البعض: "أن الدافع إلى ارتكاب الجرائم الالكترونية يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح"[1]، و مع أن الدراسات لا تظهر هذه الحقيقة على إطلاقها إذ يظهر السعي إلى تحقيق الربح دافعا أكثر تحريكا لجرائم الحاسوب من الرغبة في قهر النظام إلا أن الدافع الأخير يتجسد في نسبة مرتفعة من جرائم الحاسوب خاصة ما يعرف بأنشطة "HACKERS" المتطفلين الداخليين [2] على النظام و المتجسدة في جرائم التوصل مع أنظمة الحاسب تحديدا عن بعد.

المطلب الثاني : الدوافع الخارجية

في بعض المواقف يتأثر الإنسان و يستسلم للمؤثرات و الدوافع الخارجية بارتكابه بعض الجرائم الالكترونية، و نتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توافر هذه المؤتمرات، فان الأمر يؤول في النهاية الى ارتكابه لجريمة الالكترونية،هذا و تتعدد المؤثرات التي تدفع الإنسان إلى اقتراف مثل هذا السلوك سواء كان بدافع الانتقام،جنون العظمة،التعاون و التواطؤ على الأضرار و التهديد.

الفرع الأول : دافع الانتقام و إلحاق الضرر برب العمل

قد يكون الانتقام مؤثرا في ارتكاب تلك الجرائم،و مثال ذلك قيام محاسب شاب بالتلاعب بالبرامج الالكترونية بإحدى المنشآت بحيث بعد رحيله من المنشأة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات و ديون المنشأة[3] ،و لقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل و المشكلات المالية و من طبيعة علاقات العمل المنفردة في حالات معنية، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة،مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب،باعثها الانتقام من المنشأة أو رب العمل.

وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيسي و الغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لارتكاب الجريمة.

الفرع الثاني : الرغبة في قهر النظام و التفوق على تعقيد و سائل التقنية

يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم و مستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجاد و غالبا ما يجدون الوسيلة الي تحيطها، و يتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي الجرائم الالكترونية الذين يمضون وقتا طويلا أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب و شبكات المعلومات لإظهار تفوقهم على وسائل

[1] أحمد خليفة ملط -المرجع السابق -ص 90

[2] حسب ترجمة غرفة التجارة العربية البريطانية،و الحادق المأجور حسب ترجمة الأستاذ كامل سعد

[3] أنظر comment se protéger contre le crime informatique. temps réels P264-1984

التقنية ،و إن هذا الدافع هو أكثر الدوافع التي يجري استغلالها قبل المنظمات الجرمية (مجموعات الجريمة المنظمة) لأجل استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة.هذا و إن كان الفعل الواحد قد يعكس دوافع متعددة و خاصة، فمحرك أنشطة الإرهاب الالكتروني و حروب المعلومات دوافعه سياسية و إيديولوجية ،في حين أن أنشطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة، و قد تتداخل و تشترك هته الدوافع في الفعل الواحد فتتمازج دون إمكانية التفرقة بينها.

ويمكننا أخيرا أن نضع التصور "الرياضي" التالي لدوافع بعض الهجمات الشائعة في حقل جرائم الالكترونية :

- ❖ حروب المعلومات و الإرهاب الالكتروني = دوافع سياسة أو فكرية
- ❖ إنكارالخدمة للمواقع التجارية و الخدمة = التحدي و قهر النظام + أفعال ثارية وأحقاد موظفين + التنافسية بأنشطة غيرمشروعة
- ❖ احتيال الكمبيوترواحتيال الانترنت = استيلاء على المال أو المنافع و تحقيق الربح
- ❖ الاستيلاء على المعلومات = التنافسية + ابتزاز الأفراد و تحقيق المكاسب + المنافع المالية + الأفعال الثارية + الإعداد للهجمات ذات الدوافع المالية
- ❖ إتلاف المعطيات وتخزين الأنظمة = الأحقاد والدوافع الثارية + إخفاء أنشطة جريمة أخرى + التنافسية غيرالمشروعة + التحدي وتحديدا بالنسبة لبرامج الفيروسات.

1. المرحلة الأولى:

بظهور استخدام الكمبيوتر و ربطه بالشبكة في الستينات إلى السبعينيات ،ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة و تدمير أنظمة الكمبيوتر و التجسس الالكتروني ،و شكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة جرمية مستجدة ؟و هل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال الالكترونية؟ ، فبقيت محصورة في إطار السلوك اللااخلاقي دون النطاق القانوني و مع توسع الدراسات تدريجيا و خلال السبعينات بدا الحديث عنها كظاهرة إجرامية جديدة.

2. المرحلة الثانية:

و في الثمانينات ظهر نوع جديد من الجرائم ارتبط بعمليات اقتحام نظم الحاسوب عن بعد و نشر الفيروسات عبر شبكات الكمبيوتر ،الذي سبب تدمير الملفات و البرامج أين شاع اصطلاح ﴿الهاكرز﴾، المعبر عن مقتحمي النظم [1]،و بقي دائما الحديث عن دوافع هذه الجرائم محصور في اختراق امن المعلومات و إظهار التفوق التقني من قبل مرتكبي هذه الأفعال الذين لم يتعدوا فئة صغار السن العباقرة في هذا المجال ، لكن بتزايد خطورة هذه الممارسات أصبح من الضروري إعادة تصنيف الفاعلين و تحديد طوائفهم خاصة بعد تحول الجريمة من مجرد مغامرة و إبداء التفوق إلى أفعال تستهدف التجسس و الاستيلاء على البيانات الاقتصادية و الاجتماعية و السياسية و العسكرية .

3. المرحلة الثالثة:

[1] عبد الفتاح مراد :شرح جرائم الكمبيوتر و الانترنت.http://mourad_dr.tripad.com

شهدت التسعينيات تطورا هائلا في مجال الجرائم التقنية و تغيرا في نطاقها و مفهومها ،بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة و اقتحام شبكات المعلومات ،أين أصبحت مواقع الانترنت التسويقية النشطة، أكثر عرضة للهجمات التي ظهرت بسببها أنماط جديدة من الجرائم ،مثل أنشطة إنكار الخدمة، أساسها تعطيل نظام تقني و منعه من القيام بعمله المعتاد، و الذي يرتب انقطاع النظام عن الخدمة لساعات، فينتج عنه خسائر مالية بالملايين ،كما توسعت جرائم نشر الفيروسات عبر شبكة الانترنت ، لما تسهله من وصولها إلى ملايين المستخدمين في نفس الوقت ، ليفتح الباب على مصراعيه لمختلف الأفعال الغير السوية المتطورة بتطور التقنية.

و قد سجلت عبر هذه المراحل مجموعة من القضايا منها سنة 1988 قضية" موريس الشهيرة " أين تم نشر فيروس الكتروني عرف ب : "دودة موريس" عبر ألاف الكمبيوترات من خلال الانترنت ،و في عام 1995 تم هجوم عرف باسم: "IP-SPOOFING "ا لذى أدى لوقف عمل أجهزة أصلية و تشغيل أخرى وهمية، لتبرز قضية الجحيم العالمي التي اختص بها مكتب التحقيقات الفدرالية لتمكنها من اختراق موقع البيت الأبيض الأمريكي ، لتليها الكثير من الحوادث كحادثة شركة اوميغا،فيروس مليسا،و غيرها التي سنحاول التطرق لبعضها في المطالب الموالية.

التحويل الالكتروني الغير المشروع للاموال :

يتم ولوج مخترقي الشبكات الى بيانات حساب الاخرين، من خلال الحصول على كلمة السر المدرجة في ملفات انظمة الكمبيوتر الخاصة بالمجني عليه ، مما يسمح للجاني بالتوغل في النظام الالكتروني وعادة ما يكون هؤلاء من العاملين على ادخال البيانات في ذاكرة الجهاز او من قبل المتواجدين على الشبكة اثناء عملية تبادل البيانات و تتم عملية التحويل الالكتروني للاموال باحد الطرق الموالية :

1 **الاحتيال " النصب ":**

يتم ذلك بطرق احتيالية يوهم من اجلها المجني عليه بوجود مشروع كاذب او يحدث الامل لديه بحصول ربح، فيسلم المال للجاني بطريق معلوماتي اومن خلال تصرف الجاني في المال، وهو يعلم ان ليس له صفة التصرف فيه، و قد يتخذ اسم او صفة كاذبة ، تمكنه من الاستيلاء على مال المجني عليه فيتم التحويل الالكتروني للاموال ،و ذلك من خلال اتصال الجاني بالمجني عليه عن طريق الشبكة او يتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعده في ايهام الحاسب و الاحتيال عليه فيسلمه النظام المال .

ويرى الدكتور محمد سامي شوا: انه لا يوجد أي اشكال عندما يكون الاستلاء على الاموال ناشىء عن التلاعب في البيانات المدخلة او المختزنة في النظام او برامجه من قبل شخص، ليستخرج باسمه او اسم شركائه شكات او فواتير بمبالغ غيرمستحقة، لكن يثور الاشكال عندما يكون محل الاستيلاء نقود كتابية او بنكية عن طريق القيد الكتابي ، باعتبار ان الارصدة او فوائدها لا تعد منقولات فكيف يتم الاستلاء عليها وتحويلها نتيجة تلاعب ببيانات الحاسب الالي و بالتالي الاستلاء المادي على المال .

ومن اجل ذلك ذهب معظم التشريعات التي اعتبار هذه الارصدة بمثابة ديون لا يمكن ان تكون محلا للاختلاس،رغم ان بعض الدول اعتبرتها اموال وتصلح ان تكون محلا للتحويل، خاصة امام ما يحققه ذلك من ربح للجاني وخسارة فادحة للمجني عليه،منها الولايات المتحدة التي أصدرت عدة قوانين اعتبرت من خلالها الأموال الكتابية او البنكية عبارة عن اموال ،كذلك في الجزائر فان المستندات و الأوراق المالية تعد من الأموال ، بينما في التشريع الفرنسي ، فقد ابتكر نظرية التسليم العـادل la théorie remise par équivalent و التي أقرتها محكمة النقض الفرنسية و بموجب أصبح نص المعاقب على الاحتيال و النصب التقليدي " المادة 313 قانون فرنسي جديد " تنطبق على جميع أفعال التلاعب في البيانات المنقولة عبر شبكة الانترنت و التي تؤدي الى الغاء رصيد مدين او خلق رصيد دائن بمبالغ غير مستحقه من خلال تزييف أمر التحويل او تغيير مساره اوبياناته ، مما ينتج عه تحويل رصيد و فوائد ، شخص لحساب الفاعل او عن طريق انتحال شخصية الغير للقيام بالتحويل الالكتروني للنقود .

2. الاحتيال باستخدام بطاقات الدفع الالكتروني عبر الانترنت :

يعتمد نظام بطاقة الدفع الالكتروني على عمليات التحويل الالكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة الى رصيد التاجراوالدائن الذي يوجد به حسابه و ذلك من خلال شبكة التسوية الالكترونية للهيئات الدولية " هيئة الفيزا كارد visa card ،هيئة الماستر كارد master" و تعطي بطاقة الدفع الالكتروني الحق للعميل بالحصول على السلع و الخدمات عبر الشبكة عن طريق تصريح كتابي اوتليفوني، بخصم القيمة على حساب بطاقة الدفع الالكتروني [1]الخاصة به ،وتتم العملية بدخول العميل او الزبون الى موقع التاجر على الشبكة و يختار السلع المراد شراءها و يتم التعاقد بملأ النموذج الالكتروني ببيانات بطاقة الائتمان الخاصة بالمشترى وعنوانه فيقوم محاسب المتجر بخصم قيمه السلع من بطاقة الدفع الالكتروني و إرسالها إلى المشترى و أمام التطور التكنولوجي أصبحت إمكانية خلق مفاتيح البطاقات و الحسابات البنكية بالطرق الغير المشروعة ممكنة عبر قنوات شبكة الانترنت.

ويمكن الاحتيال باستخدام بطاقات الإئتمان من قبل صاحب البطاقة الشرعي و ذلك باسائته لاستخدام بيانات البطاقة الائتمانية اثناء مدة صلاحيتها ، بدفع ثمن السلع و الخدمات عن طريق الشبكة بملا الاستمارة رغم علمه ان رصيده غير كافي لتغطية هذه المبالغ ،او أن يقوم بتحويل رصيده من بنك لأخر وهو يعلم انه تجاوز رصيده الحقيقي ،وفي صورة أخرى يتم الغش باستخدام بيانات البطاقة الائتمانية بعد مدة صلاحيتها أو إلغاؤها ، فقد يكون البنك مصدر البطاقة قد الغاها اثناء مدة صلاحيتها بسبب سوء استخدامها من العميل الذي يتعين عليه إعادتها للبنك ، و الذي قد يمتنع عن ذلك و يستمر في استعمالها باستخدام بياناتها في تعاملاته عبر الشبكة، وهو ما يشكل جريمة النصب بمجرد ملا البيانات لإقناع الغير بوجود ائتمان وهمي، لان البطاقة قد خلعت عنها قيمتها كأداة ائتمان خاصة بتحقق تسليم البضاعة او السلع المشترات او تمكينه من الاستفادة بالخدمات[2] .

[1] يوجد الى جانب بطاقة الائتمان مجموعة من البطاقات المخصصة للتعاملات المالية : بطاقة الحساب، بطاقة الصراف الالي ، ضمان الشبكات.....

[2] محمد امين احمد الشوابكة ـ المرجع السابق صفحة 197

ويرى الفقيه jeandidier [1] ان قيام الحامل القانوني باستعمال بطاقة ملغاة في سحب النقود او التحويلات الالكترونية لأوراق البنوك ،لا يشكل جريمة ، لأنه يفترض في أجهزة السحب الالكتروني المرتبطة مباشرة (on–line) بحسابات العملاء في البنك ان ترفض اجراء أي تسليم او تحويل للنقود التي يطلبها الحامل إذا كانت تزيد عن رصيده في البنك ،أما إذا كانت البطاقة منتهية الصلاحية تعين على الحامل اعادتها للبنك المصدر لكنه اذا استعملها للوفاء فلا نكون أمام جريمة النصب إنما مجرد الكذب لصلاحية البطاقة، وهو الأمر الذي يتعين على التاجر المتعامل معه التحقق من الأمر ، في إطار الالتزامات التعاقدية والا تحمل جانب من المسؤولية بتحميله الضرر وحده .

وقد يكون الغش في استخدام البطاقة من قبل الغير، في حالة التقاطها عبر الشبكة و استعمالها بطريقة غير مشروعة في سحب النقود الرقمية او الوفاء بها، و بذلك تكون بياناتها محلا للسرقة من خلال تداولها عبر شبكة الانترنت بين العميل والتاجر بواسطة التجسس او الخداع او الحصول عليها باستخدام تقنية التفجـير " إغراق الموقع "،وقد ذهبت المحاكم الفرنسية إلىان سرقة بيانات بطاقة الائتمان و استخدامها بصورة غير شرعية، يشكل جريمة النصب على أساس انتحال الغير لاسم كاذب في حين يرى جانب من الفقه ان هذا الفعل شكل جريمة السرقة باستعمال مفتاح مصطنع باعتبار ان البطاقة الائتمان تعدمفتاح مصطنع لان النصوص القانونية لم تحدد بدقة ما هي المفاتيح المصطنعة [2]

ومن الأمثلة الواقعية لاحتيال " بطاقات الائتمان واقعة المتطفل hacher كيفيين ميتنك الذي أسندت إليه تهمة استخدام دخول احتيالي للكمبيوترللحصول على 20.000 بطاقة ائتمانية من شركة (netcom) للاتصالات في سان جوس بكاليفورنيا [3]

وقد تكون بطاقات الائتمان محلا للتزوير و ذلك بتخليق أرقام بطاقات ائتمان خاصة ببنك معين من خلال تزويد الحاسب بالرقم الخاص للبنك مصدر البطاقة بواسطة برامج تشغيل خاصة وقد اكتشفت بعض البنوك تكراراعتراض بعض حاملي بطاقات الدفع الالكتروني على عمليات لم يقوموا باجرائها و تبين للبنوك أنها عمليات تمت عن طريق شبكة الانترنت من قبل بعض الهواة و المخربين [4]

ومن الامثلة زعم عصابة من "الهاكرز" [5] بمدينة الإسكندرية المصرية تضم خمسة أشخاص الاستيلاء على حسابات بطاقات "في" الخاصة بعملاء البنوك، لكن الشاب الفرنسي جان كلود كان أكثر نبلا من أفراد العصابة المصرية، فقد استطاع تصميم بطاقة صرف آلي وسحب بها مبالغ من أحد البنوك ثم ذهب إلى البنك وأعاد إليه المبالغ وأخبرهم أنه فعل ذلك ليؤكد لهم أن نظام الحماية في بطاقات الصرف الخاصة بالبنك ضعيف ويمكن اختراقه، إلا أن ذلك لم يمنع الشرطة الفرنسية من إلقاء القبض عليه ومحاكمته، و لهذه الاحداث اثر بالغ على المواطن الجزائري الذى اجده متخوف جدا من بطاقات الدفع الالكتروني التي بدات توزع عبر نقاط

[1] جميل الصغير ـ المرجع السابق ـ صفحة 82
[2] سامي الشوا ـ المرجع السابق ـ صفحة 117
[3] Thomas j.semdinghoff/op/cit/p484
[4] جميل الصغير ـ المرجع السابق ـ صفحة 32
[5] http://www.arabia-inform.com/

البريد وطنيا و يحبذ بقاء التعامل بالشيك، لان هذه البطاقات ستكون محلا للاحتيال او السرقة الالكترونية، او مهما كان المصطلح المناسب فالاصح هو ان المبلغ المالي الذى تحمله لن يكون بمامن و الكثير ممن وصلته لا يستعملها.

وان مجال الجرائم المرتكبة على أموال عبر الشبكة جد واسع ولا يمكن حصره سواء لان الاختلاف في التكييف للوقائع لم يستقر فيه على رأي، خاصة أمام الفراغ القانوني الحاصل ،ومن جهة أخرى أمام تزايد رقعة مجال هذه الجرائم وما يخلق يوميا من أساليب جديدة في الاحتيال و التخريب و الاستحواذ على المال و الأفكار ، فلا يسعنى حصر كل أنواع الجرائم الواقعة على المال عبر الشبكة من مخدرات تجارة الأسلحة ،انتهاكات حقوق الملكية الفكرية الذي يعد لوحده موضوع الساعة ويتطلب بحث خاص به وكذا غسيل الاموال،و التي عادة ما تأخذ شكل الجريمة المنظمة، لتبقى ضرورة صدور نصوص قانونية تحصر الأفعال و الممارسات اليومية خاصة أمام الإحصائيات المسجلة و المتنامية.

أولا : مدى خضوع البرامج للنشاط الإجرامي في جريمة النصب

النشاط الإجرامي في النصب هو الاستيلاء على الحيازة الكاملة لمال مملوك للغير عن طريق إحدى وسائل الاحتيال المحددة قانونا على سبيل الحصر. فإذا لجأ الجاني إلى إحدى الطرق الاحتيالية، و حمل المجني عليه على تسليم دعامة مادية مثبتا عليها أحد البرامج التي تخصه ثم استولى الجاني عليها بعد ذلك فإن النشاط الإجرامي في جريمة النصب يتحقق و تقع الجريمة.

والإشكال الذي يطرح نفسه في هذا الصدد هو هل من المتصور أن تقع هذه الجريمة على المعلومات التي يتكون منها البرنامج فقط؟ و هل يتصور أن يتحقق النشاط الإجرامي لجريمة النصب من خلال الطرق الاحتيالية التي يلجأ إليها الجاني، و التي يترتب عليها وقوع المجني عليه في غلط يدفعه إلى أن ينقل إليه شفهيا عن طريق القول محتويات برنامجه الذي يلتقطه الجاني و يحفظ في ذاكرته؟ و بعبارة أخرى هل النقل من خلال القول يعادل التسليم بناءا على غلط؟ و هل الالتقاط أو سماع الجاني للمعلومات يعادل الاستيلاء [1] ؟. والواقع أن مسألة إمكانية الاحتيال على نظام الحاسب و إيقاعه في غلط قد اختلف بشأنها الفقه و التشريع، فيرى اتجاه من الفقه عدم إمكانية وقوع فعل الاحتيال على الحاسب و إيقاعه في غلط إذ لابد لتتوافر هذه الجريمة أن يكون الجاني و المجني عليه أشخاصا طبيعية يتحقق بواسطتهما التسليم و الاستلام . و بالتالي فهو متصور إذا تم خداع للشخص المكلف بمراقبة البيانات أو مراجعته [2] ،و على العكس هناك اتجاه يرى إمكانية وقوع فعل الاحتيال على الحاسب، و تصور إيقاعه في غلط و هو ما تبنته الدول الأنجلومكسوتية و جانب من الفقه الفرنسي، و السبب في ذلك أن النصوص المتعلقة بجريمة النصب جاءت تتسم بالعموم و الشمول بحيث يمكن الاستناد على هذه السمة لمد تطبيق أحكام تلك النصوص على فعل الاحتيال الواقع على الحاسب.أما عن وجوب حصول الاستيلاء على المال المنقول المملوك للغير بإحدى طرق الاحتيال فإن الاستيلاء على مال الغير هو النتيجة اللازمة قانونا

[1] علي عبد القادر القهوجي- المرجع السابق - ص 105 – 106.
[2] هشام فريد رستم –قانون العقوبات ة مخاطر تقنية المعلومات مكتبة الآلات الحديثة –أسيوط 1995 ص 123

لاكتمال تكوين الواقعة في الجريمة. و تطبيق فكرة الاستيلاء في المجال الالكتروني تثير مسألتين: النقود البنكية و بطاقات الائتمان.

1- **النقود البنكية** : تقتضي جريمة النصب أن يقوم الجاني بحيازة المال محل الجريمة حيازة مادية، و هو ما يستلزم كذلك أن يكون الاستيلاء ماديا من قبل هذا الجاني، ففي حالة ما إذا كان محل تحقق الاستيلاء ما يعرف بالنقود الكتابية أو البنكية عن طريق إجراء ما يعرف بالقيد الكتابي بالتلاعب في البرامج و البيانات التي يترتب عليه تحويل بعضه أو كل أرصدة أصحابها الشرعيين أو فوائدها على حساب المتاعب، فمتى اعترف لهذه النقود بصفة المال فإن هذا التصرف يعد من قبيل الاستيلاء المادي المتطلب في جريمة النصب[1].

2- **بطاقات الائتمان** : استخدام هذه البطاقة للحصول على أموال الجهة المصدرة لها بطريق الغش قد يقع من المالك الشرعي لهذه البطاقة أو من الغير في حالة عثوره عليها أو سرقتها من مالكها الشرعي و هنا نفرق بين حالتين :

الحالة الأولى : في حالة استعمال البطاقة من مالكها الشرعي فهنا نفرق بين 3 فرضيات.

1- في حالة استعمالها في سحب النقود من منافذ السحب الآلي بما يتجاوز رصيده ،في حال كون هذه البطاقة صحيحة فهناك من اعتبر هذا السلوك سرقة، وهناك من اعتبره نصبا، لكن محكمة النقض الفرنسية اعتبرته إخلال بالتزام تعاقدي.[2]

2- في حالة استعمالها في سحب نقود بالرغم من إلغائها من قبل الجهة المصدرة لها، هذا السلوك يعتبره البعض مكونا لجريمة النصب على أساس أن مجرد تقديم البطاقة يهدف إلى الإقناع بوجود ائتمان وهمي لا وجود له في الواقع خاصة وأن إلغاء البطاقة يخلع عنها قيمتها كأداة ائتمان.[3]

3- استعمالها في سحب النقود بالرغم من انتهاء مدة صلاحيتها، اعتبر بعض الفقه هذا السلوك بأنه مكون لجريمة خيانة الأمانة، على أساس أن البطاقة بمثابة محرر يتم تسليمها للعميل على سبيل عارية الاستعمال.[4]

الحالة الثانية : في حالة استعمال بطاقة الائتمان من قبل الغير، نميز بين فرضيتين :

1- عند سرقة البطاقة أو العثور عليها وإجراء عملية سحب للنقود بموجبها، فهنا هذا السلوك يعتبر مكونا لجريمة النصب على أساس اتخاذ الجاني اسما كاذبا.

2- عند تزوير بطاقة الائتمان، يرى جانب من الفقه أنه في حالة قيام الغير بتزوير بطاقة الائتمان وقام باستغلالها في سحب مبالغ من أجهزة السحب الآلي للنقود يعتبر ذلك جريمة سرقة باستخدام مفتاح مصطنع، كما استبعد بعض الفقه تطبيق جريمة التزوير على أساس أن بطاقة الائتمان لا تعتبر محررا كتابيا، كما أن القضاء الفرنسي اعتبر هذا السلوك لا يكون جريمة النصب باعتبار أن هذه الجريمة تعترض علاقة مباشرة بين شخصين.

<u>خاتمة</u> :

[1] محكمة النقض قد اعتبرت أن الإبراء من دفع الأجرة يقوم مقام التسليم على الرغم من أن الجاني لم يستلم أي شيء مادي

[2] محمد سامي الشوا،- ثورة المعلومات و انعكاساتها على قانون العقوبات – دار النهضة العربية 1994 ص 105.

[3] جميل عبد الباقي صغير، جرائم التكنولوجيا الحديثة –دار النهضة العربية ص 114

[4] محمد سامي الشوا، - المرجع السابق - ص108 .

تعد هذه الدراسة حصيلة جهد متواضع قمنا به بهدف التصدي لهذا الموضوع ذو الصبغة العلمية الغربية في رأينا على رجال القانون ،غير أنه لا يجب أن يكون هذا الطابع العلمي عقبة تمنعنا من التوسع في قاعدة النقاش حول الاجرام الالكتروني ؛ و حتى لا يبق موضوع الجريمة الالكترونية من المناطق المحرمة التي يتجنب معظم الباحثين و دارسي القانون الخوض فيها.

لا ننكر الصعوبة التي واجهتنا لانجاز هذه الدراسة نظرا لنقص المراجع في هذا الميدان و نظرا لضرورة المامنا بالجوانب التقنية حتى نتمكن من الاحاطة بالجوانب القانونية ،الا أن ذلك لا يمنع اننا توصلنا في ختام دراستنا لهذا الموضوع الى عدة جوانب يمكن بلورتها فيما يلي :

1 **النتائج :**

- أظهر البحث غياب مفهوم عام متفق عليه بين الدول –حتى الأن – حول التعريف القانوني للنشاط الاجرامي المتعلق بالجريمة الالكترونية و اللأنماط المكونة لها من جهة، و كذا عدم كفاءة و ملاءمة السلطات التي ينص عليها القانون بالنسبة للتحري و اختراق نظم الكمبيوتر لأنها عادة ما تكون متعلقة بالضبط و التحري بالنسبة لوقائع مادية خاصة بالجرائم التقليدية و بالنتيجة فهي لا تتلاءم مع الوقائع " المعنوية" التي تتميز بها الجريمة الالكترونية كاختراق المعلومات المبرمجة و تغييرها في الكمبيوتر من جهة أخرى .
- السمة المميزة للكثير من الجرائم الالكترونية هي أنها من النوع العابر للحدود TRANSNATIONAL.و بالتالي فانه بات من الضروري ابرام معاهدات للتسليم أو للمعاينة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي و ان وجدت فانها غير كافية لمواجهة المتطلبات الخاصة .
- وجود قصور في قوانيننا في مجال الجرائم الالكترونية ،اذ أنه لا تزال الكثير منها تخضع للنصوص التقليدية و هو الشيء الذي يعد مساسا مباشرا لمبدأ الشرعية من جهة و الذي ينعكس سلبا في مجال المتابعة اذ انه يؤدي الى افلات الكثير من الجناة من العقاب. و نظرا لنسبية الحماية من خلال النصوص التقليدية لجرائم الأموال نتيجة للطبيعة المتميزة للمال الالكتروني استقر الفكر القانوني على اخضاع الالكترونية لقوانين الملكية الفكرية.
- و بالتالي خلصنا الى أن فكرة تطويع النصوص التقليدية المتعلقة بجرائم الأموال و تعديلها بما يتلاءم و طبيعة المال الالكتروني نجحت و لو نسبيا في تغطية بعض الحالات فقط ،و ان كانت لا تحقق الحماية الكافية للمال الالكتروني نظرا للطبيعة المتطورة لهذا المال و التي تختلف عن المال التقليدي ، و عليه يصبح البحث على سبيل آخر للحماية أمر لا مفر منه .

2 **الاقتراحات :**

- اعتمادا للنتائج التي توصلنا اليها من خلال دراستنا هذه سنحاول القاء الضوء على موقف المشرع الجزائري الذي اتخذه لمواجهة هذا الشكل الجديد من الاجرام الحديث ، فالملاحظ أن مشرعنا قد استدرك مؤخرا الفراغ القانوني الملحوظ في مجال الاجرام الالكتروني و قد اعتمد في ذلك حلا يضمن حماية مزدوجة للحاسب الآلي من خلال نصوص حق المؤلف من جهة، و من خلال نصوص خاصة أدمجها في قانون العقوبات من جهة أخرى .

- رغم اعتراف المشرع لبرامج الحاسب الآلي بصفة المصنف المحمي الا أنه نظرا لوجود بعض المفاهيم التقليدية لحقوق المؤلف لا تتماشى مع برامج الحاسب الآلي و التي لم بتداركها تعديل قانون الملكية الأدبية و الفنية و عليه نقترح اجراء تعديل بوضع نظام خاص بايداع برامج الحاسب الآلي مع تقصير الحماية الى أقل من 50 سنة بعد الوفاة نظرا للتطور السريع للمعلوماتية .
- استحداث نص خاص بالاعتداء على سير نظام المعالجة الآلية للمعطيات.
- استحداث نص خاص بالتزوير الالكتروني ،و كذا توسيع مفهوم المحرر ليشمل أية دعامة أخرى.
- حماية البرامج و المعلومات المعالجة بصفة مستقلة عن طريق معاقبة الاستيلاء عليها دون المساس بسلامتها أوأصالتها أو نسخ صور منها عند تشغيل الجهاز.
- وفي هذا المقام سنختم دراستنا بقول الشيخ عبد الرحمان الببيساني : "لا يكتب انسان في يومه الا قال في غده لو غير هذا لكان أحس ، و لو ترك هذا لكان أجمل و هذا من أعظم العبر و من دلائل استيلاء النقص على البشر ...".

قائمة المراجع:

1-المراجع العامة باللغة العربية :

1 - أحسن بوسقيعة – الوجيز في القانون الجزائي العام – الطبعة الثالثة – دار هومه 2006 .

2- أحسن بوسقيعة – الوجيز في القانون الجزائي الخاص- الجزء الأول-الجرائم ضد الأشخاص و الجرائم ضد الأموال- الطبعة الخامسة منقحة و متممة في ضوء النصوص الجديدة – دار هومه-2006.

3- أحسسن بوسقيعة –الوجيز في القانون الجزائي الخاص – الجزء الثاني –جرائم الفساد –جرائم المال و الأعمال –جرائم التزوير- الطبعة الثالثة منقحة و متممة في ضوء النصوص الجديدة لا سيما قانون 20 فراير 2006 المتعلق بالوقاية من الفساد و مكافحته-دار هومه -2006

4- أحمد عبد الرزاق السنهوري-الوسيط في شرح القانون المدني حق الملكية - -الجزء الثامن دار إحياء التراث العربي بيروت 1952 .

5 - محمود محمود مصطفى – شرح قانون العقوبات القيم الخاصة- الطبعة 8، 1984 مطبعة جامعة القاهرة .

6 - هشام فريد رستم –قانون العقوبات ة مخاطر تقنية المعلومات مكتبة الآلات الحديثة –أسيوط 1995.

2-المراجع الخاصة باللغة العربية :

1 - أحمد السمدان –النظام القانوني لحماية برامج الكمبيوتر – مجلة الحقوق ،الكويت،العدد 4 ،سنة 1987

2 - أحمد خليفة الملط – الجرائم الالكترونية –دار الفكر الجامعي – الطبعة الثانية 2006 .

3 - أحمد ضياء الدين خليل - الظاهرة الإجرامية بين الفهم و التحليل - دار الطويعي للطاعة طبعة 1992/1.

4 - أسامة أحمد المناعسة ، جلال محمد الزعبين صايل فاضل الهواوشة -جرائم الحاسب الآلي و الانترنت- دار وائل للنشر ، الأردن **2004**

5 - أمال قارة- حماية الجزائية للمعلوماتية في التشريع الجزائري- دار هومة الطبعة الأولى 2006.

6 - جميل عبد الباقي صغير، جرائم التكنولوجيا الحديثة -دار النهضة العربية .

7 - عبد الرشيد مأمون شديد الحق الأدبي للمؤلف النظرية العامة و تطبيقاتها دار النهضة القاهرة 1978.

8 - عزة محمود أحمد خليل -مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي- دراسة مقارنة في القانون المدني و الشريعة الاسلامية – رسالة دكتورا- مقدمة لكلية الحقوق 1994 .

9 - عكاشة محي الدين، محاضرات في الملكية الأدبية و الفنية-ديوان المطبوعات الجامعية ،الجزائر 2001

10 - علي عبد القادر القهوجي الحماية الجنائية لبرامج الحاسب الآلي-الدار الجامعية للطباعة و النشر بيروت 1999.

11 - محمد العقاد -جريمة التزوير في المحررات الحاسب الآلي -دراسة مقارنة -بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون- دار النهضة العربية القاهرة 1995ص 36.

12 - محمد أمين الرومي -جرائم الكمبيوتر و الانترنت -دار المطبوعات الجامعية- السكندرية 2005

13 - محمد حسام لطفي – النظام القانوني لحماية الحقوق الذهنية في مصر- بحث منشور في كتاب ندوة حقوق المؤلفات الفكرية في مصر

14 - محمد سامي الشوا- ثورة المعلومات و انعكاساتها على قانون العقوبات – دار النهضة العربية 1994.

15 - محمد فتحي عبد الهادي-مقدمة في علم المعلومات – تبة غريب القاهرة 1984 .

16 - نائلة عادل محمد فريد قورة -جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية- منشورات الحاتي الحقوقية 2005

17 - هدى قشقوش -جرائم الحاسب الالكتروني في التشريع المقارن -الطبعة الأولى دار النهضة العربية القاهرة 1992.

18 - هشام فريد رستم -جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة- بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة و معاملة المجرمين -مجلة الأمن العام العدد 151-1995 .

المراجع باللغة الفرنسية :

1- Pierre Catala : La propriété de l'information, cité par f. Toubal ; le logiciel –

2 - Analyse juridique FUDUL .L.G.D.J.1986

3- Benlkadi Kamel : Les sites algériens vulnérables journal El Watan du 23/12/2002 n°-3668.

4- Carbonnier (M) : Droit civil P U E Paris 1973 T 3 les biens N° 17-18

5- Chamoux : La loi sur la fraude informatique : De nouvelles incriminations J.C.P1988 doct 3321

6- Fidemann (K) Frundes et délits d'affair commis à l'aide d'ordinateurs électroniques (Revue drpeu et crim 1984).

7- G. Delmare : Sécurité informatique (Ressource informatique N° 1 juillet)

8- Pierre Catala : Ebauche D'une Théorie Juridique de l'information, 1983-

9- Rose Philippe : la criminalité informatique que sais je 1er édition PU 1988

10- Rollant : Réflexions sur le vol d'usage J C P 1 doctorat

11-Roman (M) Faux : Juris class 1996 art 441/1 à 441/12 n°19-

المراجع باللغة الانجليزية :

12- Andre Lucas, Protection of information Bases, Kuwait First Conference, Ministry of Justice, 15-17 Feb.1999, Kuwait.

13 - Parker (Donn B) Figding computer crime A new Framework for protecting information 1998

14- Suthreland (Eduin H) "White collar criminality " Gers (Gilbert) in white collar criminal The offender in business the professions atherton press 1968

15-Related crime on computer - The recommandation N R89

نعيمة بوبرطخ
naimaboubertakh258@gmail.com
جامعة قسنطينة 1

خصوصية المفهوم العام للجريمة الإلكترونية

The specificity of the general concept of cybercrime

ملخص :

تعد الجريمة الإلكترونية نتاجا للثورة التكنولوجيا ، وأهم الانعكاسات السلبية لظاهرة العولمة على الصعيد الاجتماعي، وعلى المستوى الوطني والدولي، و قد دفع ظهورها وتطورها وانتشارها الواسع ، وإلحاقها الاذى والضرر بمصالح الأفراد والمؤسسات والدول، إلى ضرورة وضع قواعد قانونية لمواجهتها، وتسليط الضوء عليها بالدراسة والتحليل من طرف الفقه الجنائي، الذي حاول اكتشاف طابعها الخاص، الذي يميزها عن غيرها من الجرائم التقليدية، من حيث التعريف، و الخصائص، و سمات المجرم، واسبابها وتصنيفاتها.

***Summary*:**

Cybercrime is a product of the technological revolution, and the most important negative impact of the phenomenon of globalization on the social, national and international level, and its emergence and development have promoted its wide dissemination, and its infliction of harm and damage to the interests of individuals, institutions and countries, the need to establish legal rules to deal with them and to highlight them through the study and analysis of criminal jurisprudence, which has attempted to discover their particular character, which distinguishes them from other traditional crimes, in terms of definition, characteristics of the criminal, their causes and their classifications.

مقدمة:

لقد أصبح العالم في القرن الواحد و العشرين كله متعولما اختيارا أم إجبارا ، وكما للعولمة من تداعيات إيجابية على الفرد و الجماعة ، و على كل الأصعدة الاقتصادية و السياسية والاجتماعية و الثقافية والتكنولوجية ، فإن لها وجه آخر ، هي آثار سلبية طالت كل الدول ، التي كان لها نصيب منها ، لكن بدرجات متفاوتة.

فدفعت بيئة العولمة وما صاحبها من ظواهر تابعة لها ، و تطورات وخاصة في مجال تكنولوجيا الإعلام و الاتصال ، بالفرد أن يقتحم مجال الفضاء الإلكتروني ، بأفعال و سلوكيات ألحقت أضرارا بالغة بمصالح الغير سواء كان شخصا طبيعيا او معنويا ، و لأنه لا قانون بغير مجتمع ، وبضرورة مصاحبة و مسايرة القواعد القانونية للمجتمع في كل تطوراته ، فصل القانون في هذا الأمر و اطلق عليها وصف الجريمة ، فسميت بالجريمة الإلكترونية.

وتكمن اهمية موضوع الجريمة الإلكترونية كونها من الجرائم المستحدثة ، التي ظهرت وتطورت بفعل العولمة و التطور التكنولوجي و ظهور شبكة الأنترنت ، باعتبارها استعمالا غير مشروع للتقنية المعاصرة ، ومهددا حقيقيا لأمن المعلومات في القطاعين الخاص و العام، ومهددا للأمن الوطني للدول ، و للأمن الإقليمي و الدولي بسبب استخدامها من طرف الجماعات الإرهابية ، و في مختلف صور الجرائم العابرة للقارات.

لذا،فقد جذب هذا الموضوع اهتمام الباحثين في القانون الوطني و الدولي على حد سواء ، كما عرف جدلا فقهيا واسعا لدى الفقه الجنائي، لذا سنحاول من خلال هذه الدراسة وضع إطارا مفاهيميا للجريمة الإلكترونية ، وطبعا مع مراعاة خصوصيتها ، من خلال طرح الإشكاليات التالية : ماهو تعريف الجريمة الإلكترونية ؟ ماهي خصائصها ومسبباتها؟ ماهي أهم تصنيفاتها؟

و إنه لدراسة هذا الموضوع، قسمنا دراستنا إلى ثلاثة أقسام ، فتناولنا تباعا المفهوم ، ثم الأسباب ، ثم الأنواع ، بالإستعانة بالمنهج الوصفي التحليلي ، الذي يتلاءم مع تفاصيل وعموميات هذه الدراسة.

أولا _ مفهوم الجريمة الإلكترونية: لا يوجد اتفاق بين الباحثين حول تسمية و تعريف الجريمة الإلكترونية ، فظهرت العديد من الآراء ، التي حاولت التركيز على جانب محدد على حساب الآخر، دون أن تضع تعريفا جامعا مانعا لها.

1 / _ الجريمة الإلكترونية اصطلاحا: لم يتفق الفقهاء حول تسمية موحدة للجريمة الإلكترونية، فمن أصل حوالي 200 مصطلح منبثق من التشريعات الوطنية ، التي استخدمتها الدول للرد على الاستبيان الدولي ، بغرض تحديد مفهومها ، تم استخدام أقل من 5% لاصطلاح " الجرائم الإلكترونية" ، و ذلك في العنوان أو السياق التشريعي، و كان المصطلح الأكثر شيوعا في مختلف التشريعات هو " جرائم الكمبيوتر " و " جرائم الاتصالات الالكترونية"، و كذا " جرائم تكنولوجيا المعلومات " و " الجرائم ذات التقنية العالية".

كما استعملت العديد من المفردات ضمن التشريعات الجنائية للدلالة عليها، فنجد على سبيل المثال لا الحصر: الدخول غير المصرح به لنظام الكمبيوتر، التدخل في نظام الكمبيوتر أو البيانات، و كذا تعبير " الجرائم المشار إليها في هذا القانون[1] .

وتفاديا لهذه الأزمة الاصطلاحية ، فإن مؤتمر القانون والأنترنت المنعقد في لشبونة بتاريخ 26 جانفي 2001 ، قد ألح على اعتماد مصطلح " الجريمة الإلكترونية " Cybercrime، مع ضرورة التفريق بينها و بين غيرها من الجرائم الممكن ارتكابها عبر الأنترنت [2]، ليشير الاصطلاح الأول إلى السلوكيات و الأفعال الخارجة عن القانون ، أما الثاني فيستعمل لوصف فكرة جزء من الحاسب أو عصر المعلومات [3].

[1] _ ذياب موسى البداينة، الجرائم الإلكترونية ، المفهوم و الأسباب، ضمن أعمال الملتقى الموسوم : الجرائم المستحدثة في ظل المتغيرات و التحولات الاقليمية والدولية، من 2 إلى 4 أفريل 2014، كلية العلوم الاستراتيجية ، المملكة الأردنية الهاشمية ، ص5 .

[2] _ معزوز ربيع ، زروقي عاسية ، الجريمة الإلكترونية و إجراءات مواجهتها في التشريع الجزائري، المجلد 7 ، العدد 2 ،2001 ، ص362.

[3] _ ذياب موسى البداينة ، المرجع نفسه ، ص3.

2 / التعريف الفقهي للجريمة الإلكترونية :هناك اختلاف واضح بين الفقهاء في تعريفهم للجريمة الإلكترونية ، فمنم من عرفها من وجهة نظر تقنية محضة ، بقولهم بأنها : " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي ، بطريقة مباشرة أو غير مباشرة ، كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود ".

في حين ذهب اتجاه آخر ، إلى وضع تعريف لها بالتركيز على الجانب القانوني، فيرون بضرورة تعريف المفردات المتعلقة بجرائم ارتكاب الحاسب الآلي ، و المتمثلة في : " الحاسب الآلي " ، "برنامج الحاسب الآلي " ، " البيانات ، الممتلكات ، الدخول ، الخدمات الحيوية "[1] .

كما ذهب فريق آخر إلى اتخاذ وسيلة ارتكاب الجريمة أساسا صلبا لوضع تعريف للجريمة الإلكترونية، كما هو الحال عند الفقيه الألماني " تاديمان" ، الذي عرفها بأنها: " كل أشكال السلوك غير المشروع ، أو الضار بالمجتمع ، و الذي يرتكب باستخدام الحاسب الآلي".

وهنالك اتجاه آخر ركز على الجانب الموضوعي ، فيرون بأنه لا يكفي إطلاق وصف الجريمة الإلكترونية بمجرد استخدام الحاسب الآلي ، و لكن يشترط أن يقع الفعل داخل نظام الحاسب الآلي لاحتسابها جريمة إلكترونية ، فعرفها بأنها : " نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب ، أو التي ترسل عن طريقه "، وأيضا : " غش معلوماتي ينصرف إلى كل سلوك غير مشروع ، يتعلق بالمعلومات المعالجة ونقلها".

كما ركز آخرون على الجانب المعرفي لا على الوسيلة و لا على الموضوع، كونها مرتبطة بالجانب المعرفي الفني باستخدام الحاسب الآلي بأنها : " أية جريمة يكون متطلبا لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب الآلي"، وأنها : " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"[2].

و قام آخرون بتعريفها وفقا لمعيار الربح، باشتراط أن يحقق الجاني ربحا من الفعل غير المشروع ، لكن هذا الأمر غير وارد بشكل دائم في الجرائم الإلكترونية ، كما أن الفعل المرتكب لا يكون دائما بشكل عمدي ، إنما قد يحصل بطريقة غير مباشرة، و رغم ذلك عرفها هذا الاتجاه تعريفا واضحا و بسيطا، بأنها الاعتداءات التي يمكن ان ترتكب بواسطة الوسائل الإلكترونية بغرض تحقيق الربح[3]، أو كما عرفها الفقيه الفرنسي " ماس"بأنها :" الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية ، بغرض تحقيق الربح"[4] .

3 / _ خصائص للجريمة الإلكترونية : تتميز الجريمة الالكترونية بالعديد من الخصائص ،التي تميزها عن الجريمة التقليدية ، باعتبارها جريمة ذات طابع حاص.

أ / _الجريمة الإلكترونية عابرة للحدود : فهي تتخطى الحدود الجغرافيةلاتصالها بعالم الأنترنت ، وتقنية

---

[1] _ سعيد بن سالم البادي ، و آخرون ، الجريمة الإلكترونية في المجتمع الخليجي ، وكيفية مواجهتها ، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان ، 2016 ، ص 20.

[2] _ سعيد بن سالم البادي ، و آخرون ، المرجع نفسه ، ص 21 ، 22.

[3] _ عبد الله دغش العجمي ، المشكلات القانونية و العملية للجرائم الإلكترونية ، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، 2014 ، ص 13.

[4] _ عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية و أزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العدد 7، 2011، ص 113.

المعلومات ، حيث تتأثر بهذه الجريمة ، وفي آن واحد الكثير من الدول، بسبب السرعة الهائلة في تنفيذها، و حجم الأموال و الأشخاص المستهدفة من خلالها.

لذا بات من الضروري إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم ، عن طريق إبرام الإتفاقيات الدولية الخاصة بتسليم المجرمين ، و الوسائل الكفيلة بمكافحة هذا النوع من الجرائم.

ب / _ يتميز مرتكبو الجرائم الالكترونية بصفات خاصة : يتميز المجرم فيالجرائم الإلكترونية عن غيره من المجرمين العاديين ، الذين جنحوا إلى السلوك الإجرامي النمطي بعدة خصائص عددها الأستاذ parker، فيمايلي :

_ الجاني شخص متخصص ، و محترف في تنفيذ الجريمة الإلكترونية.

_ لا يقوم الجاني باللجوء إلى العنف في تنفيذ الجريمة ، فهو مجرم ذكي يتمتع بالمهارة والمعرفة ، و بدرجة عالية من الثقافة.

_ هناك عدة أنواع من مرتكبي هذه الجرائم :

* الأشخاص الذين يرتكبون الجرائم الإلكترونية بغرض التسلية و المزاح مع الآخرين دون إحداث أي ضرر و يسمونهم Pranskers .

*الأشخاص الذين يستهدفون الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم، بهدف الفضول ، أو اكتساب الخبرة أو لمجرد القدرة على اختراق هذه الأنظمة، و يسمون Hackers

* الأشخاص الذين يستهدفون إلحاق خسائر بالمجني عليهم ، دون أن يكون الحصول على مكاسب مالية ضمن هذه الأهداف ، و يندرجون تحت طائفة مخترعي فيروسات الحاسبات الآلية، وموزعيها ، و يسمون Malicieuses hackers .

* الأشخاص الذين يهدفونإلى إلحاق الأذى بالمجني عليهم، ويكون الباعث إيجاد حلول لمشاكل مادية تواجه الجاني ، لا يستطيع حلها بالطرق العادية ، و يسمون .Personnel probleme solvers .

* الأشخاص الذين يهدفون إلى تحقيق ربح مادي ، بطريق غير مشروع ، و يسمون .Creen criminals.

ج/ _ صعوبة الإثبات في الجرائم الإلكترونية : من أهم خصائص الجريمة الإلكترونية أنها صعبة الإثبات لأسباب ترجع إلى الجاني ، أو إلى المجني عليه ، و إلى وسيلة تنفيذها[1] ، حيث تتم هذه الجريمة بشكل منظم من إقليم دولة واحدة باستخدام الأنترنت، إضافة إلى أن الجاني مجرم محترف ذكي و مثقف، لا يترك آثارا جانبية خارجية للجريمة ، مما يصعب إثباتها ، كما أن المجني عليه في غالب الأمر مؤسسات عامة أو خاصة ، يمتنعون عن الإبلاغ عنها تجنبا للإساءة إلى السمعة ، وهز الثقة ،فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية[2].

[1] _ مخلد ابراهيم الزعبي ، فاعلية القوانين و التشريعات العربية في مكافحة الجرائم الإلكترونية ، المجلة العربية للنشر العلمي، العدد 37 ، تشرين الثاني 2021، ص 283 ، 284 .

[2] _مخلد ابراهيم الزعبي ، المرجع نفسه ، ص 285.

ثانيا –اسباب الجريمة الالكترونية : لقد تعددت و تنوعت أسباب الجريمة الإلكترونية ، و التي حاول الفقه الجنائي تجميعها و ترتيبها و تصنيفها وفقا لثلاثة مستويات.

1/ – أسباب الجريمة الالكترونية على المستوى الفردي:

أ/ – البحث عن التقدير : هناك بعض الجرائم الالكترونية التي يرتكبها الشباب الطائش وصغار السن، و ذلك من باب التحدي ، و حب الظهور في الاعلام ، و غالبا ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينات.

ب/ _ الفرصة : لقد وفرت التقنيات الحديثة فرصا غير مسبوقة لانتشار الجريمة الالكترونية ، كما تلعب البيئة و ترتيباتها دورا كبيرا في انتاج الجريمة و الخروج على القواعد الاجتماعية ، فوقت الانحراف عن قواعد الامتثال ليلا و نهارا ، و في أي مكان ، وكذا عدم وجود الرقابة الصارمة ، كلها عوامل تزيد من فرصة ارتكاب الجرائم الالكترونية ، خاصة وأن المعلومات هدفا سهل المنال ، ومحققا للمنفعة السريعة ، و بالتالي يمكن سرقتها أو سرقة محتوياتها ، لذا تعتبر الجريمة الالكترونية فرصة مربحة و قليلة المخاطر ، كما أن احتمالية كشف الفاعل فيها ضئيلة.

كما خلقت تكنولوجيا المعلومات و الاتصالات و الاستخدام المتزايد للأنترنت، فرصا جديدة للمجرمين.

ج/_ ضبط الذات المنخفض : والمقصود أن انخراط الفرد في السلوك الإجرامي يحدث بسبب وجود الفرصة ، مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض ، و إن توفر هذه الصفة الأخيرة مع وجود الفرصة لارتكاب السلوك الطائش ، يعدان عاملين مؤثرين في ارتكاب السلوك الطائش ، و إن نقص ضبط الذات ناتج عن التنشئة الاجتماعية الناقصة ، حينما يفشل الآباء في مراقبة سلوك الطفل ، كما لا يلاحظون سلوكه المنحرف حينما يحدث ، وكذا إهمال معاقبتة .

و في حقيقة الأمر ، فان الأشخاص ذوو الضبط الذاتي المنخفض ، لا يميلون فقط الى السلوكات المنحرفة ، إنما في الأغلب غير ناجحين في المدرسة أو العمل أو الزواج[1]، كما أثبتت الدراسات أنهم أكثر ميلا لارتكاب الجريمة الالكترونية.

د/_ النشاط الروتيني : يمكن تفسير زيادة ضحايا الجريمة الالكترونية ، إلى التغييرات الحاصلة في الأنشطة اليومية للبشر، حيث اصبحوا يتواصلون من خلال استخدام النت و شبكات التفاعل الاجتماعي ، مثل الفيس بوك و الايميل و المواقع و غيرها ، والتي خلقت فرصا للجناة المتحفزين مع وجود أهداف قيمة و سهلة في الحيز الفضائي ، و في ظل غياب المراقبة.

فيرى " كوهين وفيلسون" ، أنه من المرجح أن تحدث الجريمة حينما تتلاقى ثلاثة عوامل أساسية ، تتمثل في الجاني المتحفز ، الهدف المناسب ، وكذا غياب الرقابة ، ويضيف بأن تخلف أي عنصر كاف لمنع حدوث الجريمة.

2/_ أسباب الجريمة على المستوى المجتمعي:

[1] _ اسراء جبريل رشاد مرعي ، الجرائم الإلكترونية ، " الأهداف _ الاسباب _ طرق الجريمة و معالجتها "، مجلة الدراسات الاعلامية ، المركز الديمقراطي العربي ، العدد الأول ، جانفي 2018، ص 432 ، 433.

أ / _ التحضر: و نقصد به هجرة الشباب من الأرياف إلى المدن الكبرى و المناطق الحضرية، والذين يجدون أنفسهم فيما بعد عاجزين عن مواجهة تكاليف الحياة الحضرية الباهضة ، فيلتفتون الى الاستثمار في الجريمة الالكترونية ، التي لا تتطلب في الواقع راس مال كبير.

ب/_ البطالة : شأنها شأن الجريمة التقليدية ، ترتبط الجريمة الإلكترونية بالبطالة و الظروف الاقتصادية الصعبة ، و التي تنتشر عادة بين فئة الشباب ، فتكون بذلك انعكاسا للمثل النيجيري القائل " العقل العاطل عن العمل هو ورشة لعمل الشيطان "، لذا يلجأ الشباب العاطلين عن العمل المتعلمين إلى الجريمة الالكترونية.

ج/_ الضغوط العامة : و نقصد بها الظروف العامة التي يتعرض لها المجتمع من فقر و بطالة و أمية ، و كذا الظروف الاقتصادية الصعبة ، فتتولد المشاعر السلبية الساخطة ضد الظروف والمجتمع خاصة عند فئة الشباب ، فيحاولون التأقلم بطرق سلبية مع هذه الظروف ، ومنها الاتجار الالكتروني بالجنس و البشر ، و الجريمة الالكترونية وغيرها[1].

د/_ البحث عن الثراء : يلجأ بعض البشر إلى الجريمة الإلكترونية بغرض الحصول على الأموال بطرق مشروعة و غير مشروعة ، و كذا بحثا عن المتعة[2].

ه/_ ضعف إنفاذ القانون و تطبيقه في الجريمة الالكترونية : حيث أنه توجد الكثير من الدول لازالت لم تطور تشريعاتها و اجهزة العدالة فيها، لكي تتمكن من محاربة الجرائم الالكترونية ومختلف أساليبها[3].

3/_ أسباب الجريمة الالكترونية على المستوى الكوني :

أ/_ التحول للمجتمع الرقمي : في وقتنا الحالي أصبح الأفراد يقضون جزء من حياتهم اليومية في الفضاء الإلكتروني ، فينشؤون الشبكات و المواقع ، و يدخلون في علاقات اجتماعيةجديدة، و هم على تواصل دائم مع ما يجري في العالم الخارجي ، وكل هذه الأنشطة تتطلب توفر جهاز كمبيوتر موصول بالأنترنت ، مع ضرورة توفر عنصر المعرفة بالأمور التقنية ، وإن كانت ضئيلة .

ب / _ العولمة : إن ظهور ما يسمى " الفضاء الإلكتروني " أو " العالم الافتراضي" ، خلق ظواهر جديدة و فرصا مباشرة للجريمة ، وفرتها أجهزة الكمبيوتر، فتظهر الفروق في سلوكيات الأفراد بين العالمين المادي و الافتراضي ، فقد يرتكبون جرائم في العالم الإلكتروني لا يرتكبونها في الواقع المادي ، بسبب مكانتهم الإجتماعية ، كما أن عدم ظهور الهوية و ضعف عوامل الردع تحفز هي الأخرى السلوك الإجرامي في العالم الافتراضي.

لذا ، يتطلب هذا العصر وجود مؤسسات أمنية مصممة للتعامل مع هذا التغير السريع ، ترتكز على الإبداع و الشفافية ، و إرضاء العملاء " المجتمع" [4]، مؤسسات ذات سرعة عالية في نشر المعلومات ، و إعلام

---

[1] _ اسراء جبريل رشاد مرعي ، المرجع نفسه ، ص 434، 435.

[2] _ مخلد ابراهيم الزعبي، المرجع السابق ، ص 285.

[3] _ عبد السلام محمد المايل ، عادل محمد الشربجي، الجريمة الالكترونية في الفضاء الالكتروني، المفهوم ، الأسباب ، سبل المكافحة مع التعرض لحالة ليبيا ، مجلة آفاق للبحوث و الدراسات ، العدد 4، جوان 2019، ص 249 ، 250 .

[4] _ اسراء جبريل رشاد مرعي ، المرجع السابق ، 436 ، 437.

الجمهور ، مؤسسات قادرة على إعادة تصميم ذاتها لمواجهة المستجدات ، و سريعة التغير في عالم الجريمة الإلكترونية.

ج/_ الترابط الكوني: حسب التقارير و الدراسات الرسمية ، التي تؤكد أن فضاء الأنترنت خلق فرصا جديدة للمجرمين في التواصل مع الضحايا ، بسبب السمات الفريدة للأنترنت، المتمثلة في عدم الكشف عن هوية الشخص، وسهولة الاستخدام ، و نقل المعلومات بسرعة وبدقة فائقة وبكميات كبيرة ، الى العديد من الضحايا عبر غرف الدردشة ، البريد الإلكتروني ، لوحات الرسائل ، مواقع ويب، و كل ما يحتاجونه مهارات الحاسوب الأساسية و أجهزة الكمبيوتر المتصلة بالأنترنت ، و هذا يعني أن جهاز كمبيوتر واحد يوفر العديد من الوسائل لارتكاب مجموعة من الجرائم [1].

د/_ انكشاف البنية التحتية المعلوماتية : لقد حدد التقرير الرئاسي الأمريكي المتعلق بحماية البنية التحتية الحساسة ، خمس قطاعات تتكون منها ، وذلك بناء على خصائصها المشتركة ، وتتمثل هذه القطاعات في:

* **قطاع الاتصال و المعلومات** : والذي يشمل شبكات الاتصالات العامة، الانترنت، الحاسبات في المنازل، الاستخدام الأكاديمي و الحكومي، و كذا التجاري.

* **قطاع التوزيع المادي** : والذي يشمل الطرق السريعة للمواصلات، وخطوط السكك الحديدية والموانئ ،خطوط المياه ، المطارات ، شركات النقل، خدمات الشحن التي تسهل انتقال الأشخاص و البضائع.

* **قطاع الطاقة:** ويشمل الصناعات التي تنتج الطاقة ، توزيع الطاقة الكهربائية ،البترولوالغاز الطبيعي.

* **قطاع المال و البنوك** : ويشمل البنوك، نظم الرواتب ، شركات الاستثمار ، القروض المتبادلةالتبادلات الأمنية و المادية.

* **قطاع الخدمات الإنسانية الحيوية:**و يشمل نظم التزويد بالمياه، خدمات الطوارئ ، الخدمات الحكومية (البطالة، الضمان الاجتماعي ، تعويض الإعاقات ، إدارة سجلات المواليد...).

وما تجدر الإشارة إليه ، أنه من الصعب ربط التهديدات الالكترونية بمكان أو زمان محدد، أو جماعة معينة ، فقد تصدر من هاو ، أو من طفل أو محترف أو جماعة ارهابية أو جماعة تنافسية ، أو استخبارات أجنبية ، لذا فقد حددت العديد من الدراسات و الأبحاث خمس فئات مهددة للبناء التحتي المعلوماتي :

- التهديدات الخارجية المحايدة : و تشمل التنصت ، تحليل الاشارات ، تحليل الذروة.
- الهجوم على نظام عامل.
- الهجوم الداخلي.
- الهجمات للوصول الى تعديل النظام " خرق حماية الدخول، الانكشاف"[2].

ثالثا / _ أنواع الجريمة الإلكترونية:لقد صنفت الجرائم الإلكترونية إلى العديد من التصنيفات وفقا للعديد من المعايير ، لكن الراجح أنها تقسم إلى ثلاثة أنواع:

1 / **الجرائم التي تستهدف الأشخاص** : وهي تشمل :

[1] _ اسراء جبريل رشاد مرعي ، المرجع نفسه ، ص 438.
[2] _ ذياب موسى البداينة، المرجع السابق ، ص 18 ، 19.

* **جريمة التهديد** : وهو التهديد الجسيم ضد نفس المجني عليه أو ماله ، أو ضد نفس أو مال الغير، و الذي قد يكون مصحوبا بالأمر ، أو طلب القيام أو الامتناع عن فعل ، عن طريقة وسيلة الأنترنت .

* **انتحال شخصية** : وهو استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانته، وقد تميزت بسرعة الانتشار خاصة في الأوساط التجارية ، وتتم من خلال جمع أكبر قدر من المعلومات للشخصية المراد انتحالها للاستفادة منها لارتكاب جرائمه ، عن طريق استدراج الشخص للإدلاء بمعلوماته الشخصية كالاسم و اللقب ، رقم بطاقة الائتمان للتمكن من الوصول لماله أو سمعته...عن طريق الغش.

* **انتحال شخصية احد المواقع** : من خلال اختراق احد المواقع للسيطرة عليه، ليقوم المجرم بتركيب برنامج خاص به ، باسم الموقع المشهور.

* **جرائم السب و القدف** : وذلك للمساس بشرف الغير و سمعتهم ، فيقوم المجرم بنشر معلومات مغلوطة عن الضحية ، و يكون القذف و السب كتابيا أو عن طريق المطبوعات أو الرسوم ، عبر البريد الالكتروني أو الصوتي ، صفحات الويب...إلخ.

كما تضم الجرائم الإلكترونية الواقعة على الأشخاص ، كل الأفعال المتعلقة بالأنترنت والحاسبات لترويج الدعارة و الفاحشة [1].

2 / الجرائم التي تستهدف الأموال: وهيتشمل :

* **السرقة الواقعة على البنوك** : تتم سرقة المال بالطرق المعلوماتية عن طريق اختلاس البيانات والمعلومات الشخصية للمجني عليهم ،والاستخدام لشخصية الضحية ليقوم بعملية السرقة المتخفية، ما يؤدي بالبنكالى التحويل البنكيللأموال الالكتروني او المادي الى الجاني، حيث يستخدم الجاني الحاسب الالي لدخول شبكة الانترنيت ، والوصول الى المصارف والبنوك،وتحويل الاموال الخاصة بالعملات الى حسابات اخرى.

* **تجارة المخدرات عبر الانترنت:** تتعلق بالترويج للمخدرات وبيعها،والتحريض على استخدامها، وصناعتها بمختلف انواعها.

* **غسيل الأموال:** تمارس عبر الانترنت، حيث استفاد الجناة مما وصل اليه عصر التقنية المعلوماتية ، لتوسيع نشاطهم غيرالمشروع في غسيل اموالهم،و كذا لتشفير عملياتهم وسهولة نقل الاموال واستثمارها ، في محاولة منهملإعطائها الصبغة الشرعية.

* **الاستعمال غير المشروع للبطاقات الائتمانية:** رافق استخدام البطاقات الائتمانية، الاستلاء عليها باعتبارها نقودا الكترونية ، وذلك اما بسرقة ارقام البطاقات ، ثم بيع المعلومات للآخرين، منخلال الحصول على كلمة السرالمدرجة في ملف انظمة الحاسب الالي للضحية ، عن طريق الاحتيال،وذلك بإيهامه بحصوله على أرباح ،فيقدم الضحية معلومات تمكن الجاني من التصرف في ماله.

[1] _ سورية ديش، انواع الجرائم الالكترونية واجراءات مكافحتها، مجلة الدراسات الاعلامية ، المركز الديمقراطي العربي، العدد 1، جانفي ، 2018، ص 241 ، 242 .

* **الجرائم الواقعة على حقوق الملكية الفكرية و الأدبية :** يمكن أن يكونالنظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفكرية ، والسطو على المعلومات التي يتضمنها نظام معلوماتي آخر، و تخزين واستخدام هذه المعلومات دون إذن صاحبها ، فيعد ذلك اعتداء على الحقوق المعنوية و على قيمتها المادية[1].

* **قرصنة البرمجيات :** هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية ، على اسطوانات وبيعها للناس بسعر أقل ، وجريمة نسخ المؤلفات العلمية و الأدبية بالطرق الإلكترونية المستحدثة ، حيث أن المعلومات الأدبية و الفكرية ذات قيمة أدبية و مادية ، بالإضافة إلى براءة الإختراع، التي تخول لمالكها حق معنوي و آخر مالي.

3/ _ الجرائم الواقعة على أمن الدول :

* **الارهاب:** تستخدم المجموعات الارهابية حاليا تقنية المعلومات لتسهيل الاشكال النمطية من الاعمال الاجرامية،وبث الاخبار المغلوطة، وتوظيف بعض صغار السن، وتحويل بعض الاموال في سبيل تحقيق اهدافها.

ويقوم الارهابيون في العصر الحديث باستخدام الانترنت لاستغلال المؤيدين لأفكارهم ، وجمع الاموال لتمويل برامجهم الارهابية، وللاستيلاء على المواقع الحساسة وسرقة المعلومات ، و نشر الفيروسات،وذلك في ظل وجود برامج الكمبيوتر القوية و سهلة الاستخدام ،والتي يمكن تحميلها مجانا.

* **التجسس:**يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات والمؤسسات الوطنية أو الدولية، وتستهدف بشكل خاص التجسس العسكري، السياسي ،وحتى الاقتصادي،وذلك باستخدام التقنية المعلوماتية، وهذه العملية تمارس من قبل دولة على دولة، او من شركة على شركة و غير ذلك ، بهدف الاطلاع على المعلومات الخاصة المؤمنة في جهاز الحاسب الآلي ،وغير مسموح بالاطلاع عليها،كأن تكون من قبيل أسرار الدولة[2].

خاتمة :

بعد دراستنا لموضوع بحثنا المعنون ب" خصوصية المفهوم العام للجريمة الإلكترونية "، و الذي حاولنا من خلاله الاجابة على الاشكاليات المطروحة ، من خلال تقسيم دراستنا إلى ثلاثة أقسام ، فتناولنا تباعا التعريف ، الخصائص ، الأسباب و التصنيفات ، و قد توصلنا في نهاية بحثنا إلى مجموعة من النتائج و التوصيات ، نورد أهمها فيمايلي :

أولا –النتائج:

1 – لم يتفق الفقه العربي و الغربي على تعريف جامع مانع للجريمة الإلكترونية ، فكل فريق حاول وضع تعريف لها ، بالتركيز على جانب محدد و على حساب جوانب أخرى ، متجاهلين أنها جريمة ذات طابع خاص ، كونها من الجرائم المستحدثة ، وفي حالة تطور مستمر، وتتطلب أداة ذات تقنية عالية ، ومجرم متخصص و محترف ، و له درجة عالية من الذكاء ، له مهارات و قدرات تقنية تمكنه من ارتكاب جرمه

[1] _ سورية ديش ، المرجع السابق ، ص 243، 244.
[2] _ سورية ديش ، المرجع نفسه ، ص 245 ، 246.

العابر للحدود، دون انتقال من مكان لآخر، فترتكب الجريمة بكل عناصرها القانونية ، و تلحق أضرارا معنوية أو مادية بالغير ، سواء الأفراد أو المؤسسات أو حتى الدول ، من خلال اختراق النظام المعلوماتي.

2 – إن أسباب و دوافع ارتكاب الجريمة الإلكترونية ، منها ما هو ذو طابع عام كالعولمة ، والتحول للمجتمع الرقمي ، ومنها ما هو ذو طابع خاص ، كسن الجاني و مستواه التعليمي، فقد يكون مجرد شاب هاو ، كما قد يكون متعلما و محترفا لكنه فقير ، أو محترفا ، غنيا وفضوليا، كما قد يكون محبا أو كارها أو متعصبا ، أو مؤيدا لقضية، لذا يمكن القول أن أسباب ارتكاب هذا النوع من الجرائم هي الظروف و العوامل الخاصة بكل مجرم على حدة ، إضافة إلى المسببات العامة المعروفة.

3 –توجد العديد من المعايير التي تم الاعتماد عليها في تصنيف الجرائم الإلكترونية ، لكن التصنيف الراجح ، قائم على حسب الطرف الواقع عليه السلوك الإجرامي، فإما على الأشخاص أوالأموال ، أو على أمن الدول، و هذا يعني أن أضرارها يمكن أن تطال الجاني إقتصاديا أوسياسيا، أو اجتماعيا أو أخلاقيا أو مهنيا أو عسكريا ، أو أمنيا.

ثانيا –التوصيات:

– ضرورة وضع نظام قانوني على مستوى القوانين الداخلية والقانون الدولي، للجريمة الإلكترونية ، بتجريمها وطنيا و دوليا من خلال نصوص قانونية واضحة ، و شاملة ، ومتضمنة لكل المفردات التقنية المتعلقة بهذا النوع من الجرائم ، لتبقى مهمة الفقيه سواء على المستوى الوطني أو الدولي ، تفسيرها و شرحها وفقا لما يتناسب و إرادة المشرع.

2 –تخصيص أقسام في كليات الحقوق على مستوى الجامعات ، لتدريس الجريمة الإلكترونية ، و التعريف بعمومياتها وجزئياتها ، مع تشجيع الباحثين في هذا المجال.

3 – تشجيع إنتاج برامج مكافحة الجرائم الإلكترونية ، باعتبارها جريمة الكترونية ، فلابد من محاربة و مكافحة التقنية بالتقنية الأكثر تطور منها.

4 – التعاون و التنسيق بين الدول من خلال ابرام المعاهدات الدولية الثنائية و المتعددة الأطراف لمكافحة الجريمة الإلكترونية ، و التخفيف من أضرارها، و كذا تلك المتعلقة بتسليم المجرمين والمساعدة القضائية ، و تبادل الخبرات قانونيا و قضائيا و تكنولوجيا و أمنيا.

5 – تأسيس مراكز وطنية لتدريب الشرطة ، للوقاية من الجريمة الإلكترونية و مكافحتها.

قائمة المراجع:

أولا : الكتب

– سعيد بن سالم البادي ، و آخرون ، الجريمة الإلكترونية في المجتمع الخليجي ، و كيفية مواجهتها ، أكاديمية السلطان قابوس لعلوم الشرطة ، سلطنة عمان ، 2016.

ثانيا : مذكرات الماجستير

– عبد الله دغش العجمي ، المشكلات القانونية و العملية للجرائم الإلكترونية ، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، 2014.

ثالثا: المجلات

– اسراء جبريل رشاد مرعي ، الجرائم الإلكترونية ، " الأهداف _ الاسباب _ طرق الجريمة ومعالجتها "، مجلة الدراسات الاعلامية ، المركز الديمقراطي العربي ، العدد الأول ، جانفي 2018.

– سورية ديش، انواع الجرائم الالكترونية واجراءات مكافحتها، مجلة الدراسات الاعلامية ، المركز الديمقراطي العربي، العدد 1، جانفي ، 2018.

– عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية و أزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العدد 7، 2011 .

– عبد السلام محمد المايل ، عادل محمد الشربجي، الجريمة الالكترونية في الفضاء الالكتروني، المفهوم ، الأسباب ، سبل المكافحة مع التعرض لحالة ليبيا ، مجلة آفاق للبحوث و الدراسات ، العدد 4، جوان 2019.

– مخلد ابراهيم الزعبي ، فاعلية القوانين و التشريعات العربية في مكافحة الجرائم الإلكترونية ، المجلة العربية للنشر العلمي، العدد 37 ، تشرين الثاني 2021.

– معزوز ربيع ، زروقي عاسية ، الجريمة الإلكترونية و إجراءات مواجهتها في التشريع الجزائري، المجلد 7 ، العدد 2 ،2001 .

رابعا : الملتقيات

– ذياب موسى البداينة، الجرائم الإلكترونية ، المفهوم و الأسباب، ضمن أعمال الملتقى الموسوم : الجرائم المستحدثة في ظل المتغيرات و التحولات الاقليمية والدولية، من 2 إلى 4 أفريل 2014، كلية العلوم الاستراتيجية ، المملكة الأردنية الهاشمية .

بطيحي نسمة
nesmabettihi@yahoo.com
جامعة سطيف 2

ماهية الجرائم الإلكترونية:

(دراسة تحليلية في مفهوم الجريمة الإلكترونية وخصائصها وأنواعها)

الملخص:

وُجِدت الجرائم الإلكترونية مع ظهور أنظمة الحاسب الآلي ووسائل الاتصال واتساع استخدامها في حياة الإنسان. وهي من الجرائم الخطيرة بالنظر لحجم الخسائر الكبير الناجم عنها؛ كونها تستهدف البيانات والمعلومات بمدلولها التقني الواسع، كما أن آثارها قد تتجاوز حدود الدولة الواحدة.

وقد أسالت هذه الظاهرة الإجرامية الجديدة الكثير من الحبر حول مفهومها وتحديد أنواعها من جانب الفقه القانوني، ذلك أن فهم هذه الجريمة من شأنه أن يساعد في تحديد وسائل مكافحتها وردع مرتكبيها، كما أدلت التشريعات أيضا بِدَلوِها في هذه المسألة.

الكلمات الدالة: الجريمة الإلكترونية – الحاسب الآلي – وسائل الاتصال – المعلومات.

Abstract:

Cybercrime have been found with the advent of computer systems and means of communication and their wide use in all areas of life, it is a serious crime in view of large losses that result from it, as it targets data and information, and its effects may exceed the borders of a single country.

This new criminal phenomenon has sparked controversy over its concept and the determination of its types by jurisprudence and various legislations, because understanding this crime would help in identifying the means of combating it and deterring its perpetrators.

Keywords*: cyber crime – computer – communication Tools – information.*

مقدمة:

تتنوع الجرائم وتختلف أنواعها مع مرور الزمن، فعندما اخترع الإنسان أنظمة الحاسب الآلي ووسائل الإتصال، ساهمت هذه الأخيرة في تطوير حياته، كما سهلت أمور حياته، لِمَا لها من قدرات تقنية استثنائية، غير أنها بالمقابل لم تسلم من أيادي المجرمين، الذين استغلوها لأغراضهم غير المشروعة، وظهر على إثر ذلك نوع جديد من الجرائم سُمِيَ بالجرائم الإلكترونية.

أولا: أهمية الدراسة

وقد ارتأينا من خلال الدراسة الحالية أن نسلط الضوء على هذه الظاهرة الإجرامية الجديدة، من خلال تحديد مفهومها، المرتبط أساسا بأدوات التكنولوجيا الحديثة، المُسَماة بأنظمة الحاسب الآلي ووسائل الإتصال،

كما أن توضيح معالم هذه الجريمة بطريقة أفضل يتجسد من خلال التعرف على خصائصها، التي جعلت منها جريمة فريدة من نوعها، سواء كان ذلك بين الجرائم التقليدية أو الحديثة منها، كما تهدف هذه الدراسة أيضا إلى الوقوف على الأنواع المختلفة والأصناف المتشعبة التي تندرج ضمن إطار الجرائم الإلكترونية.

إضافة إلى ذلك يعد التعرف على بعض الجوانب السلبية لأدوات التكنولوجيا الحديثة من الأهمية بمكان في نشر الوعي وأخذ الحيطة والحذر.

ثانيا: إشكالية الدراسة

طرحت الجريمة الإلكترونية – ولازالت تطرح – بالنظر لحداثتها عديد الإشكاليات على الصعيد القانوني، لاسيما في شقه المتعلق بالقانون الجنائي، وقد أثرنا من خلال هذه الدراسة أحد أهم هذه الإشكاليات، التي نعرضها بالصياغة التالية: **هل من الممكن الوصول لتحديد مفهوم دقيق للجريمة الإلكترونية، وكذا حصر أنواعها، بالشكل الذي يساعد في رسم السياسة الجنائية السليمة في مكافحة هذه الجريمة وردع مرتكبيها؟**

ثالثا: تقسيم الدراسة

سنحاول في (المبحث الأول) أن نتعرف على **مفهوم الجريمة الإلكترونية** ، من خلال البحث في **تعريفها**(المطلب الأول) و **خصائصها**(المطلب الثاني)،وفي (المبحث الثاني)نتناول **أنواع الجرائم الإلكترونية**، بتقسيمها إلى نوعين، يتمثل النوع الأول في **الجرائم الإلكترونية التي يعد النظام المعلوماتي وسيلة في ارتكابها** (المطلب الأول)، والنوع الثاني المتمثل في **الجرائم الإلكترونية التي يعتبر النظام المعلوماتي هدفا لها** (المطلب الثاني).

المبحث الأول: مفهوم الجريمة الإلكترونية

ظهرت الجرائم الإلكترونية بظهور تكنولوجيا المعلومات، حيث تعد من المظاهر المصاحبة لها، وقد تفردت هذه الجرائم عن غيرها من الجرائم، التقليدية منها والحديثة، بمجموعة من المميزات.

لتوضيح ملامح هذه الجريمة ارتأينا أن نخصص (المطلب الأول) للبحث في **تعريف الجريمة الإلكترونية**، و(المطلب الثاني) **لخصائصها**.

المطلب الأول: تعريف الجريمة الإلكترونية

بذل الفقه الجنائي مجهودا كبيرا في تعريف الجريمة الإلكترونية، كما سعى المشرع الجزائري بدوره إلى تحديد موقفه حيال هذه المسألة. نبحث في (الفرع الأول) في **الجهود الفقهية المبذولة لتعريف الجريمة الإلكترونية**، ونخصص (الفرع الثاني) لدراسة **موقف المشرع الجزائري من ذلك.**

الفرع الأول: الجهود الفقهية المبذولة لتعريف الجريمة الإلكترونية

عرفت مسألة تعريف الجريمة الإلكترونية [1] اختلافا وجدلا فقهيا كبيرا، مِمَا دفع إلى القول أن هذه الجريمة تستعصي على التعريف، نحاول توضيح هذا الإختلاف – باختصار– من خلال تقسيم هذه التعاريف ضمن ثلاث أصناف رئيسية، هـي:

أولا: التعاريف التي ترتكز على أداة ارتكاب الجريمة

يتجه جانب من الفقه إلى أن الفعل الإجرامي يندرج ضمن قائمة الجرائم الإلكترونية إذا استُخدِم النظام المعلوماتي في ارتكابه، أي عُدَ هذا الأخير وسيلة رئيسية في اقترافه، ومن هذا المنطلق عرف أصحاب هذا الإتجاه الجريمة الإلكترونية على أنها أي فعل إجرامي يرتكب باستخدام الحاسب الآلي، أو أنها أي سلوك إجرامي يستخدم فيه الحاسب الآلي كأداة رئيسية [2]، كما اتجه آخرون إلى القول أنها تلك الجرائم التي تلعب فيها البيانات والبرامج المعلوماتية دورا رئيسيا[3].

ثانيا: التعاريف التي ترتكز على محل الجريمة

يرى أنصار هذا الإتجاه أنه لابد من اعتماد محل الجريمة كمعيار في تحديد هذه الجرائم، فهم يرون أن الجريمة الإلكترونية تعتبر كذلك إذا ما كان محلها جهاز الحاسب الآلي (أي النظام المعلوماتي) [4]. لذلك عرف هذا الإتجاه الجريمة الإلكترونية على أنها كل سلوك غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تلك التي تُحَول عن طريقه[5].

ثالثا: التعاريف التي ترتكز على طبيعة المجرم المعلوماتي

يعتمد أصحاب هذا الإتجاه على معيار شخصي محض يقوم علىمدى معرفة الجاني بالتقنية المعلوماتية، لذلك عرفت الجريمة الإلكترونية وفقا لهذا الإتجاه على أنها ذلك الفعل الإجرامي الذي يكون فيه الجاني مُلِما بتقنية المعلومات وبأنظمة الحاسب الآلي[6].

والحقيقة أن أيا من التعاريف السابق ذكرها لم تسلم من النقد:

فما يعاب على **الإتجاه الأول**، الذي يركز على وسيلة ارتكاب الجريمة، أنه تعريف بالغ العمومية والإتساع؛ إذ اعتبر مناصروه أن وصف الجريمة الإلكترونية ينطبق على كل فعل مجرم يُقترف باستعمال نظام الحاسب الآلي وهو ما لا يمكن قبوله، على أساس أن هناك الكثير من الجرائم ترتكب بِمَعية أنظمة الحاسب الآلي ومع ذلك تبقى جرائم عادية [7]، كجرائم التشهير التي تتم عبر وسائل التواصل الإجتماعي،كما أنه من المعروف أن المشرع إذا أراد أن يجرم فعلا معينا فإنه لا ينظر – في الغالب – إلى وسيلة اقترافه، إنما يأخذ في الإعتبار خطورة هذا الفعل على أمن المجتمع.[8]

كما لم يسلم **الإتجاه الثاني** من النقد، حيث فصل أصحابه في نطاق الجرائم الإلكترونية، لتقتصر على جرائم المساس بالنظام المعلوماتي، وإهمالهم لتلك التي ترتكب بواسطة النظام المعلوماتي ويكون لهذه الأخيرة دور جوهري في ارتكابها كجرائم الإحتيال المعلوماتي، جرائم التلاعب ببطاقات الإئتمان الممغنطة[9].

بالنسبة **للإتجاه الثالث**، الذي يركز على مهارات مرتكب الجريمة الإلكترونية، فإنه بدوره لم يسلم من النقد، من منطلق أنأدوار الجناة في الجريمة الإلكترونية تتنوع بين التخطيط والتحضير والتنفيذ، ومن الوارد أن لا تتوفر لدى البعض منهم المهارة والمعرفة التقنية، كما أنه معيار مرن وغير دقيق، ذلك أن الأخذ بهذا المعيار يقودنا إلى التساؤل عن معايير تحديد المعرفة التقنية للقول بقيام الجريمة؟[10]

نخلص على ضوء ما أبديناه من اختلاف فقهي بشأن تحديد مفهوم الجريمة الإلكترونية، أنه من الصعب تحديد تعريف جامع ومانع للجريمة الإلكترونية، حتى أنه قيل عن هذه الجريمة أنها تقاوم التعريف، ولعل السبب في ذلك يرجع – ربما– إلى حداثة هذه الجريمة المرتبطة أساسا بتكنولوجيا المعلومات، هذا المجال الذي يتسم بالمرونة وسرعة التطور، ناهيك عن أن استخدام هذه الأداة التكنولوجية الحديثة من طرف الجناة لم يسفر عن جرائم جديدة وُجدت بوجود هذه التكنولوجيا فحسب، بل أن هذه الأداة استُخدمت أيضا في ارتكاب الجرائم التقليدية المعروفة كجرائم السرقة والإحتيال، ما أدى بدوره إلى طرح إشكالات عديدة على الصعيد القانوني.

الفرع الثاني: موقف المشرع الجزائري من تعريف الجريمة الإلكترونية

تدخل المشرع الجزائري بموجب القانون رقم 15/04 المؤرخ في 2004/11/10[11]، بتجريم طائفة من الأفعال تحت مُسمى جرائم (المساس بنظام المعالجة الآلية للمعطيات)، ولم يعرف هذه الجرائم إلا بعد صدور القانون رقم 04/09 المؤرخ في 26 أوت 2009 المتضمن القواعد الخاصة للوقاية من هذه الجرائم [12]، التي جاء في المادة الثانية (2) منه أن الجرائم المتصلة بتكنولوجيا الإعلام والإتصال هي:(جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية).

والملاحظ أن التعريف الذي جاء بالمادة الثانية من القانون رقم 04/09 أعلاه، كان واسعا، حيث اعتبر أن أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية تعتبر من قبيل الجرائم الإلكترونية، وقد استحسن البعض من الشراح ذلك على أساس أنه بالإمكان إدخال أنواع جديدة من الجرائم قد تظهر مستقبلا نتيجة ما تفرزه التكنولوجيا الحديثة من جديد في هذا المجال [13]، في الوقت الذي انتقد بشدة غيرهم من الشراح خوض المشرع في تعريف الجريمة الإلكترونية، خاصة وأن التعريف جاء واسعا وفضفاضا، الأمر الذي يتعارض مع ما تقتضيه النصوص الجنائية من الدقة والوضوح، ورأوا أنه كان من الأجدر على المشرع أن لا يخوض في هذه المسألة ويترك أمر البحث فيها للفقه[14].

بين هذا الرأي وذاك، نعتقد أن تدخل المشرع الجزائري في قانون العقوبات وحتى في القانون رقم 04/09، لم يكن لغرض تحديد تعريف للجريمة الإلكترونية أو حصر أنواعها، إنما كان لاعتبارات عملية بحتة، تتمثل فـي:

من جهة، إن تدخل المشرع بالتجريم في قانون العقوبات لطائفة محددة من الجرائم، وهي تلك الجرائم الجديدة، التي تسمى عادة بالجرائم المعلوماتية البحتة، كجريمة الدخول إلى النظام المعلوماتي أو جرائم إتلاف المعطيات ونحوها، هذه الأخيرة لا يمكن للنصوص التقليدية في قانون العقوبات أن تحتوي الإشكالات التي تطرحها، كونها مرتبطة وجودا وعدما بأنظمة الحاسب الآلي، لذلك كان لزاما على المشرع أن يتدخل بالتجريم تطبيقا لمبدأ شرعية الجرائم والعقوبات وردعا للجناة الذين يستغلون التكنولوجيا لأغراض إجرامية، لاسيما بعد أن اكتسحت أنظمة الحاسب الآلي كافة المجالات على المستوى الوطني.

ولا يعن اقتصار المشرع بالتجريم لقائمة محددة من الأفعال في قانون العقوبات أن نية المشرع اتجهت إلى أن غيرها من الأفعال لا يعد من قبيل الجرائم الإلكترونية.

من جهة ثانية، وفيما يخص تدخل المشرع الجزائري لاحقا بموجب القانون رقم 04/09، فإن ذلك كان لغرض تحديد مجال تطبيق الإجراءات المحددة في القانون رقم 04/09، بما معناه أن المشرع أقر بأنه يمكن تحصيل الدليل الجنائي للجرائم المحددة بالمادة الثانية أعلاه، التي يساهم النظام المعلوماتي في ارتكابها (وهي جرائم المعالجة الآلية للمعطيات المجرمة في القسم السابع مكرر من قانون العقوبات، الجرائم التي ترتكب بواسطة النظام المعلوماتي، الجرائم التي يسهل ارتكابها بواسطة النظام المعلوماتي)، بالإعتماد على الإجراءات الواردة بهذا القانون، وعليه فإنه ينبغي أن يُحمل هذا التعريف محملا ضيقا يقتصر على القانون رقم 04/09، ولا ينصرف إلى الجزم بأن المشرع الجزائري قد فصل بصفة نهائية في مفهوم الجريمة الإلكترونية، بدليل أن المشرع نص في المادة الثانية من القانون أعلاه أنه: ((يُقصد في مفهوم هذا القانون ....)).

نشير أن اللجوء إلى التعريف لم يقتصر على المشرع الجزائري، بل خطت على نهجه تشريعات أخرى، من ذلك مثلا ما أقدم عليه المشرع الكويتي في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات [15] الذي عرف ما سماه بالجريمة المعلوماتية على أنها: ((كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون))، كذلك فعل المشرع القطري في المادة الأولى من قانون مكافحة الجرائم الإلكترونية[16].

المطلب الثاني: الخصائص المميزة للجريمة الإلكترونية

تتميز الجريمة الإلكترونية عن غيرها من الجرائم بمجموعة من المميزات الخاصة، التي جعلت منها جريمة فريدة من نوعها، تتمثل فـي:

الفرع الأول: الجريمة الإلكترونية جريمة عابرة للحدود

تعد الجريمة الإلكترونية على حد وصف البعض من قبيل الجرائم العابرة للحدود الوطنية أو الجرائم ذات الطبيعة المتعدية الحدود، كونها ترتكب في بيئة افتراضية غير محسوسة لا تعترف بالحواجز الجغرافية، الأمر الذي يجعل من الممكنأن يرتكب الجاني الجريمة دون أن يكون متواجدا ماديا في مسرحها، ما يؤدي بدوره إلى إلى أن ينفصل الفعل أو النشاط الإجرامي عن نتيجته مكانا وزمانا[17].

وقد خلفت هذه الطبيعة المتميزة للجريمة الإلكترونية العديد من المشاكل القانونية، حول تحديد الدولة صاحبة الإختصاص القضائي، وتحديد القانون الواجب تطبيقه، وكذا الإشكاليات التيتتعلق بإجراءات الملاحقة القضائية، ومن ثمة فإن التحري والتحقيق بشأن هذه الجرائم يحتاج إلى خبرة فنية عالية المستوى[18].

الفرع الثاني: الجريمة الإلكترونية صعبة الإثبات

إن تحصيل الدليل الجنائي في الجرائم الإلكترونية من الصعوبة بمكان، كونها ترتكب في عالم افتراضي تغيب فيه الآثار المادية الملموسة، ما يزيد من الأمر صعوبة هو أن الجاني عادة ما يستخدم تقنيات

حماية فعالة عقب ارتكاب جرمه بغية عرقلة الوصول إلى الدليل ومن ثمة الإفلات بسهولة من قبضة العدالة[19].

إنه من الأمور الصعبة في العالم الإفتراضي نسبة السلوك الإجرامي لشخص معين، وهو ما جاء تأكيده في عدة قرارات قضائية، على نحو القرار الذي قضت به محكمة استئناف باريس في 2007، حينما أكدت على أن عنوان البروتوكول (IP)لا يدل إلا على تسلسل أرقام مرتبطة بآلة وليس بشخص[20].

الفرع الثالث: الجرائم الإلكترونية جرائم خالية من العنف

كثيرا ما وُصِفَت الجرائم الإلكترونية بالجرائم الناعمة ، كونها أقل عنفا من الجرائم التقليدية كالسرقة والقتل وجرائم الإرهاب والمخدرات التي تتطلب جهدا عضليا كبيرا، فالمجرم في الجرائم الإلكترونية لا يحتاج في نقل البيانات من حاسب إلى آخر أو السطو على أرصدة البنوك سوى للمسة زر بسيطة على حاسبه الآلي[21].

الفرع الرابع: امتناع المجني عليهم في الجرائم الإلكترونية عن التبليغ

تتميز الجريمة الإلكترونية بالتكتم وعدم التبليغ عنها من طرف ضحاياها، ويرجع ذلك إلى التخوف من الفضيحة كما هو عليه الشأن فيما يخص الجرائم الإلكترونية التي تمس بخصوصيات الأفراد، أو التخوف من إمتناع الأشخاص عن التعامل مع الضحية – كما لو كانت بنكا أو شركة – في حال علموا بالهجمات الإلكترونية التي وقعت ضحيتها، مخافة الإضرار بمصالحهم[22].

من جهة أخرى، قد تتخوف الشركات التجارية من أن ينجم عن عمليات التحري والتحقيق التي تقوم بها الشرطة حجز لأجهزتها أو تعطيل لشبكاتها لمدة طويلة، ما قد يلحق بها خسائر مادية كبيرة، فإجراءات التحقيق الخاطئة إذا قد تؤدي إلى خسائر كبيرة من الممكن أن تتجاوز ما قد تتسبب فيه الجريمة في حد ذاتها[23].

من كل ذلك نخلص إلى أن خصائص الجريمة الإلكترونية هي ما جعلت منها جريمة شديدة الخطورة على الأفراد وأمن الدول، ما يجعل من الضروري أن يتم التعامل معها بطريقة تتناسب مع خصوصيتها وطبيعتها.

المبحث الثاني: أصناف الجرائم الإلكترونية

تتعدد الجرائم الإلكترونية، فهي ليست نوعا واحدا، غير أنه يمكن تصنيفها إلى مجموعتين أساسيتين، هما: الجرائم التي **يعتبر فيها النظام المعلوماتي أداة للجريمة** ، وهنا نكون أمام جريمة تقليدية، غير أنها ارتكبت بأسلوب غير تقليدي، والجرائم **التي يعد النظام المعلوماتي فيها هدفا للجريمة** ، وقد يحدث هذا النوع من الجرائم داخل المؤسسات من طرف موظفيها وعمالها، أو من أشخاص خارجيين عنها. نتناول كل نوع من هذه الجرائم في مطلب مستقل.

المطلب الأول: الجرائم التي يعتبر النظام المعلوماتي وسيلة لارتكابها

يقوم الجناة بالإستفادة من المزايا التي تحوز عليها أنظمة الحاسب الآلي وشبكات الإتصال، وارتكاب الجرائم العادية المعروفة، سواء تلك التي تستهدف المساس بأمن الدولة واستقرارها، أو سلب أموال الغير دون وجه حق أو المساس بحرمة حياتهم الخاصة.

نتعرف في (الفرع الأول) على **جرائم الإعتداء الإلكترونية على أمن الدولة واستقرارها** ، وفي (الفرع الثاني) على **جرائم الإعتداء الإلكترونية المرتبطة بالأموال** ، ونخصص (الفرع الثالث) للبحث في **جرائم الأموال الإلكترونية المرتبطة بالأشخاص.**

الفرع الأول: جرائم الإعتداء الإلكترونية المرتبطةبأمن الدولة واستقرارها

قد تمثل أنظمة الحاسب الآلي مصدر تهديد كبير، لاسيما لو تم استخدامها للإعتداء على قطاعات استراتيجية وهامة كقطاع الدفاع الوطني أو الهيئات العامة، فلختراق المواقع الأمنية والعسكريةللدولة قد يؤدي إلى الإطلاع على معلومات تتعلق بأسرار الدولة وقراراتها السياسية، ما قد يعرض أمنها واستقرارها للخطر. ومن أمثلة الهجمات التي استهدفت مواقع تابعة لمؤسسات الدولة الحساسة، ذلك الإختراق الذي تعرض له النظام المعلوماتي الخاص بسلاح البحرية الفرنسية عام 1994 وقد تم الحصول من وراء هذه العملية على معلومات عسكرية هامة تخص السفن التي تستخدمها الجيوش التابعة للدول الأعضاء في حلف شمال الأطلنطي، وعلى إثر هذه الهجمات أقدمت السلطات العسكرية الفرنسية على تصميم برامج جديدة لحماية أنظمتها[24].

على هذا الأساس، تشدد المشرع الجزائري في مقدار العقوبة فيما لو أقدم الجناة على ارتكاب جرائم الدخول أو التلاعب بالمعطيات وكان ذلك بهدف المساس بالهيئات العامة للدولة، حيث جاء في المادة 394 مكرر3 من قانون العقوبات على أنه :((تُضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفلع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد)).

كذلك جرم المشرع الجزائري بنص تجريمي منفرد أفعال المساس بأنظمة المعالجة الآلية للمعطيات التي تتم لغرض إرهابي؛ إذ نصت المادة 87 مكرر12 من قانون العقوبات، (المستحدثة بموجب القانون رقم 16 – 02 المؤرخ في 19 يونيو 2016، المتمم والمعدل للأمر رقم 66 – 156 المؤرخ في 8 يوليو 1966[25])أنه: ((يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 د.ج إلى 500.000 د.ج كل من يستخدم تكنولوجيا الإعلام والإتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أوتقع أنشطتها تحت طائلة أحكام هذا القسم، أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة)).

وإدراكا من المشرع الجزائري بخطورة الهجمات الإلكترونية التي تطال مؤسسات الدولة العامة، قام باستحداث إجراءات جديدة في سبيل البحث والتحري عن مرتكبي هذه الجرائم، الذين يستهدفون المساس بأمن الدولة واستقرارها، حيث سمح باللجوء إلى مراقبة الإتصالات الإلكترونية للجماعات الإرهابية وتفتيش الأنظمة

المعلوماتية لغرض البحث عن أدلة تفيد في البحث عن مرتكبي هذه الجرائم، في هذا الإطار نصت المادة الثالثة (3) من القانون رقم 04/09 أنه: ((مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية))

الفرع الثاني: جرائم الإعتداء الإلكترونية المرتبطةبالأموال

سمحت الثورة التكنولوجية الحديثة بظهور نوع جديد من المعاملات يسمى بالمعاملات الإلكترونية، الذي يختلف عن المعاملات التقليدية، ونتج عن ذلك ظهور أشكال إجرامية جديدة تستهدف الحصول على العائدات المالية بطرق غير مشروعة، على نحو التحويل الإلكتروني غير المشروع وغسيل الأموال الإلكتروني:

أولا: التحويل الإلكتروني غير المشروع للأموال

تتم عمليات التحويل الإلكتروني غير المشروع من خلال التلاعب في أنظمة المعالجة الآلية للمعطيات، بُغية الحصول دون وجه حق على خدمات أو أموال أو أصول معينة، كأن يتم مثلا التلاعب في البيانات المصرفية ونتائج الميزانية والمستحقات المالية[26].

ويعمد الجناة إلى استخدام وسائل كثيرة في عمليات التحايل الإلكترونية، كالبحث عن الرقم السري للمستخدم مثلا، أو عن طريق انتحال شخصية وهمية وإيهام المحتال عليه بوجود مشروع مربح وبالتالي تحويل الأموال إلى رصيد المحتال[27]، ومثل هذه الأفعال من الخطورة بمكان كونها قد تتجاوز الحدود الإقليمية لأكثر من دولة، الأمر الذي قد يضر بالإقتصاد الوطني، كما أن هذه الجريمة قد تؤدي إلى إفلاس شركات وبنوك كبرى في الدولة[28].

وعلى الرغم من ذلك، إلا أنه على الصعيد القانوني لا توجد نصوص قانونية خاصة تعالج مثل هذه المسائل، مع العلم أن اللجوء إلى النصوص القانونية المتعلقة بجرائم الأموال، يعد غير كاف لاحتواء الإشكالات المتعلقة بمثل هذه السلوكات الإجرامية الخطيرة، سواء من حيث التجريم (حيث تطرح هذه الأفعال صعوبة تكييفها وفقا للنصوص التجريمية لجرائم الأموال كونها تنصب على بيانات إلكترونية غير مادية)، أو من حيث العقاب (كون أن بعض التحويلات المالية الإلكترونية قد تحتاج لردعها فرض عقوبات أشد من تلك المحددة في نصوص جرائم الأموال).

ثانيا: عمليات تبييض الأموال الإلكترونية

تعد جريمة تبيض الأموال من أخطر الظواهر الإجرامية التي تهدد اقتصاد الدول، وترتكز هذه الجريمة على قيام الجاني بتحويل الأموال ذات المصادر غير المشروعة(كأن تكون من عائدات جرائم

المخدرات أو السرقات ونحوها) إلى أموال مشروعة، من خلال فصلها عن مصدرها الأصلي بعدة طرق ووسائل تعتمد على الإخفاء والتمويه.

وقد استغل المجرمون ومبيضوا الأموال التطور التكنولوجي لتحديث تقنياتهم في غسل الأموال القذرة على النحو الذي أصبح من الصعب الكشف عنها والقضاء عليها، وتتعدد صور وأساليب اقتراف جريمة تبييض الأموال بواسطة الوسائط الإلكترونية، فمن الممكن أن يتم ذلك مثلا عن طريق البنوك الإلكترونية، التي تعد من أحدث الوسائل التي تسهل عمليات تبييض الأموال غير المشروعة؛ إذ تسمح هذه الوسيلة لمبيضيالأموال تحويل كميات كبيرة من الأموال بسرعة وأمان، كون هذه البنوك تعمل في سرية كاملة بحيث يكون المتعاملين غير معلومي الهوية، كما أن هذه البنوك لا تخضع لأية قوانين[29].

الفرع الثالث: جرائم الإعتداء الإلكترونية المرتبطة بالأشخاص

استخدم الجناة أدوات التكنولوجيا الحديثة في الإعتداء على الأشخاص، ونستعرض فيما يلي بعض الإعتداءات الأكثر انتشارا، حيث نتناول **جرائم الإعتداء على الخصوصية المعلوماتية** (أولا)، ثم **جرائم السب والقذف المعلوماتية.**

أولا: جرائم الإعتداء على الخصوصية المعلوماتية

يعد الإعتداء على الحق في الخصوصية المعلوماتية من أبرز أشكال الجرائم الإلكترونية المرتبطة بالأشخاص. وتظهر العلاقة بين الحق في الحياة الخاصة وأدوات التكنولوجيا الحديثة من خلال ما تقدمه هذه الأدوات من خدمات هامة، كونها باتت تعتبر مستودعا للكثير من أسرار الأشخاص، فيما بات يعرف ببنوك أو قواعد البيانات، التي تضم معلومات لا حصر لها عن الأفراد، سواء كانت تتعلق بوضعهم العائلي أو المادي أو الصحي أو التعليمي أو المهني، وهذا الأمر قد يفتح المجال على مصراعيه لإساءة استخدامها أو توجيهها توجيها مُنحرفا بُغيَة مراقبة الأفراد والكشف عن خصوصياتهم.

إن حجم المخاطر الكبير الناجم عن هذه التكنولوجيات الحديثة لفت الإنتباه إلى أهمية الحماية القانونية للحق في الخصوصية المعلوماتية، لذلك لجأت مختلف الدول إلى سن تشريعات خاصة بحماية المعطيات الشخصية، وكانت المبادرات الأولى لهذه الحماية على المستوى الأوروبي مع نهاية السبعينيات، ولم يسن المشرع الجزائري تشريعا خاصا في هذا الأمر إلا سنة 2018، بموجب القانون رقم 07/18 المؤرخ في 10 يونيو 2018، المتعلق بحماية المعطيات الشخصية [30]، هذا الأخير قام بتنظيم مسألة جمع وتخزين بيانات الأفراد الشخصية، كما أنشأ هيئة خاصة تتكفل بمراقبة مدى احترام الهيئات العامة والخاصة التي تقوم بتخزين بيانات الأفراد للمقتضيات القانونية المحددة في القانون رقم 07/18، كما جرم المشرع الجزائري أيضا كافة أشكال التعدي على الحق في الخصوصية المعلوماتية، كالنشر غير المشروع للبيانات الشخصية، تجاوز غرض المعالجة المرخص به، الجمع غير المشروع للمعطيات الشخصية.

ثانيا: جرائم السب والقذف المعلوماتية

أتاحت وسائل التواصل الإجتماعي والمواقع الإلكترونية فرصا أكثر للتواصل بين الأفراد، كما أن هذا التواصل يتم في عالم افتراضي بسرعة كبيرة، بين عدد لا محدود من الأفراد. وقد سهلت هذه الوسائل في الوقت ذاته ارتكاب جرائم السب والقذف؛فالمتصفح لصفحات مواقع التواصل الإجتماعي أو القارئ لتعليقات الزوار بالصحف الإلكترونية، سينتبهحتما إلى العدد الكبير لجرائم السب والقذف عبر الأنترنت أو الهاتف، سواء كان ذلك من خلال المكالمات أو الرسائل أو مواقع التواصل الإجتماعي، مثل فيس بوك أو واتساب وغيرها، ولغرض البحث عن الشهرة وسعيا للحصول على أكبر عدد ممكن من المشاهدات أصبح بعض الأفراد لا يفرقون بين المسموح والمحظور، فيخوضون في كلام يسيء لكرامة غيرهم دونما ضمير ولا أخلاق[31].

وقد عمل المشرع الجزائري على حماية الأشخاص من أفعال السب والقذف التي يتعرضون لها، من خلال المادة 296 من قانون العقوبات،إضافة إلى وجود بعض القوانين الخاصة التي تكرس الحماية القانونية للأفراد في هذا المجال، كقانون الإعلام[32]، حيث نصت المادة 92 من ذات القانون أنه: ((يمنع انتهاك الحياة الخاصة للاشخاص وشرفهم واعتبارهم)).

نشير إلى أن المادة 21 من اتفاقية مكافحة جرائم تقنية المعلومات، التي صادقت عليها الجزائر[33]، قد أوصت الدول الأعضاء على تشديد العقوبات في الفرض الذي ترتكب فيه الجرائم التقليدية باستخدام الأداة المعلوماتية.

المطلب الثاني: الجرائم التي يعتبر النظام المعلوماتي هدفا لها

إن استخدام أنظمة الحاسب الآلي في ارتكاب الجرائم أسفر عنه ظهور نوع جديد من الجرائم، ليس له مثيل في قانون العقوبات التقليدي، سُمِي بجرائم المعالجة الآلية للمعطيات أو الجرائم الإلكترونية البحتة، كونها جرائم متصلة وجودا وعدما بأنظمة الحاسب الآلي.

وقد قام المشرع الجزائري، (وغيره من المشرعين في الدول العربية والغربية)، بتنظيم هذا النوع الجديد من الجرائم، بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، المتعلق بتعديل قانون العقوبات، ويمكن معالجة هذه الجرائم من خلال التطرق في (الفرع الأول) **لجريمة الدخول أو البقاء في النظام** ، وفي (الفرع الثاني) **لجريمة التلاعب بالمعطيات داخل النظام** ، وفي (الفرع الثالث) نخصصه **لجريمة إساءة استخدام معطيات النظام المعلوماتي.**

الفرع الأول: جريمة الدخول أو البقاء إلى النظام المعلوماتي

تعد جريمة الدخول أو البقاء داخل النظام المعلوماتي أهم جريمة من الجرائم الإلكترونية، على أساس أن الدخول إلى النظام يكون عادة هو الخطوة الأساسية الأولى في ارتكاب باقي الجرائم الإلكترونية. وقد جرم المشرع الجزائري هذا الفعل في المادة 394 مكرر من قانون العقوبات، التي تنص على أنه:((يعاقب بالحبس من ثلاثة أشهر إلى سنة، وبغرامة من 50.000 د ج إلى 200.000 د ج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 د ج إلى 150.000 د ج)).

والملاحظ أن المشرعجرم فعلين إجراميين في نص واحد، هما **فعل الدخول إلى النظام** أي الولوج داخله دون أن يكون للجاني الحق في ذلك، كما لم يغفل المشرع عن **تجريم فعل البقاء** أيضا، والذي يحدث عادة عندما يلج الجاني بطريق الخطأ أو الصدفة إلى النظام، كأن يجرب شخص معين عدة أرقام فيكتشف صدفة الرقم السري للنظام وبدلا من أن يقطع صلته بالنظام يستمر داخله عمدا[34].

ما ينبغي التأكيد عليه أيضا هو تأثر المشرع الجزائري بالطابع التقني لهاتين الجريمتين، بدليل إدراجه لمصطلحات ذات طابع تقني (الدخول – البقاء – معطيات معلوماتية – تخريب نظام اشتغال المنظومة) في صلب نص التجريم. وبمناسبة الحديث عن الطابع التقني لهذه الجريمة، نشير إلى أن عملية الدخول إلى النظام قد لا تحتاج أحيانا خبرة فنية عالية؛ إذ من الممكن أن تتم بمجرد العثور بصفة تلقائية على الرقم السري للنظام، كما قد يتطلب الدخول أحيانا خبرة فنية كبيرة، كأنيتحصلالجانيعلى كلمةالسر عنطريقبرامجمعينةأومنخلالاستغلالالثغاراتالبرمجية، التييتركهاالمبرمجونعادة لدخول لاحقا وإحداث بعض التعديلاتلغرضالتطوير، وتُترك فيما بعد دون إغلاق ، كما قد يستخدم الجاني أساليباتدليسية منخلالاللجوءمثلاإلىبرامجالمحادثة، حينها يعمدالجانيإلىإرسالملفإلىالضحية، ويُخبره أن هذا الملف يتضمن ألعاب أو يحتوي على تخفيضاتللسلعأوجوائزا أومسابقاتأوغيرهامنوسائلالإغراء، فينخدعالمجنيعليهويستقبلالملف، كما قد يلجأ الضحية بنفسه إلى مواقع غير معروفة تُغريه بتحميل برامج وملفاتمجانيةويكونمنبينهابرامجالإختراق[35].

هذا وقد نص المشرع الجزائري في الفقرتين الثانية والثالثة من المادة 394 مكرر من قانون العقوبات، علىأنه إذا أقدم الجاني على المساس بمعطيات النظام، من خلال الحذف أو الإتلاف مثلا، أو المساس بوظائفه، بعد تمام دخوله إلى النظام، فإنه يعاقب بعقوبات أشد، حتى لو تم ذلك بصفة غير متعمدة، ولعل من القضايا التي تظهر خطورة مثل هذه الأفعال ما قام به الطالب الأمريكي موريس، من أفعال تخريب وإعاقة باستخدام برنامج الدودة لعدد معتبر من الأنظمة، التي كان من بينها، النظام المعلوماتي التابع لوكالة الأنباء الأمريكية (NASA)، ولم تكن نية الجاني حينها إعاقة النظام أو تكبيده خسائر مادية، بل أن ذلك تم على إثر وجود ثغرة أمنية في نظام الضحية تمكن على إثرها من الدخول، وبسبب خطإ في كتابة الشفرة، قام البرنامج بإعادة نفسه مئات المرات في كل جهاز تمكن من الوصول إليه[36].

الفرع الثاني: جريمة التلاعب بالمعطيات المعلوماتية داخل النظام المعلوماتي

تناول المشرع الجزائري في المادة 394 مكرر 1 من قانون العقوبات الحماية الجنائية للمعطيات المعلوماتية، وتنص هذه المادة أنه: ((يعاقب بالحبس من ستة (6)أشهر إلى ثلاثة (3) سنوات وبغرامة من 500.000 دج إلى 4.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها)).

بذلك حصر المشرع الجزائري قائمة اللأفعال المجرمة التي تطال المعطيات المعلوماتية، التي من شأنها إحداث تغيير في وضعية النظام، ومن ثمة الإضرار به، وتتمثل في: **فعل الإدخال**، ويقصد به إدراج أو إقحام عناصر معلوماتية جديدة على دعامة النظام، كمن يقوم بإدخال برنامج فيروسي مثلا، **وفعل الإزالة**، كأن يقدم الجاني على تحطيم المعطيات أو محوها، **وفعل التعديل**، من خلال استبدال المعطيات الموجودة بداخل النظام المعلوماتي بمعطيات أخرى.

وقد قصد المشرع الجزائري بموجب المادة 394 مكرر 1 من قانون العقوبات تضييق مجال التجريم في ثلاث أشكال إجرامية فقط هي إدخال المعطيات، إزالتها أو تعديلها، وقد جاءت هذه الأفعال المجرمة على سبيل الحصر لا المثال، ما يعني أن مجال التجريم لا يشمل أفعالا أخرى كنسخ المعطيات أو نقلها مثلا، ونعتقد أنه من الأفضل لو تدخل المشرع الجزائري وأضافها إلى قائمة الأفعال المجرمة، لغرض حل بعض الإشكالات القانونية التي لازالت تكتنف التشريع الجزائري، كمشكل سرقة المعلومة مثلا.

الفرع الثالث: جريمة إساءة استخدام معطيات النظام المعلوماتي

جرم المشرع الجزائري إساءة استخدام معطيات النظام المعلوماتي في المادة394 مكرر 2 من قانون العقوبات، التي جاء فيها أنه:((يعاقب بالحبس من شهرين (2) إلى ثلاث(3) سنوات وبغرامة من 1000000 دج إلى 5000000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

1 -تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتيةيمكن أن تُرتكب بها الجرائم المنصوص عليها في هذا القسم.

2 -حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم))

وقد جرم المشرع الجزائري فيالمادة 394 مكرر2 من قانون العقوبات في **بندها الأول على أفعال سابقة** على ارتكاب جريمة الدخول وجريمة التلاعب بالمعطيات وغيرها من الجرائم الإلكترونية، ومن هذه الأفعال السابقة مثلا فعل تصميم البرامج الخبيثة وحيازة كلمات المرور وأدوات القرصنة، أو أية أدوات أخرى يكون الغرض منها المساس بالنظام المعلوماتي من حيث سريته، سلامته وإتاحته، وإقدام المشرع على تجريم هذه السلوكات يرجع إلى إدراكه أن الخطورة أحيانا تكمن حتى في مراحل سابقة على ارتكاب هذا النوع من الجرائم، كما أن التغاضي عن هذه الأفعال سوفيجر معمرورالوقتإلى ما يشبه السوق السوداء في إنتاج وتوزيع مثل هذه الأجهزة والأدوات[37].

كما عاقب في المادة 394 مكرر2 من ق ع في **بندها الثاني**، على أفعال إجرامية لاحقة على ارتكاب جريمتي الدخول أو التلاعب بالمعطيات، تتمثل في: فعل حيازة المعطيات، إفشائها أو نشرها (كمن يقدم مثلا على نشر معلومات تبين طريقة قرصنة واختراق المواقع) أو استعمالها لأي غرض كان ، على أن تكون هذه المعطيات ناتجة عن أحد الجرائم الإلكترونية.

خاتمة:

منذ ظهور الجريمة الإلكترونية كمُسمَى جديد لظاهرة إجرامية جديدة وثيقة الصلة بأدوات التكنولوجيا الحديثة (أنظمة الحاسب الآلي ووسائل الإتصال)، بات الحديث عن مفهومها من الأهمية بمكان، كما أن البحث في أنواعها المختلفة لا يقل أهمية، من باب أن ذلك يساعد وبشكل كبير في إيجاد الطرق الكفيلة بمكافحتها وردع مرتكبي هذا النوع الجديد من الجرائم.

في هذا الإطار – وإجابة على الإشكالية المطروحة سابقا – يُمكِن القول أنه على الرغم من الجهود الحثيثة المبذولة في مجال تعريف الجرائم الإلكترونية، سواء كان ذلك على الصعيد الفقهي أو التشريعي، إلا أن هذه الجهود لم تنتهِ إلى تحديد تعريف جامع ومانع لهذه الجريمة، كما أنه لم يحصل لِحَد الآن اتفاق على أصنافها، ولعل ذلك يرجع من جهة إلى حداثة هذه الظاهرة الإجرامية، كونها متصلة بأدوات التكنولوجيا الحديثة (أنظمة الحاسب الآلي ووسائل الإتصال)، التي تتميز هي الأخرى بالمرونة وسرعة التطور، ومن جهة أخرى إلى تشعبها وتعدد أنواعها على النحو الذي يصعب على الحصر، ذلك أن استخدام الجناة لأنظمة الحاسب الآلي في ارتكاب الجرائم نجم عنه ظهور جرائم جديدة، ليس لها مثيل في قانون العقوبات التقليدي، كما تم إقحامها أيضا في ارتكاب الجرائم التقليدية، كسرقة المعلومة وإساءة استخدام بطاقة الإئتمان الممغنطة وغيرها، مع ما أسفر عنه ذلك من إشكاليات كثيرة.

نسرد فيما يلي ما توصلت إليه الدراسة من نتائج هامة، مع إرفاقها بجملة من التوصيات.

أولا: النتائج

– إن تجريم المشرع الجزائري لبعض الأشكال من الجرائم الإلكترونية في القانون رقم 15/04 المعدل والمتمم لقانون العقوبات، ضمن مُسمَى جرائم ((المساس بأنظمة المعالجة الآلية للمعطيات))، لا يَعنِ أنه حصر قائمة الأفعال التي تندرج ضمن الجرائم الإلكترونية، بل أن تدخله كان لتجريم الأفعال الإجرامية التي يصعب على قانون العقوبات التقليدي احتوائها، تطبيقا لمبدأ شرعية الجرائم والعقوبات.

وعلى الرغم من ذلك، يمكن القول أن هذه الخطوة من جانب المشرع الجزائري تعتبر خطوة إيجابية في سبيل مواجهة الأشكال الجديدة من الإجرام؛

– إن التعريف الذي جاء به المشرع الجزائري في القانون رقم 04/09 المتعلق بالوقاية من الجرائم الإلكترونية، كان لاعتبارات عملية بحتة، تمثلت في تحديد مجال تطبيق الإجراءات التي استحدثها المشرع الجزائري في إطار البحث والتحقيق في هذه الجرائم، ولا ينطبق عليه مفهوم التعريف بالمعنى الفني لهذه الكلمة؛

– تتعدد وتتنوع أشكال الجرائم الإلكترونية، فهي ليست على نوع واحد، بين الحديث منها، وهي التي يطلق عليها الفقه عادة تسمية الجرائم الإلكترونية البحتة، التي كان لزاما على التشريعات المختلفة التدخل بنص مستقل لتجريمها، وهو الأمر الذي فعله المشرع الجزائري بموجب القانون رقم 15/04 المعدل والمتمم لقانون العقوبات؛

– أثرت الأداة المعلوماتية على طريقة ارتكاب الجرائم التقليدية أيضا، ويتجسد هذا التأثير في جرائم المساس بأمن الدولة واستقرارها، وكذا في جرائم الأموال والأشخاص. حيث زادت من خطورتها، كما سهلت من ارتكابها وصعبت في الوقت نفسه من أمر اكتشافها وإثباتها.

ولم يبق المشرع الجزائري مكتوف الأيدي حيال ذلك، حيث عزز قانون العقوبات بجملة من النصوص العقابية، خاصة فيما يتعلق بالجرائم الإرهابية.

غير أن هذه الجهود لازالت غير كافية، لاسيما فيما يتعلق بجرائم الأموال المعلوماتية (التحويلات المالية غير المشروعة)، كما أن استعمال الجناة للأدوات التكنولوجية في ارتكاب الجريمة لابد من اعتباره في بعض الحالات ظرفا مشددا.

ثانيا: التوصيات

بالرغم من الجهود الوطنية المبذولة في سبيل مكافحة الجرائم الإلكترونية، لابد على المشرع الجزائري أن ينتبه إلى ضرورة:

– تجريم أفعال الإعتداء المعلوماتية التي تستهدف نهب أموال الأفراد والسطو عليها، بالنظر لعدم كفاية النصوص الجنائية الناظمة لجرائم الأموال في قانون العقوبات؛

– تنسيق التشريع الداخلي مع الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، التي أكدت على ضرورة تشديد العقوبات، فيما لو ارتكبت الجرائم التقليدية بإيعاز ودعم الأداة المعلوماتية.

قائمة المراجع:

أولا: القوانين

1. الأمر رقم 156/66 المؤرخ في 8 يونيو 1996، المتضمن قانون العقوبات، المعدل والمتمم بموجبالقانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، (جريدة رسمية: عدد 71، سنة 2004).
2. قانون رقم 04/09 المؤرخ في 5 سبتمبر 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، (جريدة رسمية: عدد 47، لسنة 2009).

ثانيا: الكتب

1. جميل عبد الباقي الصغير، **الأنترنت والقانون الجنائي**، (الأحكام الموضوعية للجرائم المتعلقة بالأنترنت)، دار النهضة العربية، القاهرة، 2001.
2. سعيد الوردي، **جرائم السب والقذف عبر وسائل التواصل الإجتماعي والمواقع الإلكترونية** ، (دراسة فقهية وقضائية مقارنة)، الطبعة الأولى، مطبعة الأمنية، الرباط، 2020.

ثالثا: رسائل الدكتوراه

1. بشان عبد النور، **الجوانب الموضوعية لمعالجة الجريمة المعلوماتية** ، رسالة دكتوراه علوم، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، السنة الجامعية 2018/2017؛
2. بطيحي نسمة، **الإعتداءات ذات الصلة بالنظام المعلوماتي** ، رسالة دكتوراه علوم، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، السنة الجامعية: 2020/2019؛
3. شنتير خضرة، **الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)** ، رسالة دكتوراه الطور الثالث ()LMD، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية بأدرار، السنة الجامعية: 2021/2020.
4. ملياني عبد الوهاب، **أمن المعلومات في بيئة الأعمال الإلكترونية** ، رسالة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، السنة الجامعية 2017/2016.

رابعا: المقالات

1. بردال سمير، **خصوصية الجرائم المرتبطة بنظام الحاسب الآلي ومظاهر تميزها عن الجرائم التقليدية** ، مجلة البحوث في الحقوق والعلوم السياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة بن خلدون، تيارت، المجلد 2، العدد 4، 2016.
2. بن نقي سفيان، **جريمة غسيل الأموال بين الوسائط الإلكترونية والنصوص التجريمية** ، مجلة الأبحاث القانونية والسياسية، تصدر عن جامعة محمد لمين دباغين، كلية الحقوق والعلوم السياسية، المجلد 3، العدد2، 2021.
3. سعاد محمد عبد الجواد بلتاجي ،**جريمة التحويل الإلكتروني غير المشروع للأموال بواسطة الإحتيال على النظام المعلوماتي وبطاقات الدفع الإلكتروني** ، دراسة فقهية مقارنة ، مجلة كلية الدراسات ا لإسلامية والعربية للبنات بكفر الشيخ، العدد الثالث، المجلد الثاني، 2019.
4. صراع كريمة ،**الأبعاد الإقتصادية للجريمة الإلكترونية** ، مجلة الدراسات التسويقية و إدارة الأعمال، المجلد 2، العدد 1 جانفي 2018.
5. معاشي سميرة، **الجريمة المعلوماتية**، (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة المفكر، تصدر عن كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد الـ 17، جوان 2018.

[1] اختلفت المصطلحات التي وُصِفت بها الجريمة الإلكترونية؛ بين من سماها بـ (الجريمة المعلوماتية) وآخرون أطلقوا عليها تسمية (جرائم الكمبيوتر)، واتجاه ثالث تبنى تسمية (جرائم الأنترنت) أو (الجرائم السيبرانية).انظر، ملياني عبد الوهاب، **أمن المعلومات في بيئة الأعمال الإلكترونية** ، رسالة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان،السنة الجامعية 2017/2016، ص 19.

[2] بردال سمير، **خصوصية الجرائم المرتبطة بنظام الحاسب الآلي ومظاهر تميزها عن الجرائم التقليدية** ، مجلة البحوث في الحقوق والعلوم السياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة بن خلدون، تيارت، المجلد 2، العدد 4، 2016، ص 79.

[3]معاشي سميرة، **الجريمة المعلوماتية**، (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة المفكر، تصدر عن كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العد الـ 17، جوان 2018، ص 402.

[4]ملياني عبد الوهاب، المرجع السابق، ص 20، 21

- عرف المشرع الجزائري النظام المعلوماتي في المادة الثانية من القانون رقم 04/09 المؤرخ في 5 سبتمبر 2009 المتضمن الوقاية من الجرائم الإلكترونية على أنه: (أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين).

[5]بشان عبد النور، **الجوانب الموضوعية لمعالجة الجريمة المعلوماتية** ، رسالة دكتوراه علوم، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، السنة الجامعية 2018/2017، ص 53؛ معاشي سميرة، المرجع السابق، ص 402.

[6]بردال سمير، المرجع السابق، ص 80.

[7]شنتير خضرة، **الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)** ، رسالة دكتوراه الطور الثالث (LMD)، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية بأدرار، السنة الجامعية: 2021/2020، ص 10.

[8]ملياني عبد الوهاب، المرجع السابق، ص 20.

[9]المرجع نفسه، ص 21.

[10]معاشي سميرة، المرجع السابق، ص 404، 405.

[11]قانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، (جريدة رسمية: عدد 71، لسنة 1966).

[12]قانون رقم 04/09 المؤرخ في 5 سبتمبر 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، (جريدة رسمية: عدد 47، لسنة 2009).

[13]شنتير خضرة، المرجع السابق، ص 12.

[14]راجع فيما يخص خوض المشرع الجزائري في تعريف الجريمة الإلكترونية وتعريفات تقنية أخرى تخص الجريمة الإلكترونية، بطيحي نسمة، **الإعتداءات ذات الصلة بالنظام المعلوماتي** ، رسالة دكتوراه علوم، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، السنة الجامعية: 2020/2019، ص. ص (13-16).

[15]قانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات (جريدة الكويت اليوم، العدد 1244، السنة 61).

[16]قانون رقم 14 لسنة 2014 المتعلق بقانون مكافحة الجرائم الإلكترونية (جريدة رسمية عدد 15، سنة 2014، ص 9).

[17]معاشي سميرة، المرجع السابق، ص 411.

[18]ملياني عبد الوهاب، المرجع السابق، ص 57،58.

[19]بشان عبد النور، المرجع السابق، ص 65.

[20]شنتير خضرة، المرجع السابق، ص 18.

[21]شنتير خضرة، المرجع السابق، ص 15؛ بردال سمير، المرجع السابق، 82.

[22]بشان عبد النور، المرجع السابق، ص 64.

[23]شنتير خضرة، المرجع السابق، ص17.

[24]جميل عبد الباقي الصغير، **الأنترنت والقانون الجنائي**، (الأحكام الموضوعية للجرائم المتعلقة بالأنترنت)، دار النهضة العربية، القاهرة، 2001، ص 33.

[25]جريدة رسمية: (عدد 37، سنة 2016، ص 4).

[26]سعاد محمد عبد الجواد، **جريمة التحويل الإلكتروني غير المشروع للأموال بواسطة الإحتيال على النظام المعلوماتي وبطاقات الدفع الالكتروني**، دراسة فقهية مقارنة، مجلة كلية الدراسات الإسلامية والعربية للبنات بكفر الشيخ، العدد الثالث، المجلد الثاني، 2019، ص 403.

[27]صراع كريمة، **الأبعاد الإقتصادية للجريمة الإلكترونية** ، مجلة الدراسات التسويقية وإدارة الأعمال، المجلد 2، العدد 1 جانفي،2018، ص 42.
[28]سعاد محمد عبد الجواد، المرجع السابق، ص 389.
[29]بن نقي سفيان، **جريمة غسيل الأموال بين الوسائط الإلكترونية والنصوص التجريمية** ، مجلة الأبحاث القانونية والسياسية، تصدر عن جامعة محمد لمين دباغين، كلية الحقوق والعلوم السياسية، المجلد 3، العدد2، 2021، ص 160.
[30]القانون رقم 07/18 المؤرخ في 10 يونيو 2018، المتعلق ببحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34، لسنة 2018.
[31]في تفصيل ذلك، راجع سعيد الوردي، **جرائم السب والقذف عبر وسائل التواصل الإجتماعي والمواقع الإلكترونية**،(دراسة فقهية وقضائية مقارنة، الطبعة الأولى، مطبعة الأمنية، الرباط، 2020؛ إنسام سمير طاهر الحجامي،**جريمتي القذف والسب عن طريق الأنترنت**، مجلة رسالة الحقوق،السنة السابعة، العدد الثاني، 2015.
[32]القانون العضوي رقم 05/12 المؤرخ في 12 جانفي 2012، جريدة رسمية:(عدد 2، لسنة 2012).
[33]الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 252/14، المؤرخ في 18 سبتمبر 2014، (جريدة رسمية: عدد 57، لسنة 2014).
[34]بطيحي نسمة، المرجع السابق، ص 65.
[35]بشان عبد النور، المرجع السابق، ص. ص (311- 317).
[36]بطيحي نسمة، المرجع السابق، ص 87.
[37]المرجع نفسه،ص 145.

سلطانة عبد الرحمان زكريا
zakariasoltana382@gmail.com
جامعة محمد طاهري بشار

الجريمة الالكترونية كمفهوم مستحدث

الملخص

الجريمة الالكترونية نوع جديد من الجرائم رافق تطور تكنولوجيا الإعلام والاتصال، وشكلت ما يعرف بالجريمة المستحدثة، وهي تقع داخل الفضاء الافتراضي في ما يعرف بمواقع التواصل الاجتماعي، وتكون في شكل قرصنة حسابات أو نصب أو تشويه سمعة أو تنمر الكتروني، وقد شكل هذا النمط المستحدث من الجرائم محل دراسة للعلوم التي التي تهتم بالجريمة والانحراف

الكلمات المفتاحية: جريمة الكترونية / موقع / انترنت

Abstract

cybercrime is a new type of crime that has accompanied the development of information and communication technology, it formed what is known as the newly created crime, it is located inside the virtual space in what is known as social networking sites, it can be in the form of account hacking, fraud, defamation, or cyber bullying, this new type of crime has been the subject of a study for the sciences that are concerned with crime and delinquency.

Keywords: *cyber rime/ site / internet*

مقدمة:

منذ القدم سعى الانسان الى تطوير حياته و تسهيلها، وذلك عن طريق العلم والاكتشافات التي من شأنها أن تساهم في التطور وازدهار الحياة اليومية للإنسان، ومن بين تلك الاكتشافات نجد ميدان الاعلام والاتصال، حيث تعتبر الانترنت أهم ما توصل إليه الانسان نظرا لدورها الكبير في الحياة والخدمات العظيمة التي تقدمها.

فالأنترنت ثورة في عالم المعلومات فرضت نفسها في شتى المجالات الحياتية، خصوصا مجال الاتصال حيث ظهرت مواقع التواصل الاجتماعي التي أصبحت ظاهرة عالمية واسعة الانتشار د فعت العلاقات الاجتماعية من الواقع الفعلي إلى العالم الافتراضي.

ورغم الجوانب الايجابية المتعددة للأنترنت ومساهمتها الفعالة في التواصل بين الناس عن طريق مواقع التواصل الاجتماعي إلا أنها كانت مهدا لظهور نوع جديد من الجرائم عرف بالجريمة الالكترونية، حيث تتم هذه الجرائم عبر الفضاء الافتراضي وتعتمد في تخطيطها بصورة أساسية على شبكة المعلومات، حيث تتمثل هذه الجرائم غي انتحال الشخصيات والتزوير وتشويه السمعة والنصب والاحتيال وقرصنة الحسابات الالكترونية والتنمر تميز القرن العشرين باختراعات هائلة في مجال التقنيات وتعتبر الحاسبات الالكترونية أهمها، حيث استحدثت شبكات ونظم المعلومات، وسميت هذه التقنية بالنظام المعلوماتي، وقد ارتبطت الجرائم

الالكترونية أو كما تسمى بالجرائم المعلوماتية بنظم نظم المعالجة الآلية للمعلومات، وقد تميزت في البداية بالغموض بالشكل الذي جعل الكثيرين الى القول بأن الجريمة المعلوماتية هي أشبه بالخرافة ولا وجود لتهديد حقيقي من ناحية الحاسبات الالكترونية.

ومنه فإن الجريمة الالكترونية هي الشكل الحديث من الجرائم التي واكبت التطور التقني الهائل، والتي استلزمت من المشرعين دراستها ووضع نصوص قانونية لها حتى تكون في الإطار القانوني لها، يتم الحد منها ذلك لأن غالبية أفراد المجتمع أصبحوا متمكنين في مجال التقنيات، إذ أصبح كل فرد معرض لهذا النوع من الجرائم، سواء بدور المجرم أو دور الضحية.

مفاهيم البحث

الانترنت:

هو نظام ووسيلة اتصال من الشبكات الحاسوبية يصل ما بين حواسيب حول العالم ببروتوكولات موحدة، حيث يربط الانترنت ما بين ملايين الشبكات الخاصة والعامة في المؤسسات الأكاديمية والحكومية ومؤسسات الأعمال، ويتباين في نطاقه ما بين المحلي والعالمي، ويتصل بتقنيات مختلفة، من الأسلاك النحاسية والألياف البصرية والوصلات اللاسلكية، كما تتباين تلك الشبكات في بنيتها الداخلية تقنيا وإداريا، إذ تدار كل منها بمعزل عن الأخرى لا مركزيا ولا تعتمد أيا منها في تشغيلها على الأخريات.[1]

شبكات أو مواقع التواصل الاجتماعي

شبكة التواصل الاجتماعية هي وسيلة الكترونية حديثة للتواصل الاجتماعي، حيث إنها تكون بنية اجتماعية افتراضية تجمع بين أشخاص أو منظمات تتمثل في نقاط التقاء متصلة بنوع محدد من الروابط الاجتماعية؛ إذ يجمع المشاركين فيها صداقة أو قرابة أو مصالح مشتركة، أو توافق في الهواية أو الفكر، أو رغبة في التبادل المادي أو المعرفي، أو محبة أو كراهية لشيء معين، أو علاقات عقدية أ ودينية، أو تناسق في المعرفة أو المركز الاجتماعي.[2]

وتعرفها هبة محمد خليفة بأنها شبكة مواقع فعالة جدا في تسهيل الحياة الاجتماعية بين مجموعة من المعارف والأصدقاء، كما تمكن الاصدقاء القدامى من الاتصال ببعضهم البعض، وبعد سنوات طوال، وتمكنهم أيضا من التواصل المرئي والصوتي وتبادل الصور وغيرها من الإمكانات التي توطد العلاقة الاجتماعية بينهم.[3]

وهي مواقع على شبكة الانترنت يستطيع من يملك حسابا فيها القيام بالتواصل بعدة طرق (كتابة، صوتا وصورة) مع من يريد سواء من يملكون حسابا في هذه المواقع، سواء أكانوا أشخاصا طبيعيين كالأصدقاء القدامى أو أصدقاء العمل أو زبائن... أو أشخاص معنويين كالشركات والمؤسسات.. حيث يمكن تبادل الأفكار والآراء والمشاعر أو الترويج لسلعة أو منتج معين وإنجاز الأعمال.. فيمجتمع افتراضي.."[4]

---

[1] ليلىأحمدجرار،الفيسبوكوالشبابالعربي،مكتبةالفلاحللنشروالتوزيع،الطبعةالاولى،الكويت، 2012،ص 23

[2] أحمدحسنعبدالعليمحسنالخطيب، (مجلةالدراساتالافريقيةوحوضالنيل: الجرائمالمعلوماتيةالواقعةعبرمواقعالتواصلالاجتماعيقراءةفيقانونمكافحةجرائمتقنيةالمعلوماتالمصريرقم 175 لسنة 2018 ونظاممكافحةجرائمالمعلوماتيةالسعودي 1428 ه)، العدد السادس، 2019، المركزالديمقراطيالعربي-ألمانيا،برلين، ص 112

[3] علي خليل شقرة، الإعلام الجديد (شبكات التواصل الاجتماعي)، دار أسامة للنشر والتوزيع، الطبعة الأولى 2014، الاردن، ص 59

[4] المرجع السابق، ص 60

تتميزمواقعالتواصلالاجتماعيبإغراءوجذبالشباببشكلكبير ،وهذامايؤديبهمإلىالإدمانعليها ،والتعلقوالارتباطبها ،واستخدام هالفتراتطويلة ،مايؤثرسلباعلىالفردوالمجتمع ،منخلالهدرالطاقاتوفقدانالإحساسبقيمةالوقت ،خصوصاالدىالأفرادالذينيبح ثونعنالتسليةوملأأوقاتالفراغ ،للتخلصمنالإحباطوالملل ،وكذاالانشغالعنأمورأساسيةفيالحياةمثلاالجلوسمعأفرادالعائلةومم ارسةالأنشطةالاجتماعيةالمختلفة ،والاغترابعنالمحيطالاجتماعي ،مايفرزسلوكياتعديدةكاللامبالاةوعدململالمسؤولياتو الهروبمنالمشاكلوعدمملواجهتها.[1]

الجريمة الالكترونية:

وردت عدة تعريفات للجريمة الالكترونية نذكر من بينها:

*يقصد بجرائم المعلوماتية تلك الافعال أو الأنشطة الإجرامية أو الأنشطة العمدية (أو المقصودة) التي تستخدم فيها تقنيات الحاسب الآلي الرقمية وتستهدف إيقاع الضرر أو الأذى بالأشخاص أو الأموال أو الممتلكات سواء كان هذا الضرر ماديا أو معنويا كما أن تلك الجرائم تتم ف بيئة المعالجة الآلية للبيانات وعبر أجهزة الحاسب الآلي.[2]

عناصر هذا التعريف:[3]

1- جرائم المعلوماتية هي أفعال إجرامية مقصودة أو عمدية لأنه ليست هناك جريمة بدون قصد مسبق أو نية متعمدة وبالتالي فإن الأفعال التي تصدر عن شخص عن طريق الخطأ أو الصدفة أو بدون نية لارتكاب جرائم (كان يدخل على قاعدة بيانات حكومية بطريق الخطأ ودون قصد أو يستطيع الولوج الى بيانات محظورة دون قصد منه) لا تعتبر جرائم من الناحية القانونية لانعدام القصد والنية المسبقة.

2- يتم استخدام التقنيات الرقمية مثال الحاسب الآلي في ارتكاب جرائم المعلوماتية ويعني ذلك قدرة الجاني على استخدام التكنولوجيا بكفاءة ويعني ذلك أيضا اختلاف طبيعة الجاني في هذه النوعية من الجرائم عن غيرها من الجرائم التقليدية.

3- لابد من وجود ضرر أوأذى سواء للأشخاص أو الأموال أو الممتلكات ولا يقتصر ذلك الضرر على النواحي المادية بل يشمل كذلك الجوانب والنواحي النفسية مثل (الإيذاء بالتشهير او القذف والسب على الانترنت).

4- تتم هذه الجرائم في بيئة الحاسبات الالكترونية أو في بيئة المعلومات الرقمية التي تعتبر مسرحا لارتكاب هذه الجرائم.

*يقصد باصطلاح الجريمة المستحدثة جرائم التقنية، وقد نعتت بالمستحدثة لأنها شكلت ثورة على نظم الجريمة المختلفة، فإن كانت تقترب من الجريمة التقليدية من حيث الأركان العامة والخاصة، واحتياجها لفاعل ومجني عليه وموضوع، إلا أنها اختلفت عنها من حيث صفات الفاعل وميزاته، وطبيعة السلوك الإجرامي المنفرد بخاصية معنوية فريدة، ومسرح للجريمة ذي طابع معنوي، بالإضافة الى تشعب وتنوع أصنافها وعدم

[1] حداديوليدة، (مجلةدراساتلجامعةالأغواط: الشبكاتالاجتماعيةمنالتواصلإلىخطرالعزلةالاجتماعية)، العدد 36، سبتمبر 2015، قسم علوم الإعلام والاتصال، كلية العلوم الانسانية والاجتماعية، جامعةمحمدلمينديباغين-سطيف، الجزائر، ص 50

[2] منال محمد عباس، الانحراف والجريمة في عالم متغير، دار المعرفة الجامعية للنشر والتوزيع، الاسكندرية، 2011، ص 137

[3] المرجع السابق، ص 137 و 138

قدرة النصوص الجزائية العقابية التقليدية على الإحاطة بهذه الصور الجديدة التي ابتكرها عقل الفاعل، والتي لا تنسجم وقاعدة تكييف معروفة.[1]

*أما الدكتور هاني خميس فيذكر أنه نظرا لكثرة تلك التعريفات التي ذكرت لجرائم المعلوماتية فإنه يجب تصنيفها وذلك على النحو التالي:[2]

أ- تعريفات مرتبطة بتوافر المعرفة بتقنية المعلومات:

وتعتبر الجريمة المعلوماتية من وجهة نظر هذه التعريفات "أي نشاط غير قانوني تكون فيه المعرفة بتكنولوجيا الحاسب الآلي أساسية لارتكابه ومثال ذلك تعريف جاي لجرائم الحاسب بأنها الأفعال أو الأنشطة غير القانونية التي لا يمكن ارتكابها بكفاءة ونجاح إلا من خلال المعرفة بتكنولوجيا الحاسب الآلي.

ب- تعريفات حول وسيلة ارتكاب الجريمة الالكترونية:

ومثال ذلك تعريف قاموس علم الإجرام لجرائم المعلوماتية بأنها تشير الى استخدام تكنولوجيا الحاسب الآلي والانترنت في تنفيذ أنشطة إجرامية في مجال الاقتصاد والسياسة والأنشطة المجتمعية الأخرى التي تؤثر على الحياة الطبيعية للمجتمعات الإنسانية وكذلك تعريف "أوجست بيكوى" لجرائم المعلوماتية بأنها "استخدام الحاسب الآلي لارتكاب أفعال غير قانونية مثل الغش والاحتيال للحصول على المال والخدمات والامتيازات وأسرار العمل"

ج- تعريفات حول موضوع الجريمة المعلوماتية:

والجريمة المعلوماتية من وجهة نظر واضعي هذه التعريفات ليست هي التي يكون الحاسب الآلي فيها أداة أو وسيلة لارتكابها، بل هي التي تقع على الحاسب الآلي نفسه ومثالها الدخول غير المشروع على الحاسب الآلي للتلاعب في البيانات والبرامج.

خصائصالجريمةالالكترونية:

1- عابرة للحدود:هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت للعديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة الى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.[3]

2- صعوبة اكتشاف الجريمة المعلوماتية:تتم الجريمة المرتكبة عبر الانترنت خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة.[4]

[1] جلال محمد الزعبي، أسامة أحمد المناعسة، جرائمتقنيةنظمالمعلوماتالالكترونيةدراسةمقارنة، دار الثقافة للنشر والتوزيع، الطبعة الاولى، عمان، 2010، ص 62

[2] هاني خميس، الجرائم المعلوماتية، في: علي جلبي وآخرون، القاموس العصري في العلم الاجتماعي، مطبعة البحيرة طبعة تجريبية، 2007، ص 147، ص 148

[3] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الطبعة الأولى 2008، عمان، 2010، ص 51

[4] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 6 مارس 2013، ص 19

3- صعوبة إثبات الجريمة الالكترونية:الجريمة الالكترونية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة.[1]

لذا فهذه الجرائم لا تترك أثرا لها بعد ارتكابها، علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت، فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الانترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها.[2]

4- أسلوب ارتكابها:ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا طانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل والاختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة... فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها (soft crime) لا تحتاج الى العنف ، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.[3]

5- عدم وجود مفهوم محدد ومشترك للجريمة المعلوماتية:يرجع ذلك بالأساس الى اختلاف النظم القانونية في دلو العالم، ويظهر ذلك جليا من خلال اختلاف الفكر القانوني حول حماية المعلومات، فهناك من يرى بأن المعلومات ذات طبيعة خاصة ولا يطبق عليها الشرط المادي الضروري لتعريف الجريمة، ويرى البعض الآخر أن المعلومات تأخذ قيمة مالية ومادية بصفتها حقا خاصا ينسب لشخص محدد.[4]

6- جريمة مستحدثة

7-

مرتكبالجريمةهوشخصذوخبرةفائقةفيمجالالحاسبالآلي:يطلقعلىمرتكبالجريمةالالكترونيةأوالمعلوماتيةاسمالمجرمالالك ترونيأوألمعلوماتي،فهويختلفعنالمجرمالتقليديبتميزهبخصائصمعينة،إذيتمتعالمجرمالالكترونيبخبرةفائقةفيمجالالحاسب الآليوطريقةاستخدامهله،كمايتمتعبمعرفةفائقةفيعالمالحاسوبلكييتمكنمنارتكابجريمتهبطريقةذكيةوالعملعلىإخفائها،وعد متركأثارورائه.ولقدرمزالأستاذ" باركور (parker)للخصائصالتييتميزبهاالمجرمالالكترونيبكلمة (M.A.R.K.S)بمعنيالمهارة(SKILLS)،المعرفة(KNOWLEDGE)، الوسيلة(RESOURES)، (ANJHERTY)، وأخيراالباعث (MOUTIVES)

فإنلميتمتعالمجرمالالكترونيبهذهالخصائصالتيتميزهعنغيرهمنمرتكبيالجرائمفلايمكنأنتتحققجريمته،كماأنهلايمكناعتبار

[1]نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الطبعة الأولى 2008، عمان، 2010، ص 56

[2]المقصوديمحمدبنأحمدبنعلي: (الجرائمالمعلوماتيةخصائصهاوكيفيةمواجهتهاقانونياً : التكاملالدوليالمطلوبلمكافحتها)، جامعةالإماممحمدبنسعودالإسلامية. كليةعلومالحاسبوالمعلومات، المؤتمرالدوليالأوللمكافحةالجرائمالمعلوماتية، 2015، السعودية. ص 27

[3]نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الطبعة الأولى 2008، عمان، 2010، ص 57

[4]محمدلموسخ، (دفاترالسياسةوالقانون: تنازعالاختصاصفيالجرائمالإلكترونية)، العدد 2، 2009، قسم الحقوق، جامعة قاصدي مرباح ورقلة، الجزائر، ص 145

همجرمالكترونيبحيثتلعبوسيلةارتكابالجريمةدورافيتحققالجريمةالالكترونيةوإلااعتبرتكأيجريمةتقليديةلهذاعلىالمجرمأنيك ونلديهدرايةبوسيلةالإجرامالالكتروني (الحاسوب) بالإضافةإلىوجودشبكةالانترنيتومعرفتهالكافيةبهذهالعناصرلتحقيقجريمتهالمسماةبالجريمةالالكترونية.[1]

-8

الجريمةالالكترونيةتتسمبالخطورةالبالغة:تعتبرالجريمةالالكترونيةجريمةبالغةالخطورة،نظرالأغراضهاالمتعددةوحجمال خسائرالتيتحدثعندارتكابها،مقارنةبالجريمةالتقليدية،كماأنهذاالنوعمنالجرائمتستهدفمعنويات،وليسماديامحسوسة،كماأ نهاتكونسلوكياتغيرمألوفة،ويقومبهامجموعةمنالأشخاصممايجعلالوصولإلىالجانيأوالقائمبالجريمةالالكترونيةأمرأصعب اكماساهمتفيتسهيلالقيامبجرائمأخرى،تتمثلفيإيجادوسائلتجعلملاحظةالجرائمالتقليديةأمراصعبا عندماترتكببباستخدامج هازالكمبيوتر.[2]

أنواع الجرائم الالكترونية

يميز الدكتور هلالي أحمد بين جرائم المعلوماتية التي تقع داخل حدود الدولة وتلك التي تقع خارج الحدود وتكون عابرة للحدود وهو يرى أن الجريمة المعلوماتية بصفة عامة التي تقع داخل حدود الدولة تكون خاضعة لاختصاصها القانوني طبقا لمبدأ الاختصاص الاقليمي لقانون العقوبات، أما الجرائم المعلوماتية عابرة الحدود فهي التي تمس أقاليم عدة دول وهو يعرفها بأنها "كل عمل أو امتناع يأتيه الانسان بواسطة نظام معلوماتي معين، إما اعتداء على حق أو مصلحة أو أية بيانات معلوماتية يحميها القانون، وإما بإضرار بالمكونات المنطقية للحاسب ذاته أو بنظام شبكة المعلومات المتصلة به إذا كانت الواقعة تمس حدود أكثر من دولة" [3]

*الجريمة الالكترونية المالية :

أصبح الاعتماد على الشبكات المعلوماتية شبه مطلق في عالم المال والأعمال، مما يجعل هذه الشبكات نظرا لطبيعتها المترابطة، وانفتاحها، هدفا مغريا للمجرمين، ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل ملموس بالانطباعات السائدة والتوقعات، والتشكيك في صحة هذه المعلومات أو تخزينها بشكل بسيط يمكن أن يؤدي الى نتائج مدمرة، وإضعاف الثقة في النظام الاقتصادي. [4]

*السب والقذف والتشهير الالكتروني:

وهذه أشكال مستحدثة من الجرائم حينما يستخدم بعض الأفراد قدراتهم على إنشاء المواقع الالكترونية في الهجوم على أشخاص أو مؤسسات بألفاظ وأوصاف يعاقب عليها القانون، كما يعمد بعض الأشخاص لنشر صور زائفة وأكاذيب تلحق الضرر بسمعة الأشخاص أو الهيئات أو حتى مجرد نشر الشائعات والأقوال

[1] رشيدةفاريش، نورةقاوش، تأثيرمواقعالتواصلالاجتماعيفيانتشارالجريمة الالكترونية في وسط المراهقين، مذكرة ماستر، تخصص إتصال، قسم العلوم الانسانية، كليةالعلومالإنسانيةوالاجتماعية، جامعة البويرة، 2018/2017، ص 64 و 65

[2] رشيدةفاريش، نورةقاوش، تأثيرمواقعالتواصلالاجتماعيفيانتشارالجريمة الالكترونية في وسط المراهقين، مذكرة ماستر، تخصص إتصال، قسم العلوم الانسانية، كليةالعلومالإنسانيةوالاجتماعية، جامعة البويرة، 2018/2017، ص 65

[3] هلالي عبد اللاه أحمد، جرائم المعلوماتية عابرة الحدود...أساليب المواجهة وفقا لاتفاقية بودابست، دار النهضة العربية، طبعة أولى، القاهرة، 2007، ص 31

[4] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 6 مارس 2013، ص 21

الملفقة التي تحط من قدرتهم أو تسئ الى مراكزهم الاجتماعية والاقتصادية.[1]

*التحرش الالكتروني :

تشير دراسات أجريت على أشخاص يستخدمون التحرش الالكتروني كوسيلة لإزعاج ضحاياهم، الى أنهم يعانون من تقدير ذات معين، وليست لديهم القدرة على المواجهة وجها لوجه، وأن لديهم مقدارا من اضطراب الشخصية النرجسية الذي يقلل من قدرتهم على تقدير نتائج أفعالهم، كما أن استخدامهم التحرش الالكتروني يشعرهم بمزيد من القوة والسيطرة التي تتطلبها نرجسيتهم، وهوسهم المرضي بملاحقة ضحاياهم في كل زمان ومكان، وهو ما يوفره بسهولة الاتصال الدائم لهم ولضحاياهم على الشبكة العنكبوتية من خلال أجهزة الهواتف والأجهزة المحمولة الأخرى، المرتبطة في شكل دائم بالأنترنت، حيث تقوم استراتيجيتهم في إيذاء الآخرين على الإصرار والمطاردة، وتتبع أصدقائهم ومن يتفاعلون معهم على شبكات التواصل الاجتماعي ليروجوا إشاعاتهم عن ضحاياهم وتشويههم أمامهم.[2]

كما أن انتشار ثقافة الاستعراض من خلال نشر الصور والمعلومات الشخصية بحثا عن الاهتمام والانتباه من جانب الآخرين والفراغ النفسي والعاطفي الذي يدفع الأشخاص لقضاء ساعات طويلة على شبكة الانترنت أو في استخدام الأجهزة الالكترونية، وتفاقم مشاكل الإدمان الالكتروني، أدت الى زيادة التحريض على ممارسة التحرش من خلال الانترنت، وبالتالي زيادة إمكان تعرض الشبكة والأجهزة الالكترونية الى هذا التحرش.[3]

التنمر الالكتروني:

هو شكل من أشكال الأذى والعدوان الذي يمارس عبر مواقع وسائل الاتصال الرقمية الحديثة (الهواتف الذكية، الكمبيوتر، اللوحات الالكترونية...) مثل نشر منشورات بهدف الاستهزاء بالضحية أو تشويه السمعة، او ارسال رسائل الكترونية تسبب الأذى النفسي للضحية مثل التهديد أو الاستهزاء بعيوبه.

أشكالالتنمرالإلكتروني

ويصفالتراثالبحتيأنماطامختلفةمنالتنمرالإلكترونيفيضوءالوسيلةالتييتماستخدامهاوهما :[4]

- التنمرالمباشر : ويكونعلىشكل:

إستخداماالانترنت / الهاتفالخلويللتهديدأوالاهانة/ إرسالملفاتتحملفيروساتعنعمد/ إرسالصورأورسومتوضيحيةفاحشةأومهددة

- التنمرغيرمباشر : وهوالتنمرالذييحدثدونأنيلاحظالضحيةذلكفيالحال:

تصفحبريدإلكترونيلشخصما،التنكروخداعشخصماوالتظاهربأنهشخصأخر؛

نشرمايسئإلىالآخرعبرالهاتفالمحمولوالبريدالإلكترونيوبرامجالدردشة .

أسباب الجريمة الالكترونية

[1] منال محمد عباس، الانحراف والجريمة في عالم متغير، دار المعرفة الجامعية للنشر والتوزيع، الاسكندرية، 2011، ص 188

[2] حسنين شفيق، الإعلام الجديد والجرائم الالكترونية، التسريبات التجسس الارهاب الالكتروني، دار فكر وفن للطباعة والنشر والتوزيع، مدينة 6 اكتوبر، 2015، ص 303

[3] حسنين شفيق، الإعلام الجديد والجرائم الالكترونية، التسريبات التجسس الارهاب الالكتروني، دار فكر وفن للطباعة والنشر والتوزيع، مدينة 6 اكتوبر، 2015، ص 304

[4] مباركة مقراني، التنمر الالكتروني وعلاقته بالقلق الاجتماعي دراسة ميدانية على تلاميذ السنة الثانية ثانوي مدمني مواقع التواصل الاجتماعي ببعض ثانويات مدينة ورقلة،مذكرة ماستر، كلية العلوم الاجتماعية، قسم علم التربية، جامعة ورقلة، 2018/06/10، 2018/2017، ص 18

إنما أحدثتهمواقعالتواصلالاجتماعيوالتيهيعبارةعنمواقعاجتماعيةالكترونيةعلىالانترنتمنإتاحةلمستخدميهاالإنشاءمدونات الالكترونية،وإجراء المحادثات،وإرسالالرسائل،كماتتيحمشاركةالصوروملفاتالفيديووالملفات،وتيسرللمستخدميننشرملفات،والكتابةحولموضوعاتمحددةمنالممكنأنتدخلضمندائرةاهتمامممشتركينآخرين،وتمكنهممنالتعليقعلىتلكالمواضيعوإبداء آرائهمفيها،كانلهالدورالأكبرفيعمليةتسهيلارتكابالجرائمحيثأنهذهالمواقعلعبتدورالوسيطالأكبروالفعاللتطويرعمليةسرعة وسهولةارتكابالجرائمالالكترونيةفزيادةوسائلالتواصلوتطورهايؤديبدورهالىزيادةوسائلالجريمةالالكترونيةوتطورها.[1]

وللهاتف الجوال بين أنواع الهاتف ميزات خاصة، حيث يعتبر تطورا مهما في وسائل الاتصال والتواصل الاجتماعي، فقد أصبح بإمكان أي إنسان مهما بلغت ثقافته أو درجة تعليمه أن يستعمل الهاتف أينما كان، ويتواصل – بإجراء الحديث أو بإرسال رسائل قصيرة – مع أي كان في أي زمان ومن أي مكان، دون أن يضطر الى الذهاب الى موقع تلفون في محل أو بيت أو الى تلفون عمومي... بل أصبح بفضل انتشار استعمال الهاتف الخلوي الاستغناء عن الهاتف الأرضي حتى في البيوت والمحلات. ولا يقتصر عمل الهاتف الجوال على كونه أداة اتصال صوتي أو مقروء عن طرق الرسائل، بل أصبح بالإمكان استخدام هذا الهاتف كجهاز حاسوب محمول باليد يستطيع حامله معرفة آخر الأخبار السياسية والاقتصادية والرياضية فور حدوثها عبر طريق الاشتراك في خدمة الانترنت، أو الربط مع القنوات الفضائية. كما يمكن استخدام هذا الهاتف كوسيلة إعلان تتيح من خلاله النشر والاطلاع على الإعلانات المختلفة.[2]

*أسباب الجريمة على المستوى الفردي:

1- البحث عن التقدير :هناك بعض الجرائم الالكترونية التي يرتكبها شباب طائش وصغر السن، وذلك من باب التحدي، وحب الظهور في الإعلام، وغالبا ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينيات.[3]

2- الفرصة :لقد وفرت التقنيات الحديثة والانترنت فرصا غير مسبوقة لانتشار الجريمة الالكترونية وتلعب البيئة وترتيباتها دورا كبيرا في انتاج الجريمة والخروج على القواعد الاجتماعية فوقت الانحراف عن قواعد الامتثال ليلا ونهارا وفي أي مكان وعدم وجود رقابة كلها عوامل تزيد من فرصة ارتكاب الجريمة الالكترونية وقد تشكل المعلومات هدفا سهلا المنال ويحقق المنفعة السريعة، وبالتالي يمكن سرقتها أو سرقة محتوياتها فهي فرصة مربحة وقليلة المخاطر واحتمالية لكشف للفاعل فيها ضئيلة[4]

3- ضبط الذات المنخفض: أظهرت الدراسات أيضا أن ضبط الذات المنخفض والاستعداد لتحمل المخاطر من أجل تحقيق مكاسب قصيرة الأجل وهذا قد ينطبق على الأفعال التي يمكن أن تسهل أو تتعزز بواسطة وسائط الاتصالات الالكترونية والانترنت بالإضافة الى ذلك يتعرض الأفراد على الانترنت لنماذج التعلم الإجرامي والأقران قد يكونون أكثر ميلا للانخراط في الجريمة الالكترونية ونظرية التعلم الاجتماعي نظرية قد يكون لها تطبيق خاص عندما يتعلق الأمر بالجرائم الالكترونية فالمجرمون غالبا ما يحتاجون الى تعلم تقنيات

[1] شريندبابنة،جرائمالانترنتفيالمجتمعمنمنظوراجتماعي،دارالحامدللنشروالتوزيع،الطبعةالأولى، 2015،الأردن،ص 88

[2] علي خليل شقرة، الإعلام الجديد (شبكات التواصل الاجتماعي)، دار أسامة للنشر والتوزيع، الطبعة الأولى 2014، الاردن، ص 84

[3] إسراء جبريل رشاد مرعي: (مجلة الدراسات الإعلامية: الجرائم الالكترونية "الأهداف - الأسباب - طرق الجريمة ومعالجتها") العدد الأول، يناير 2018، قسم علوم الإعلام والاتصال، المركز الديمقراطي العربي، ألمانيا، ص 432

[4] المرجع السابق، ص 432

فالنظرية العامة للجريمة ونظرية التعلم الاجتماعي تريان أن الأفراد يتصرفون في البيئة الافتراضية كما يتصرفون في العالم الحقيقي.[1]

4- النشاط الروتيني:يمكن تفسير زيادة ضحايا الجريمة الالكترونية من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية فمع ظهور شبكة الانترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية والترفيه والتجارة الخ. إن التغييرات في أنشطة الناس الروتينية مثل استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك والإيميل والمواقع وغيرها قد خلقت فرصا للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة.[2]

5- الدوافعالذهنية (المتعةوالتحديوالرغبةفيفهمالنظاماوالمعلوماتيوإثباتالذات):

قدتكونالدوافعلارتكابالجريمةالمعلوماتيةمجردالشغفبالإلكترونياتوالرغبةفيتحديوقهرالنظاموالتفوقعلىتعقيدوسائلالتقنية،ف اختراقالأنظمةالإلكترونيةوكسرالحواجزالأمنيةالمحيطةهذهالأنظمةقديشكلمتعةكبيرةلمرتكبيهاوتسليةتغطيأوقاتفراغه.[3]

مميزات الجريمة الالكترونية

تتميزجرائمالانترنتبطبيعةخاصةتتمثلفيصعوبةاكتشافهاوضبطمقترفيهاكماتتميزأيضابأساليبترتكابهاإذيغلبعليهاالطابعال فنيالتقنيعكسالجرائمالبدويةالتقليدية،ونظراللأهميةالتييلعبهاالحاسوبفيمجالالتطورالمعلوماتيإلاأنالحاسوبالآليلهسلبياتك مالهمنإيجابياتفمرتكبوجرائمالانترنتاستغلوالتطويرخبراتهمالوسائلالتقليديةلارتكابالجرائمحيثطوروسائلجديدةلتناسبهذاال تطورالتكنولوجيفيمجالالحاسوبليسلمواكبةوتنميةالمعارفوإنماللاعتداء عليه،وتختلفالأساليبباختلافالعنصرالذيلايكونمحلال لاعتداء(معداتالحاسوبالمادية) أياالأسطواناتوالشرائطالممغنطة.[4]

وتتميز الجرائم الالكترونية بصعوبة متابعتها حيث إنها في الغالب لا تترك أصرا، فليست هناك أموال وممتلكات مفقودة، وإنما هي أرقام تتغير في السجلات، ومعظم الجرائم الالكترونية ربما يتم اكتشافها بالصدفة، وبعد وقت طويل من ارتكابها، كما أن الجرائم الالكترونية تتميز بالدقة والتعقيد التقني، وغالبا من يرتكب تلك الجرائم يتمتع بالذكاء.[5]

مميزات المجرم المعلوماتي عن المجرم التقليدي:

لم يعد للمجرم – في ظل نظام العولمة الثقافية – سمات فيزيقية أو اجتماعية محددة كما كان معروفا في النظريات السابقة، كما هو الحال في النظرية التي أطلقها (لامبروزو). لكن في عصر الإلكترونيات والفضائيات الحديثة، هناك سمات أخرى ثقافية وتقنية واقتصادية ظهرت مع بداية عصر "الكوكبية" Globaization أو ما نطلق عليه الآن "عصر العولمة الثقافية" بحيث أصبح العالم اليوم قرية واحدة.ويمكن النظر الى الجرائم الالكترونية الرقمية باعتبارها جرائم تهدد الأمن الاجتماعي، وبخاصة لمجتمعاتنا العربية

[1] المرجع السابق، ص 433

[2] إسراء جبريل رشاد مرعي: (مجلة الدراسات الإعلامية: الجرائم الالكترونية "الأهداف - الأسباب - طرق الجريمة ومعالجتها") العدد الأول، يناير 2018، قسم علوم الإعلام والاتصال، المركز الديمقراطي العربي، ألمانيا، ص 434

[3] سعيد نسيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013/2012، ص 61

[4] هدى حامد قشقوش، درائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، بدون ط، ص 125

[5] ثنيان ناصر آل ثنيان، إثبات الجريمة الالكترونية دراسة تأصيلية تطبيقية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستير تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2012، ص 1

الاسلامية، حيث أن تعرض هذه المجتمعات لقيم وسلوكيات المجتمعات الغربية، قد يؤدي الى تغييرات ثقافية من شأنها أن تعرض بعض الأبنية الاجتماعية لمجتمعاتنا الى انهيار بعض النظم الاجتماعية والثقافية، وكذلك قد تؤدي الى التفكك الاجتماعي بشكل عام.[1]

المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي ويقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي التي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشيفرة الخاصة بالدخول الى النظام الذي يحتوي على المعلومات، والتي تعطي الفاعل مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها.[2]

إن ممارسة الجريمة في عصر تدفق المعلومات والبيانات عبر الشبكة العمالقة "الانترنت" جعل من الصعب تحديد سمة معينة من السمات التي كانت معروفة من قبل في النظريات التقليدية عن المجرم بصفة عامة، والممارسات الاجرامية بصفة خاصة، بل إن هناك خصائص جديدة أصبح يتحلى أو يتصف بها "المجرم الالكتروني" في العصر الحديث، أولها وأهمها على الإطلاق تلك المعرفة التقنية بأساليب الحاسبات الآلية والانترنت. لذلك أصبح هناك خصائص ثقافية وتقنية واقتصادية لدى المجرم الالكتروني لم تكن موجودة لدى المجرم التقليدي، ومن هنا جاءت "عالمية الجريمة" التي تمارس من خلال تكنولوجيا المعلومات والاتصالات، فلم تعد للمجرم ولا لنوعية الجريمة التي تمارس نفس الأدوات أو الخصائص التقليدية، بل أصبحت جريمة ذات مواصفات تكنولوجية عالية، لكنها مازالت تمثل نفس الغرض الذي تمارس من أجله، وهو الاعتداء على النفس أو المال أو العرض، وحتى الأمن العام للدولة كلها بصفة عامة وعلى المواطن بصفة خاصة.[3]

ووفقا لعلم الإجرام المعلوماتي فإن الفاعل في جرائم التقنية يختلف الى حد ما عن الفاعل التقليدي من عدة أوجه منها:[4]

1- أن الفاعل في جرائم التقنية يمتاز بالذكاء والفطنة وهو عادة من ذوي المعرفة التقنية الكافية.

2- أنه يمتاز بالهدوء فهو يستعمل عقله وذكاءه ووسائل التقنية البعدية ولا يحتاج الى أدنى درجة من العنف لإيقاع النتيجة المقصودة.

3- أن الفاعل هنا أيضا وفي ظروف معينة لا تكتنفه أخطار جرمية كتلك التي تظهر في سلوك وتصرفات الفاعل التقليدي، إذ غالبا ما يسعى الفاعل الى إظهار مقدرته وذكاءه التقني فقط، فيرتكب الفعل دون أن يلحق أي ضرر بالشبكة أو أجهزة الحاسب الآلي، أو بأحد من الغير.

وأما العوامل المتعلقة بالضحايا فيتمثل أهمها في إحجام المجني عليهم عن الإبلاغ عن الجريمة المعلوماتية خوفا من الفضيحة، والسبب في ذلك هو أن أكثر الجرائم المعلوماتية تقع داخل المؤسسات المالية وأكثر ما يحرص عليها القائمون عليها هذه المؤسسات هو السمعة المالية للم

[1] مصطفى عمر حمادة، الأنثروبولوجيا والضبط الاجتماعي، دار المعرفة الجامعية، 2011، الاسكندرية، ص 145

[2] المرجع السابق، ص 80

[3] مصطفى عمر حمادة، الأنثروبولوجيا والضبط الاجتماعي، دار المعرفة الجامعية، 2011، الاسكندرية، ص 147

[4] جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية دراسة مقارنة، دار الثقافة للنشر والتوزيع، الطبعة الاولى، عمان، 2010، ص 72

ؤسسةولذلكفهميفضلونتحملالخسائرالتيقدتلحق ▪
مبسببهذهالجرائمعلىألايعرفالمتعاملونمعهمبأنالنظامالمعلوماتيةفيالمؤسسةقدتمالتلاعب بهانتيجةلقصورما.[1]

الركن المادي والركن المعنوي للجريمة الالكترونية في المنظور القانوني:

الركن المادي في الجريمة الالكترونية:إن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية واتصال بالأنترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب، لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذا البرنامج بنفسه، وكذلك قد يحتاج الى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.[2]

الركن المعنوي في الجريمة الالكترونية: ويتضح الركن المعنوي للجريمة من خلال توضيح الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني.[3]

غير أنه ورغم هذا التوافق بين جميع الجرائم في وجوب توافر الركن المعنوي فيها، إلا أن هناك استثناءات فيما يخص الجريمة المرتكبة عبر الانترنت، وذلك في ظل الطبيعة اللامادية للجريمة، والسرعة في ارتكابها، حيث لا تدع المجال لتحديد الفعل من عدمه فما بالك بتحديد القصد الجنائي فيها، بالإضافة الى اختلاف طبيعة المجرمين، حيث ينفرد المجرمون الذين يقومون بأفعالهم غير المشروعة عبر الانترنت عن نظرائهم في الجريمة التقليدية فيما يخص الباعث.[4]

لميجدالمشرعالجزائريبدامنتعديلقانونالعقوباتلسدماكانمنفراغقانونيفيهذاالمجال، وكانذلكبموجبالقانونرقم15/04 المؤرخ في 2004/11/10 المتمموالمعدللأمر 156/66 المتضمنقانونالعقوباتوالذيأقرلهالقسمالسابعمكررمنهتحتعنوان:

المساسبأنظمةالمعالجةالآليةللمعطيات،ولقدجاءفيعرضأسبابهذاالتعديلأنالتقدمالتكنولوجيوانتشاروسائلالاتصالالحدي ثةأدىإلىبروزأشكالجديدةللإجرام،ممادفعبالكثيرمنالدولإلىالنصعلىمعاقبتها،

وأنالجزائرعلىغرارهذهالدولتسعىمنخلالهذاالمشروعإلىتوفيرحمايةجزائيةللأنظمةالمعلوماتيةوأساليبالمعالجةالآليةللمعط يات،وأنهذهالتعديلاتمنشأنهاسدالفراغالقانوني.وقدقدرالمشرعفيتدخلهذاأنجوهرالمعلوماتيةهوالمعطياتالتيتدخلإلىالحا سبالآليفتحولإلىمعلوماتبعدمعالجتهاوتخزينها،فقامبحمايةهذهالمعطياتمنأوجهعدةلذلكفقدآثرالمشرعالجزائرياستخدامهلم صطلحالمساسبنظمالمعالجةالآليةللمعطيات،وينصرفهذاالمصطلحوفقالدلالةالكلمةإلىالمعلوماتوالنظامالذييحتويعليها بمافيذلكشبكاتالمعلومات،ليخرجبذلكمننطاقالتجريمتلكالجرائمالتييكونالنظامالمعلوماتيوسيلةلارتكابها،وحصرهافقطفي صورالأفعالالتيتشكلاعتداءعلىالنظامالمعلوماتي،أيالجرائمالتييكونالنظامالمعلوماتيمحلالها(الفرعالأول) .ثمفيمرحلةلاحقةاختارالمشرعالجزائريللتعبيرعنالجريمةالمعلوماتيةمصطلحالجرائمالمتصلةبتكنولوجياتالإعلاموالات

[1] سعيد نسيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013/2012، ص 65

[2] قطب محمد علي، (2010)، الجرائم المعلوماتية وطرق مواجهتها. مملكة البحرين، وزارة الداخلية، الأكاديمية الملكية للشرطة، ص 2.

[3] المرجع السابق، ص 2.

[4] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 6 مارس 2013، ص 72

صالبموجبالقانونرقم 04/09المتضمنالوقايةمنهذهالجرائمومكافحتها(الفرعالثاني).[1]

وقد استلزم التطور التقني تطورا أيضا في طرق إثبات الجريمة والتعامل معها، فالجرائم التقليدية العادية يسهل –غالبا– تحديد مكان ارتكابها، بل أن ذلك يعتبر خطوة أولية وأساسية لكشف ملابسات الجريمة، في حين أنه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع جرائم التقنية الرقمية الحديثة، وذلك لأن الرسائل والملفات الالكترونية تنتقل من نظام الى آخر في ثواني قليلة، كما انه لا يقف أمام نقل هذه الرسائل والملفات أي حدود جغرافية مكانية أو زمانية.[2]

من الصعوبة بما كان أن نحدد على وجه لدقة الحجم الحقيقي لجرائم المعلوماتية عبر العالم ويعود ذلك لعدد من الأسباب:[3]

1– أنه لا توجد إحصائيات رسمية في كثير من الدول عن حجم هذه الجرائم نظرا لحداثتها ولعدم اكتشافها.

2– أن معظم هذه الجرائم لا يتم الإبلاغ عنها من الضحايا وخاصة المؤسسات التي تتعرض لهذه الجرائم تخشى من أن تفقد ثقة عملائها.

3– أن هذه الجرائم متنوعة تنوعا شديدا ومن ثمة يصعب حصرها بجميع أشكالها وبالتالي فالإحصاءات الموجودة قد تتناول جانب منها أو أشكال معينة من جرائم المعلوماتية ويظل الجزء الأكبر غير محدد من حيث حجمه ومدى انتشاره.

خاتمة

أضافت الانترنت ومواقع التواصل الاجتماعي الى حياة الملايين من البشر الكثير، حيث سهلت التواصل فيما بينهم، وفتحت آفاقا جديدة لتشكل شخصياتهم وعاداتهم الاجتماعية حول ثقافة الشبكات الاجتماعية والتواصل عبر الانترنت، ولتي كان لها تأثير سلبي و إيجابي على طبائعهم، فمجرد الانضمام لمواقع التواصل الاجتماعي يجعلهم ينضمون ضمنيا الى ثقافة الموقع والمجتمع الالكتروني الذي صاروا جزءا منه وعقدة من عقد الشبكة الاجتماعية، وقد أصبح الاعتماد على التقنية يزداد يوما بعد يوم في مختلف المجالات، ورغم ما لهذه الوسائل من فوائد إلا أن لها وجها آخر يتمثل في الاستعمال السيء والضار لهذه التقنيات الحديثة، ومنه أصبحت الجريمة الالكترونية خطرا يهدد العالم بأسره، حيث تكمن خطورتها في سهولة تنفيذها مع شدة أثرها وضررها، حيث يقوم المجرم بها وهو في بيته أو مكتبه أو المقهى.

لقد أتاحت مواقع التواصل الاجتماعي لمستخدميها إنشاء مدونات الكترونية وإجراء محادثات وإرسال الرسائل، ومشاركة الصور ومقاطع الفيديو والملفات، كما مكنتهم من الكتابة حول موضوعات محددة حيث يمكن أن تكون تلك الموضوعات ذات اهتمام من الآخرين المشاركين في هذه المواقع، حيث يشاركون في النقاش حولها والتعليق عليها، وهذا ما يمكن أن يكون له دور كبير في تسهيل ارتكاب الجرائم الالكترونية، حيث أن هذه

[1] سعيد نسيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013/2012، ص 41

[2] مصطفى عمر حمادة، الأنثروبولوجيا والضبط الاجتماعي، دار المعرفة الجامعية، 2011، الاسكندرية، ص 145

[3] منال محمد عباس، الانحراف والجريمة في عالم متغير، دار المعرفة الجامعية للنشر والتوزيع، الاسكندرية، 2011، ص 143

المواقع هي الوسائط الالكترونية ذات الدور الفعال في ارتكاب الجرائم الالكترونية، حيث يمكن القول أن تطور هذه المواقع يعني تطور الجريمة الالكترونية بطبيعة الحال.

المراجع

- ليلىأحمدجرار،الفيسبوكوالشبابالعربي،مكتبةالفلاحللنشروالتوزيع،الطبعةالاولى،الكويت، 2012
- فيصل أبو عيشة، الأعلام الالكتروني، دار أسامة للنشر والتوزيع، عمان، 2014
- أحمدحسنعبدالعليمحسنالخطيب، (مجلةالدراساتالافريقيةوحوضالنيل: الجرائمالمعلوماتيةالواقعةعبرمواقعالتواصلالاجتماعيقراءةفيقانونمكافحةجرائمتقنيةالمعلوماتالمصريرقم 175 لسنة 2018 ونظاممكافحةجرائمالمعلوماتيةالسعودي 1428 هـ)، العدد السادس، 2019، المركزالديمقراطيالعربي- ألمانيا،برلين
- علي خليل شقرة، الإعلام الجديد (شبكات التواصل الاجتماعي)، دار أسامة للنشر والتوزيع، الطبعة الأولى 2014، الاردن
- صالح العلي، مهارات التواصل الاجتماعي أسس ومفاهيم وقيم، دار الحامد للنشر والتوزيع، الطبعة الاولى، عمان، 2015
- حداديوليدة، (مجلةدراساتلجامعةالأغواط: الشبكاتالاجتماعيةمنالتواصلإلىخطرالعزلةالاجتماعية)، العدد 36، سبتمبر 2015، قسم علوم الإعلام والاتصال، كلية العلوم الانسانية والاجتماعية، جامعةمحمدلمينديباغين- سطيف، الجزائر
- منال محمد عباس، الانحراف والجريمة في عالم متغير، دار المعرفة الجامعية للنشر والتوزيع، الاسكندرية، 2011
- حسنين شفيق، الإعلام الجديد والجرائم الالكترونية، التسريبات التجسس الارهاب الالكتروني، دار فكر وفن للطباعة والنشر والتوزيع، مدينة 6 اكتوبر، 2015
- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائمتقنيةنظمالمعلوماتالالكترونيةدراسةمقارنة، دار الثقافة للنشر والتوزيع، الطبعة الاولى، عمان، 2010
- هاني خميس، الجرائم المعلوماتية، في: علي جلبي وآخرون، القاموس العصري في العلم الاجتماعي، مطبعة البحيرة طبعة تجريبية، 2007
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الطبعة الأولى 2008، عمان، 2010
- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 6 مارس 2013
- المقصوديمحمدبنأحمدبنعلي: (الجرائمالمعلوماتيةخصائصهاوكيفيةمواجهتهاقانونياً : التكاملالدوليالمطلوبلمكافحتها)، جامعةالإماممحمدبنسعودالإسلامية. كليةعلومالحاسبوالمعلومات، المؤتمرالدوليالأوللمكافحةالجرائمالمعلوماتية، 2015، السعودية
- محمدلموسخ، (دفاترالسياسةوالقانون: تنازعالاختصاصفيالجرائمالإلكترونية)، العدد 2، 2009، قسم الحقوق،

جامعة قاصدي مرباح ورقلة، الجزائر

– رشيدةفاريش، نورةقاوش، تأثيرمواقعالتواصلالاجتماعيفيانتشارالجريمة الالكترونية في وسط المراهقين ، مذكرة ماستر، تخصص إتصال، قسم العلوم الانسانية، كليةالعلومالإنسانيةوالاجتماعية، جامعة البويرة، 2018/2017

– هلالي عبد اللاه أحمد، جرائم المعلوماتية عابرة الحدود...أساليب المواجهة وفقا لاتفاقية بودابست، دار النهضة العربية، طبعة أولى، القاهرة، 2007

– مباركة مقراني، التنمر الالكتروني وعلاقته بالقلق الاجتماعي دراسة ميدانية على تلاميذ السنة الثانية ثانوي مدمني مواقع التواصل الاجتماعي ببعض ثانويات مدينة ورقلة ،مذكرة ماستر، كلية العلوم الاجتماعية، قسم علم التربية، جامعة ورقلة، 2018/06/10، 2018/2017

– محمد عادل ريان، جرائم الحاسب الآلي وأمن البيانات، العربي، 1995

نقلا عن: سليمان محمود عطا الله، علم النفس الجنائي، الأكاديميون للنشر والتوزيع، الطبعة الأولى، الأردن، 2016

– شريندبابنة،جرائمالانترنتفيالمجتمعمنمنظوراجتماعي،دارالحامدللنشروالتوزيع،الطبعةالأولى، 2015،الأردن

– إسراء جبريل رشاد مرعي: (مجلة الدراسات الإعلامية: الجرائم الالكترونية "الأهداف – الأسباب – طرق الجريمة ومعالجتها") العدد الأول، يناير 2018، قسم علوم الإعلام والاتصال، المركز الديمقراطي العربي، ألمانيا

– سعيد نسيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013/2012

– هدى حامد قشقوش، درائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، بدون ط

– ثنيان ناصر آل ثنيان، إثبات الجريمة الالكترونية دراسة تأصيلية تطبيقية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستير تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2012

– مصطفى عمر حمادة، الأنثروبولوجيا والضبط الاجتماعي، دار المعرفة الجامعية، 2011، الاسكندرية

– قطب محمد علي، (2010)، الجرائم المعلوماتية وطرق مواجهتها. مملكة البحرين، وزارة الداخلية، الأكاديمية الملكية للشرطة، ص 2.

بشيخ أم الخير
–جامعة ابن خلدون – تيارت
oumelkheirbecheikh@gmail.com

حايطي فاطيمة
–جامعة ابن خلدون – تيارت
dhaifatima94@gmail.com

الجريمة الالكترونية في ظل التشريع الجزائري

الملخص:

أدى التطور الهائل في مجال التكنولوجيا والإعلام إلى ظهور أنماط مستحدثة من الجرائم اصطلح على تسميتها بالجرائم الالكترونية، والتي تتم عبر معدات و أجهزة إلكترونية، أو باستخدام شبكة الانترنت لارتكابها، لذلك ارتأينا من خلال هذه المداخلة التعرف على هذا النمط الجديد من الجرائم الحديثة نسبيا من حيث ماهيتها وخصائصها، كما تهدف الدراسة إلى التعرف على أنواع الجرائم الإلكترونية في الجزائر في ضوء التشريع الجزائري و جهود الدولة الجزائرية في مواجهة هذه الجرائم التي أصبحت تشكل خطرا الأمن الداخلي للدولة و اقتصادها.

الكلمات المفتاحية: الجريمة الالكترونية، الجريمة المعلوماتية، الحاسب الآلي.

***Summary*:**

The tremendous development in the field of technology and media has led to the emergence of new patterns of crimes termed as cybercrime, which are carried out through electronic equipment and devices, or using the Internet to commit them, so we decided through this intervention to identify this new type of relatively recent crimes from Where it is and its characteristics, the study also aims to identify the types of cybercrime in Algeria in the light of the Algerian legislation and the efforts of the Algerian state in the face of these crimes, which have become a threat to the internal security of the state and its economy.

***Keywords**: electronic crime, information crime, computer.*

مقدمة:

يشهد العالم منذ منتصف القرن العشرين تقدما هائلا تتجلى أبرز مظاهره في التكنولوجيا الجديدة للمعلومات والاتصالات، و لاشك أن هذه التكنولوجيا الحديثة و نتيجة للتقنيات العالية التي تقوم عليها والتي تتمثل في استخدام الحواسيب والشبكات المعلوماتية التي تربط بينها، تقدم للدول و أجهزتها الأمنية الكثير من الإمكانيات التي تساهم في رفع كفاءتها و تطوير قدرتها على التصدي للجريمة. كما أنها شكلت قفزة حضارية في حياة الأفراد.

حيث تعتمد مختلف القطاعات و المؤسسات في الوقت الحالي في أداء عملها على استخدام الحواسيب والشبكات المعلوماتية نظرا لما تتمتع به من عنصري الدقة والدقة.

إلا أن هذا الجانب الإيجابي لعصر التكنولوجيا لا ينفي الانعكاسات السلبية التي أفرزتها هذه الوسائل التقنية الحديثة و استغلالها على نحو غير مشروع و بصورة تضر بمصالح الأفراد والجماعات، حيث أدي

التطور المذهل والمتسارع والمتلاحق لتكنولوجيا المعلوماتية وشبكات المعلومات إلى ظهور نمط جديد و هو الجريمة الالكترونية أو الجريمة المعلوماتية أو التقنية، وما استتبعه ذلك من مصطلحات جديدة.

وبالنظر إلى خصوصية الجريمة الالكترونية وخطورتها وحداثتها وعدم تماشيها مع القوانين التقليدية، استلزم الأمر تدخل المشرع بسن نصوص قانونية، وبناءا على ما تقدم تم طرح الإشكالية التالية ما مفهوم الجريمة الالكترونية؟، وما هي جهود الدولة في سبيل التصدي إلى هذه الجريمة باعتبارها تتم باستخدام وسائل تكنولوجية حديثة و تقنيات عالية التي يصعب اكتشافها وإثباتها؟

وللإجابة على هذه الإشكالية تم تقسيم خطة البحث إلى مبحثين، المبحث الأول تطرقنا فيه إلى التعريف بالجريمة الالكترونية وتبيان أهم الخصائص والسمات التي تتميز بها، وفي المبحث الثاني تطرقنا إلى ذكر أنواع هذه الجريمة وإلى جهود الدولة الجزائرية في التصدي لهذا النوع من الجرائم.

المبحث الأول: ماهية الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من الآثار السلبية التي خلفتها التقنية العالية كونها تهدد حياة الأفراد والمجتمعات، ونتيجة لتطورها المستمر وسرعة انتشارها واجه الفقهاء صعوبة في إيجاد تعريف جامع مانع لها، حيث تباينت التعريفات تبعا لعدة معايير ومن أجل التعرف على ماهية الجريمة المعلوماتية لابد من تعريفها وبيان خصائصها وأنواعها وذلك على النحو التالي:

المطلب الأول: تعريف الجريمة الإلكترونية

تعددت التسميات التي تطلق على الجرائم الإلكترونية وتنوعت بين الجرائم المعلوماتية ، الجرائم السيبرانية، جرائم الأنترنت ... وهذا ما انجر عنه عدم وضع تعريف موحد لهذه الظاهرة حيث اختلفت تعريفات الجرائم الإلكترونية وتنوعت بين تعريفات فقهية وأخرى قانونية تستند كلها إلى عدة معايير وأسس، لذا فسنبحث في هذا الفرع التعريف الفقهي والقانوني للجريمة المعلوماتية:

الفرع الأول: التعريف الفقهي

لم يجمع الفقه على وضع تعريف جامع مانع للجريمة الإلكترونية بل اختلف في تعريفه لهذه الجريمة[1]، فهناك من عرفها على أساس وسيلة ارتكابها، وهناك من عرفها على أساس موضوعها أو محلها، واتجاه عرفها على أساس معيار شخصي الجاني، واتجاه أخير جمع بين عدة معايير في تعريفها.

أ/ تعريفها على أساس وسيلة ارتكابها:

يرتكز هذا التعريف على وسيلة ارتكاب الجريمة الإلكترونية والمتمثلة في الحاسب الآلي بمختلف أنواعه حيث عرفت على أنها "كل فعل إجرامي يستخدم الكمبيوتر أو الحاسب الآلي في ارتكابه كأداة رئيسية"[2]، وطبقا لهذا التعريف يمكن أن ترتكب جل الجرائم التقليدية بواسطة الحاسب الآلي.

---

[1] - لورنس سعيد الحوامدة ، الجرائم المعلوماتية ،أركانها وآلية مكافحتها، دراسة مقارنة، مجلة الميزان للدراسات الاسلامية و القانونية،2017 ، ص06

[2]- بوذراع عبد العزيز، خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير، جامعة الجزائر 1، 2011، ص14.

ب/ تعريفها على أساس موضوع الجريمة:

يعرف هذا الاتجاه الجريمة الإلكترونية على أنها كل سلوك غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي [1]، ومن هذا التعريف نستنتج أنه يجب الاعتداء على الحاسب الآلي أو نظامه لقيام هذه الجريمة.

ج/ تعريفها على أساس معيار شخصي:

يستند هذا التعريف إلى معيار شخصي حيث يستوجب أن يكون الفاعل ملمّا بتقنية المعلومات واستخدام الحاسب الآلي وقد أورد الدكتور هشام رستم تعاريف مختلفة في هذا الشأن منها :[2] "أنها أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنيات الحاسب"[3].

د/ تعريفها على أساس الجمع بين عدة معايير:

نظرا لعدم نجاعة التعاريف السابقة للجريمة الإلكترونية عمد أصحاب هذا الاتجاه إلى الجمع بين كل المعايير السابقة وعرفوها على أنها "الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها، أو يكون الحاسب الآلي نفسه ضحيته".[4]

الفرع الثاني: التعريف القانوني

تعرف الجريمة الإلكترونية من الناحية القانونية على أنها مجموعة الأنشطة المعاقب عليها قانونا والتي تربط بين الفعل الإجرامي والثورة التكنولوجية ،[5] والتي ينتج عنها حصول المجرم على فوائد مادية ومعنوية، مع تحميل الضحية خسارة مقابلة، أما بالنسبة للمشرع الجزائري وفي تعديله لقانون العقوبات بموجب القانون رقم 04-15 لم يعرّف الجريمة المعلوماتية بل اكتفى بالعقاب عليها تحت عنوان –الجرائم الماسة بنظام المعالجة الآلية للمعطيات– ونظرا للانتقادات الموجهة إليه على هذا القصور تدخل المشرع مرة أخرى لتدارك ذلك من خلال قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وعرفها بموجب المادة الثانية منه بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ار تكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.[6]

ويقصد بنظام الاتصالات الالكترونية كل" تراسل أو إرسال أو استقبال لعلامات أو صور أو معلومات

---

[1] - عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة الشرق الأوسط،2014، ص12.

[2]- معاشي سميرة، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، العدد السابع، ص277.

[3]- محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، ط1، عمان، 2004، ص08.

[4]- كتاب أعمال المؤتمر الدولي الرابع عشر، الجرائم الالكترونية، طرابلس، 24_25 مارس 2017، ص99.

[5]- شينار سامية،الجريمة الالكترونية في منظور الشباب الجامعي مدخل نفسي _ قانوني، مجلة الباحث للدراسات الأكاديمية، المجلد 06، العدد 02، 2019، ص389.

[6]- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير، قانون جنائي، جامعة قاصدي مرباح، 2013/2012، ص11.

مختلفة بواسطة أية وسيلة إلكترونية.[1]

ويلاحظ على هذا التعريف أن المشرع الجزائري قد اعتمد على معيار الجمع بين عدة معايير في تعريفه للجريمة الإلكترونية من وسيلة ارتكابها المتمثلة في نظام الاتصالات الالكترونية، ومعيار موضوع أو محل الجريمة والمتمثل في المساس بأنظمة المعالجة الآلية للمعطيات المحدد في قانون العقوبات، وعلى معيار القانون الواجب التطبيق المتمثل في قانون العقوبات والقوانين المكملة له.[2]

وعليه وبناء على هذه التعريفات الفقهية والقانونية للجريمة الإلكترونية يمكننا تعريفها بأنها: "كل سلوك غير مشروع إرادي يرتكبه الشخص المسؤول جنائيا داخل بيئة افتراضية يقع على النظام المعلوماتي أو بواسطته ويمس بالأشخاص أو الأموال أو أمن الدولة"

الفرع الثالث: التمييز بين الجريمة الإلكترونية والجريمة المعلوماتية:

تباينت المصطلحات الدالة على الجريمة الواقعة عبر الأنترنت وتعددت بين جرائم الأنترنت وجرائم الكمبيوتر والجرائم الالكترونية والجريمة المعلوماتية وغيرها وفي هذا يرى جانب من الفقه أن مصطلح الجرائم الالكترونية أوسع وأشمل من مصطلح الجرائم المعلوماتية ذلك أن جرائم الكمبيوتر أو الإلكترونية تشمل كافة الجرائم التي تقع على الحاسبات أو بواسطتها سواء تمثلت في الحاسب الآلي أو مختلف الأجهزة الالكترونية الأخرى، بحيث يستخدم الحاسب في هذه الجرائم كأداة لارتكاب الجريمة أو محلا لها، أما عن مصطلح الجرائم المعلوماتية فيشمل مفهوم الاعتداء على المعلومات والبرامج الموجودة داخل الأجهزة الإلكترونية [3] ، كالحاسب الآلي بحيث يدخل في هذا المفهوم كل نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الأنترنت[4]، كالتسلل إلى ملفات خاصة أو انتهاك حقوق الملكية الفكرية أو الابتزاز أو استغلال الأطفال والاعتداء عليهم...

المطب الثاني: خصائص الجريمة الإلكترونية

للجريمة **الإلكترونية** طبيعة خاصة تميزها عن غيرها من الجرائم التقليدية وذلك نتيجة ارتباطها بتقنية الاتصالات والمعلومات، حيث أضفت هذه التقنيات خصائص معينة على هذا النوع من الاجرام والتي انعكست أيضا على مرتكب الجريمة **الإلكترونية** والذي أصبح يعرف بالمجرم المعلوماتي، والذي يتميز بدوره عن المجرم التقليدي،[5] وعليه سوف نحاول التطرق فيما يلي إلى بعض السمات الخاصة للجريمة المعلوماتية أولا ثم إلى أهم السمات التي تميز المجرم المعلوماتي ثانيا.

1/ سمات الجريمة الإلكترونية:

نظرا لارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الأنترنت أصبحت تتميز بمجموعة من

[1]- المادة 02 من قانون رقم 04/09 المؤرخ في 14 شعبان 1430 الموافق ل 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47، 2009.

[2]- كتاب أعمال المؤتمر الدولي الرابع عشر ، المرجع السابق، ص100.

[3]- لورنس سعيد الحوامدة، المرجع السابق، ص07.

[4]- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2008، ص56.

[5]- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، 2010-2011، ص17.

الخصائص لعل أهمها ما يلي:

أ/ الجريمة الإلكترونية جريمة ناعمة ومغرية : تعتبر الجريمة **الإلكترونية** جريمة ناعمة لأنها لا تتطلب العنف لارتكابها أو استعمال أدوات خطيرة في تنفيذها أو بذل مجهود عضلي [1]، بل تحتاج للذكاء والحيلة، وهي جريمة مغرية لأنها سريعة التنفيذ فغالبا ما تنفذ بوسائل سهلة وسريعة وعن بعد دون التواجد في مسرح الجريمة وفي المقابل يتحصل منها الجاني على فوائد ومكاسب هائلة.

ب/ جريمة عابرة للحدود الدولية : فالجريمة المعلوماتية لا تعترف بالحدود الجغرافية نتيجة للطابع العالمي لشبكة الأنترنت الذي جعل دول العالم في حالة اتصال دائم مما يسهل ارتكاب الجريمة من دولة إلى أخرى[2] ، فقد يكون المجرم في بلد والمجني عليه في بلد آخر [3]، وهذا ما يسمى بتلاشي الحدود بين الدول في العالم الافتراضي، بحيث يرتكب الجاني جريمته عن بعد ودون تواجده في مسرح الجريمة من خلال جهاز الحاسب الآلي، كما أضاف الأستاذ محمد محي الدين عوض أن جريمة الحاسوب تعتبر مشكلا جديدا للإجرام العابر للحدود والوطنية أو الإقليمية أو القارية [4] ، مما جعلها تخلق إشكالات عديدة حول تحديد الدولة صاحبة الاختصاص القضائي، وكذا القانون الواجب التطبيق عليها وإجراءات ملاحقتها، وفي هذا تظافرت العديد من الدول في سبيل مكافحتها من خلال عقد الاتفاقيات والمؤتمرات بهذا الشأن.

ج/ جريمة صعبة الاكتشاف والإثبات: تمتاز الجريمة **الإلكترونية** بصعوبة اكتشافها وهذا راجع لعدم تركها لآثار مادية،[5] نتيجة للطابع التقني الذي تمتاز به ،[6] فهي جرائم ترتكب في العالم الافتراضي (عالم الأنترنت) بشكل مستتر حيث لا تترك أي أثر خارجي ملموس أو مرئي علاوة على صعوبة الاحتفاظ الفني بآثارها [7]K وعدم الإبلاغ عندها تجنبا للإساءة إلى السمعة ،[8] فهي تنصب على البيانات والمعلومات المخزنة في نظم الحواسيب والتي يسهل على الجاني التلاعب بها أو محوها وتدميرها في زمن قصير جدا، مما يصعب عملية إثباتها، علاوة على أنها تحتاج لوجود خبرة فنية في المحقق للتعامل معها.

2/ سمات المجرم المعلوماتي:

يسمى المجرم الذي يقترف الجرائم **الإلكترونية** بالمجرم المعلوماتي والذي يتميز عن غيره من المجرمين التقليديين بعدة خصائص لعل أبرزها ما يلي:

أ -يتمتع المجرم المعلوماتي بالمهارة والمعرفة الجيدة بمجال تكنولوجيا المعلومات والاتصالات والتي يكتسبها عن طريق الدراسة في هذا المجال أو عن طريق الخبرة المكتسبة في الحياة.[9]

ب -يعتبر المجرم المعلوماتي مجرما ذكيا ومحترفا في تنفيذ جريمته والتعامل مع شبكة الأنترنت.[1]

---

[1]- زبيدي البشير، واقع جرائم تكنولوجيا الإعلام والاتصال في العالم وآليات مكافحتها، مجلة الدراسات الاقتصادية المعاصرة، العدد 3، 2017، ص79.

[2]- خالد ممدوح إبراهيم، المرجع السابق، ص44.

[3]- عبد الله دغش العجمي، المرجع السابق، ص20.

[4]- معاشي سميرة، الجريمة المعلوماتية، دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة المفكر، العدد 17، جوان، 2018، ص411.

[5]- خالد ممدوح إبراهيم، المرجع السابق، ص45.

[6]- لورنس سعيد الحوامدة، المرجع السابق، ص11.

[7]- خالد ممدوح إبراهيم، المرجع السابق، ص45.

[8]- كتاب أعمال المؤتمر الدولي الرابع عشر، المرجع السابق، ص102.

[9]- سوير سفيان، المرجع السابق، ص23.

ج/نظرا للتطور المستمر لتقنية المعلومات وسهولة التعامل مع الأنترنت اتسع نطاق وحجم المتعاملين مع الكمبيوتر مما أدى إلى ظهور عدة طوائف للمجرمين المعلوماتيين، فهناك:

– **طائفة المتطفلون :** وهم الذين يستهدفون الدخول إلى أنظمة الحواسب الآلية غير المصرح لهم بدخولها بغرض تحدي النظام واختراقه أو اكتساب الخبرة ويسمون بـ hackers[2].

– **طائفة المخترقون:** تستهدف هذه الطائفة التسلل إلى أجهزة وأنظمة الحواسيب واختراقها والعبث بمحتوياتها بهدف إلحاق خسائر بالمجني عليه دون أن يكون بالضرورة هدفهم الحصو ل على مكاسب مالية، ويندرجون تحت طائفة مخترعي فيروسات الحاسبات الآلية وموزعيها ويسمون "Malicieuses hakers[3]".

– **طائفة الحاقدون:** وتسمى هذه الطائفة بـ"Crakers" حيث ترتكب اعتداءاتها الإجرامية بدافع الانتقام والثأر وتشويه السمعة، فليس لها أي هدف سياسي أو مادي من ارتكاب هذه الجريمة [4]، بل تهدف إلى إلحاق الأذى بالمجني عليه.[5]

المبحث الثاني: أنواع الجرائم الإلكترونية وجهود الدولة الجزائرية في مكافحتها:

سنتطرق في هذا المبحث الى تعداد بعض أنواع الجرئم الالكترونية التي نصت عليها بعض الاتفاقات الدولية ووردت في قانون العقوبات الجزائري ، و ذلك في المطلب الأول و سنعتمد في المطلب الثاني إلى تسليط الضوء على الجهود الدولة الجزائرية في مواجهة الجريمة الالكترونية

المطلب الأول: أنواع الجرائم الالكترونية:

تباينت أشكال وصور الجريمة **الإلكترونية** مما أدى إلى عدم اتفاق الفقهاء على معيار واحد لتصنيفها وذلك حسب المعيار الذي يستند إليه التقسيم، وبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته، وعليه سوف نعرض لأهم هذه التقسيمات على النحو التالي:

الفرع الأول: الجرائم الواقعة على النظام المعلوماتي:

يستهدف هذا النوع من الجرائم المكونات المادية والمعنوية للنظام المعلوماتي [6]، حيث نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2014 على صور الجرائم التي تستهدف تقنية المعلومات في المواد من 6 إلى 11 منها،[7] كما أحدث المشرع الجزائري قسما خاصا في قانون العقوبات القسم السابع مكرر من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال الذي عنونه بـ "المساس بأنظمة المعالجة الآلية للمعطيات" والذي نصت أحكامه على أشكال الجريمة المعلوماتية ضمن المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 منه، وتتمثل هذه الجرائم فيما يلي:

---

[1]- جورج إسحاق حنين، ورقة عمل بعنوان الجرائم المعلوماتية والالكترونية عبر شبكة الأنترنت وسبل مواجهتها، مركز المعلومات والتوثيق، ص08.

[2]- كتاب أعمال المؤتمر الدولي الرابع عشر، المرجع السابق، ص101.

[3]- نفس المرجع ، ص101.

[4]- عبد الله دغش العجمي، المرجع السابق، ص22.

[5]- كتاب أعمال المؤتمر الدولي الرابع عشر، المرجع السابق، ص102.

[6]- المرجع نفسه، ص104.

[7]- زهيرة كيسي، صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014، مجلة العلوم القانونية والسياسية، المجلد 10 العدد 1، أفريل 2019، ص781.

أ/ جريمة الدخول والبقاء غير المشروع في المنظومة المعلوماتية:

نصت عليها المادة 6 من الاتفاقية العربية[1] ، والمادة 394 مكرر من قانون العقوبات الجزائري، حيث تتحقق هذه الجريمة بالولوج والاتصال بكل أو بجزء من النظام المعلوماتي والوصول إلى البيانات المخزنة داخله[2] . بغرض الاطلاع عليها لمجرد التسلية أو الرغبة في اختراق النظام.

ب/ جريمة التزوير والاحتيال المعلوماتي:

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على جريمة التزوير والاحتيال المعلوماتي الواقعتين على البيانات الموجودة داخل النظام المعلوماتي وذلك بالتلاعب فيها وإدخال معلومات غير صحيحة عليها[3] ، كما نص المشرع الجزائري عليها في المادة 394 مكرر 1 حيث اعتبر كل من أدخل بطريق الغش معطيات في نظام المعالجة أو أزال أو عدّل في مضمونها تحت طائلة العقاب.[4]

ج/ جريمة الاعتداء على سلامة البيانات وإساءة استخدامها:

نصت الاتفاقية العربية على الأفعال المادية المكونة لهذه الجريمة، كما نص المشرع الجزائري في المادة 394 مكرر 2 قانون العقوبات على نفس الصورة، حيث تتحقق هذه الجريمة متى قام الجاني بإحدى الأفعال التالية:

- تصميم أو تجميع أو توفير أو الاتجار في معطيات مخزنة أو معالجة مرسلة عن طريق منظومة معلوماتية.
- حيازة أدوات أو برامج أو استعمالها لأي غرض كان.[5]

الفرع الثاني: الجرائم الواقعة بواسطة النظام المعلوماتي:

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتنفيذها مما جعلها تعتبر جرائم تقليدية منصوص عليها في أغلب القوانين ولكن ارتكابها بواسطة تقنية المعلومات جعلها من قبيل الجرائم المعلوماتية والتي تقسم بدورها إلى ثلاث فئات هي:

أ/ الجرائم المعلوماتية الواقعة على الأشخاص:

مع تطور شبكة الأنترنت أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها مما جعلها عرضة للانتهاك من طرف مجرمين محترفين، حيث يقصد بجرائم الاعتداء على الأشخاص تلك الأفعال غير المشروعة التي تمس بالمقومات الأساسية للشخص، وتعتدي على شخصيته الطبيعية والعضوية، فتمس بذلك حقه في الحياة وسلامة الجسد وحقه في صيانة شرفه وعرضه [6]، وعلى هذا ظهرت عدة أنواع للجرائم المعلوماتية الواقعة على الأشخاص والتي تمثلت في:

---

[1]- المادة السادسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 08 سبتمبر 2014، ج.ر، العدد57 المؤرخة في 28 سبتمبر 2014.

[2]- المادة 394 مكرر من قانون رقم 156/66 المؤرخ في 08 صفر 1386 الموافق لـ 8 يوليو 1966، والمتضمن قانون العقوبات المعدل والمتمم بالقانون رقم 01/14 المؤرخ في 2014/02/04.

[3]- زهيرة كيسي، المرجع السابق، ص784.

[4]- المادة 394 مكرر 1 من قانون العقوبات الجزائري.

[5]- المادة 394 مكرر 2 من قانون العقوبات الجزائري.

[6]- هروال نبيلة هبة، جرائم الأنترنت، أطروحة دكتوراه، جامعة أبي بكر بلقايد، تلمسان، 2013-2014، ص73.

– جرائم التهديد والمضايقة والمطاردة عبر الأنترنت وخاصة عن طريق البريد الالكتروني، وذلك بإرسال الرسائل لترويع وابتزاز الأشخاص أو عن طريق مواقع التواصل الاجتماعي المختلفة [1]، والاعتداء على حرمة حياتهم الخاصة بالاطلاع على المعلومات دون وجه حق ومراقبة الاتصالات.

– وكذا جرائم القذف والسب وتشويه السمعة للمساس بشرف وكرامة الأشخاص عن طريق إفشاء ونشر صور أو معلومات بواسطة وسائل الاتصال أو الكتابة أو المبادلات الالكترونية من صفحات الويب وغرف الدردشة.

– كما يضاف إلى هذه الجرائم جرائم انتحال الشخصية والتي تتمثل في استغلال الشخص للمعلومات الشخصية لشخص آخر [2]، للاستفادة من سمعته أو ماله أو صلاحياته من أجل الحصول على امتياز مادي [3]، أو لإخفاء هوية الشخص المجرم لتسهيل ارتكابه لجرائم أخرى، كما يمكن أيضا انتحال شخصية موقع[4].

– كما تعتبر الجرائم الأخلاقية من أهم وأخطر الجرائم الالكترونية الواقعة على الأشخاص والتي تأخذ أشكالا متعددة، كجريمة التحرش الجنسي وجريمة نشر وصناعة الإباحة المرتبطة بالكبار والأطفال، حيث يتعرض الأطفال للاستغلال عبر الأنترنت [5]، وذلك عن طريق نشر صور لمواد إباحية تظهر أطفال في ممارسات جنسية مختلفة من أجل إفساد أخلاقهم واستدراجهم للاعتداء عليهم [6]، وسنعيد التطرق لهذه النقطة في المحور الثالث الخاص ببيان صور مخاطر المعلوماتية على الأطفال.

ب/ الجرائم المعلوماتية الواقعة على الأموال:

في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات الالكترونية تطورت وسائل الدفع والوفاء والتداول المالي وأصبحت تتم عبر شبكة الأنترنت ،[7] مما سهل الاعتداء على هذه المعاملات وذلك بشتى الطرق أهمها:

– جرائم السرقة والنصب والتحويل الالكتروني للمال والتي تكون باختلاس المعلومات داخل الفضاء الافتراضي ونقلها من حيازة صاحبها إلى حيازة الغير وذلك بالدخول على بعض المواقع وسرقة بطاقات الائتمان مثلا أو سرقة أموال من حسابات بعض العملاء في المسار وذلك باستخدام فيروسات وأساليب خاصة او برمجيات وصفحات وهمية يعدها الجاني لإيقاع الناس والاستلاء على أموالهم[8].

– جرائم الاعتداء على الملكية الأدبية والفنية والتي يقوم فيها الجاني بالاعتداء على المصنفات بواسطة الأنترنت وذلك بإنزال نسخ من كتب أو مقالات وترويجها أو الترويج لأفكار غيره ونسبتها له [9]، ولعل أهم صورة لهذه الجريمة هي جريمة التقليد.

[1]- كتاب أعمال المؤتمر الدولي الرابع عشر، المرجع السابق، ص102.
[2]- أحمد مسعود مريم، المرجع السابق، ص23.
[3]- كتاب أعمال المؤتمر الدولي الرابع عشر، المرجع السابق، ص103.
[4]- خالد ممدوح إبراهيم، المرجع السابق، ص70.
[5]- كتاب أعمال المؤتمر الدولي الرابع عشر، المرجع السابق، ص103.
[6]- بودبة سعيدة، المرجع السابق، ص86.
[7]- زبيدي البشير، المرجع السابق، ص79.
[8]- هروال نبيلة هبة، المرجع السابق، ص193.
[9]- المرجع نفسه، ص207.

– كما ظهرت جرائم غسيل الأموال عبر الأنترنت التي ساعدت على تطورها وانتشارها بسرعة فائقة وسهّلت للمجرمين ارتكابها، وكذا جرائم ترويج المخدرات التي أصبحت تتخذ من المواقع الالكترونية مسرحا لتسويقها وتعليم كيفية صناعتها واستهلاكها[1].

ج– الجرائم المعلوماتية الواقعة على أمن الدولة:

تعد الجرائم الواقعة على أمن الدولة من أخطر الجرائم الالكترونية لتميزها بالطابع الدولي والتي سهّلت الأنترنت ارتكابها دون بذل أي جهد مع تحقيق أكبر عدد ممكن من الضحايا ومن أبرز هذه الجرائم:

– **الإرهاب الالكتروني:** ويعرف على أنه العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الالكترونية والصادر ضد الحكومات أو الشعوب أو المجتمع الدولي لتحقيق أهداف سياسية أو دينية أو اجتماعية،[2] ويتم الترويج من خلالها لأفكار ومعتقدات المنظمات الإرهابية.

– **الجريمة المنظمة:** حيث استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة من وسائل الاتصال عبر الأنترنت من أجل التخطيط وتنفيذ عملياتها الإجرامية بسهولة ويسر وسرعة فائقة[3].

– **التجسس الالكتروني:** حيث يقوم المجرم بالتجسس على الدول والمؤسسات الوطنية والدولية والاطلاع على مختلف الأسرار العسكرية والاقتصادية والسياسية للدول.[4]

– **جرائم المساس بالأمن الفكري:** وهي من أخطر هذه الجرائم لكونها تؤدي إلى التأثير على معتقدات وتقاليد المجتمعات، حيث أصبحت شبكة الأنترنت وسيلة سهلة لارتكابها مما سهّل خلق الفوضى في المجتمعات والمساس بالنظام الداخلي والعام لها.[5]

المطلب الثاني: جهود الدولة الجزائرية في مواجهة الجريمة الإلكترونية

لم تعرف الجزائر قبل سنة 2004 قوانين تطبق على النظم المعلوماتية أو على تكنولوجيا الإعلام والاتصال، لكن أمام تزايد الإجرام المعلوماتي كان لابد للمشرع من إيجاد الإطار القانوني المناسب الذي يمنع الاعتداء على هذه النظم أو الاستعمال السيء لها. و لسد الفراغ القانوني واقتداء بأغلب دول العالم قام المشرع باستصدار قوانين معدلة و متممة لقانون العقوبات تارة و استصدار قوانين خاصة أهمها على الإطلاق القانون 09-04 المؤرخ في 2009/07/05 المتضمن الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

كما تم إنشاء وتسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة إلى وحدات قضائية وأخرى تابعة لسلك الأمن والدرك الوطني.

[1]- كتاب أعمال المؤتمر الدولي الرابع عشر، المرجع السابق، ص103.
[2]- هروال نبيلة هبة، المرجع السابق، ص333.
[3]- زبيدي البشير، المرجع السابق، ص79.
[4]- كتاب أعمال المؤتمر الدولي الرابع عشر، المرجع السابق، ص103.
[5]- زبيدي البشير، المرجع السابق، ص79.

الفرع الأول: الحماية القانونية والتشريعية للجريمة الالكترونية

وتتمثل في كل من قانون العقوبات، وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والتعديلات التي مست قانون الإجراءات الجزائية.

تعديل قانون العقوبات:

استحدث المشرع الجزائري القسم السابع مكرر من قانون العقوبات من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات بنص المواد 394 مكرر إلى المادة 394 مكرر 7،[1] واستقراء هذه المواد يتضح أن المشرع قسم الجرائم الإلكترونية إلى أربع طوائف تتعدد بحسب المصالح المحمية التي تتمثل أساسا في سرية هذه المعطيات أو تكاملها و في وفرتها و في تكاملها هي:

الطائفة الأولى: وتتضمن جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير، وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات.

الطائفة الثانية: الجرائم الإلكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي.

الطائفة الثالثة: الجرائم المتعلقة بأمن الدولة و مؤسساتها كجرائم التجسس والإرهاب.

الطائفة الرابعة: الجرائم الالكترونية للشخص المعنوي و التي تعادل عقوبتها خمس مرات عقوبة الشخص الطبيعي 394 مكرر4 من قانون العقوبات.[2]

وفي عام 2006 أدخل المشرع الجزائري تعديلا آخر على قانون العقوبات بموجب قانون رقم 23/06 المؤرخ في 20 ديسمبر 2005 .حيث مس هذا التعديل القسم السابع مكرر و الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و قد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص الواردة في هذا القسم من القانون 15/04.[3]

ويرجع البعض سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى و شيوع ارتكابه فقط من الطبقة المثقفة، بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الأنترنت كوسيلة لنقل المعلومات.[4]

قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

إن تفاقم الاعتداءات على معطيات على معطيات الحاسب الآلي خاصة مع ضعف الحماية الفنية، استدعى تدخلا تشريعيا صريحا، فقد استدرك المشرع الجزائري الفراغ القانون من خلال هذا القانون، حيث

[1]- القانون رقم 15/04 المعدل و المتمم للأمر 155/66 الصادر بتاريخ 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات.

[2]- سعيد بوزنون ، مكافحة الجريمة الإلكترونية في التشريع الجزائري ، مجلة العلوم الإنسانية ، جامعة الإخوة منتوري، قسنطينة ، المجلد 30 ، عدد3، ديسمبر 2019 ، ص49.

[3]- القانون رقم 23/06 المعدل و المتمم لقانون العقوبات المؤرخ في 20 ديسمبر 2006.

[4]- بلفكرات رشيد، بنزعمة عبد القادر، الجريمة الإلكترونية كتهديد للأمن الوطني الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة، المجلد الرابع، مارس 2019، ص517.

أجاز المشرع مراقبة الاتصالات الالكترونية، غير أنه حدد الحالات التي يسمح فيها باللجوء إلى المراقبة الالكترونية، مع اشتراط الحصول على إذن مكتوب من السلطة القضائية المختصة، كما جاء في القانون جواز التفتيش ولو عن بعد، بالإضافة إلى الإجراء المترتب عن التفتيش وهو الحجز في المواد 5و6 .[1]

قانون الإجراءات الجزائية الجزائري:

بالنسبة لمتابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية ، كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة. غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية في المادة 37 من قانون الإجراءات الجزائية.[2]

ونص على التفتيش في المادة 45 الفقرة 7 (1)، حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من إجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، لا تطبق الأحكام الواردة في المادة 44 من (ق.إ.ج.ج) إذا تعلق الأمر بالجرائم الإلكترونية[3].

الفرع الثاني: الأجهزة المختصة في متابعة الجريمة الالكترونية في التشريع الجزائري

لعل من ابرز الهيئات المختصة والتي قامت الدولة الجزائرية في مجال مكافحة الجرائم الالكترونية هي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. إضافة إلى المديرية العامة للأمن الوطني، وكذا الهيئات القضائية الجزائية المتخصصة.

1 -الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

أنشئت هذه الهيئة بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

ومن مهامها، تفعيل التعاون القضائي و الأمني الدولي و إدارة و تنسيق عمليات الوقاية و المساعدة التقنية للجهات القضائية و الأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية .في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.[4]

2 -الهيئات القضائية الجزائية المتخصصة:

أنشئت بموجب القانون 04-14 المؤرخ في 2004/11/10 المعدل و المتمم لقانون الإجراءات الجزائية [5]تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 32 ، 37 ، 40، من (ق.إ.ج.ج) تتمتع بمباشرة مهامها في دائرة الاختصاص الإقليمي الموسع طبقا للمرسوم التنفيذي رقم 06-348 المؤرخ في 2006/01/05 .بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام و الاتصال المرتكبة

[1]- مكافحة الجريمة الالكترونية في التشريع الجزائري، بوعناد فاطمة زهرة، مجلة الندوة للدراسات القانونية، العدد الأول، 2013، ص64.

[2]- الأمر رقم 155/66 المؤرخ في 8 يونيو 1966 ، المتضمن قانون الإجراءات الجزائية المعدل و المتمم بالقانون رقم 07/17 المؤرخ في 27 مارس 2017 ، الجريدة الرسمية ، رقم 20 بتاريخ 20 مارس2017

[3] - المادة 45 من قانون الاجراءات الجزائية المعدل والمتمم بقانون رقم 06 -22 مؤرخ في 20 ديسمبر 2006، الجريدة الرسمية- عدد 84 ص6.

[4] - سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية، بمحكمة سيدي محمد، ص11.

[5]- القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 ، يعدل و يتمم الأمر رقم 66-155 المؤرخ في 08 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، الصادر بالجريدة الرسمية رقم 71 بتاريخ 10 نوفمبر 2004.

في الخارج حتى و لو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09-04.

المديرية العامة للأمن الوطني:

تتصدى هذه المديرية للجريمة الالكترونية من عدة جوانب منها الجانب التوعوي، بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية التوعوية، وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية، و كذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شانها توعية المواطن حول خطورة الجرائم الإلكترونية.

ودائما في إطار مكافحة الجريمة الالكترونية و نظرا للبعد الدولي عادة ما يتخذه هذا النوع من الجرائم، أكدت الجزائر على عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية و منظمة الشرطة الجنائية الإفريقية.[1]

خاتمة:

في ختام هذا البحث المتواضع والذي حاولنا من خلاله الالمام بجوانب الموضوع وما يطرحه من اشكالات توصلنا إلى عدة نتائج هامة كما قدمنا بعض الاقتراحات والتوصيات التي رأينا أنها مفيدة لموضوع الدراسة وذلك كما يلي:

1/ النتائج:

1 -تعتبر الجريمة الإلكترونية من الجرائم المستحدثة التي أفرزتها الثورة الالكترونية والتي لا زالت في تطور دائم ومستمر وهذا ما أدى إلى عدم الاتفاق على تعريف جامع مانع لها.

2 -تختلف الجريمة الالكترونية عن نظيرتها التقليدية من حيث أساليب ارتكابها وموضوعها وتتميز بذلك عنها بعدة خصائص، حيث تعتبر جريمة صعبة الاكتشاف والاثبات وعابرة للحدود، كما يتميز مرتكبها عن المجرم العادي بذكائه ومهاراته ومعرفته بأساليب التقنية العالية.

3 -تتباين أشكال الجرائم المعلوماتية بين جرائم واقعة على الحاسب الآلي وأخرى واقعة بواسطته لتشمل جرائم المساس بالأشخاص و الواقعة على الأموال.

4 -2/ الاقتراحات:

1 -من واجب الدولة ممارسة الرقابة اللازمة على المواد الواردة في الأنترنت بما تملك من وسائل تقنية وقانونية لحجب المواقع المشبوهة،

2 -تكثيف تنظيم المؤتمرات والملتقيات العلمية من قبل الأكاديميين والمختصين في مجال حماية الأفراد و المؤسسات من مخاطر المعلوماتية بصفة خاصة وتطورات ومخاطر الجرائم المستحدثة بصفة عامة من أجل إيجاد سبل لتوفير الحماية لهم والتقليل من حجم الجرائم المعلوماتية.

[1]- بلفكرات رشيد ،بنزعمة عبد القادر ، المرجع السابق، ص520.

3 -تكثيف الجهود الدولية والوطنية للحد من جرائم المعلوماتية والوصول إلى الحلول الكفيلة بحماية الأفراد وتحقيق أمنهم في الفضاء الرقمي. و كذا من أجل سلامة المن الداخلي .

قائمة المصادر المراجع :

النصوص القانونية :

– الأمر رقم 155/66 المؤرخ في 8 يونيو 1966 ، المتضمن قانون الاجراءات الجزائية المعدل و المتمم بالقانون رقم 07/17 المؤرخ في 27 مارس 2017 ، الجريدة الرسمية ، رقم 20 بتاريخ 20 مارس201

– قانون رقم 156/66 المؤرخ في 08 صفر 1386 الموافق لـ 8 يوليو 1966، والمتضمن قانون العقوبات المعدل والمتمم بالقانون رقم 01/14 المؤرخ في 2014/02/04 .

– قانون رقم 04/09 المؤرخ في 14 شعبان 1430 الموافق ل 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر عدد 47، 2009.

– الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 08 سبتمبر 2014، ج.ر، العدد57 المؤرخة في 28 سبتمبر 2014

الكتب :

1 -خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2008،

– محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، ط1، عمان، 2004 .

الرسائل العلمية :

– لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها، دراسة مقارنة، مجلة الميزان للدراسات الاسلامية والقانونية،2017 .

–عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة الشرق الأوسط،2014.

–رسائل الماجستير بوذراع عبد العزيز، خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير، جامعة الجزائر 1، 2011.

الابحاث و المجلات :

– معاشي سميرة، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، العدد السابع.

–كتاب أعمال المؤتمر الدولي الرابع عشر، الجرائم الالكترونية، طرابلس، 24_25 مارس 2017،

– شينار سامية،الجريمة الالكترونية في منظور الشباب الجامعي مدخل نفسي _ قانوني، مجلة الباحث للدراسات الأكاديمية، المجلد 06، العدد 02، 2019،

– سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الاجرام، جامعة أبو بكر بلقايد، تلمسان، 2010–2011 .

– زبيدي البشير، واقع جرائم تكنولوجيا الاعلام والاتصال في العالم وآليات مكافحتها، مجلة الدراسات الاقتصادية المعاصرة، العدد 3، 2017.

– معاشي سميرة، الجريمة المعلوماتية، دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة المفكر، العدد 17، جوان، 2018.

– جورج إسحاق حنين، ورقة عمل بعنوان الجرائم المعلوماتية والالكترونية عبر شبكة الأنترنت وسبل مواجهتها، مركز المعلومات والتوثيق.

– سعيد بوزنون ، مكافحة الجريمة الإلكترونية في التشريع الجزائري ، مجلة العلوم الإنسانية ، جامعة الإخوة منتوري ،قسنطينة ، المجلد 30 ، عدد3، ديسمبر 2019..

– بلفكرات رشيد ، بنزعمة عبد القادر ، الجريمة الإلكترونية كتهديد للأمن الوطني الجزائري ،مجلة العلوم القانونية و الاجتماعية ، جامعة زيان عاشور بالجلفة ، المجلد الرابع ، مارس 2019

– مكافحة الجريمة الالكترونية في التشريع الجزائري ، بوعناد فاطمة زهرة ، مجلة الندوة للدراسات القانونية العدد الاول ، 2013 .

– سالم عبد الرزاق ، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية ، بمحكمة سيدي محمد .

خالدية بلحاج
besmafarha@gmail.com
جامعة جيلالي ليابس سيدي بلعباس

ماهية الجرائم الإلكترونية الاقتصادية

ملخص:

أدى الاستعمال الهائل للوسائل التكنولوجية الحديثة لا سيما الانترنت منها إلى ظهور نوع جديد من الجرائم أطلق عليه اسم "الجرائم الإلكترونية" هذه الأخيرة التي لم تترك مجالا إلا اخترقته بما في ذلك المجال الاقتصادي الذي شهد عديد الجرائم، جرائم ناعمة عابرة لحدود الدول صعبة الاكتشاف والتتبع لأن أغلبها لا يتم الإبلاغ عنها،ما دفع الكثيرين إلى البحث في ماهيتها وأنواعها.

الكلمات المفتاحية: الجرائم الإلكترونية ذات البعد الاقتصادي، المفهوم، الأنواع.

***Summary*:**

The massive use of modern technological means, especially the Internet, has led to the emergence of a new type of crime called "electronic crimes", the latter of which left no room but penetrated, including the economic field, which witnessed many crimes. Soft cross-border crimes are difficult to detect and track because most of them are not reported, which prompted many to research their nature and types.

مقدمة:

مما لا شك فيه أن الاقتصاد عالم كبير تطور بتطور البشرية فقد بني قديما على الفلاحة بشتى مجالاتها فانحصرت الجرائم وقتها في كل ما يمس بها، واتسعت رقعته لتشمل الصناعة والتجارة ومجالات التبادلات المالية وفق الأنماط المختلفة، فأصبح بيئة خصبة لمختلف أنواع الجرائم، لا سيما الجريمة الإلكترونية التي اعتلت سلم الجرائم لتصبح جريمة العصر بكل ما تعنيه الكلمة، حيث اخترقت الجريمة الإلكترونية مختلف المجالات الاقتصادية لتلحق الضرر بالأفراد فقط بل بالشركات والمؤسسات والدول، وهذا ما أدى بنا إلى طرح الإشكال التالي: "ما هي الجرائم الإلكترونية الاقتصادية؟

وفي سبيل المحاولة للإجابة على الإشكال المطروح والبحث في الإطار المفاهيمي للجريمة الإلكترونية الاقتصادية، اتبعت الخطة التالية:

المحور الأول: مفهوم الجريمة الإلكترونية الاقتصادية.

أولا: تعريف الجريمة الإلكترونية والاقتصادية.

ثانيا: أركان الجريمة الإلكترونية الاقتصادية.

المحور الثاني: خصائص وبعض أنواع الجريمة الإلكترونية الاقتصادية.

أولا: مميزات الجريمة الإلكترونية الاقتصادية.

ثانيا: بعض أشكال الجريمة الإلكترونية الاقتصادية.
متبعة في ذلك المنهاج الوصفي التحليلي، راجية أن يحظى طرحي بالتوفيق.

المحور الأول: مفهوم الجريمة الإلكترونية الاقتصادية.

يقضي البحث في مفهوم الجريمة الإلكترونية الاقتصادية، التطرق إلى تعريفها وتبيان أركانها.

أولا: تعريف الجريمة الإلكترونية الاقتصادية.

يتبادر إلى الذهن أن الجريمة الإلكترونية الاقتصادية هي لأول وهلة جريمة إلكترونية ذات بعد اقتصادي أو هي جريمة اقتصادية اقترفت بطريقة آلية إلكترونية، ولهذا سوف أتطرق إلى تعريف الجريمة الإلكترونية على حدة ثم تعريف الجريمة الاقتصادية عموما لنصل إلى الجمع بين التعريفين في محالة لإيجاد تعريف جامع حول الجريمة الإلكترونية الاقتصادية.

1 تعريف الجريمة الإلكترونية:

تعددت التسميات للدلالة على هذه الجرائم فمنهم من يستعمل مصطلح "الجرائم المعلوماتية" أو الجرائم المرتكبة عبر الانترنت أو جرائم الحاسب الآلي وغيرها، وبهذا تعددت التعريفات أيضا وذلك وفقا للتطور التكنولوجي المواكب للوسائل التقنية المستعملة فيها واختلاف زاوية النظر إليها، فهناك اتجاه يستند في تعريفها إلى وسيلة ارتكاب الجريمة، حيث عرفها مكتب التقنية في الولايات المتحدة بانها "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا.[1]

وعرفها الفقيه (تايدمان Tiedman) "كل أشكال السلوك غير المشروع (أو الضار بالمجتمع) الذي يرتكب باستخدام الحاسب".[2]

وهناك من يعرفها بالاستناد إلى موضوع الجريمة، حيث عرفها الفقيه (روسبلات Rsblat) بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف، او الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحول عن طريقه"[3]، فيما ذهب اتجاه ثالث إلى تعريف الجريمة الإلكترونية بالنظر إلى مرتكب الجريمة، حيث عرفها دافيد تومسون بأنها جرائم يكون متطلب لاقترافها أن تتوفر لدى فاعلها معرفة ودراية بتقنية المعلوماتية.

ولقد تعرضت هذه التعريفات إلى عديد الانتقادات وذلك لعدم دقتها واعتمادها على وصف الجريمة لا تحديد ماهيتها ولهذا ظهرت تعاريف أخرى لتحديد مفهوم الجريمة الإلكترونية.[4]

---

[1]- محمود أحمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، 2005، ص15.

[2]- خلدون عيشة، الطبيعة الخاصة للجريمة الإلكترونية وصورها، جامعة الجلفة، ص114.

[3] - خلدون عيشة، نفس المرجع، نفس الصفحة.

[4]- عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق والحريات، العدد2، 2014، ص73.

حيث عرفها البعض الآخر أنها: "كل فعل أو امتناع عمدي ينشأ عن استخدام غير مشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية".[5]

وجاء في مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا سنة 2000 بأنها "جريمة يمكن ارتكابها بواسطة نظام حاسوبي شبكة حاسوبية أو داخل نظام حاسوب، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".[6]

ومصطلح المعلوماتية أدق كونها تشمل الحاسب وسائر المبتكرات والتقنيات الحالية والمستقبلية، المستحدثة في التفاعل مع المعلومات، لأنه يمكن تصور هذه الجرائم من زاويتين:

الأولى: أن الجاني يرتكب جرائمه باستخدام المعلوماتية، سواء تعلق الأمر بالاعتداء على الأشخاص أو على الأموال.

الثانية: أن المجرم يجعل المادة المعلوماتية محلا وموضوعا لجرائمه.[7]

كما عرفت بأنها "كل فعل غير مشروع اقترن بالتواصل مع منظومات معلوماتية وشركات تواصل خاصة به، والتي يحميها القانون ويوجب عقابا لها".[8]

2 تعريف الجريمة الاقتصادية:

يتفق البعض أن الجريمة الاقتصادية هي فعل مجرم مخالف للقانون يمس مصلحة اقتصادية، وبما أن كلمة "اقتصاد" تشمل عديد المجالات فإن الفقهاء تباينوا في تقديم تعريف دقيق للجريمة الاقتصادية فهناك من اعتمد على المعنى الضيق للجريمة الاقتصادية وهناك من تبنى المعنى الواسع للجريمة الاقتصادية.

أ. الاتجاه الضيق في تعريف الجريمة الاقتصادية:

بريادة الفقيه جون برادال Jean pradel الذي عرفها بكونها تلك الجريمة المتعلقة بمجال السوق والمبادلات التجارية سواء كانت تجمع بين منتج أو بين موزع ومستهلك وسواء كانت هده المبادلات تتعلق بمنتج أو خدمة"[9]حيث حصر مجال الجريمة الاقتصادية في المبادلات التجارية فقط.

كما عبرت محكمة النقض الفرنسية عن هدا المفهوم أيضا حيث عرفتها بأنها: "الجريمة التي من شأنها أن تمس بإنتاج وتوزيع واستهلاك وتداول السلع والخدمات " [10]، حيث يبقى مجال المبادلات الموضوع الأساسي للجريمة الاقتصادية.

---

[5]- خلدون عيشة، المرجع السابق، ص115.

[6]- حوالف حليمة، ط/د، مهاجيف.ز، معالم الجريمة المعلوماتية في القانون الجزائري، مقال منشور بمجلة البحوث القانونية والسياسية، مجلد 03، العدد16، 2021، ص142- 143.

[7]- خلدون عيشة، المرجع السابق، ص115.

[8]- حوالف حليفة، المرجع السابق، ص143.

[9]- إيهاب الروسان، خصائص الجريمة الاقتصادية، دراسة في المفهوم والأركان، فاتر السياسة والقانون، تونس، ص75.

[10]- نبيل بنخدير، خصائص الجريمة الاقتصادية وآثارها الخاصة والعامة مجلة البحوث القانونية والاقتصادية، مجلد 04، عدد 01، 2021، ص207.

أما الفقيه جان لارجيبه J largvier أن الجريمة الاقتصادية مرتبطة برأس المال منطلقا من القواعد القانونية المنظمة للمادة الاقتصادية.[11]

ب. الاتجاه الواسع في تعريف الجريمة الاقتصادية:

ومن بين مؤيدي هدا الاتجاه الفقيه فريج Vrij الذي يرى أن الجريمة الاقتصادية هي جريمة موجهة ضد إدارة الاقتصاد المتمثلة في القانون الاقتصادي والسياسة الاقتصادية التي ترتبط بالنظام العام الاقتصادي".[12]

كما عرف الأستاذ نيفودا الجريمة الاقتصادية بأنها: "تلك الجريمة التي تلحق ضررا مباشرا أو غير مباشر أو تهدد مصالح الاقتصاد الوطني أو النظام الاقتصادي ذاته بحيث يتضمن القانون الجنائي عناصره".[13]

ويتضح من خلال التعريف السابق أن الجريمة الاقتصادية اتسع مداها لتشمل جرائم صغيرة يعاقب عليها جزائيا ويخلص البعض إلى أنها تمارس بأسلوبين:

الأول: جرائم رجال الأعمال أو ما يعرف بجرائم الياقات البيضاء، والثاني: يتمثل في توفير السلع والخدمات غير المشروعة أو بأسلوب غير مشروع وهو ما أطلق عليه بالجريمة المنظمة.[14]

3 الجمع بين التعريفين: تعريف الجريمة الإلكترونية الاقتصادية:

منّ اهم التعريفات والذي اعتبر جامعا ومانعا، بخصوص الجريمة الإلكترونية ذات البعد الاقتصادي جاء فيه: "هي كل سلوك إنساني فعلا كان أو امتناعا، يرتب أضرارا بمصلحة اقتصادية يحميها القانون، أو يمثل اعتداءا على المواد الاقتصادية المملوكة أو التي يحوزها الأفراد والمؤسسات بما يرتب عليها ضررا.[15]

كما عرفت منظمة التعاون الاقتصادي والتنمية والخاصة باستبيان الغش المعلوماتي سنة 1982 الوارد ضمن التقرير البلجيكي بانها: "فعل أو امتناع من شانه الاعتداء على الأموال المادية والمعنوية يكن ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات".

وعليه فإن الجريمة الإلكترونية الاقتصادية هي كل فعل غير مشروع ذو صيغة اقتصادية متصل بتقنية الحاسب الآلي ويرتب نتائج اقتصادية.[16]

ثانيا: أركان الجريمة الإلكترونية:

كما هو معلوم فإن أركان أي جريمة ثلاثة وهي الركن الشرعي، الركن المادي والركن المعنوي.

1. الركن الشرعي للجريمة الالكترونية الاقتصادية:

[11]- إيهاب الروسان، المرجع السابق، ص75.
[12]- إيهاب الروسان، المرجع السابق، ص75.
[13]- نبيل بن خدير، المرجع السابق، ص207.
[14]- نبيل بن خدير، المرجع نفسه، صفحة نفسها.
[15]- حورية قويقح، المرجع السابق، ص244.
[16]- حورية قوقح، المرجع نفسه، صفحة نفسها.

يقصد بالركن الشرعي وجود نص قانوني يجرم الفعل ويعاقب عليه، فلا جريمة ولا عقوبة ولا تدابير أمن إلا بنص قانوني، وبعد الفراغ القانوني الذي كانت تعاني منه المنظومة التشريعية في هذا المجال سعت الجزائر لسده بتعديل قانون العقوبات وذلك بالقانون 15/04[17] والقانون 04/09[18] المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وفي المادة الاقتصادية التي تمتاز بالديناميكية وعدم الاستقرار إضافة إلى جملة من التشعبات والتعقيدات التي تتطلب دراية فنية تضطلع فيه الإدارة والسلطة المتدخلة بدور ريادي لدرايتها بحركيتها وكنتاج لهذا نراجع دور المشرع في نظام الجريمة في المادة الاقتصادية الذي لا يمكن أن يسايرها جمود القاعدة الجزائية التقليدية ولا يعد هذا إنقاصا من قيمة مبدأ الشرعية بل تأكيد عليه، فالسلطة التنظيمية تستمد سلطتها في وضع محتوى التجريم من النصوص التفويضية، بمقتضى مناشير ومراسيم وقرارات يتم إصدارها لغرض تنظيم الحياة الاقتصادية، إلا أن الفقه وجه انتقادات كبيرة لهذه الإحالة إلى السلطة التنفيذية، إذ أن الغدارة لا توقع عقوبات سالبة للحرية ويكون لها دور كبير في تحديد الجريمة بينما يجب الرجوع للنص التشريعي أجل توقيع العقاب، فالتفويض التشريعي هنا يعتبر إذن آلية العمل في مجال الإجرام الاقتصادي، لضمان وجود تنظيم قانوني تقني وفني يصعب على النص التشريعي بلوغه غير أنه قد يتسبب في تحريف عناصر التجريم وتعدد مصادره ما يؤدي إلى تضخم تشريعي يصعب الإلمام به.[19]

2. الركن المادي للجريمة الاقتصادية الإلكترونية:

يعتبر الركن المادي للجريمة هو السلوك المادي (الإيجابي أو السلبي) غير المشروع بهدف الوصول إلى غاية ما ويحدد له القانون العقاب اللازم شريطة أن يكون له مظهرا خارجيا ملموسا فلا يعاقب القانون على النيات، إذن فالركن المادي مبني على عناصر ثلاث هي: السلوك الإجرامي، النتيجة الإجرامية وعلاقة السببية بين السلوك والنتيجة.

السلوك الإجرامي: وهو فعل الجاني الذي يحدث أثرا ما في العالم الخارجي، وقد يكون إيجابيا (بعمل ما) أو سلبيا (الامتناع عن عمل ما).

النتيجة الإجرامية: وهي الأثر المادي الذي يخلفه العمل الإجرامي على السببية بين السلوك والنتيجة، وهي الرابطة بين السلوك الإجرامي والنتيجة المحققة التي تدل على أن النتيجة هي أثر السلوك الإجرامي وتعد شرطا أساسيا لتحديد المسؤولية.[20]

---

[17]- قانون 15- 04 مؤرخ في 11 ربيع الثاني 1436هـ الموافق للفاتح فيفري 2015 المتعلق بالقواعد العامة المتعلق بالتوقيع والتصديق الإلكتروني.

[18]- قانون 09- 04 المؤرخ في 14 شعبان 1430هـ الموافق ل05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[19]- إيهاب الروسان، المرجع السابق، ص84.

[20]- عبد المومن بن صغير، المرجع السابق، ص87.

وكما يكتف الغموض تحديد الركن المادي في الجرائم الإلكترونية يزداد هذا الغموض في مجال الجرائم الإلكترونية ذات البعد الاقتصادي، فتحديد الركن المادي في الجرائم الإلكترونية عامة يشير إلى جملة من الصعوبات التي تفرضها طبيعة الوسط الذي تتم فيه الجريمة والمتمثل في الجانب التقني، وهذا ما يميز ركنها المادي حيث يجب أن تتم بواسطة جهاز حاسب آلي أو بيئة رقمية ويتطلب معرفة بداية هذا النشاط والشروع فيه وأيضا نتيجته، ويصعب الفصل بين الأعمال التحضيرية والشروع في النشاط الإجرامي حيث أن السلوك الإجرامي في المجال الرقمي يبدأ بمجرد الضغط على زر في الحاسب الآلي فيتم تدمير النظام المعلوماتي أو حصول تزوير أو سرقة عن طريق التسلل إلى أرصدة عملاء البنوك مثلا، وكذلك النتيجة الإجرامية تثير بعض التساؤلات حيث يتعدى مداها العالم الافتراضي لتشمل دولا وأقاليم وكذا رابطة السببية من السلوك والنتيجة حيث يصعب معرفة السبب أو الأسباب الحقيقية لتحديد المسؤوليات بالنظر إلى التطور الهائل في مجال وسائل الاتصال وتنوع أساليبها.[21]

وفي الجرائم الاقتصادية يتصرف التجريم فيها في الغالب إلى نتائج خطرة محتمل وقوعها أو حصول ضرر منها حيث يدخل المشرع بهدف الوقاية منها.[22]

ومن هذا المنظور صنفت الجرائم الاقتصادية ضمن طائفة جرائم الخطر أو الجرائم الشكلية والتي تقع بالاكتفاء بالسلوك الإجرامي دون النظر إلى تحقق النتيجة التي يصبو إليها، فالمسؤولية الجزائية قائمة على أساس الخطأ من ناحية أولى ليتم التخلي عنه للمسؤولية الموضوعية من جهة ثانية.

والخطأ الجنائي هو خرق لقاعدة قانونية آمرة أو ناهية اقترنت بعقوبة جزائية، ويتحقق الخطأ نتيجة لفعل إيجابي أو سلبي مجرم بنص قانوني معاقب عليه.[23]

3. الركن المعنوي للجريمة الاقتصادية الإلكترونية:

يعتبر الركن المعنوي من أهم أركان الجريمة حيث أنها يربط بين ماديات الجريمة وشخصية مرتكبها، وهو يقوم على فكرة القصد الجنائي فهو الذي يعتد على الإثم في نفسية الجاني لذلك يقال أن الفعل لا يكون آثما إلا إذا كانت النفس آثمة أي النية في إحداث الضرر ويقصد الجنائي يقوم على العلم والإرادة، حيث بعد العلم (بالواقع وبالقانون) حالة نفسية في ذهن الجاني والوعي بحقيقة الواقع وتوقع النتيجة الإجرامية كأثر مباشر للفعل الذي أقدم عليه وأن الإرادة الرغبة المصاحبة للنشاط النفسي الموجه لأعضاء الجسم من أجل إحداث النتيجة الإجرامية.[24]

وفي مجال الجرائم ذات الطابع الاقتصادي عموما فإن جانب من الفقهاء يرى أن القصد الجنائي فيها قائم على العلم ذلك أنه لا يوجد دور كبير للإرادة فيها سواء اتجهت إرادة الجاني إلى تحقيق نتيجة أم بقيت في إطار السلوك وهو امر غير مقبول عند البعض الآخر من الفقهاء فكيف يمكن تصور تحقق القصد الجنائي بالعلم دون

[21]- عبد المومن بن صغير، المرجع السابق، ص89.
[22]- إيهاب الروسان، المرجع السابق، ص86.
[23]- إيهاب الروسان، المرجع السابق، ص87.
[24]- نبيل بن خدير، المرجع السابق، ص211.

الإرادة، فيما ذهب البعض إلى أبعد من ذلك في إشارة إلى توفر عنصر الغاية أو الهجف الذي دفع المجرم إلى ارتكاب جريمته.[25]

المحور الثاني: خصائص وأشكال الجريمة الإلكترونية الاقتصادية:

في سبيل التعرف أكثر على الجرائم الإلكترونية الاقتصادية كان لزاما التعريج على مميزات وخصائص هذا النوع من الجرائم وكذا إبراز بعض أنواعها.

أولا: خصائص الجريمة الإلكترونية الاقتصادية:

تمتاز الجريمة الإلكترونية الاقتصادية بالمزج بين خصائص الجريمة الإلكترونية والجريمة الاقتصادية التقليدية حيث يمكن إجمالها فيما يلي:

1. صعوبة اكتشافها وتتبعها، وذلك بسبب قدرة مقترفها على محو الأدلة وهدم ترك آثار خارجية، وهي صعبة الإثبات كونها تتطلب اختصاصيين في المجال الإلكترونية والاقتصادي على حد سواء ويبقى عبء الإثبات على عاتق الإدارة فالأعوان المناط بها مهام المراقبة والمعاينة أو التحقيق لهم كافة الصلاحيات لإيجاد الآليات المناسبة للكشف عنها.
2. هي جرائم عابرة للحدود، فأجهزة الاتصال الحديثة توصل المجرم إلى أبعد نقطة دون أن يتحرك من مكانه يكفيه كبسة زر.
3. هي جرائم ناعمة مغرية للمجرمين، لا تحتاج جهدا أكبر ولا أسلحة فتاكة ولا أموال كثيرة لتحضيرها أو ارتكابها يكفي جهاز حاسب آلي ومعلومات كبيرة وإتقان تطبيقات المعطيات الآلية.
4. تمتاز بخصائص مرتبطة بشخص الجاني، حيث أغلبهم ذوو مستوى علمي ودراسي ودراية بالمجال الإلكتروني والاقتصادي حيث يقسم هؤلاء إلى عدة أصناف:

أ -الهواة (هم فضوليون يعتبرون أساليبهم غير المشروعة مجرد تسلية وربما قد لا تشكل أي خطر.[26]

ب -الهاكرز والكراكرز وهو القراصنة.[27]

ج -الطائفة الحاقدة أو المخادعون وتصب جرائمهم على الأموال والتلاعب بالحسابات في المصارف والبنوك.

د -الجواسيس ومهمتهم استخباراتية تهدف إلى جمع المعلومات لمصلحة دولهم أو بعض الشركات ولهم كفاءة عالية في مجال إخفاء الأدلة.

5. تمتاز بخصائص متعلقة بشخص المجني عليه وإن كانت فردا أو شركة أو جهة رسمية، تستخدم جهاز الحاسب الآلي في مزاولة نشاطاته الاقتصادية وتختزن معلوماته المهمة فيه، والكثير منهم يفضل التكتم

[25]- نبيل بن خدير، المرجع السابق، ص211.

[26]- خلدون عيشة، المرجع السابق، ص118.

[27] - صراج كريمة، قبش جمال، الأبعاد الاقتصادية للجريمة الإلكترونية، مجلة الدراسات التسويقية وإدارة الأعمال، مجلد 02، عدد01، جانفي 2018، ص38.

الجريمة التي كان ضحية لها بغية الحفاظ على السمعة الطيبة والابتعاد على كل أشكال الإشهار والفضيحة.

6. خصوصية الجرائم الإلكترونية الاقتصادية من حيث العقوبة فالتشريع في مجالها يتطلب العلم بمشاكل الحياة الاقتصادية وأبعادها المختلفة مما يسهل تحقيق وتطبيق السياسة الاقتصادية العامة للبلاد وارتكاب جرائم تمس بها هو أقرب إلى مخالفة لأوامر السلطة فتوكل مهام التي قبض فيها إلى لجان إدارية لذا فالعقوبة قد تكون إدارية أو جزائية تتسم بالقسوة فعقوبة المساس باقتصاد البلاد يصل إلى حد الإعدام في بعض الدول ولا يعترف بمبدأ القانون الأصلح للمتهم.
7. تغير جرائم خطر في كثير منها وإن لم تحقق ضررا ويعاقب عليها حتى وإن رضي المجني عليه بها.

ثانيا: بعض أشكال الجرائم الإلكترونية الاقتصادية.

تأخذ الجريمة الإلكترونية الاقتصادية العديد من الأشكال منها المالية والتجارية وغيرها وعليه سأتطرق إلى بعض أنواع هذه الجرائم مبرزة أهم خصائصها وأركانها.

1. التحويل الإلكتروني غير المشروع للأموال والسطو على الحسابات المصرفية والبنكية: وهي جريمة مالية تمثل في نقل مبالغ مالية بطريقة آلية من حساب مصرفي إلى آخر بصفة غير شرعية سواء عن طر يق فيروسات إلكترونية خاصة يمكن من اختراق الحسابات المصرفية وسرقة أموالها مثل فيروس (Spyeye) الذي أضر بحوالي 217 بنكا حول العالم.
2. التلاعب بأسعار الأسهم في الشركات في البورصات العالمية بطرق غير مشروعة: او ما يسمى بالمضاربة غير المشروعة كعملية بيع وشراء الأوراق المالية بناء على معلومات مسببة من خلال التي يحصلون عليها من الفارق الطبيعي لأسعار الأوراق المالية في زمان ومكان معين بهدف الحصول على أرباح من جراءها، حيث تحدث توجيه زائف للأسعار بهدف التأثير على أسعار الأسهم والعملات.[28]
3. جريمة الغش في المبيعات: والغش عمل عمدي ينصب على تزييف مواصفات سلعة معينة أو تصنيعها بشكل مغاير للقواعد المعمول بها في أصول الصناعة يقصد إغراء الزبون والربح السريع مما قد يلحق ضررا بالمستهلك لهذه السلعة بشكل عام وقد بأخذ الغش عدة صور منها عدم ذكر المنشأ، عدم التقيد بالوزن المحدد انتهاء صلاحية المنتج بالتلاعب بالتواريخ.[29]
4. الاطلاع على المعلومات السرية للصفقات: ما يؤدي ربما إلى التلاعب بنتائجها أو مجاباة طرف على حساب طرف آخر، مع إمكانية بيع المعلومات إلى أطراف مشاركة فيها.

[28]- قيصر محمود عبيس، جريمة التلاعب بأسعار الأوراق النقدية المضاربة غير الشرعية، بحث مقدم سنة 2016، ص06.
[29]جريمة الغش، منتديات الجلفة، تاريخ الزيارة: 2022/07/19، الساعة 18:40.

5. الجرائم المرتبطة بالبطاقات الائتمانية أو بطاقات الدفع الالكترونية سواء تعلق الأمر ببيانات مزورة أو نسخ بالبيانات على جهاز البيع الإلكتروني لطباعتها على بطاقة أخرى واستعمالها في عمليات بيع وهمية وغيرها من الجرائم المرتبطة بهذه البطاقات.[30]
6. اختراق المواقع الإلكتروني والعبث بمخازن المعلومات بمختلف الشركات: فمن جهة قد يكلف الشركات خسارة زبائنها وقيتها المالية وتحريف بعض المعطيات الخاصة بالشركة والمتعاملين معها.

وهذه بعض الجرائم المنتشرة التي تلحق ضررا بالفرد وبالشركات والمؤسسات وليست كلها.

الخاتمة:

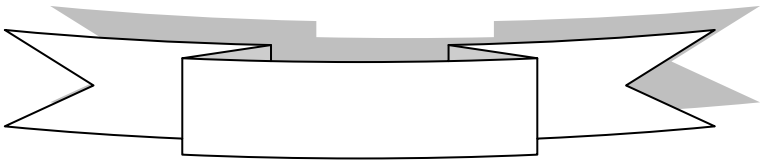
استعمال الوسائل الإلكترونية الحديثة قد غزى لكل العوالم بما في ذلك عالم الجريمة الذي لم يسلم منه مجال من مجالات الحياة المختلفة، حيث مس الاقتصاد، وهو ما اصطلح عليه بالجريمة الإلكترونية الاقتصادية جريمة ناعمة لا تحتاج إلى عنف أو قوة أو سلاح بل معرفة كافية باستعمال الأجهزة الإلكترونية التي ساهمت في إضفاء صعوبة على اكتشاف مرتكبها وتتبع أثره.

المراجع:

1. إيهاب الروسان، خصائص الجريمة الاقتصادية، دراسة في المفهوم والأركان، فاتر السياسة والقانون، تونس، ص75.
2. بوسعيد أسامة، الجرائم الواقعة على بطاقات الدفع الإلكتروني، مذكرة تخرج لنيل شهادة ماستر في القانون العام، جامعة البويرة، السنة الجامعية 2020- 2021، ص32.
3. جريمة الغش، منتديات الجلفة، تاريخ الزيارة: 2022/07/19، الساعة 18:40.
4. حوالف حليمة، ط/د، مهاجيف.ز، معالم الجريمة المعلوماتية في القانون الجزائري، مقال منشور بمجلة البحوث القانونية والسياسية، مجلد03، العدد16، 2021، ص142- 143.
5. خلدون عيشة، الطبيعة الخاصة للجريمة الإلكترونية وصورها، جامعة الجلفة.
6. صراج كريمة، قبش جمال، الأبعاد الاقتصادية للجريمة الإلكترونية، مجلة الدراسات التسويقية وإدارة الأعمال، مجلد02، عدد01، جانفي 2018، ص38.
7. عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق والحريات، العدد2، 2014، ص73.
8. قانون 09- 04 المؤرخ في 14 شعبان 1430هـ الموافق ل 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[30] بوسعيد أسامة، الجرائم الواقعة على بطاقات الدفع الإلكتروني، مذكرة تخرج لنيل شهادة ماستر في القانون العام، جامعة البويرة، السنة الجامعية 2020- 2021، ص32.

9. قانون 15- 04 مؤرخ في 11 ربيع الثاني 1436هـ الموافق للفاتح فيفري 2015 المتعلق بالقواعد العامة المتعلق بالتوقيع والتصديق الإلكتروني.
10. قيصر محمود عبيس، جريمة التلاعب بأسعار الأوراق النقدية المضاربة غير الشرعية، بحث مقدم سنة 2016، ص06.
11. محمود أحمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، 2005.
12. نبيل بنخدير، خصائص الجريمة الاقتصادية وآثارها الخاصة والعامة مجلة البحوث القانونية والاقتصادية، مجلد04، عدد01، 2021، ص207.



زيوش عبد الرؤوف
ziouche.abderaouf@cuillizi.dz
المركز الجامعي الشيخ آمود بن مختار– إيليزي

زغيشي مصطفى
mostefa.zeghichi@cuillizi.dz
المركز الجامعي الشيخ آمود بن مختار– إيليزي

الجرائم الإلكترونية الاقتصادية: المفهوم والأسباب

مقدمة:

تمتاز الجرائم الالكترونية الاقتصادية بتأثيراتها السلبية على مجالات متعددة وخطورتها البالغة على المستويين الدولي والوطني، وتتسع دائرة هذه الخطورة أكثر فأكثر بظهور أنماط مستحدثة من تلك الجرائم لم تكن معروفة من قبل نتيجة التغيرات العالمية التي خلقت بيئة مناسبة لتنامي ظاهرة الاجرام الالكتروني بصفة عامة والاقتصادي على وجه الخصوص، كما أن دوافع ارتكاب هذا النوع من الجرائم كثيرة ومتعدد من الصعب حصرها جميعها، سيما إذا علمنا أن هذه الدوافع تتفاوت وفق نوعها ونوع المستهدف بها ونوع الجاني ومستوى تنفيذها.

انطلاقا من هنا نتساءل حول مفهوم الجريمة الالكترونية الاقتصادية وهل هذا النوع من الجرائم يتميز بخصائص متفردة تميزه عن باقي الجرائم الاقتصادية التقليدية المعروفة؟، ثم ما هي الأسباب التي تدفع إلى ارتكاب هكذا نوع من الأفعال غير المشروعة؟

الدراسة تهدف للإجابة على هذه الاشكالية، من خلال تقسيم الموضوع إلى محورين أساسيين:

المحور الأول: ماهية الجريمة الالكترونية الاقتصادية

المحور الثاني: أسباب الجرائم الالكترونية الاقتصادية

المحور الأول: ماهية الجريمة الالكترونية الاقتصادية

تتعد الجرائم الاقتصادية في العصر الحديث ولعل أبرزها تلك التي تستهدف المعالجة الآلية للمعطيات والمعلومات عبر استخدام وسائل الاعلام الآلي، من خلال أنشطة غير مشروعة مثل السرقة، الاحتيال، الولوج بدون وجه حق إلى مواقع الغير والاعتداء على خصوصيتها.

أولا: مفهوم الجريمة الالكترونية

تعتبر الجرائم الالكترونية (المعلوماتية) جرائم مستحدثة [1] ومعقدة لارتباطها بوسائل التقنيات الحديثة من أجهزة كمبيوتر وشبكات الأنترنت، لذا فقد ارتبط مصطلح هذه الجريمة بالتطور التكنولوجي الذي عرفه النشاط الإنساني بمناسبةاستخدام الكمبيوتر وما يتبعه من أعمال غير مشروعة تمارس من خلال شبكة المعلومات مما صعب من عدم الوصول الى تعريف جامع مانع لهذا المفهوم.

1 -التعاريف الفقهية للجريمة الالكترونية

إن الجريمة الالكترونية باعتبارها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال المادية أو المعنوية [2]، عرفت تعاريف فقهية متعددة ومختلفة باختلاف وجهة نظر أصحابها والسند الم عتمد في ذلك سواء أكان موضوع الجريمة أو وسيلة ارتكاب الجريمة أو الجاني (الفاعل).

لقدعرف روسبالت"Rosbalt"الجريمة الالكترونية بأنها: "نشاط غير مشروع، موجه لنسخ أو تغير أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي، أو حتى التي تحول عن طريقه"[3].

استند Rosbalt في تعريفه هذا إلى موضوع الجريمة والذي يمكن أن يكون نشاط غير مشروع، موجه لنسخ أو تغير أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي.

أما كالوستايدمان"Tiedemann" فعرفها على أنها :"كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي ارتكب باستخدام الحاسب"[4]، وعرفها مكتب التقنية في الولايات المتحدة الأمريكية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا [5]، وقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 تعريف الجريمة الالكترونية بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[6].

ركزت هذه التعاريف على وسيلة ارتكاب الجريمة والتي يمكن أن تكون الحاسب (جهاز الاعلام الالي) أو البرامج المعلوماتية (نظام حاسوبي) أو أي بيئة إلكترونية أخرى.

في تعريف آخر عرفها David Tompson بأنها "جرائم يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"[7]، بالتالي يكون هذا التعريف قد ارتكز على الفاعل أو الجاني مقترف الجريمة الالكترونية الذي يشترط فيه معرفته بتقية الحاسب.

من خلال التعاريف السابقة يمكن القول أن الجريمة المعلوماتية تقع بطريقتين: تقع إما باستخدام الوسيلة المعلوماتية: وهي تستخدم سلوك يمس الحق أو المصلحة لآخر أو آخرين يحميها القانون لارتكاب سلوك التعدي على قواعد حماية الآداب العامة، وإما تقع على الوسيلة المعلوماتية: وهي التي تتضمن سلوك يقع على الوسيلة ذاتها أو محتواها بغية الإضرار بآخرين دون عبرة بالباعث كالولوج الغير مصرح به، أو الإتلاف أو زرع الفيروسات أو القرصنة التي تحدث على الوسيلة ذاتها أو محتواها[8].

2 -التعريف القانوني للجريمة الالكترونية

عرف قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996 نظام المعلومات على أنه: " النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو استلامها او تخزينها لتجهيزها على أي وجه آخر"، في حين استعمل المشرع الجزائري مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات" من خلال قانون رقم : 09-

04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[9]،حيث عرفت المادة 2 منه نظام المعلومات:"المنظومة المعلوماتية هي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو المترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين".

كما عرفت ذات المادة الجرائم المتصلة بأنظمة المعالجة الآلية للمعطيات بقوله: "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات و أية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالاتالالكترونية".

استقراء لهذه المادة، يتضح أن المشرع الجزائري جعل من نظام المعالجة الآلية للمعطيات الركن الأساسي الذي لابد من توافره في الجريمة فان تخلف هذا الركن فلا وجود للجريمة أصلا، وهذه الجرائم جاءت على سبيل الحصر في المادة 394مكرر إلى المادة 394مكرر7 قانون العقوبات الجزائري[10]، حيث أفرد القسم السابع مكرر من هذا القانون تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات تعزيزا للحماية واقرارا لمبدأ محاربة الافلات من العقاب.

ثانيا: مفهومالجريمة الالكترونية الاقتصادية

تسبب الجريمة الالكترونية الاقتصادية أضرار بالغة الخطورة على التنمية الاقتصادية بصفة خاصة، وعلى الاقتصاد العالمي بصفة عامة، وتعد اليوم من أكثر الجرائم انتشارها بسبب الفوائد والعوائد الطائلة غير المشروعة التي يجنيها الجاني من هذه الجريمة. وعليه فإن تعريف الجرائم الالكترونية الاقتصادية يستوجب التطرق الى تعريف المجرم الاقتصادي الالكتروني ثم الجريمة الاقتصادية الالكترونية.

1 تعريف المجرم الالكتروني الاقتصادي

المجرم الاقتصادي الالكتروني هو كل شخص يرتكب سلوك إيجابي أو سلبي يصبو لتحقيق أرباح من خلال الإضرار بالاقتصاد، و لعل أهم ما يميز المجرم الاقتصادي في البيئة الرقمية هو كونه خبير بالمسائل المعلوماتية، و له القدرة على التدمير الهادئ و التلاعب بالمعلومات و البيانات، و ممارسة الإجرام دون عنف و ضد أي قطاع، و على ذلك سلط عليه القانون مسؤولية جنائية بوصفه فاعل أصلي بالجريمة أو شريك[11]. بالتالي فانالمجرم الاقتصادي الالكتروني هو مجرم ذكي، إذ لا يمكن لشخص عادي لا يتقن الحاسوب والانظمة المعلوماتية أن يمارس الاجرام الاقتصادي المعلوماتي، لأن المجرم الالكترونييتميز بصفات خاصة ومعرفة بالأنظمة المعلوماتية يستطيع القيام بنشاطه الاجرامي باستعمال تقنيات الاعلام الآلي ويستطيع حل المشكلات التي قد تواجهه[12].

لذلك فالمجرم الاقتصادي الرقمي (الالكتروني) ليس شخصا عاديا بل لا بد أن يتمتع ببعض الصفات والمميزات منها: معرفة وخبرة بالمسائل المعلوماتية، القدرة على الحاق أضرار بالبيانات والمعلومات، ممارسة الجريمة دون استخدام العنف.

2 تعريف الجرائم الالكترونية الاقتصادية:

تعتبر الجريمة الاقتصادية هي كل سلوك إنساني فعلا كان أو امتناعا، يرتب أضرارا بمصلحة اقتصادية يحميها القانون، أو يمثل اعتداء على الموارد الاقتصادية المملوكة أو التي يحوزها الأفراد والمؤسسات والدولة بما يترتب عليها ضررا[13].

كما عرفت الجريمة الاقتصادية الالكترونية منظمة التعاون الاقتصادي والتنمية والخاصة باستبيان الغش المعلوماتي عام 1982م والذي أوردته بلجيكا في تقريرها بأنها كل: "فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات" [14].بالتالي فالجريمة الاقتصادية الالكترونية هي تلك الجرائم المضرة بمصلحة اقتصادية باستخدام المنظومات المعلوماتية فيترتب عليه وصول غير مشروع غير مرخص به إلى معلومات أو موارد تم تخزينها على المنظومات المعلوماتية، بهدف النسخ أو الإلغاء أو النقل أو التخريب أو التجسس أو العبث في هذه البيانات والمعلومات.

من أجل تحقيق عوائد مالية عن طريق عمليات التزوير والاحتيال، يمكن ان تظهر الجرائم الاقتصادية الالكترونية في صور متعددة منها:

– التحويل الإلكتروني غير المشروع للأموال والسطو على بطاقات الائتمان؛

–القمار وغسيل الأموال عبر الانترنيت؛

– السطو على أموال البنوك[15].

وعموما يمكن القول أن الجريمة الالكترونية الاقتصادية هي جريمة ذات طبيعة خاصة ومعقدة كونها تتميز بمجموعة من الخصائص منها: أنها جريمة ناعمة سهلة الاخفاء والحذف وتخريب المعلومات، عابرة للحدود أي ذات طبيعة دولية يقوم بها الجاني دون تكبد عناء السفر الى البلد المستهدف وتصيبآثار هذا الهجوم (الاعتداء) عدة بلدان أخرى مرتبطة بنفس النظام، صعوبة اكتشافهاوإثباتها لكونها تتطلب أدلة تقنية دقيقة تتعلق بنظام المعلومات وبرامج القرصنة.

المحور الثاني: أسباب الجرائم الالكترونية الاقتصادية

ارتأينا في ذكر أسباب الجرائم الالكترونية الاقتصادية تقسيم هذا المحور إلى عنصرين؛ العنصر الأول نتناول فيه الأسباب العامة أو الرئيسية للجرائم الالكترونية الاقتصادية؛ والعنصر الثاني نتناول فيه الأسباب المشتقة من خصائص الجريمة الالكترونية في ذاتها.

أولا:الأسباب العامة للجرائم الالكترونية الاقتصادية:

لا تختلف الأسباب العامة الدافعة إلى ارتكاب الجريمة الإلكترونية الاقتصادية عن باقي أنواع الجرائم الأخرى، ومن أبرزها:

1 -**السبب المادي (الربح وكسب المال):** وذلك رغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتراف جرائمهم من اجل تحقيق المكاسب المالية[16]، كما أن مخاطر الإجرام الأقل وضوحا في الشبكة العنكبوتية يدفع العديد من مجرمي الإنترنت إلى الانخراط في استعمال البرامج الضارة بغرض سرقة الهويةوالهجمات الاحتيالية لطلب المال(مثل: سرقة أرقام البطاقات الائتمانية أو اختراق أنظمة بنكية ومراكز الصرافة)[17].

2 -**السبب الشخصي (الذاتي):** بعض الأشخاص يقومون بارتكاب عدد من المخالفات من أجل المتعة وإثبات قدراتهم في العالم الافتراضي، عن طريق إلحاق الضرر بالآخرين، أو بدافع الانتقام أو حب الاستطلاع والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات.

أو يكون السبب نفسي من شخص لديه خلل نفسي أو أمراض نفسية تنعكس على السلوك.

3 -**السبب الاجتماعي:** وتتمثل في الاختراقات للأجهزة الشخصية والتعرف على نقاط الضعف لدى الآخرين، أو من أجل البحث عن مكانة اجتماعية مرموقة (البحث عن التقدير).

4 -**السبب السياسي والعسكري:** التطور العلمي والتقني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الحاسوب، وبذلك أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية.

5 -**السبب القومي والوطني:** وهو أن يقوم الهاكرز بالهجوم على مواقع معادية تختلف مع قيم وعادات مجتمع ما بتدمير أو تغيير هذه المواقع، مما يؤدي إلى منعها من تهديد فكر وسلوك أفراد ذلك المجتمع[18].

كما يدخل في مفهوم العنصرين السببين السابقين (السبب السياسي والعسكري؛ السبب القومي والوطني)،ما يمارسه بعض الأشخاص (مجموعات)من عمليات الهجوم الالكتروني على أشخاصآخرين أو جماعات أخرى لأهداف معينة (انتقام–تهديد–تشويش–زعزعة الأمن– الابتزاز)، كما تقوم بعض الحكومات بالتجسس والحصول على معلومات خاصة بالعدو[19].

❖ من الفقه ما يعدد عوامل أخرى على أنها أسباب أدت لانتشار الجريمة الالكترونية الاقتصادية، نذكر منها على سبيل المثال:

- **الخلل في التوازن الاجتماعي والاقتصادي (البحث عن الثراء):** حيث تم ثراء البعض على حساب الأخرين، وظهر التفاوت الطبقي، الذي هيأ المناخ لتنامي ظاهرة الجريمة الاقتصادية الالكترونية[20].
- **عدم التطبيق الجيد للقانون وفساد القائمين على المال العام:** إن خرق القوانين يؤدي إلى إضعاف ثقة الشعب بالدولة التي تصدرها، وتولداللامبالاة بالمال العام، من خلال عدم ثقة المواطن بالقائمين على هذا المال[21]خاصة إذا ما رأوا مظاهر الفساد فيهم وبالتالي عدم الالتزام الطوعي بتلك القوانين، بل يتعدى الأمر إلى تجرأ العديد من الأشخاص على أفعال غير مشروعة مجرمة قانونا في ظل غياب الردع والعقوبات المقررة في تلك النصوص القانونية.

- **العولمة والتحول إلى المجتمع الرقمي:**

فظهور وسائل الاتصال والأجهزة الحديثة والاستعمال الواسع للنظم المعلوماتية في هذا العصر مكن من ظهور وانتشار الجرائم الالكترونية بأنواعها سواء ما تعلق بها من الجرائم الاقتصادية (كجرائم التجارة الالكترونية، جرائم الغش الجبائي، غسيل الأموال، قرصنة المعلومات...الخ)، أو الجرائم ذات الطابع السياسي، أو المتعلقة بأمن الدولة، التي قد تقع على أشخاص طبيعية أو معنوية.

ثانيا:الأسباب الخاصة للجرائم الالكترونية الاقتصادية:

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الالكترونية الاقتصادية مشتقة من خصائص الجريمة الالكترونية نفسها، نوجز أهمها فيما يلي:

1 -الجريمة الالكترونية جريمة عابرة للحدود:

هذا ما يجعل الجريمة الاقتصادية الالكترونية تحمل نفس الحالة في الوصف والخطورة، فتتسم هي أيضا بالطابع الذي يجعل معظم دول العالم في حالة اتصال دائم على الخط On Line، فتصبح الجريمة الالكترونية الاقتصادية لا تعترف بالحدود بين الدول والقارات فهي تعتبر شكل جديدا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة [22]، يستفيد مقترفوها من أثر التقنية في اختزال المسافات، واخفاء الأثر الالكتروني، وكذا السرعة الزمنية الهائلة في تداول المعلومات والحصول عليها، ووقوع كثير من العمليات الالكترونية في نفس الوقت، ضمن ما يعرف باللحظية المعلوماتية، والعمل عن بعد الذي يعدم التواجد المادي للمجرم المعلوماتي، ويصعب عملية البحث بشأنه، ويقتضي تتبع المعاملات الالكترونية التي تتجاوز حدود الدولة الواحد، في حرص على الربط بين الفعل والنتيجة الاجرامية له، من خلال المعطيات محل الجريمة، ما يجعلها المفضلة لدى المجرمين المعلوماتيين لأنها أكثر أمانا لهم[23].

2 -صعوبة إثبات الجريمة الالكترونية وقلة الابلاغ عن وقوعها:

وهاتين خاصيتين مرتبطتين، فالجرائم المعلوماتية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، وهي خطيرة وصعبة الاكتشاف، بحيث يفضلها المجرم الالكتروني لأنه يعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها، وما يساعد من ازدياد عدم التعرف على مرتكبي الجرائم الالكترونية إحجام الأشخاص والبنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم معلوماتية وذلك إما لعدم اكتشاف الضحية لها أو تجنيا للإساءة لسمعتها (خشية التشهير) وهز ثقة العملاء فيها، وكذلك إخفاءأسلوب ارتكاب الجريمة خوفا من قيام أخرين بتقليد هذا الأسلوب[24].

3 -الجريمة الالكترونية الاقتصادية جريمة مستحدثة:

هذا ما خلق عالم افتراضي –يسميه البعض "الفضاء الالكتروني"– يفسر انتشار الظاهرة ومحفز للأشخاص الذين يظهر فرق في امتثالهم ومخالفتهم بين العالم الافتراضي والعالم المادي (الحقيقي)، فهؤلاء الأشخاص قد يرتكبون جرائم في العالم الافتراضي لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم.

بالإضافة إلى مرونة الهوية، وعدم ظهور الهوية وضعف عوامل الردع تحفز السلوك الاجرامي في العلم الافتراضي[25].

الخاتمة:

نخلص إلى القول بأن الجريمة الإلكترونية الاقتصادية أصبحت ظاهرة إجرامية جديدة، وسمة بارزة في بداية القرن 21، وتعد اليوم من أكثر الجرائم انتشارها بسبب الفوائد والعوائد الطائلة غير المشروعة التي يجنيها الجاني من هذه الجريمة.

وتميزها بهذه الخصائص يجعلها تختلفعن الجرائم الاقتصادية التقليدية العروفة سابقا، إذ أن المجرمين في هذا المجال أو كما يسمون " الهاكرز" يتميزون بالذكاء في استخدام وسائل تقنية متطورة، وتنفيذ جرائمهم سواء في عمليات إرسال الفيروسات المخربة للمواقع والأنظمة، أو سرقة الأموال والسطو على أرصدة المصارف، وتحويل الأموال أو سرقة البيانات المهمة أو إتلافها، كما تتميز الجريمة بالسرعة في التخطيط والتنفيذ، وبجهد وتكاليف أقل بكثير من الجهد والأموال الكبيرة، التي كانت تنفق في تنفيذ الجرائم التقليدية.

أما من حيث الأسباب أو دوافع فلا تختلف الأسباب العامة الدافعة إلى ارتكاب الجريمة الإلكترونية الاقتصادية عن باقي أنواع الجرائم الأخرى، إلا أن هناك عدد من الأسباب الأخرى التي يمكن اشتقاقها من خصائص الجريمة الالكترونية نفسها، كل ما أتينا على ذكره في الدراسة يستوجب دون شك لفت النظر إلى خطورة الظاهرة مع ايجاد حلول قانونية من جهة وتشديد الرقابة الداخلية والدولية والتنسيق بينهما على الحد منها ومكافحتها.

فيما يخص التوصيات نأتي على ذكر أهمها:

- ضرورة توعية وتحسيس الأشخاص بالجرائم الالكترونية الاقتصادية وعقوباتها ومخاطرها التي تمس بعنصر الثقة بين الأفراد والسلطة العامة.
- تطوير وتفعيل القوانين الداخلية للحد من هذه الظاهرة وتعزيز التعاون الدولي لمكافحتها.
- تجفيف منابع الجرائم الالكترونية الاقتصادية من خلال مجابهة الأسباب الدافعة إلى ارتكابها.

الهوامش:

[1]– الشكري عادل يوسف عبد النبي، الجريمة المعلوماتية و أزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، مج. 5، ع. 7، 2008، ص. 112.

[2]– محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994، ص. 14.

[3]– اسامة احمد المناعسة وجلال محمد الزعبي، جرائم الحاسب الالي والانترنيت: دراسة مقارنة، دار وائل للنشر و التوزيع، عمان، 2001، ص. 75.

[4]-Klaus TIEDEMANN, Fraudes et autres, délits d'affaires commis à l'aide d'ordinateurs électroniques, Revue de droit pénal et de criminologie, N°04, Palais de justice, Bruxelles, 1985, P.612.

[5]– أحمد خليفة الملط، الجريمة المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2006، ص. 84.

[6]– بوضياف إسمهان، الجريمة الاكترونية والاجراءات التشريعية لمواجهتها في الجزائر،مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، عدد 03، مجلد 03 ، 2018، ص ص. 348–375.

[7]– اسامة احمد المناعسة وجلال محمد الزعبي، مرجع سابق، ص.77.

[8]– هيثم عبد الرحمان البقلي، الجرائم الالكترونية الواقعة على العرض بين الشريعة والقانون المقارن، ط 1، دار العلوم للنشر والتوزيع، القاهرة، 2010، ص.16.

9– الجريدة الرسمية عدد 47 مؤرخة في 16 أوت 2009.

10– القانون رقم، 04–15 ،الصادر في 10 نوفمبر 2004 ،يعدل ويتمم الأمر رقم 156/66 ،الصادر في 08 جوان 1966 ، المتضمن قانون العقوبات، ج ر. العدد 71.

[11]– سالم محمد علي ، الجريمة المعلوماتية ، مقال منشور مجلة جامعة بابل ، عدد خاص، 2007، ص .39.

[12]– عمار عباس الحسيني، جرائم الحاسوب والانترنيت، ط6، منشورات زين الحقوقية، بيروت، 2017، ص.61.

13– عبد الله الصعيدي، الجريمة الاقتصادية، المفهوم والأنواع ، دورية الفكر، شرطة الشارقة،العدد 15 ،ص 135.

14– يوسف حسن يوسف، الجرائم الدولية للأنترنيت، ط1، الاصدارات القانونية، القاهرة، 2011، ص.14.

15– دقيش جمال، صراع كريمة، الأبعاد الاقتصادية للجريمة الالكترونية ، مجلة الدراسات التسويقية وادارة الاعمال، جامعة بشار، المجلد 2، العدد1، 2018، ص ص 35–53.

16– عبد السلام محمد المايل، عادل محمد الشربجي، الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم– الأسباب–سبُل المكافحة مع التعرض لحالة ليبيا، مجلة أفاق للبحوث والدراسات، المركز الجامعي ايليزي، العدد الرابع، جوان 2019، ص. 249.

17–علاء الدين فرحات،تأثير الجرائم الالكترونية على البنى السوسيو اقتصادية، مجلة دفاتر السياسة والقانون، جامعة ورقلة، عدد خاص، جوان 2018،ص. 155.

18–عبد السلام محمد المايل، عادل محمد الشربجي، مرجع سابق، ص. ص 248– 249.

19– علاء الدين فرحات،مرجع سابق،ص. 155.

20–منصف شرفي ، إلياس بوضياف، الجريمة الاقتصادية: أسبابها وطرق مكافحتها في الجزائر ، مجلة معارف للعلوم القانونية والاقتصادية، المركز الجامعي بريكة، معهد الحقوق، المجلد الثاني، العدد الثالث، 2021، ص. 93.

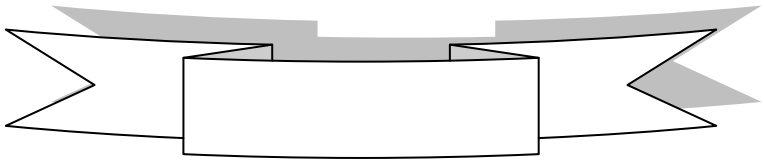
21–منصف شرفي، إلياس بوضياف، مرجع سابق، ص. 94.

22–علاء الدين فرحات، مرجع سابق، ص. 151.

23– مونة مقلاتي، راضية مشري ، الجريمة الالكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، جامعة جيجل، المجلد السادس، العدد الأول، جوان 2021، ص. 497.

24–علاء الدين فرحات، مرجع سابق، ص. 152.

25–ذياب موسى البداينة، الجرائم الالكترونية: المفهوم والأسباب، ورقة علمية مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية، خلال الفترة 2–2014/09/4، عمان، الأردن، ص. 16.



منية شوايديية
chouaidia.mounia@univ-guelma.dz
مخبر الدراسات القانونية البيئية
جامعة 8 ماي1945 – قالمة–

كحل الراس سماح
kahalerras.samah@univ-guelma.dz
مخبر الدراسات القانونية البيئية
جامعة 8 ماي 1945– قالمة–

القانون الواجب التطبيق على الجرائم الاقتصادية الالكترونية

الملخص:

إن استخدام الوسائل التكنولوجيا أحدث العديد من المتغيرات على مختلف الأصعدة السياسية والاجتماعية والاقتصادية، فكان له آثار ايجابية من جهة وآثار سلبية من جهة أخرى، ومن بين هذه الأخيرة ظهور الجرائم الالكترونية في إطار مكافحتها سعت معظم الدول في العالم للتعاون من أجل إيجاد حلول تشريعية وتحديد قانون الواجب التطبيق يتناسب مع طبيعتها الخاصة، نظرا لتميزها بكونها جريمة عابرة للحدود لا تخضع لنطاق إقليمي محدد.

الكلمات المفتاحية: *الجرائم الالكترونية، التعاون الدولي، القانون الواجب التطبيق، جريمة عابرة للحدود.*

مقدمة:

نتيجة لاستخدام وسائل التكنولوجيا الحديثة بطريقة غير مشروعة ظهر نوع جديد من الجرائم المستحدثة التي يطلق عليها الجرائم الالكترونية أو الجرائم المعلوماتية، أو جرائم الانترنت، هذه المصطلحات تعبر عن مجموعة من الجرائم المرتبطة بالأنظمة الالكترونية والشبكة المعلوماتية [1]، اختلف الفقهاء ومعظم المشرعين في إعطاء تعريف دقيق للجريمة الالكترونية نظرا لحداثتها، فعرّفتها منظمة التعاون الاقتصادي والتنمية الخاصة باستبيان الغش المعلوماتي سنة 1982 بأنها:" **كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة غير مباشرة عن تدخل تقنية المعلومات"[2].**

فقد أصبحت الجرائم الالكترونية ذات انعكاسات وآثار اقتصادية كبيرة وذلك بسبب اتجاه أغلب الدول في العالم نحو نظام اقتصادي جديد يرتكز على العولمة، الذي أدى إلى التحول من مرحلة الاقتصاد التقليدي إلى مرحلة الاقتصاد الرقمي، وكذا تحول المعاملات التجارية والمالية إلى شكل الكتروني، وهذا ما زاد من خطورة الجرائم

[1] بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة مسيلة، المجلد 3، العدد3، سبتمبر2018، ص349.

[2] حورية قويقح، الابعاد الاقتصادية للجريمة الالكترونية، مجلة الاصلاحات الاقتصادية والاندماج في الاقتصاد العالمي، المدرسة العليا للتجارة، المجلد 14، العدد2، أكتوبر2020، ص243.

الالكترونية، فحسب آخر الإحصائيات [3] فإن الأضرار التي لحقت الاقتصاد العالمي بسبب هذه الجرائم والتهديدات الالكترونية تبلغ تريليون دولار سنويا،التي كان يتوقع أن تتجاوز 6 تريليون سنة 2021، ولا تزال في تزايد مستمر لحد الساعة، وهذا ما دفع معظم الدول في العالم سواء الدول الأوروبية أو العربية بما فيها الدولة الجزائرية للبحث في ايجاد حلول جذرية قانونية للحد ومكافحة هذا النوع من الجرائم المستحدثة من خلال وضع نصوص قانونية تتناسب مع الطبيعة القانونية الخاصة بهذه الجرائم.

تكمن أهمية هذه الورقة البحثية في محاولة تسليط الضوء على الجهود الدولية المبذولة لمكافحة هذه الجرائم المستحدثة، وايجاد حلول تشريعية لمواجهتها.

إن دراسة هذا الموضوع تهدف أساسا إلى إبراز القانون الواجب التطبيق على الجرائم الالكترونية بصفة عامة والجرائم الاقتصادية الالكترونية بصفة خاصة.

انطلاقا من هذا تتمحور إشكالية موضوعنا حول: **فيما يتمثل القانون الواجب التطبيق على الجرائم الاقتصادية الالكترونية؟.**

يستلزم موضوع الدراسة إتباع المنهج التحليلي أساسا وذلك بايجاد أسس تحديد القانون الواجب التطبيق على هذا النوع من الجرائم، والمنهج المقارن من خلال معرفة الجهود الدولية المبذولة لمكافحة الجريمة الاقتصادية الالكترونية في التشريعات المقارنة والتشريع الجزائري.

المبحث الأول:أسس تحديد القانون الواجب التطبيق .

نتيجة للتطور التكنولوجي وظهور الفضاء الالكتروني انتشر نوع جديد من الجرائم المستحدثة التي يطلق عليها تسمية الجرائم الالكترونية التي يمكن أن تكون في عدة صور منها الجرائم الاقتصادية الالكترونية، ونظرا لحداثة هذا النوع من الجرائم وجدت صعوبة في تطبيق الأحكام القانونية الجنائية التقليدية عليها، لذا كان لابد لنا من تحديد الطبيعة القانونية لهذه الجرائم(المطلب الأول)، كما أن هذا النوع من الجرائم لا يقتصر على إقليم دولة واحدة بل هو يتجاوز حدود الدول لذا لابد من تحديد مدى خضوعها لمبدأ الإقليمية (المطلب الثاني).

المطلب الأول: تحديد الطبيعة القانونية للجرائم الاقتصادية الالكترونية.

إن تحديد الطبيعة القانونية للجرائم الاقتصادية الالكترونية يتطلب تحديد الطبيعة القانونية للجرائم الالكترونية بصفة عامة.

[3] صراع كريمة، دقيش جمال، الابعاد الاقتصادية للجريمة الالكترونية، مجلة الدراسات التسويقية وإدارة الأعمال، جامعة بشار، المجلد2، العدد1، جانفي2018، ص44، ص45.

دراسة الجرائم الالكترونية يدخل ضمن نطاق دراسة القسم الخاص لقانون العقوبات الذي يتناول العناصر الأساسية للجريمة والعقوبة المقررة لها [4]، فهي تقع على الأموال وعلى الأشخاص، غير أنها تختلف عن الجرائم التقليدية من ناحيتين:

الناحية الأولى: تتمثل في أداة الجريمة: حيث أن الأداة في الجرائم الالكترونية ذات تقنية عالية ومرتكبيها ذو دراية كافية باستعمال هذه الأدوات، ويمكن أن يبتكر طرق وتقنيات جديدة لاتمام سلوكه الإجرامي.

من الناحية الثانية: الجرائم الالكترونية من الجرائم المستحدثة ظهرت نتيجة التقدم التكنولوجي حيث يصعب معاقبة الجاني وفقا للنصوص الجنائية التقليدية، بل تحتاج إلى سن نصوص قانونية قادرة على استيعاب خصوصية هذه الجريمة[5].

الجريمة الالكترونية أو المعلوماتية تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، فلا يمكن تطبيق النصوص الجنائية التقليدية عليها، حيث أن تطبيقها يثير إشكالات عديدة أهمها مشكلة إثبات الجريمة التي تتطلب وجود أثر مادي للجريمة، وفي هذا النوع من الجرائم المستحدثة يمكن للجاني محو الأدلة في وقت قصير خاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال، فقد تكون البيانات التي يتم البحث عنها مشفرة ولا يمكن إجبار الجاني على فك الشفرة، كما أنه هناك صعوبة ملاحقة المجرم المعلوماتي المقيم في دولة أجنبية لا تربطها اتفاقية بالدولة التي تحقق فيها السلوك الإجرامي، لذا يمكن القول أن الجرائم الالكترونية بصفة عامة والجرائم الاقتصادية بصفة خاصة ذات طبيعة قانونية خاصة[6] تستلزم وضع أحكام تشريعية تتناسب مع خصوصيتها.

المطلب الثاني: مدى تطبيق مبدأ الاقليمية على الجرائم الاقتصادية الالكترونية.

إن مبدأ الاقليمية المعمول به في التشريعات الحديثة يقوم على سيادة كل دولة على الجرائم التي تحدث في اقليمها ولا يمتد إلى حدود دولة أخرى وإلا يعد اعتداء على سيادة الدولة الأخرى، فقانون العقوبات يمثل أهم مظاهر سيادة الدولة على الجرائم التي ترتكب في حدود إقليمها سواء كان الجاني أو المجني عليه وطنيا أو

---

[4] علي أحمد عبد الزعبي، الطبيعة القانونية للجريمة المعلوماتية، ص248، تمّ التصفح عبر الموقع الالكتروني https://www.almerja.com، بتاريخ2022/08/30، على الساعة17و34دقيقة.

[5] أحمد أسامة حسينة، الجريمة الالكترونية بين الشرعية الجنائية والإجرامية، مجلة جامعة الازهر غزة، المجلد19، عدد خاص بمؤتمر كلية الحقوق، سنة2017، ص18-19.

[6] محمد علي سالم، حسون عبيد هجيج، الجريمة المعلوماتية، مجلة بابل للعلوم الانسانية العراق، المجلد14، العدد6، سنة2007، ص90-91.

أجنبيا[7]، وهذا ما ذهب إليه المشرع الجزائري في نص المادة 3 من قانون العقوبات بقولها:" يطبق قانون العقوبات على كافة الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجنائية"

غير أن انتشار التكنولوجيا واستخدام الانترنت أدى إلى إزالة كل الحدود الجغرافية بين الدول فأصبح العالم عبارة عن قرية صغيرة، وأصبح التواصل بين أفرادها لا يكلف سوى شراء حواسيب وأجهزة اتصال متطورة ووصلها بشبكة الانترنت [8]، حيث أطلق البعض على شبكة الانترنت بأنها **"الامبراطورية التي لاتغيب عنها الشمس"**[9]وهذا ما جعل الجرائم المرتكبة من خلال استخدامها لاتخضع لنطاق اقليمي محدود، فمن أهم الخصائص التي تميز الجريمة الالكترونية نتيجة ارتباطها بشبكة الانترنت، فهي تمس أكثر من دولة في آن واحد بسبب السرعة الهائلة في تنفيذها وحجم الأموال والأشخاص المستحدثة، وأحسن مثال لذلك هي قضية عرفت باسم مرض نقص المناعة المكتسبة ايدز، التي حدثت عام 1989 حيث قام أحد الأشخاص وهو "**جوزيف بيب**" بنسخ أحد البرامج بهدف إعطاء بعض النصائح الخاصة بمرض الايدز، غير أن هذا البرنامج يحتوي على فيروس يؤدي إلى تعطيل جهاز الحاسوب، ويقوم الجاني بطلب مبلغ مالي لتوفير عنوان الكتروني مضاد للفيروس، وقد تمّ إلقاء القبض على الجاني في ولاية **أوهايو** بالولايات المتحدة الأمريكية وطلبت المملكة المتحدة تسليم الجاني لإرساله البرنامج عبر أراضيها وتمت محاكمته أمام القضاء الانجليزي[10].

نتيجة لخاصية الجريمة العابرة للحدود والطابع الافتراضي لهذه الجريمة المستحدثة التي لا تتلائم مع معيار محل وقوع الجريمة الذي يحدد الاختصاص القضائي، فهنا يثار إشكال الاختصاص الاقليمي لتحديد القانون الواجب التطبيق من بين جملة من قوانين الدول التي ارتكبت الجريمة الالكترونية على اقليمها، فلا يمكن تطبيق مسألة الاختصاص الاقليمي للجرائم التقليدية التي تقرها القوانين المختلفة مما يجعل عملية تحديد

---

[7] عبد المومن بن صغير، تطبيق النص الجنائي بين الاقليمية والعالمية في ظل عولمة مكافحة الجرائم المستحدثة، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد10، العدد3، ديسمبر2019، ص61-62.

[8] عبد الصديق شيخ، الوقاية من الجرائم الالكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية،المركز الجامعي تندوف، المجلد4، العدد1، سنة2020، ص195.

[9] بخدة صفيان، وقاص ناصر، الطبيعة القانونية للجرائم المستحدثة ووسائل ارتكابها جريمة الانترنت نموذجا، مجلة البحوث القانونية والسياسية، جامعة طاهر مولاي -سعيدة- ، المجلد3، العدد1، سنة 2021، ص125.

[10] مخلد ابراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الالكترونية، المجلة العربية للنشر العلمي، مركز البحث وتطوير الموارد البشرية رماح- الأردن-، العدد37، سنة2021، ص283-284.

الدولة صاحبة الاختصاص مسألة صعبة من الناحية العملية [11]، وهذا ما يفرض الزامية التعاون الدولي لمكافحة هذه الجريمة فقد سعت مختلف الدول في العالم على بذل جهودها لمواجهة المستجدات الحديثة المتعلقة بالجرائم الالكترونية، خاصة مسألة الاختصاص الاقليمي، فوزير خارجية الهند للاتصالات ونظم المعلومات تحدثعن خطر الجرائم الالكترونية ومشكلة أنها عابرة للحدود بمقولة شهيرة له في قمة الجرائم الالكترونية التي عقدت في الهند سنة 2012 بقوله: " **لم يعد السؤال المطروح حول كيفية قيام الدول بحماية أمنها، بل أصبح السؤال عن كيفية قيام العالم بحماية نفسه**"، بموجب ذلك تشكلت فرق في معظم الدول في العالم لايجاد حلول لهذه الاشكالات[12].

فقد ذهب المجلس الاوروبي إلى عقد اتفاقية "**بودابست**" سنة2001 المتعلقة بالجرائم الالكترونية التي قدمت صورا لمكافحة الجرائم الالكترونية حيث نصت المادة 22 منها على " **أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها التي يراها لازمة لكي يحدد اختصاصه بالنسبة لكل جريمة تقع وفقا لما هو وارد في المواد من (2إلى11) من الاتفاقية الحالية عندما تقع الجريمة:**

أ- داخل النطاق المحلي للدولة

ب- على ظهر سفينة تحمل علم تلك الدولة

ج- على متن طائرة مسجلة في هذه الدولة

د- بواسطة رعاياها إذا كانت الجريمة معاقبا عليها جنائيا في المكان الذي ارتكبت فيه، وإذا كانت الجريمة لاتدخل في أي اختصاص مكاني لأي دولة أخرى، ولكل طرف أن يحتفظ لنفسه بالحق في عدم التطبيق، أو عدم التطبيق إلا في حالات وفي ظل شروط خاصة، قواعد الاختصاص، المنصوص عليها في الفقرة الأولى(ب و د) من هذه المادة أو في أي جزء من هذه الفقرات"[13].

كما قامت الأمم المتحدة في إطار مكافحة الجرائم الالكترونية بعقد الكثير من الملتقيات والمؤتمرات من بينها عقد اتفاقية خاصة سنة 2000 لمكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية ثم عقد مؤتمر

[11] أحمد أسامة حسينة، المرجع السابق، ص26.

[12] أنور محمد صدقي المساعدة، إشكالية الاختصاص في الجرائم الالكترونية، المجلة الدولية للقانون، جامعة قطر ، المجلد2018، العدد 4، سنة 2019، ص7-8

[13]عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، سنة2014، ص100.

بالبرازيل في أفريل 2010 تمّ التطرق فيه إلى تحليل ظاهرة إحصائيات متعلقة بالجريمة الالكترونية وإجراءات التحقيق فيها، والأدلة الالكترونية، المساعدة التقنية الدولية، خدمات الانترنت، التعاون الدولي للتصدي للجريمة الالكترونية[14]، وعقد مؤتمر دولي للتكنولوجيا والمعلومات في دبي سنة 2012، اقترح فيه الاتحاد العالمي للاتصالات إجراء تعديلات على لوائح وتشريعات الاتحاد التي تمّ اعتمادها بموجب اتفاقية دولية عام 1988، وقد وافقت على هذا الاقتراح 89 دولة ورفضته 55 دولة، ثم تمّ متابعة الموضوع في المؤتمر التالي في "**بوسان**" في كوريا الجنوبية سنة 2014، حيث تحدث الاتحاد عن موضوع الفضاء الالكتروني وضرورة وجود تنظيم دولي يحكم التشريعات الوطنية، غير أنه تمّ رفض ذلك[15].

كما ذهبت معظم الدول العربية لبذل جهودها للتعاون الدولي لمكافحة الجرائم الالكترونية، حيث تمّ عقد اتفاقية لمكافحة جرائم تقنية المعلومات في الاجتماع المشترك لمجلس وزراء الداخلية والعدل العرب المنعقد بمقر الأمانة العامة لجامعة الدول العربية القاهرة في ديسمبر 2010، وذلك بهدف تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم التقنية وتعزيز القدرة المنبثقة عن ذلك لدى كل المؤسسات والهيئات والمنظمات والمنشآت في كل من القطاعين العام والخاص بهدف تحقيق أمن شامل للمعلومات[16].

في الأخير لابد من الإشارة إلى أنه رغم الزامية التعاون الدولي لمكافحة الجرائم الالكترونية العابرة للحدود، إلا أنه هناك الكثير من العقبات التي تعترض دون تطبيق ذلك من بينها عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الالكترونية ، عدم وجود توافق قوانين الإجراءات الجزائية للدول بشأن التحقيق في تلك الجرائم، قلة الخبرة في مجال مكافحة هذا النوع من الجرائم لدى الضبطية القضائية وجهات الإدعاء والمحاكم القضائية[17].

المبحث الثاني: الجهود الدولية المبذولة لتحديد القانون الواجب التطبيق على الجرائم الاقتصادية الالكترونية.

نظرا للأهمية البالغة لايجاد أحكام قانونية تتناسب مع الجرائم المستحدثة ومكافحتها بذلت معظم الدول في العالم جهودها لصياغة نصوص قانونية جديدة لمواجهة هذا النوع من الجرائم المتطورة تكنولوجيا، فقد سعت مختلف التشريعات المقارنة لصياغة أحكام تشريعية جديدة لمكافحتها(المطلب الأول)، وهذا ما ذهب إليه

[14] صراع كريمة، دقيش جمال، المرجع السابق، ص47.

[15] أنور محمد صدقي المساعدة، المرجع السابق، ص8.

[16] صراع كريمة، دقيش جمال، المرجع السابق، ص49.

[17] عبد الله دغش العجمي، المرجع السابق، ص102.

المشرع الجزائري فقد أجرى عدة تعديلات على قانون العقوبات وقام بوضع قانون جديد يتعلق بهذا النوع من الجرائم(المطلب الثاني).

المطلب الأول: مكافحة الجرائم الاقتصادية الالكترونية في التشريعات المقارنة

سعت مختلف التشريعات المقارنة إلى تعديل الأحكام القانونية التقليدية بصورة تتناسب مع طبيعة الجرائم الالكترونية من بينها:

التشريع الفرنسي ففي سنة 1988 تمّ إصدار قانون يعدل قانون العقوبات حيث أضاف فيه المشرع الفرنسي جرائم جديدة متعلقة بالحاسوب الآلي، وتمّ تعديله أيضا سنة 1994ليتضمن مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية، كما نص في المادة17 من قانون الأمن الداخلي الفرنسي على السماح بامتداد التفتيش عن الجرائم الالكترونية إلى الحواسيب الموجودة خارج إقليم الدولة وذلك لتسهيل عمل سلطات الضبط والتحقيق[18].

تجدر الإشارة إلى أن المشرع الفرنسي قبل اصداره قانون العقوبات الجديد قام بتعديل نص المادة 4/462 سنة 1977 حيث نص بموجبها على تجريم محو وتعديل البيانات المعالجة آليا أو التدخل في طرق معالجتها، كما جرم تعطيل أو افساد عن عمد تشغيل نظام المعالجة الآلية للبيانات بموجب المادة 3/462[19].

في الولايات المتحدة الأمريكية تم اصدار قوانين خاصة لمكافحة الجرائم الالكترونية حيث صدر قانون خاص لحماية أنظمة الحاسب الآلي الفيدرالي، وقد تمّ تعديل هذا القانون مرتين سنة 1986، وفي سنة 1997 قام الرئيس الأمريكي "**بيل كلينتون**" بالتوقيع على قانون السرقة غير الالكترونية بالقرار H.R.2265 وجاء قانون " **النيت**" لتعزيز حماية حقوق الطبع والعلامة التجارية وكذا بغرض تعديل النصوص الواردة في القانون الفدرالي رقم 18 والقانون رقم 17 [20].

أما في مصر فقد تمّ عقد المؤتمر الأول لجمعيات قانون الانترنت الذي عقد في القاهرة بتاريخ 27 سبتمبر 2004 الذي وضع اللبنة الأولى لإنشاء جمعيات ومنظمات أهلية للعمل التطوعي في مجال قانون الانترنت،

[18] جنادي عبد الحق، هيشور أحمد، حقيقة الجريمة المعلوماتية والأساليب التشريعية لمواجهتها، مجلة الراسات الحقوقية، جامعة طاهر مولاي سعيدة، المجلد9، العدد1، جوان2022، ص436.

[19] زعيطي آمنة، برناوي راضية، مكافحة الجرائم الالكترونية في ضوء قانون العقوبات الجزائري دراسة مقارنة، مجلة حقوق الانسان والحريات العامة– جامعة ابن باديس مستغانم، المجلد4، العدد1، جوان2019، ص231.

[20] جنادي عبد الحق، هيشور أحمد، المرجع السابق، ص433.434.

كنتيجة لذلك تمّ تأسيس الجمعية المصرية لمكافحة الجرائم المعلوماتية والانترنت وهي منظمة غير حكومية خاضعة للقانون المصري ومشهرة تحت رقم 2176 سنة 2005[21]، غير أنه من الجانب التشريعي فقد تمّ تجريم الجرائم الالكترونية المتعلقة بالأحوال المدنية والتوقيع الالكتروني فقط دون غيرها من الجرائم الأخرى وبذلك يتم الرجوع إلى النصوص التجريمية التقليدية[22].

كما وافق أيضا مجلس الوزراء في المملكة العربية السعودية سنة 2007 على نظامي مكافحة الجرائم المعلوماتية والتعاملات الالكترونية، وذلك بغرض مكافحة الجرائم الالكترونية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقررة لها، وكذا تحديد الجهة المختصة بمتابعة وتطبيق العقوبات على المجرم المعلوماتي[23].

وفي الأردن تمّ إنشاء الجمعية الأردنية للحد من الجرائم المعلوماتية والانترنت تطبيقا لمبادئ الأمم المتحدة، فقد أكدت هذه الجمعية التزامها بمبادئ المؤتمر التأسيسي لجمعيات قانون الانترنت الذي تمّ انعقاده بالقاهرة سنة 2004 وسبق ذكره، وكذا المؤتمر التأسيسي لجمعيات قانون الانترنت الذي انعقد في القاهرة سنة 2006، بالإضافة إلى الالتزام بقرارات المؤتمر الدولي الأول لقانون الانترنت الذي انعقد في الغردقة في مصر سنة 2011[24].

المطلب الثاني: مكافحة الجريمة الاقتصادية الالكترونية في التشريع الجزائري.

تعد من أخطر الجرائم الالكترونية جرائم الأموال التي تتجسد في القيام بالعديد من أشكال السرقة لأموال المنقولة الكترونيا، ففي الكثير من الأحيان يتم الحصول على بعض الوسائل المرتبطة بحماية المعلومات مثل كلمات المرور وتفاصيل الحسابات التي يمكن أن يتوصل من خلالها المجرم المعلوماتي إلى قواعد البيانات الخاصة بشركات الأعمال والمؤسسات المالية ونقل الأموال الكترونيا وذلك من خلال إرسال أوامر بالبريد الالكتروني[25]، فكان لزاما على المشرع الجزائري مواجهة هذا النوع من الجرائم الذي له آثار اقتصادية تمس الفرد أو المؤسسات والشركات الاقتصادية، فالمشرع الجزائري كغيره من المشرعين منذ بداية ظهور هذه الجرائم المستحدثة قام بإجراء تعديلات على قانون العقوبات حتى تتناسب أحكامه القانونية مع هذا النوع من

[21] عبد الله دغش العجمي، المرجع السابق، ص103.

[22] زعيطي آمنة، برناوي راضية، المرجع السابق، ص231.

[23] جنادي عبد الحق، المرجع السابق، ص437.

[24] عبد الله دغش العجمي، المرجع السابق، ص106.

[25] عوادي مصطفى، صحراوي العيد، عنان أمال، لمحة عن المعالجة المدنية والجزائية للتجارة الالكترونية في التشريع الجزائري، مجلة الأصيل للبحوث الاقتصادية والإدارية، جامعة خنشلة، المجلد3، العدد2، ديسمبر 2019، ص92.

الجرائم، فكان أول تعديل سنة 2004 بموجب القانون رقم 04-15 [26] حيث يتمم الفصل الأول من الباب الثاني من الكتاب الثاني لهذا الأمر في القسم السابع مكرر تحت عنوان " **المساس بانظمة المعالجة الآلية للمعطيات**" ويشمل المواد من 394 مكرر إلى 394 مكرر 7، التي تنص على العقوبات المفروضة على مرتكبي الجرائم الالكترونية[27]، فقد استحدث المشرع بموجب هذا القانون جملة من الأحكام القانونية التي جرّم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات وحدد لكل فعل منها جزاء،حيث نص في المادة **394 مكرر 2: " يعاقب بالحبس من شهرين إلى ثلاث(3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:**

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"

كما قام بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة الخاصة لهذه الجرائم من خلال تعديل قانون الإجراءات الجزائية بموجب القانون رقم 06-22 [28]، حيث تضمن تدابير إجرائية مستحدثة تتعلق بالجرائم الالكترونية تتمثل في مراقبة الاتصالات الالكترونية تسجيلها والتسرب، كما استحدث المشرع أحكام تشريعية تتناسب مع الطبيعة الخاصة للجرائم الالكترونية وذلك بموجب إصدار قانون جديد خاص بها رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها [29]، فقد تضمن هذا القانون الكثير من الآليات المستحدثة وذلك بإنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها [30] التي لم يتم تنصيبها بعد، وكذا القواعد المتعلقة بالاختصاص الاقليمي لقانون العقوبات الجزائري حيث وسع من الاختصاص الاقليمي للسلطة القضائية في متابعة الجرائم التي تمس المؤسسات الدولية والدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني [31]، كما نص على المساعدة القضائية الدولية المتبادلة بموجب المادة 16 بقولها: " **في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها يمكن السلطات المختصة تبادل المساعدة**

---

[26] القانون رقم 04-15 المؤرخ في 10 نوفمبر2004 يعدل ويتمم الامر رقم66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، جريدة رسمية العدد71، المؤرخة في 10 نوفمبر 2004، ص8.

[27] المادة 12 من القانون رقم 04-15 المذكور سابقا.

[28] القانون رقم 06-22 المؤرخ في 20 ديسمبر2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ 8 يونيو 1966، المتضمن قانون لإجراءات الجزائية، جريدة رسمية العدد84، الصادرة بتاريخ 24 ديسمبر 2006، ص4.

[29] القانون رقم09-04 المؤرخ في 5 غشت2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية العدد 47، الصادرة بتاريخ 16 غشت 2009، ص5.

[30] المادة 13 من القانون رقم 09-04 المذكور سابقا.

[31] المادة 15 من القانون رقم 09-04 المذكور سابقا.

القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني، يمكن في حالة الاستعجال ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزت الفاكس أو البريد الالكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية لتأكد من صحتها"

كما منح المشرع الجزائري للمراقبة الالكترونية للاتصالات وتفتيش نظم المعلوماتية الصفة الشرعية القانونية حيث نص على الحالات التي تسمح باللجوء إلى المراقبة الالكترونية بموجب المادة 4 من القانون 09-04 المذكور سابقا، كما نص على التزام مقدمي الخدمات بتقديم مساعدات للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من هذا القانون تحت تصرف السلطات[32]، وقد نص المشرع على العقوبة الجزائية المفروضة عليهم في حالة مخالفة أو عدم تنفيذ إعذار الهيئة الوطنية المكلفة بمكافحة الجرائم الالكترونية بلحبس من سنة إلى 3 سنوات وبغرامة من 2.000.000 إلى 10.000.000دج أو بإحدى هاتين العقوبتين، وذلك بموجب المادة 2 من القانون رقم 16-02[33] التي استحدثت المادة 394 مكرر 8 المعدل والمتمم لقانون العقوبات رقم 66-156.

الخاتمة:

يثير موضوع القانون الواجب التطبيق على الجرائم الاقتصادية الالكترونية اهتمام الباحثين والقانونيين، نظرا لخطورة الجرائم الالكترونية بصفة عامة على الأفراد والمجتمع لما لها من آثار مادية وغير مادية تضر بالاقتصاد العالمي ككل والاقتصاد الوطني خاصة، لذا كان من الضرور معرفة القانون الواجب التطبيق على المجرم المعلوماتي ، من خلال ورقتنا البحثية توصلنا إلى جملة من النتائج نوجزها كالآتي:

1- الجريمة الاقتصادية الالكترونية ذات طبيعة خاصة تستوجب سن أحكام قانونية تتناسب مع خصوصيتها.

2- الجريمة الالكترونية تمتاز بأنها جريمة عابرة للحدود تخضع لنطاق اقليمي محدود، وهذا ما أثار اشكالية مدى تطبيق مبدأ الاقليمية على هذا النوع من الجرائم المستحدثة، ولحل هذه الاشكالية فرضت الزامية التعاون الدولي ونتج عنه ابرام عدة اتفاقيات دولية لمكافحة الجريمة.

3- المشرع الجزائري كغيره من المشرعين بذل جهوده لوضع أحكام قانونية تتناسب مع الطبيعة الخاصة للجرائم المستحدثة، فقد أصدر قانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها فرض ضمن أحكامه عقوبات على مرتكبي هذه الجرائم، كما تضمن إنشاء هيئة وطنية للوقاية من هذه الجرائم غير أنه لم يتم تنصيبها بعد.

بناءا عليه نقترح مجموعة من التوصيات تتمثل في:

---

[32] المادة 10 من القانون رقم 09-04 المذكور سابقا.

[33] القانون رقم 16-02 المؤرخ في 19 يونيو 2016 يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، جريدة رسمية العدد37 المؤرخة في 22 يونيو2016، ص4.

1- ضرورة وضع قواعد قانونية مرنة تتماشى مع الطبيعة الخاصة للجرائم الاقتصادية الالكترونية.
2- ضرورة تعزيز التعاون الدولي والاقليمي للتصدي ومتابعة الجرائم الالكترونية بصورة عامة.
3- تنصيب الهيئة الوطنية للوقاية من الجرائم الالكترونية المنصوص عليها في القانون رقم 09-04..
4- ضرورة تفعيل أحكام القانون 09-04 بما يتماشى مع التطور الحاصل في عالم الجريمة الالكترونية وآثارها على الاقتصاد الوطني.

قائمة المصادر والمراجع:

أولا: النصوص القانونية:

1- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ 8 يونيو 1966، المتضمن قانون لإجراءات الجزائية، جريدة رسمية العدد 84، الصادرة بتاريخ 24 ديسمبر 2006، ص4

2- القانون رقم 09-04 المؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية العدد 47، الصادرة بتاريخ 16 غشت 2009، ص5.

3-القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 يعدل ويتمم الامر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، جريدة رسمية العدد71، المؤرخة في 10 نوفمبر 2004، ص8.

4- القانون رقم 16-02 المؤرخ في 19 يونيو 2016 يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، جريدة رسمية العدد37 المؤرخة في 22 يونيو2016، ص4.

ثانيا: الرسائل الجامعية:

1- عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، سنة2014.

ثالثا: المقالات العلمية:

1- أحمد أسامة حسينة، الجريمة الالكترونية بين الشرعية الجنائية والإجرامية، مجلة جامعة الازهر غزة، المجلد19، عدد خاص بمؤتمر كلية الحقوق، سنة2017.

2- أنور محمد صدقي المساعدة، إشكالية الاختصاص في الجرائم الالكترونية، المجلة الدولية للقانون، جامعة قطر ، المجلد2018، العدد 4، سنة 2019.

3- بخدة صفيان، وقاص ناصر، الطبيعة القانونية للجرائم المستحدثة ووسائل ارتكابها جريمة الانترنت نموذجا، مجلة البحوث القانونية والسياسية، جامعة طاهر مولاي –سعيدة، المجلد3، العدد1، سنة 2021.

4- بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة مسيلة، المجلد 3، العدد3، سبتمبر 2018.

5- جنادي عبد الحق، هيشور أحمد، حقيقة الجريمة المعلوماتية والأساليب التشريعية لمواجهتها، مجلة الراسات الحقوقية، جامعة طاهر مولاي سعيدة، المجلد9، العدد1، جوان2022.

6- زعيطي آمنة، برناوي راضية، مكافحة الجرائم الالكترونية في ضوء قانون العقوبات الجزائري دراسة مقارنة، مجلة حقوق الانسان والحريات العامة- جامعة ابن باديس مستغانم، المجلد4، العدد1، جوان2019.

7- صراع كريمة، دقيش جمال، الابعاد الاقتصادية للجريمة الالكترونية، مجلة الدراسات التسويقية وإدارة الأعمال، جامعة بشار، المجلد2، العدد1، جانفي2018.

8- عبد الصديق شيخ، الوقاية من الجرائم الالكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية،المركز الجامعي تندوف، المجلد4، العدد1، سنة2020.

9- عبد المومن بن صغير، تطبيق النص الجنائي بين الاقليمية والعالمية في ظل عولمة مكافحة الجرائم المستحدثة، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد10، العدد3، ديسمبر2019.

10- عوادي مصطفى، صحراوي العيد، عنان أمال، لمحة عن المعالجة المدنية والجزائية للتجارة الالكترونية في التشريع الجزائري، مجلة الأصيل للبحوث الاقتصادية والإدارية، جامعة خنشلة، المجلد 3، العدد 2، ديسمبر2019.

11- قويقح حورية ، الابعاد الاقتصادية للجريمة الالكترونية، مجلة الاصلاحات الاقتصادية والاندماج في الاقتصاد العالمي، المدرسة العليا للتجارة، المجلد 14، العدد2، أكتوبر2020.

12- محمد علي سالم، حسون عبيد هجيج، الجريمة المعلوماتية، مجلة بابل للعلوم الانسانية العراق، المجلد14، العدد6، سنة2007.

13- مخلد ابراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الالكترونية، المجلة العربية للنشر العلمي، مركز البحث وتطوير الموارد البشرية رماح- الأردن-، العدد37، سنة2021.

رابعا: المواقع الالكترونية:

1-علي أحمد عبد الزعبي، الطبيعة القانونية للجريمة المعلوماتية، ص 248، تمّ التصفح عبر الموقع الالكتروني https://www.almerja.com، بتاريخ2022/08/30، على الساعة17و34دقيقة.

بن دعاس لمياء
lamis.bendaas@gmail.com
كلية الحقوق جامعة باتنة

خصوصية الجريمة الالكترونية "التعريف –الأنواع–الخصائص"

ملخص:

تتمتع الجريمة الالكترونية بخصوصية تجعلها تنفرد عن باقي الجرائم وخاصة الجرائم التقليدية، تجعل قواعد الاثبات العادية امامها عاجزة عن كشفها ومتابعة الجناة فيها وتحديدهم وتحديد مسرح الجريمة، فهي جريمة عابرة للحدود الوطنية وفي غالب الاحيان تكون جريمة منظمة ، ومقترنة بالتقنية الحديثة" الانترنت" ، ومن الصعب حصرها في انواع محددة ، فمنها ما يقع على الاموال ومنها ما يقع على الاشخاص ومنها ما يقع على امن الدولة ، ومنها ما يقع على النظام المعلوماتي ، فهي جريمة متجددة ومتطورة والهدف من هذه الدراسة هو ابراز خصوصيتها من خلال التطرق لمفهومها وخصائصها وانواعها.

الكلمات المفتاحية: الجريمة الالكترونية، الجرائم الواقعة بواسطة النظام المعلوماتي، الجرائم الواقعة على النظام المعلوماتي.

Summary:

Electronic crime has a specific mark that makes it unique to the rest of the crimes, especially traditional crimes, that makes the rules of regular proof in front of it are unable to detect it and follow up on the perpetrators in it and identify them and determine the crime scene, it is a transient crime of national borders and most often is an organized crime, associated with modern technology "the Internet", and it is difficult Carrying it to specific types, some of which fall on the money, including what falls on people, including what falls on the security of the state, and some of them falls on the information system, it is a renewed and advanced crime and the goal of this study is to highlight its specificity by touching on its concept, characteristics and types.

Keywords :*Electronic crime, crimes by the information system, crimes against the information system.*

مقدمة: برزت في الآونة الاخيرة طائفة من الجرائم المستحدثة التي اقترن ظهورها بظهور الأنترنيت وما طرحته من متغيرات على الحياة البشرية في جميع جوانبها وفي كل الميادين ، فاستخدام الحاسوب والهاتف النقال افرز العديد من الممارسات غير المشروعة ، التي تحتاج الى تدخل مختلف التشريعات لتنظيمها في الاطار القانوني اللازم لذلك ، ففي الشق الدولي حاول المجتمع الدولي سن مجموعة من الصكوك الدولية من اجل مكافحة الجريمة الالكترونية بمختلف انواعها ، كما حاولت التشريعات على المستوى الداخلي مواءمة قوانينها مع الاتفاقيات الدولية استجابة لالتزاماتها الدولية ، وهو ما فعله المشرع الجزائري عندما نص على

الجريمة الالكترونية في قانون العقوبات حيث تبنى مصطلح "جريمة المساس بأنظمة المعالجة الالية للمعطيات" وجرم مختلف الممارسات التي تشكل مساس بالأنظمة المعلوماتية" ، وقد اختلفت التشريعات في تسمية الجريمة الالكترونية على غرار المشرع الجزائري ، وبعض التشريعات الاخرى التي تبنت مصطلح الجريمة المعلوماتية، كما اختلف الفقهاء في تحديد موضوع او محل الجريمة الالكترونية، فمنهم من وسع في محلها ومنهم من ضيق في محلها، والاقرب الى الصواب هو من اعتبر انه من الصعب تحديد محلها خاصة مع التطورات الحاصلة في عصر العولمة وترك ذلك مفتوحا ، وهو ما ينعكس كذلك على تحديد انواعها المختلفة ، وهو ما سيتم طرحه من خلال هذه الدراسة بالإجابة على الاشكالية التالية : ما هو مفهوم الجريمة الالكترونية واهم تقسيماتها؟

وللإجابة على هذه الاشكالية تم تخصيص خطة ثنائية مكونة من مبحثين لذلك، خصص المبحث الاول لمفهوم الجريمة الالكترونية، والمبحث الثاني لأنواعها.

المبحث الأول: مفهوم الجريمة الإلكترونية:

تنفرد الجريمة الإلكترونية بعدة خصائص تجعلها تختلف عن باقي الجرائم، فالمجرم في الجريمة التقليدية ليس مثل المجرم في الجريمة الإلكترونية التي يصعب فيها الإثبات بالطرق التقليدية، لذلك وجب فرض نصوص قانونية تتلاءم مع خصوصية هذه الجريمة، وسنحاول من خلال هذا المبحث التطرق لتعريف الجريمة الإلكترونية وخصائصها. في مطلب أول وثاني.

المطلب الأول: تعريف الجريمة الإلكترونية:

لم يجر الاتفاق بين فقهاء القانون الجنائي على الوصف القانوني الصحيح أو التسمية الدقيقة لمصطلح الجريمة الإلكترونية، فهناك عدد من المفاهيم المتقاربة والتي ترتبط بالإجرام الإلكتروني، والغش المعلوماتي، والجريمة التي تقع بواسطة التقنية الحديثة "الأنترنيت" عامة.

تطرح إشكالية التشابه والاختلاف بين الجريمة الإلكترونية والجريمة المعلوماتية، في مسألة هل أن الجريمة الإلكترونية تحوري الجريمة المعلوماتية أو العكس[1].

فهناك من يرى أن استخدام لفظ الجريمة الإلكترونية من شأنه أن يدخل فيه جرائم الحاسوب، والجرائم التي يطلق عليها البعض الجرائم المعلوماتية والغش المعلوماتي أو جرائم الاعتداء على معطيات الحاسب الآلي وجرائم الأنترنت، وبالتالي فهو مصطلح واسع يدخل في إطاره العديد من السلوكات الإجرامية.

وبالتالي فالجريمة الإلكترونية أوسع من الجريمة المعلوماتية، التي يدخل في إطارها الجرائم المرتكبة على الحاسوب أو جرائم الحاسوب، أما الجريمة الإلكترونية فهي جريمة المعالجة الآلية للمعطيات سواء باستخدام الحاسوب أو أية وسيلة أخرى، وهو الأمر الذي أكدته اتفاقية بودابست أو الاتفاقية المتعلقة بالجريمة الإلكترونية والتي صادق عليها المجلس الأوروبي في المجر "بودابست"[2].

[1] نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي 144 عن الجرائم الإلكترونية، طرابلس، 2017، ص 04.

[2] نمديلي رحيمة، المرجع السابق، ص 04.

فقد كان لا بد من طرح التفرقة بين المصطلحين حتى يتسنى لنا تحديد المفهوم الاصطلاحي للجريمة الإلكترونية في فرع أول والمفهوم القانوني للجريمة الإلكترونية في فرع ثاني.

الفرع الأول: التعريف الاصطلاحي للجريمة الإلكترونية:

ليس هناك إجماع على تعريف الجريمة الإلكترونية من حيث محلها أي الجرائم التي تدخل في نطاقها، كما يقول "فان دير هلست ونيف" أن هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة .... وفي أغلب الأحيان تستخدم المصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف".

ويدور تعريف الجريمة الإلكترونية حول الجرائم التي يتم ارتكابها بواسطة الحاسوب أو بأي نوع من المعدات الرقمية، ويتم استخدام مصطلح الإلكترونية للتعبير عن فكرة جزء من الحاسوب أو عصر المعلومات[1].

كما أن الجريمة الإلكترونية هي "مصطلح حديث يعبر عن تصرف غير قانوني وغير مشروع، وهي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الجريمة، وهي نمط م أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بالمعلومات".

كما تعرف بأنها: "الجريمة الناجمة عن إدخال البيانات مزورة في الأنظمة وإساءة استخدام المخرجات في الابتزاز المالي واللعب ببيانات الكمبيوتر أو أنها كل فعل إجرامي من شأنه الاعتداء على الماديات أو المعنويات"[2].

كما عرفها البعض بأنها "تلك الأعمال غير المشروعة التي تكون شبكة الانترنت أو إحدى تطبيقاتها أما وسيلة لها أو ضحية مستهدفة من قبل الفاعل أو الفاعلين".

أو هي "مجموعة الأعمال غير القانونية التي تتم عبر شبكة الأنترنيت، أو تثبت عبر محتواها"[3].

أو إنها "تلك الجرائم التي لا تعرف الحدود الجغرافية أو التي يتم ارتكابها بواسطة الحاسب الآلي عن طريق الانترنت، أو بواسطة شخص على دراية فائقة بهما"[4].

وفي الأخير يمكن القول أنه يمكن تعريف الجريمة الإلكترونية بأنها "السلوكات أو الأفعال الإجرامية التي يتم ارتكابها بواسطة جهاز الحاسوب وكافة المعدات التقنية مثل الهاتف النقال"

الفرع الثاني: التعريف الدولي للجريمة الإلكترونية:

في هذا المجال تعتمد مجموعة من التعريفات للجريمة الإلكترونية على مجموعة من العناصر تمكن تحديدها في الآتية.

---

[1] ذياب موسى البدانية، ورقة علمية بعنوان الجرائم الإلكترونية: المفهوم والأسباب، في الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولاتالإقليمية والدولية، كلية العلوم الاستراتيجية، عمان، الأردن، 2014، ص 3.

[2] شينار سامية، الجريمة الإلكترونية في منظور الشباب الجامعي، مدخل نفسي، قانوني، مجلة الباحث للدراسات الأكاديمية، المجلد 6، العدد 2، 2019، ص 5.

[3] معزوز ربيع، زروقي عايشة، الجريمة الإلكترونية وإجراءات مواجهتها في التشريع الجزائري، مجلة

[4] معزوز ربيع، زروق عايسة، المرجع السابق، ص 360.

– هناك عدد محدود من الأفعال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة تشكل جوهر الجريمة الإلكترونية[1].

– هناك أعمال تكون متصلة بالحاسوب من أجل تحقيق مكاسب شخصية أو مالية أو تحقيق ضرر مثل جرائم الهوية وجرائم محتويات الكمبيوتر، تؤثر على إمكانية تحديد أو الوصول إلى تعاريف قانونية للمصطلح الكلي.

فالملاحظ أن هناك عدد قليل من الصكوك الدولية القانونية أو الإقليمية التي عرفت الجريمة الإلكترونية، فمثلا لا اتفاقية مجلس أوروبا للجرائم الإلكترونية، ولا اتفاقية جامعة الدول العربية ولا مشروع اتفاقية الاتحاد الافريقي تضمنت تعريفا للجريمة الإلكترونية.

ومن بين الاتفاقيات التي عرفت الجريمة الإلكترونية نذكر اتفاقية كومنولث الدول المستقلة الجرائم المتصلة بمعلومات الحاسوب دون ذكر مصطلح الجريمة الإلكترونية قولها: "العمل الإجرامي الذي يستهدف معلومات الحاسوب"[2].

الفرع الثاني: تعريف الجريمة الإلكترونية في التشريع الجزائري:

أخذ المشرع الجزائري بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، على خلاف المشرع الفرنسي الذي لم يورد تعريفا للجريمة الإلكترونية إلى المادة 02 من القانون 04/09 بقوله: "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

والملاحظ بقراءة هذا التعريف أن المشرع الجزائري اعتمد على:

1/ معيار الجمع بين عدة معايير في تعريفه للجريمة الإلكترونية، وهي معيار وسيلة الجريمة والمتمثل في نظام الاتصالات الإلكترونية، والمعيار الثاني هو موضوع أو محل الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات، والمعيار الثالث وهو القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات[3].

2/ كما اعتمد المشرع الجزائري على معيار رابع في تحديده لنطاق الجريمة الإلكترونية، حيث أنه أقر أن الجريمة الإلكترونية ترتكب ضمن نطاق معلوماتي أو يسهل ارتكابها عليه وهذا هو السبب في توسيع نطاق الجرائم الإلكترونية الجزائري[4].

كما كفل الدستور الجزائري حماية الحقوق والحريات الأساسية للأفراد، حيث أكد دستور 1996م والتعديل الدستور في 2016، والتعديل الصادر في 2020[5].

حيث أكد المشرع الجزائري في دساتيره على ضمان الدولة عدم انتهاك حرية الإنسان.

[1] ذياب موسى البدانية، المرجع السابق، ص 4.
[2] ذياب موسى البدانية، المرجع السابق، ص 4، 5.
[3] نمديلي رحيمة، المرجع السابق، ص 6.
[4] نمديلي رحيمة، المرجع السابق، ص 04، 05.
[5] دستور 1996.

وأهم النصوص القانونية الواردة في الدستور والتي نصت على الجرائم الإلكترونية نجد:

المادة 38 "الحريات الأساسية وحقوق الإنسان والمواطن مضمونة، لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه، سرية المراسلات والاتصال الخاصة بكل أشكالها مضمونة"

وكذلك المادة 47[1]:

أما بالنسبة لقانون العقوبات فقد استحدث المشرع الجزائري القسم السابع مكرر من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات"[2].

بموجب القانون رقم 15/04[3]، وإلى جانب قانون العقوبات قام كذلك بسن قواعد إجرائية تتماشى مع خصوصية الجرائم الإلكترونية من خلال قانون رقم 22/06، المتضمن الإجراءات الجزائية[4].

وقد عرّف المشرع الجزائري نظام المعالجة الآلية للمعطيات بقوله: "كل نظام أو مجموعة من الأنظمة منفصلة كانت أم متصلة ببعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية المعطيات تنفيذا لبرنامج معين"[5].

المطلب الثاني: خصائص الجريمة الإلكترونية:

تنفرد الجريمة الإلكترونية بجملة من الخصائص كونها من الجرائم المستحدثة التي أصبحت اليوم حديث الساعة نظرا لما تطرحه من إشكالات قانونية خاصة من ناحية صعوبة الإثبات، وسيتم من خلال هذا المطلب عرض مختلف الخصائص التي تميز بها الجريمة الإلكترونية في فرع أول، وتخصيص الفرع الثاني لدراسة

الفرع الأول: خصائص الجريمة الإلكترونية:

أولا: تعتبر جريمة عابرة للحدود الوطنية، حيث تعتبر الجريمة الإلكترونية ذات بعد دولي، أي عابرة للحدود الوطنية، وذلك راجع لاعتمادها على التقنية الحديثة "الأنترنت" وهو ما ينتج عنه العديد من الصعوبات لا سيما فيما يتعلق بإجراءات المتابعة الجنائية ومسك الحياة[6].

ثانيا: الجريمة الإلكترونية صعبة الإثبات والاكتشاف:

لا تحتاج الجرائم الإلكترونية في ارتكابها إلى أي عنف أو سفك للدماء أو اقتحام من أجل سرقة الأموال وإنما هي عبارة عن القيام تغيير أو تعديل أو محو بيانات كليا أو جزئيا من السجلات المخزونة من ذاكرة الحاسوب، لذلك من الصعب اكتشافها واثباتها بوسائل الإثبات التقليدية[1].

---

[1]دستور 28نوفمبر 1996، بموجب المرسوم الرئاسي رقم 438/ 96المؤرخ في 7ديسمبر 1996المعدل بقانون 16/01المؤرخ في 6مارس 2016يتضمن التعديل الدستوري ،الجريدة الرسمية العدد 14،الصادرة في 7مارس 2016والرسوم الرئاسي رقم 20/251 المؤرخ 2،2 020/12/15،الجريدة الرسمية رقم 54

[2]شينار سامية، بولحبال آية، المرجع السابق، ص 392.

[3]الأمر رقم 156/66، المتضمن قانون العقوبات المعدل والمتمم بمقتضى القانون رقم 15/04 المؤرخ في 2004/11/10، الجريدة الرسمية رقم 66-155 المتضمن قانون الإجراءات الجزائية.

[4]الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية المتضمن في قانون الإجراءات الجزائية، المعدل والمتمم بالقانون رقم 22/06 المؤرخ في 2006/12/20، الجريدة الرسمية عدد 845 مؤرخة في 2006/12/24.

[5]براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، كلية الحقوق والعلوم السياسية، بدون عدد وسنة نشر، ص 126.

[6]بوضياف اسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، عدد 11، 2018، ص 355.

ثالثا: إن ارتكاب الجريمة الإلكترونية يتطلب جهاز إلكتروني وضرورة معرفة تقنية استخدامه.

فالأمر الذي يجعل الجريمة الإلكترونية ذات خصوصية هو تطلب ارتكابها وجود علم كافي بالجوانب الفنية كالتقنية لاستخدام الحاسوب والانترنت فكلما زادت الخبرة لدى الأطراف بمعرفة تقنية الحاسوب كلما زاد احتمال استخدام خبرتهم بشكل غير مشروع مع الإشارة أنه بعد ظهور الهواتف المحمولة خاصة الذكية لم يصبح الحاسوب فقط هو الوسيلة التي بواسطتها ترتكب الجريمة الإلكترونية، وإنما أصبح الهاتف النقال اليوم يتمتع بكافة الخصائص الذي تجعله محلا للجريمة الإلكترونية[2].

رابعا: الجرائم الإلكترونية، جرائم الأذكياء:

ففي معظم الأحيان ترتكب الجرائم الإلكترونية من قبل أشخاص يتمتعون بالذكاء، والدهاء يكتسبون مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسوب وكيفية عمله وكيفية تخزين المعلومات والحصول عليها، عكس الجريمة التقليدية التي لا تتطلب لارتكابها أفراد لديهم مهارات خاصة في استخدام الحاسوب، أو الهاتف المحمول ....[3].

والواضح من خلال التطرق لخصائص الجريمة الإلكترونية، مدى تميزها وانفرادها عن باقي الجرائم التقليدية، حيث فرضت العديد من المتغيرات من ناحية متابعة الحياة وصعوبة الإمساك بهم، من ناحية عدم وجود مسرح جريمة ثابت لهذه الجرائم، خاصة باعتبارها جرائم عابرة للحدود الوطنية، وكذلك من ناحية صعوبة تطبيق طرق الاثبات التقليدية عليها، وضرورة استحداث طرق أخرى تتلاءم مع خصوصيتها.

وهذا ما ذهبت إليها معظم التشريعات منها التشريع الجزائري.

المبحث الثاني: أنواع الجرائم الإلكترونية :

اختلف الفقه في تحديد أنواع الجرائم الإلكترونية، وذلك راجع إلى ظهور أنواع جديدة من حين لآخر لهذه الجريمة، حيث أنه من غير الممكن حصرها بنتيجة ارتباطها بالأنترنت والاعتماد في ارتكابها على وسائل مثل الحاسوب الآلي، فهناك من الفقهاء من يصنفها ويحدد أنواعها على أساس الوسيلة المستخدمة في ارتكاب الجريمة، ومنهم من يحدد أنواعها على أساس محل الجريمة، ولذلك يمكن ت قسيم الجريمة الإلكترونية إلى: الجرائم الواقعة على النظام المعلوماتي في مطلب ثاني.

المطلب الأول: الجرائم الواقعة بواسطة النظام المعلوماتي:

تعتبر الحاسب الآلي في هذه الجرائم هو العنصر الأساسي، ويهدف الجاني من ورائها إلى تحقيق البرح المادي بطريقة غير مشروعة، تستخدم النظام المعلوماتي في حد ذاته أو برامجه كأداة من أجل تنفيذ الجريمة[4].

---

[1] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، كلية القانون، جامعة الكوفة، العدد: 7، 2008، ص 116.

[2] أنظر: بوضياف اسمهان، المرجع السابق، ص 356.

[3] المرجع نفسه ، ص 356.

[4] سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق جامعة أبو بكر بلقايد، تلسمان، الجزائر، 2010، ص 33.

سيتم تخصيص الفرع الأول للجرائم الواقعية على الأشخاص والفرع الثاني للجرائم الواقعية على الأموال، والفرع الثالث للجرائم الواقعة على أمن الدولة.

الفرع الأول: الجرائم الواقعة على الأشخاص:

تعتبر صناعة ونشر الإباحة والجنس بالنسبة للبالغين والأطفال من أخطر الجرائم الواقعة على الأشخاص حيث يتعرض الأطفال والنساء للاستغلال الجنسي عبر الانترنت في صورة متعددة، كالتسجيلات المرئية للجرائم الجنسية العنيفة، والتقاط الصور[1].

فلقد أصبح عالم الأنترنت اليوم يعج بالصور الخليعة والأفلام الإباحية والمقالات الفاضحة والتي أصبحت مصدرا لجمع الأموال الطائلة تحت عدة مسميات حقوقية واقتصادية، والتي تتخذ عدة اشكال مثل المواقع الإباحية أو الدردشة الإباحية أو القوائم الجنسية البريدية[2].

دون أن ننسى الجرائم الإلكترونية الشخصية مثل جرائم انتحال الشخصية والتعزيز والاستدراج باستخدام شخصية شخص آخر للاستفادة من سمعته أو ماله، أو صلاحياته وسلطاته وكذلك جريمة القذف والسب وتشويه السمعة للمساس بشرف الغير وكرامتهم.

الفرع الثاني: الجرائم الواقعة على الأموال:

أدى تطور الأنترنت إلى تطور في وسائل الدفع والوفاء وأصبحت جزء لا يتجزأ من المعاملات الإلكترونية وظهرت بذلك عدة جرائم إلكترونية على الأموال كالسطو والسرقة، والتحويل الإلكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة، حيث أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريقة غير المشروعة ممكنة عير الأنترنت[3].

كما أدى ذلك إلى ظهور جريمة القمار وتبييض الأموال عبر الأنترنت بظهور الكازينوهات الإلكترونية الواقعة على الأموال جريمة المخدرات على الأنترنت حيث تتخذ المواقع الإلكترونية للترويج للمخدرات وتسويقها[4].

الفرع الثالث: الجرائم الواقعة على أمن الدولة:

انتشرت الجرائم الإلكترونية الواقعة على أمن الدولة، وكان أخطرها الإرهاب المعلوماتي والجريمة المنظمة للمعلوماتية، حيث سمحت الأنترنت للمنظمات الإرهابية لنشر أفكارها والترويج لها، وساعدت على ظهور جرائم أخرى أكثر خطورة منها مثل جريمة التجسس الإلكتروني، كما تم استغلال الأنترنت للتأثير على المعتقدات الدينية ومحاولة المساس بأمن الدولة وبنظامها الداخلي[5].

[1] نمديلي رحيمة، المرجع السابق، ص 09.
[2] قاسمي سمير، المكافحة الدولية والوطنية للإباحية الإلكترونية من منظر قانوني، المجلة العربية في العلوم الإنسانية والاجتماعية، مجلة 10، عدد 3، 2018، ص 321.
[3] خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، د ط، مصر، 2010، ص 76، 77.
[4] نمديلي رحيمة، المرجع السابق، ص 9.
[5] نمديلي رحيمة، المرجع السابق، ص 9.

ويأخذ الإرهاب الإلكتروني أشكال مختلفة منها ما يتعلق باختراق مواقع حكومية، ومنها ما يكون في شكل مجموعات تفكر مثل مستخدمي الأنترنت الذي يقومون بتعطيل الأنترنت من خلال زيادة حركة الدخول[1].

المطلب الثالث: الجرائم الواقعة على النظام المعلوماتي:

بعد أن تم استعراض مختلف الجرائم التي تقع بواسطة النظام المعلوماتي، سنحاول من خلال هذا القسم من الدراسة تناول مختلف الجرائم التي تمس النظام المعلوماتي، حيث ينقسم المطلب إلى 3 فروع، الفرع الأول: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي، الفرع (2) الجرائم الواقعة على البرامج الإلكترونية، الفرع الثالث: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي.

الفرع 1: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

المقصود بالمكونات المادية للنظام المعلوماتي الأجهزة الملحقة بالنظام المعلوماتي والتي يتم استعمالها في تشغيله كالأسطوانات والشرائط والكابلات ونتيجة الطبيعة المادية التي تتمتع بها هذه المعدات تكون الجرائم الواقعة عليها تقليدية كأن تكون محلا للسرقة وخيانة الأمانة والإحراق أو العبث بمفاتيح التشغيل، ونأخذ على ذلك مثال ما حدث في فرنسا وأدى إلى اتلاف معدات مؤسسة كبيرة ومتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية وقد تحملت خسائر قدرها 5 ملايين فرنك فرنسي[2].

الفرع الثاني: الجرائم الواقعة على البرامج الإلكترونية:

وتقسم هذه الجرائم إلى نوعين هما: الجرائم الواقعة على البرامج التطبيقية، والجرائم الواقعة على برنامج التشغيل، ويتحقق النوع الأول عن طريق تحديد البرامج في البداية ثم التلاعب به أو تعديله، ومثال ذلك ما حصل في أحد البنوك الأمريكية بقيام أحد المبرمجين بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بتقييد المصاريف الزائدة على حساب خاص به أطلق عليه تسمية Zgwick[3].

أما النوع الثاني والمتمثل في الجرائم الواقعة على برنامج التشغيل وهي البرامج المسؤولة على عمل النظام المعلوماتي، حيث تقوم عن طريق تزويد البرنامج بمجموعة من التعليمات الإضافية للوصول إليها بشيفرة تسمح بالدخول إلى جميع المعطيات الي يحتوي عليها النظام المعلوماتي، نأخذ على سبيل المثال في مدينة لوس أنجلس ما قامت به إحدى شركات التأمين الأمريكية تصميم برنامج يقوم بتصنيع وثائق تأمين لأشخاص وهميين عددهم 4600 شخص بغرض أن تتقاضى الشركة لعمولات من اتحاد شركات التأمين[4].

الفرع الثالث: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

عرّف الفقيه الفرنسي Gatala المعلومات بقوله "رسالة معبر عنها في الشكل يجعلها قابلة للنقل أو الإبلاغ للغير" كما عرفها القضاء الفرنسي بقوله "وسيلة للمعرفة قابلة لكي تحفظ أو تبلغ بواسطة الإصلاحات".

1

[2] نمديلي رحيمة، المرجع السابق، ص 10.

[3] سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق جامعة أبو بكر بلقايد، تلسمان، الجزائر، 2010، ص 24.

[4] نمديلي رحيمة، المرجع السابق، ص 10.

وتعتبر المعلومة أساس عمل النظام المعلوماتي، لما تتمتع به من قيمة اقتصادية، وتقوم الجرائم على "المعلومة" من خلال التلاعب بها بصفة مباشرة أو غير مباشرة، أو بواسطة اتلافها أو استبدالها أو محوها وهو ما يعرف بجريمة التزوير المعلوماتي[1]، نأخذ على سبيل المثال ما حدث في إسرائيل بقيام موظف بوزارة المالية بإدخال فواتير وهمية لا حصر لها، والقيام بتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي قام بإنشائها[2].

الخاتمة:

من خلال الدراسة تم التوصل لمجموعة من النتائج والتوصيات

أولا: النتائج

1/الجريمة الالكترونية جريمة مستحدثة

2/ اخذ المشرع الجزائري بمصطلح جريمة المساس بأنظمة المعالجة الالية للمعطيات بموجب القانون 15/04

3/الجريمة الالكترونية صعبة الاثبات

4/ يتطلب ارتكاب الجريمة الالكترونية جهاز الكتروني

5/ الجريمة الالكترونية عابرة للحدود الوطنية

6/ تعتبر الجرائم الواقعة على الاشخاص من اخطر الجرائم الالكترونية وابشعها ما يتم خلقه من مواقع اباحية للمتاجرة بالنساء وخاصة الاطفال.

ثانيا: التوصيات

1/ يعد الحاسوب هو فقط الوسيلة التي تستخدم في الجرائم الاخرى وانما اصبح الهاتف النقال وسيلة مهمة في ارتكابها خاصة الهواتف الذكية لذا وجب مراعاة ذلك في تعريف الجريمة الالكترونية .

2/ ان الخصائص التي تتميز بها الجريمة الالكترونية تستدعي من مختلف التشريعات سن القوانين التي تتلاءم معها وهو ما فعله المشرع الجزائري بنصه على جريمة المساس بأنظمة المعالجة الالية للمعطيات في قانون 15/04 ولكن هذا التجريم غير ملم وكافي لان هذه الجريمة في حالة تطور مستمر ودائم لذلك وجب تخصيص قانون خاص لها كمحاولة للإلمام بمختلف أنواعها.

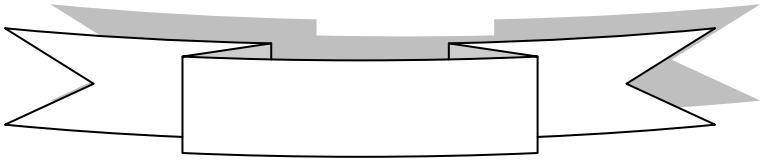
[1] المرجع نفسه، ص 10.
[2] المرجع نفسه، ص 10.

قائمة المراجع:

1. دستور 28 نوفمبر 1996، بموجب المرسوم الرئاسي رقم 438/ 96المؤرخ في 7ديسمبر 1996المعدل بقانون 16/01المؤرخ في 6مارس 2016يتضمن التعديل الدستوري ،الجريدة الرسمية العدد 14، الصادرة في 7مارس 2016والرسوم الرئاسي رقم 20/251المؤرخ 2، 020/12/15 2،الجريدة الرسمية رقم 54
2. الأمر رقم 156/66، المتضمن قانون العقوبات المعدل والمتمم بمقتضى القانون رقم 15/04 المؤرخ في 2004/11/10، الجريدة الرسمية رقم 66-155 المتضمن قانون الإجراءات الجزائية.
3. الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية المتضمن في قانون الإجراءات الجزائية، المعدل والمتمم بالقانون رقم 22/06 المؤرخ في 2006/12/20، الجريدة الرسمية عدد 845 مؤرخة في 2006/12/24.
4. براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، كلية الحقوق والعلوم السياسية، بدون عدد وسنة نشر.
5. بوضياف اسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، عدد 11، 2018.
6. خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، د ط، مصر، 2010.
7. ذياب موسى البدانية، ورقة علمية بعنوان الجرائم الإلكترونية: المفهوم والأسباب، في الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان، الأردن، 2014.
8. سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق جامعة أبو بكر بلقايد، تلسمان، الجزائر، 2010.
9. سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق جامعة أبو بكر بلقايد، تلسمان، الجزائر، 2010.
10. شينار سامية، الجريمة الإلكترونية في منظور الشباب الجامعي، مدخل نفسي، قانوني، مجلة الباحث للدراسات الأكاديمية، المجلد 6، العدد 2، 2019.
11. عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، كلية القانون، جامعة الكوفة، العدد: 7، 2008.
12. قاسمي سمير، المكافحة الدولية والوطنية للإباحية الإلكترونية من منظر قانوني، المجلة العربية في العلوم الإنسانية والاجتماعية، مجلة 10، عدد 3، 2018.

13. معزوز ربيع، زروقي عايشة، الجريمة الإلكترونية وإجراءات مواجهتها في التشريع الجزائري، مجلة

14. نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي 144 عن الجرائم الإلكترونية، طرابلس، 2017.



بن عزوز حاتم
hatem.benazouz@univ-tebessa.dz
جامعة العربي التبسي –تبسة

شريطي أسامة
oussama.cherite@univ-tebessa.dz
جامعة العربي التبسي –تبسة–

معالجة مفاهيمية لصور الجريمة الالكترونية الاقتصادية وانعكاسها على الاقتصاد

ملخص :

تتطرق هذه المداخلة إلى الجريمة الالكترونية وهي من بين الجرائم المستحدثة في العصر الحديث، إذ باتت من القضايا الراهنة في وقتنا لما لاقته من رواج كبير داخل فئات المجتمع، و قد تزامن ظهور هذا النوع من الجرائم مع تطور تكنولوجيات الحاصلة في مجال الحاسب الآلي، و شبكات الانترنت ، وقد مست هذه الجريمة جميع الميادين واخص بالذكر الميدان الاقتصادي إذ بات جزء كبير من المعاملات الاقتصادية تتم على شبكة الانترنت مما أدى ذلك بظهور حركة إجرامية مستحدثة تستهدف هذا النوع من المعاملات الاقتصادية معتمدين في ذلك على أدوات تتنوع بين مادية و أخرى برمجية hard wear soft wear تهدف هذه المداخلة إلى الوقوف على الجريمة الالكترونية الاقتصادية و أهم الأساليب التي يستخدمها المجرم ألمعلوماتي في المجال الاقتصادي معتمدين في ذلك على إعطاء أمثلة حية عن هذه البرمجيات بالإضافة إلى الطريقة المعتمدة في ذلك

الكلمات المفتاحية : الجريمة الالكترونية الاقتصادية، الاقتصاد الرقمي، القرصنة، الاحتيال، التقليد، الهجوم السيبيراني .

Abstract :

This entry deals with Cyber crime is among the newly developed crimes in the modern era, as it has become one of the current issues in our time due to its great popularity within the segments of society, and the emergence of this type of crime coincided with the development of technologies in the field of computers and Internet networks, and these Crime is all fields, especially the economic field, as a large part of economic transactions are carried out on the Internet, which led to the emergence of a new criminal movement targeting this type of economic transaction, relying on tools that vary between physical and hard wear software. This intervention aims to Standing on the economic cyber crime and the most important methods used by the information criminal in the economic field, relying on giving vivid examples of this software in addition to the method adopted in that

Keywords: *economic cyber crime, digital economy, hacking, fraud, counterfeiting, cyber attack.*

مقدمة:

يزدهر النمو الاقتصادي مع التقدم التكنولوجي ، لكن النشاط الإجرامي يستجيب ويتفاعل أيضًا مما يخلق تحديات للمنظمين والشركات المشروعة وعملائها والمراجعين والمستشارين على حد سواء.
ارتبط اسم الجريمة الالكترونية الاقتصادية تزامنا مع ظهور المعاملات الاقتصادية و المالية على شبكة الانترنت ، حيث انه وفي الآونة الأخيرة جزء كبير من الأنشطة الاقتصادية يتم على الانترنت وخصوصا في زمن جائحة كورونا، ونظرا للتدابير الوقائية كانت المبادلات التجارية و المعاملات المالية هي البديل الوحيد في ظل انتشار المرض ، ومنه فقد استحدث المجرمين طرق في سبيل ممارساتهم الإجرامية على شبكة الانترنت، كاستحداث منصات الكترونية مظلمة لبيع برامج مساعدة على الجرائم الالكترونية الاقتصادية ، وكذا برمجة برمجيات خبيثة تخدم مخططهم الإجرامي، وقد تجلت الجريمة الالكترونية في العديد من المظاهر وقد تمثلت في اختلاس الأموال ، وسرقة البيانات الشخصية ، و سرقة الملكية الفردية اختراق و قرصنة مواقع البنوك العالمية ، وكذا حسابات الأشخاص و تشير الإحصائيات أن الجريمة الالكترونية الاقتصادية قد لاقت ارتفاعا كبير حيث انه أصبحت الجريمة المالية أكثر سهولة بفضل انتشار المعلومات على الإنترنت ، إلى جانب سهولة الاتصالات والأموال التي تعبر الحدود الدولية. تعني أسواق الويب المظلمة أن الجناة لا يحتاجون حتى إلى أن يكونوا ماهرين تقنيًا.
وقد كلفت الجريمة الالكترونية خسائر مالية فاضحة سواء للأفراد او الشركات او الحكومات حيث انه من المتوقع أن تبلغ قيمة الخسائر الناتجة عن الجرائم الالكترونية بحلول عام 2025 10.5 تريليون دولار بحسب شركة cybersecurity ventures و يشمل هذا الرقم المساس باقتصاد الدولة ، حيث يمس تلف البيانات و تدميرها، و الأموال المسروقة، و فقدان الإنتاجية ، و سرقة الملكية الفكرية و سرقة البيانات الشخصية و المالية و الاختلاس و تعطيل المسار الطبيعي للأعمال ، و تكاليف استعادة البيانات و الأنظمة. (01)

1 شبكة مفاهيم :

1 -1الجريمة الالكترونية :

لا يوجد إجماع على تعريف الجريمة الالكترونية من حيث كيف تعرف، او ما هي الجرائم التي تتضمنها الجريمة الالكترونية ، حيث يتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية، و تعريف الجرائم الالكترونية باختصار : على أنها الجرائم التي ترتكب بواسطة الحاسوب و الشبكات و المعدات التقنية، حيث عرفت بأنها الممارسات التي توقع ضد الأفراد او مجموعة مع توفر باعث إجرامي، بهدف التسبب بالأذى عمدا و إلحاق الضرر به سواء كان مباشر او غير مباشر، بالاستعانة بشبكات الاتصال الحديثة وما تتبعها من أدوات الكترونية، و برمجيات.(02)

1-2الهجوم السيبراني : يدل على التسلل إلى مواقع الكترونية غير مرخص للدخول لها

بهدف تعطيل او إتلاف البيانات المتوفرة فيها او الاستحواذ عليها او هي عبارة عن سلسلة من الهجمات الالكترونية لتحقيق منفعة خاصة.(03)

1 –3 الحاسب الآلي : لغة يعني حسب و علم الحساب معنى علم الأعداد أي من العدد الدقيق و الحاسب في اللغة الانجليزية (computer) مأخوذة من كلمة (comput) اللاتينية التي تعني يحسب.

و الحاسب الآلي اصطلاحا عرفه الشاذلي و عفيفي بان هالة حساب الكترونية تستقبل البيانات ثم تقوم عن طريق الاستعانة ببرامج معينه بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة

1–4 الانترنت : تتكون كلمة internet من كلمتين interconnecting . network وقد أوجده الجيش بقصد إيجاد وسيلة اتصال موازية مستقلة و سريعة و الانترنت هو جزء من ثورة الاتصالات و يعرف البعض الانترنت بشبكة الشبكات في حين يعرفها البعض الأخر بأنها شبكة طرق المواصلات السريعة. (04)

2 خصائص الجرائم الالكترونية :

تتميز الجريمة الالكترونية بعديد من الخصائص ونذكر من بين هاته الخصائص

صعوبة الإثبات إن إثبات الجرائم الالكترونية، يحيط به كثير من الصعوبات التي تواجه سلطة الاستدلال او التحقيق الجنائي في استخلاص الدليل الجنائي، و التي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا ، فالجرائم الالكترونية لا عنف فيها و لا سفك دماء و لا أثار اقتحام و سرقة، بل هي أرقام و بيانات تمحى و تتغير و ليس لها أي اثر مرئي بمعنى أنها جرائم فنية تتطلب تكتيك معين كم أنها جرائم هادئة.

بالإضافة إلى أن هذا النوع من الجرائم تتميز بتخطيها للحدود الجغرافية ، أي اكتسابها الطابع الدولي فبعد ظهور شبكات المعلومات لم بعد هناك حدود مرئية او ملموسة تقف أمام شبكات المعلومات فالقدرة التي تتمتع بها الحاسبات الآلية في تبادل كميات كبيرة من المعلومات ، بين أنظمة يفصل بينها ألاف الأميال كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية ، بغض النظر عن المسافة بين المجرم و الأموال المستهدفة و المجني عليه .

فمن حيث دافع ارتكاب الجريمة الالكترونية حيث تستهدف الجرائم الالكترونيق تعديل على عناصر الذمة المالية، ويكون الطمع الذي إلي يشبعه الاستيلاء على المال دافعها ، و بريق المكسب السريع محركها وقد ترتكب أحيانا لمجرد قهر نظام الحاسب الآلي و تخطي حواجز الحماية المفروضة حوله او بدافع الانتقام.

بالاضافه إنها جرائم خفية ، فليس من السهولة اكتشافها لضعف القدرة الفنية للضحية وذلك مقارنة بالمجرم ألمعلوماتي، الذي يتميز من العديد من الصفات التي تميزه للقيام بهذه الجريمة ، او لخوف الضحية من الإبلاغ عن الجريمة تجنبا للإساءة إلى السمعة. (05)

3 أساليب ارتكاب الجريمة الالكترونية :

يستخدم المجرم ألمعلوماتي تقنية الاختراق لتنفيذ جريمته، من خلال التحايل على الأنظمة المعلوماتية فيكون الاختراق بالقدرة على الوصول إلى هدف معين عن طريق ثغرات نظام الحماية الخاصة، و تتم عن طريق برنامجين الأول الخادم، وهو بجهاز الضحية إذ ينفذ المهام الموكلة إليه، و الثاني يوجد بجهاز المخترق، و يسمى ببرنامج المستفيد كما أنهم يستخدمون العديد من البرامج الخبيثة نذكر منها :

3- 1 حصان طروادة : وهو عبارة عن برنامج صغير مختبئ ببرنامج اكبر وتؤدي مهامها بشكل خفي في إطلاق فيروسات ، و الدودة التي تقوم بإرسال البيانات عن الثغرات الموجودة في النظام، وإرسال كلمات المرور السرية الخاصة بالهدف ، ومن أنواعه القنابل المنطقية التي يزرعها المبرمج داخل النظام الذي يريد أن يطوره . (06)

3-2 الدودة المعلوماتية : (ver informatique)وهي برامج معلوماتية صغيرة قائمة بذاتها و غير معتمدة على غيرها وضعت بهدف تدمير و إعاقة و تشويش على شبكات، او بغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم على شبكة الانترنت ، او لإلحاق الضرر بهم او بالمتصلين بهم، وتتميز بسرعة الانتشار و في نفس الوقت يصعب التخلص منها، نظرا لقدرتها على التلون و التناسخ و أشهرها الدودة التي اخترعها (روبرت موريس) و المسماة بدودة الحب و كذلك دودة (ميليسا) و (انا كارنيكوفا) .

3-3 القنبلة المعلوماتية :(bonb informatique) و تعرف كذلك بالشفرة المعيقة او القنبلة الموقوتة ،و هي عبارة عن برامج يعد من قبل مصمم للنظام ألمعلوماتي يبثه بداخله و تكون الغاية منه جعله ينطلق او يعمل بعد فتره محددة على استعمال النظام ألمعلوماتي، بهدف تعطيله كان يتوقف عن العمل و يلصق رسالة او صورة او إشعار او تدمير او محو البيانات التي يحتويها و تجدر الإشارة إلى أنها أكثر ما تبرز في الحملات الإعلانية للبرمجيات و كذا في البرمجيات المؤجرة .(07)

4 مظاهر الجريمة الالكترونية الاقتصادية :

4-1 غسيل الأموال :

ومع نهاية القرن العشرين برزت ظاهرة غسيل الأموال عبر الانترنت لتشكل معضلة كبيرة للنظم القانونية المعاصرة، ولعل السبب الرئيسي في استجلاء هذه الظاهرة هي المدفوعات الافتراضية (cayber – payment).

وغسل الأموال هو عبارة عن معالجة لمصدر الدخل الأول و الأساسي غير مشروع، أي ناجم عن جريمة بالقيام بمجموعة من تحركات اقتصادية مشروعة ،تؤدي إلى طبع الأموال غير مشروعة المصدر بطابع المشروعية، و بطريقة لا يمكن بمقتضاها التعرف على المصدر الأساسي لها .

ويعتبر غسيل الأموال من الصور الحديثة للجرائم الاقتصادية الالكترونية، التي كثر الحديث عنها في الآونة الأخيرة و هي ظاهرة ترتبط بالجريمة المنظمة، و على الأخص الاتجار بالمخدرات و الإرهاب و تهريب الأسلحة، و الرقيق الأبيض، و الغش، و التزييف و الفساد المالي كما تتصل بالبنوك و المؤسسات

المالية الأخرى، لما توفره عملياتها من قنوات تستخدم في غسل الأموال الغير نظيفة حيث إن هذه الظاهرة الإجرامية قد تطورت مع ظهور شبكة الانترنت و اجتاحت العالم بأكمله ذلك لكون تلك الشبكة تمثل وسيلة فعالة و المسهلة لعملية تبييض الأموال وهذا ما جعل الأمر أكثر صعوبة بالنسبة للجهات المعنية بمتابعتها للمتعاملين عبر الشبكة و تحديد هويتهم او جمع أي معلومات عنهم ويرجع ذلك إلى عدة أسباب وهي :

01 إن شروط التعامل عبر الانترنت عبر الشبكة الدولية لا تتطلب إجراءات معقدة إنما فقط تدوين الاسم و رقم بطاقة الائتمان الخاصة بالمتعامل

02 إن النقود الالكترونية قد مكنت المتعاملين من تحويل مبالغ طائلة من دولة إلى أخرى بسهولة و دون مخاطر.(08)

علاوة على ذلك ، يوفر مجرمو الإنترنت أيضًا غسيل الأموال (أي "العملية التي يقوم بموجبها المجرمون بإخفاء الأموال غير المشروعة ومشروعيتها") كخدمة. يتم أيضًا غسل عائدات الخدمات التي يقدمها مجرمو الإنترنت. ينطوي غسل الأموال على ثلاث مراحل: إيداع العائدات غير المشروعة في النظام المالي (الإيداع) ، وإخفاء مصدر الأموال غير المشروعة (الطبقات) ، وإعادة إدخال الأموال في الاقتصاد مع إخفاء المنشأ (التكامل).(09)

ولتبييض الأموال اثر سيئ على الأعمال كما على النمو و على الاقتصاد و دور أكيد في دعم الجريمة المنظمة و الفساد كونه يمدها بالإمكانات المالية الضرورية لتجنيد المزيد من المجرمين و الفاسدين و يؤدي التغاضي عن تبييض الأموال إلى تأكل الاقتصاد .

4-2 القرصنة و الاعتداء على الملكية الفكرية و الصناعية :

على الرغم من عدم وجود تعريف متفق عليه عالميًا للقرصنة ، فقد تم وصفه على أنه الوصول المتعمد إلى الأنظمة أو مواقع الويب أو البيانات دون إذن أو تجاوز الوصول المصرح به ، أو التدخل المتعمد في عمل أو إمكانية الوصول الأنظمة والمواقع والبيانات دون إذن أو تجاوز الوصول المصرح به ، من أجل إحداث تغيير اجتماعي أو سياسي . (10)

كما تؤثر الجريمة المعلوماتية بشكل أساسي على الاقتصاد من زاوية الاعتداء على حقوق الملكية الفكرية عبر عملية القرصنة التي تروج للاستخدام او النسخ لبرامج و تطبيقات معلوماتية ومواد أخرى كالأفلام و الموسيقى الخاضعة لحقوق الملكية الفكرية و تساهم العديد من المواقع على الانترنت للترويج لبرامج قرصنة مجانا او بمقابل مادي و يمكن للقراصنة استهداف أجهزة بغابة تدميرها او تحقيق مكاسب مالية شخصية عندما يلجا مقتحم النظام إلى سرقة معلومة بطاقة الائتمان و تحويل الأموال من حسابات مصرفية مختلفة إلى حساب المقر صرن الخاص او أي حسابات أخرى على مستوى أخر يعتمد بعض المقرصنين على ابتزاز الشركات العالمية و تهديدها بنشر المعلومات السرية الخاصة بها فيحال عدم قيامها بدفع او تحويل المبلغ المالي المطلوب وتهدف عمليات الخداع و الاحتيال على الانترنت غالبا إلى جني الأموال حيث يستدرج المستخدم إلى إفشاء أرقام بطاقة ائتمانه او إلى إرسال حوالات مالية او

شيكات او إعطاء بياناته الشخصية و منها كلمات المرور إلى حساباته على الانترنت او إلى بريده او هاتفه .(11)

وتتحقق هذه الجريمة بالاعتداء على حقوق الملكية الفكرية للمصنفات او العناصر ذات الصلة بالأنشطة الصناعية و الزراعية و التجارية و يعرفها الفقه بأنها الحقوق التي ترد على مبتكرات جديدة كالاختراعات و الرسوم و النماذج الصناعية او على شارات مميزة تستخدم إما في تمييز المنتجات(العلامات التجارية) او تمييز المنشئات التجارية (الاسم التجاري) و تمكن صاحبها من الاستئثار باستغلال ابتكاره او علامته التجارية و اسمه التجاري في مواجهة الكافة و تشمل ملكية الصناعية براءة الاختراع و العلامات التجارية و النماذج او الرسوم الصناعية و علامات المنشأ و حماية الأصناف النباتية التي تنظمها عادة قوانين التجارة الوطنية . (12)

4 –3 السرقة الالكترونية على أموال البنوك وخدمة الانترنت المدفوعة والاحتيال على بطاقات الائتمان :

أصبحت الانترنت مجالا رحبا لمن له سلعة او خدمات تجارية يريد أن يقدمها بوسائل غير مسبوقة كاستخدام البريد الالكتروني او عرضها على مواقع على الشبكة او عن طريق ساحات الحوار(13)

حيث عرفت المادة 399 من القانون الأردني السرقة بأنه اخذ مال الغير المنقول دون رضاه و يعني اخذ المال لازالت تصرف المال الأصلي فيه وذلك عن طريق استخدام الجاني الحاسب الآلي للدخول إلى شبكات الانترنت و الوصول الغير مشروع. (14)

إلى البنوك و المصارف و المؤسسات المالية و تحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى و ذلك بإدخال بيانات غير حقيقية او تعديل او مسح البيانات الموجودة بقصد اختلاس الأموال او نقلها او إتلافها و تقوم هذه التقنية على الاستيلاء على الأموال بكميات صغيرة جدا من الحسابات الكبيرة بحيث لا يلاحظ نقصان هذه الأموال . (15)

حيث أن التطور التكنولوجي الكبير في مجال الاتصالات وظهور التجارة الالكترونية و انتشارها الكبير و اعتماد الكثير من الناس شراء حاجياتهم على شبكة الانترنت حيث امتد نشاط البطاقات عليها الذي يشكل عمليات متسارعه لكونه يعد إحدى الطرق السهلة لعملية البيع و الشراء فالتسوق عبر الانترنت أصبح يسرى في أي مكان في الأرض و في أي توقيت دون الحاجة إلى مغادرة المنزل فكل ما يحتاجه الشخص هو اتصال بالانترنت و بطاقة ائتمان سارية المفعول و قد واكب هذا ظهور الكثير من المتسللين للسطو عليها باعتبارها نقود الكترونية وتوجد العديد من الطرق تمكنهم من سرقة أرقام البطاقات الائتمانية و بالتالي استعمالها بصورة غير مشروعة وذلك عن طريق الاحتيال.(16)

ومن صور الاحتيال على أرقام بطاقات الائتمان حيث تتجلى صور الاحتيال داخل الفضاء الافتراضي عبر اختراق ألمعلوماتي لحدود نظام من النظم السائدة في هذا الفضاء وذلك بمباشرة مجموعة من الأنشطة اللامشروعة و التي تشمل

01 سرقة البرمجيات او استغلالها دون وجه إذن مسبق بذلك بعد فك الرموز و الكلمات السرية و كسر الحواجز الأمنية و استكشاف مواطن الضعف في الجهاز او الشبكة

02 الدخول إلى ساحة النظم الحاسوبية و شبكة الهواتف بأنواعها لاستغلال الموارد المتاحة فيها
03 مباشرة أعمال القرصنة على الخدمات العامة و الخاصة المتاحة على الشبكات الحاسوبية
04 تهريب الموارد المعلوماتية من نظام إلى آخر
05 تخليق أرقام بطاقات ائتمانية باعتماد معادلات رضائية و خلق بطاقات وهمية.(17)

وتعد سرقة خدمة الانترنت المدفوعة من جرائم السرقات في العالم الافتراضي يتمثل في الوصول الغير مرخص به إلى المواقع الالكترونيق او الحواسيب أم بالاختراق او بالدخول بحصان طروادة باستخدام وسيلة اتصال عن بعد حيث يتمكن المعتدي من الولوج إلى احد المواقع المسجلة على شبكة الانترنت و يقوم باستغلال ساعات خدمة مدفوعة الأجر الخاصة بالمعتدي دون إذنه وتتحقق هذه الجريمة أيضا إذا استعمل الجاني حاسوب غيره لأغراض شخصية من خلال العمل على أنظمة غير مصرح له بالعمل عليها و تشبه هذه الجريمة سرقة خدمة الاتصال و من صورها الاستيلاء على رصيد بطاقات الهواتف النقالة و تزوير بطاقة الهواتف النقالة الوصول الغير قانوني إلى لوحة توزيع المكالمات الهاتفية و التلاعب بها و بتالي خسائر اقتصادية و مالية بالنسبة للشركات القائمين على الهاتف ومنه القيام بتعويضات للضحايا.(18)

4 –4 تقليد السلع و المنتجات :

شارك مجرمو الإنترنت في مجموعة متنوعة من الجرائم الإلكترونية ، بما في ذلك الاحتيال ، والقرصنة ، وإنشاء البرامج الضارة وتوزيعها ، والابتزاز ، وجرائم الملكية الفكرية ، مثل بيع المنتجات المقلدة أو المزيفة التي تحمل علامات تجارية (مثل الملابس والإكسسوارات والأحذية والإلكترونيات والمنتجات الطبية وقطع غيار السيارات وما إلى ذلك) والملصقات والحزم وأي تصميمات أخرى لتحديد هذه المنتجات تسبب هذه الأنواع من الجرائم الإلكترونية ضررًا ماليًا ونفسيًا واقتصاديًا وحتى جسديًا (خاصة الإلكترونيات المقلدة وأجزاء السيارات ، بالإضافة إلى المنتجات الطبية المزيفة ، التي تحددها منظمة الصحة العالمية على أنها "تحريف هويتها أو تكوينها أو مصدرها عمدًا / احتياليًا" ،، وقد تم استخدامها لتمويل أشكال أخرى من الجرائم الخطيرة ، مثل الإرهاب.(19)

5انعكاسات الجريمة الالكترونية الاقتصادية على المنظومة الاقتصادية الوطنية :

للجريمة الالكترونية الاقتصادية اثر مباشر على جميع الفاعلين في المنظومة الاقتصادية، حيث تعتبر الجريمة الالكترونية الاقتصادية حجاز أمام نمو و ازدهار الاقتصاد، فهي تشكل عبا اقتصادي ضخم و ذلك من خلال العديد من النقاط و التي تمثلت في :

من مخاطر الجريمة الالكترونية الاقتصادية التسبب بالأضرار الاقتصادية للدولة من خلال تدمير النظام الاقتصادي، عن طريق التطفل على خصوصيات الدولة وعلى الأموال العامة، حيث أكد تقرير أن القطاعات الصناعية كالطاقة و التصنيع و خدمات النقل هي الأكثر عرضة لمخاطر الهجمات السبيراني ة وكان فريق الاستجابة للطوارئ و الحوادث السبيرانية في أنظمة التحكم الصناعي قد بلغ عن أكثر من 800 حادث امني

سبيراني على مستوى العالم منذ العام 2011 ، حيث وقعت غالبية الحوادث في قطاع الطاقة ، وينذر تقرير بيان التهديدات في قطاع الأمن السبيراني الصناعي ببيئة سبيرانية باتت خطيرة أكثر من السابق.(20)

إن أهم مؤشر في اتجاهات طلب العمل هو نمو الإنتاج فبالتالي : فان تباطؤ النمو الاقتصادي يعني ارتفاع في معدل البطالة، وكلما زادت الجريمة الالكترونية زاد معدل البطالة بكافة أنواعه ومن ثم تأثيراتها على التنمية الاقتصادية ، مما يؤدي إلى الانحراف و السلوك الإجرامي والذي يكون سببا في زيادة معدلات الجريمة والذي يصعب السيطرة عليه.

إن فساد السياسات الاقتصادية النقدية و المالية فعملية التسويق الالكتروني دون رقابة من شانها أن تؤدي إلى العديد من النقاط ومنها، التهرب الضريبي و الذي له العديد من الآثار الخطيرة التي تؤدي بدورها إلى الإخلال بنظام العدالة الضريبية مما يترتب عليه في النهاية إخلال الجرائم المعلوماتية بمبدأ العدالة الاجتماعية في توزيع الأعباء لضريبية ، فللتهرب الضريبي العديد من الانعكاسات و التي تتمثل في الإخلال بمبدأ قواعد التشريع الضريبي، انتشار الفساد و انعدام الأمانة .

للجرائم الالكترونية الاقتصادية اثر حقيقي على عدم الاستقرار الأمني في المجتمع من نشاط اقتصادي و استثماري ففي جو ينعدم فيه الاستقرار الأمني يجعل رجال الأعمال و المستثمرين ينفرون عن استغلال رؤوس أموالهم في تلك البلدان وهذا منعكس خطير على الركود الحتمي للاقتصاد .

وللجريمة الالكترونية الاقتصادية بدورها انعكاسات على الشركات المالية حيث تمثل هذه الجريمة هاجز مخيفا للكثير من المواقع الكبري و الشركات و البنوك، حيث تقوم بدفع الملايين لبناء أنظمة حماية خوفا من الاختراق، حيث تؤثر هذه الجرائم على الوضع المادي لهذه الشركات وتفقد الثقة لها في سوق الأعمال ، و بالتالي تكبدها العديد من الخسائر التي قد تؤدي بها إلى الإفلاس

فالمؤسسات الاقتصادية هي هيكل تنظيمي اقتصادي مستقل ماليا في إطار قانوني هدفه دمج عوالم الإنتاج من اجل الإنتاج ،او تبادل السلع و الخدمات او القيام بكليهما معا مالم تؤثر عليها عوامل خارجية او داخلية تعرقل أهدافها مثل الجرائم المعلوماتية، وهذه الجرائم لا شك أنها تؤثر على الجانب المادي لهذه المؤسسة وذلك عن طريق :

01 الاطلاع على المؤسسات السرية و الاستفادة منها

02 العبث بمخازن المعلومات الخاصة بالمنظمة او المؤسسة بحذفها او تعديلها .

03 سرقة الأموال و تحويلها .

04 عمليات الاحتيال و الابتزاز و التهديد .(21)

خاتمة :

وفي الأخير تتعدد مظاهر الجرائم الالكترونية الاقتصادية في عصرنا الحالي وذلك راجع إلى حجم المعاملات الاقتصادية التي تتم عبر الشبكة العنكبوتية لذا يراعى على المتعاملين الاقتصاديين الزبائن و الباعة و البنوك العالمية اخذ جميع الاحتياطات بخصوص حماية المعلومات الخاصة بالمتعاملين و كذا الحرص على إخفاء المعلومات الشخصية الخاصة بالأفراد وكذا تجنب التعامل مع المواقع و البرمجيات

المشبوهة و حيث ان الجريمة الالكترونية الاقتصادية لا تلقي بآثارها السلبية على الشخص الذي تمسه الجريمة بل تلقي بسلبياتها على جل الاقتصاديات العالمية و تكبدها خسائر بملايير الدولارات فضلا على أنها مجال رحب لتدعيم نوع أخر من الجرائم وفي شق تعاني القوانين الدولية قصورا في مواجهة هذا النوع من الجرائم وذلك من خلال استحداث و توسيع النصوص القانونية الدولية و التي من شانها التقليل من هذه الظاهرة وهذا راجع إلى الخصوصية التي تتميز بها هذا النوع من الجرائم .

قائمة المراجع ;

01 موقع على موقع قناة العربية بعنوان خسائر الجرائم الالكترونية العالمية https://www.alarabiya.net/aswaq/special-stories/2021/02/21، تم الاطلاع بتاريخ 2022/07/20

02 مركز هردوا لدعم الرقمي ، التعبير التنظيم القانوني و الجرائم الالكترونية مابين امن المعلومات و تقييد الحريات ، القاهرة 2017 صفحة 7 .

03 شيخه حسين الزهراني ، الطبيعة القانونية للهجوم السبيراني وخصائصه، مجلة جامعة الشارقة للعلوم القانونية ، جامعة الشارقة ، العدد 1، المجلد 17 ، شوال 1441 ، يونيو 2020 ، ، الامارات العربية المتحدة ، صفحة 774

04 قيسي نوال ، رسالة ماجستار ، الجريمة الالكترونية الموجهة ضد مستخدمي الانترنت دراسة مسحية لبعض مستخدمي الانترنت بالمملكة العربية السعودية ، كلية العلوم الاجتماعية السعودية ، جامعة الإمام محمد بن سعود الإسلامية ، صفحة 24

05 شيخه حسين الزهراني ، المرجع سابق ، صفحة 779 778

06 روان بنت عطية الله الصحفي ، المجلة الالكترونية الشاملة متعددة التخصصات ، العدد 24 ماي 2020 المملكة العربية السعودية الجرائم السبيرانية صفحة 15

07 سهيل محمد عزام ، الوجيز في جرائم الانترنت دراسات عليا في القانون ، الطبعة الأولى ، المملكة الهاشمية الأردنية ، 2009 صحة 50 51

08 سهيل محمد عزام ، المرجع سابق ، صفحة 65

09 مقال منشور على الموقع الرسمي لهيئة الأمم المتحدة https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html تم الاطلاع بتاريخ 2022/07/19

10 مقال منشور على الموقع الرسمي لهيئة الأمم المتحدة https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/hacktivism.html تم الاطلاع بتاريخ 2022/07/20

11 ، السبيرانية هاجس العصر، المركز العربي للبحوث القانونية و القضائية ، جامعة الدول العربية صفحة 136

12 عادل عزام صقف الحيط ، جرائم الذم و القدح و التحقير المرتكبة عبر الوسائط الاجتماعية ، دراسة قانونية مقارنة ، الطبعة الأولى، دار الثقافة للنشر و التوزيع ، المملكة الهاشمية الأردنية ، 2011، صفحة 164

13 مركز هردوا لدعم التعبير الرقمي ، مرجع سابق ، صفحة 09

14 الامم المتحدة ، الاقتصاد الرقمي و التحول نحو المجتمعات الذكية ، لجنة التكنولوجيا من اجل التنمية ، فبراير 2017 ، دبي ، صفحة 40

15 روان بنت عطية الله الصحفي ، مرجع سابق ، صفحة 20

16 سفيان قعلول ، الاقتصاد الرقمي في الدول العربية واقع و تحديات ، صندوق النقد الدولي 2020 ، صفحة 60

17 كريمة الحسناوي، رسالة ماجيستار ، الجريمة في مجال التجارة الالكترونية عروض القانونية المغربية ، جامعة عبد المالك السعدي المملكة المغربية ، 2019 ، صفحة 10

18 عادل عزام صقف الحيط ، مرجع سابق ،صفحة 152

19 مقال منشور على الموقع الرسمي لهيئة الأمم المتحدة

https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html تم الاطلاع عليه بتاريخ 2022/07/20

20 هلال نصار مصال، منشور على الموقع الاتي بعنوان انعكاسا الجرائم الالكترونية على المجتمع و رؤية قانونية https://www.amad.ps/ar/post/450901/ تم الاطلاع بتاريخ 2022/08/01

21 ابو بكر احمد همام ،الاثار الاقتصادية للجريمة المعلوماتية وسبل مكافحتها ، مجلة جامعة جنوب الوادي الدولية للدراسات القانونية ، العدد السادس ، 2021 ، صفحة 33

باخويا دريـــس
bakhouya1980@yahoo.com
جامعة أدرار

مهيـدي كمال
mehidikamel@gmail.com
جامعة 08 ماي 1945 قالمة

الجريمة الإلكترونية المنظمة

Cyber Organized Crime

ملخص:

أصبحت الجرائم السيبرانية تشكل خطرا عالميا يهدد البلدان النامية والبلدان المتقدمة على حد السواء، بما يؤثر سلبا على الحوكمة الذكية والتجارة الإلكترونية والاقتصاد الرقمي بصفة عامة. فالانتشار الواسع للانترنت يوفر للمجرمين إمكانية الوصول إلى الضحايا والعملاء في أي مكان في العالم من خلال الولوج إلى الشبكة، أين تنتقل المعلومات والبيانات والأموال عبر الفضاء الإلكتروني بسهولة كبيرة. حيث صارت الشبكة بيئة خصبة للمجرمين لمشاركة المعرفة والتواصل دون أن يتم اكتشافهم، وبيع البيانات والسلع والخدمات المسروقة، وغسل الأموال المكتسبة بطريقة غير مشروعة، بالإضافة إلى تبادل تكتيكات الجريمة الإلكترونية والأدوات المستخدمة لارتكابها، أين يمكن لهؤلاء المجرمين العمل بمفردهم أو في أنواع مختلفة من الجماعات الإجرامية المنظمة. تهدف هذه الورقة البحثية إلى تسليط الضوء على أنواع الجرائم السيبرانية المنظمة وأنواع الفاعلين فيها، وكذا جملة التدابير المتخذة لمكافحة الجريمة الإلكترونية المنظمة.

الكلمات المفتاحية : *الجريمة الإلكترونية المنظمة، الجريمة عبر الوطنية، القرصنة، الغسل الإلكتروني للأموال، بيع السلع المسروقة عبر الانترنت، الاعتداء على البيانات الإلكترونية.*

Abstract:

Cybercrime has become a global threat to both developing and developed countries, negatively affecting smart governance, e-commerce and the digital economy in general.

The wide spread of the Internet provides criminals with access to victims and clients anywhere in the world through network access, where information, data and money travel through cyberspace with great ease. Where the network has become a fertile environment for criminals to share knowledge and communicate undetected, sell stolen data, goods and services, launder illicitly acquired money, as well as exchange cybercrime tactics and tools used to commit it, where these criminals can work alone or in different types of criminal groups the organization.

This research paper aims to shed light on the types of organized cybercrime and the types of perpetrators in it, as well as the set of measures taken to combat organized cybercrime.

Keywords*: Organized cybercrime, transnational crime, piracy, electronic money laundering, selling stolen goods via the Internet, electronic data attack.*

مقدمة

تطورت الجريمة السيبرانية بشكل كبير لتصبح إحدى أكبر وأسرع التهديدات التي تواجه التنمية الاقتصادية على الصعيد العالمي، بما يفقد الثقة في استخدام تكنولوجيا المعلومات والاتصالات ويعيق الخطوات العملاقة التي حققتها الدول في تطوير التجارة الإلكترونية وبعث الاقتصاد الرقمي الذي يعتبر الدعامة الأساسية للتنمية المستدامة الحديثة.

إذ وصل مجموع الأضرار التي خلفتها الجرائم السيبرانية على مستوى العالم مبلغ 6 تريليون دولار أمريكي سنة 2021، وهو مبلغ يشكل ثالث أكبر اقتصاد في العالم بعد الولايات المتحدة والصين.[1]

حيث تتوقع شركة Cybersecurity Ventures، وهي أكبر شركة متخصصة في أبحاث الأمن المعلوماتي، أن تنمو تكاليف الجرائم الإلكترونية العالمية بنسبة 15٪ سنويًا على مدى السنوات الخمس المقبلة، لتصل إلى 10.5 تريليون دولار أمريكي سنويا بحلول عام 2025، مقارنة بـ 3 تريليون دولار أمريكي في عام 2015. وهذا يمثل أكبر تحويل للثروة الاقتصادية في التاريخ، ويهدد بصفة مباشرة الابتكار والاستثمار الرقمي، بشكل أكبر بكثير من الضرر الناجم عن الكوارث الطبيعية في عام واحد، وسيكون أكثر ربحية من التجارة العالمية لجميع المخدرات غير المشروعة الرئيسية مجتمعة. ويعتمد تقدير تكلفة الضرر على الأرقام التاريخية للجرائم الإلكترونية بما في ذلك النمو الأخير على أساس سنوي، مع أخذ بعين الاعتبار الزيادة الهائلة في أنشطة القرصنة التي ترعاها عصابات الجريمة المنظمة . وتشمل تكاليف الجرائم الإلكترونية إتلاف البيانات وتدميرها، سرقة الأموال، فقدان الإنتاجية، التعدي على الملكية الفكرية، سرقة البيانات الشخصية والمالية، الاختلاس، الاحتيال، تعطيل المسار الطبيعي للأعمال بعد الهجوم، التحقيق الجنائي، واستعادة وحذف البيانات والأنظمة المقرصنة والإضرار بالسمعة.[2]

وقد اكتسبت الجريمة المنظمة، باعتبارها نوعا متصاعدا من الجريمة، أشكالا جديدة من المظاهر منذ أن استخدم أعضاء الجماعات الإجرامية أدوات تكنولوجيا المعلومات والاتصالات لارتكاب جرائم، أو انتقلوا إلى الفضاء الافتراضي حيث توفر لهم هذه المساحة "مجال العمل" المثالي الذي يضمن إخفاء الهوية وعدد كبير من الضحايا ومصادر ربح ضخمة. وعلى أرض الواقع، فإن تتبع مجموعات المجرمين الإلكترونيين المنظمة واكتشاف أنشطتهم من الصعوبة بمكان، وعليه ستسعى هذه الدراسة إلى تقديم عرض عن الجرائم الإلكترونية في شكلها المنظم وكذا مجموعات المجرمين الإلكترونيين وأنواعها وخصائصها وأنواع الجرائم الإلكترونية التي ترتكب عبر الإنترنت.

بناء على ما تقدم، يمكننا طرح الإشكالية التالية: ما هي الجريمة الإلكترونية المنظمة وما سبل مكافحتها؟

---

[1] *Steve Morgan, Special Report:* ***Cyberwarfare In The C-Suite****, – Nov. 13, 2020,* Cybercrime Magazine on cybersecurityventures.com.

[2] *Ibid.*

وللإجابة عن هذه الإشكالية، اتبعنا المنهج الوصفي خصوصا عند التعرض لمفهوم الجريمة الإلكترونية وأسواق وتصنيفات الفاعلين فيها، وكذلك المنهج التحليلي للوصول إلى استنتاجات وتعميمات تساعد في التصدي لهذه الظاهرة.

تأسيسا على ما تقدم، ارتأينا تقسيم الدراسة حسب الخطة الآتية:

المبحث الأول: مفهوم الجريمة الإلكترونية المنظمة

المطلب الأول: تعريف الجريمة الإلكترونية المنظمة

المطلب الثاني: الفاعلين في الجريمة الإلكترونية المنظمة

المبحث الثاني: مكافحة أنشطة الجريمة الإلكترونية المنظمة

المطلب الأول: أنشطة الجريمة الإلكترونية المنظمة

المطلب الثاني: سبل منع الجريمة الإلكترونية المنظمة

خاتمة تتضمن النتائج والتوصيات.

المبحث الأول: مفهوم الجريمة الإلكترونية المنظمة

نتطرق من خلال هذا المبحث إلى تعريف الجريمة الإلكترونية المنظمة في المطلب الأول، ثم تصنيف الفاعلين فيها وكذا أهم الأسواق التي يمتد إليها نشاطهم في المطلب الثاني.

المطلب الأول: تعريف الجريمة الإلكترونية المنظمة

مصطلح الجريمة الإلكترونية المنظمة مركب من عنصرين أساسيين، الجريمة الإلكترونية أولا ثم التنظيم ثانيا، وبصفة عامة فإن الجرائم الإلكترونية هي أي نشاط إجرامي يتضمن جهاز كمبيوتر أو جهاز متصل بالشبكة. وبينما يتم تنفيذ معظم الجرائم الإلكترونية من أجل جني الأرباح لمجرمي الإنترنت، يتم تنفيذ بعض الجرائم الإلكترونية ضد أجهزة الكمبيوتر أو الأجهزة الأخرى مباشرة لإتلافها أو تعطيلها. كما يستخدم الآخرون أجهزة الكمبيوتر أو الشبكات لنشر البرامج الضارة أو المعلومات غير القانونية أو الصور أو المواد الأخرى.[1]

وقد قسمت وزارة العدل الأمريكية الجرائم الإلكترونية إلى ثلاث فئات:

1. الجرائم التي يكون فيها جهاز الكمبيوتر هو الهدف، مثل اختراق الشبكة.

2. الجرائم التي يتم فيها استخدام الكمبيوتر كسلاح مثل هجوم الحجب وتعطيل الخدمة.

3. الجرائم التي يتم فيها استخدام الكمبيوتر كبرنامج ملحق لجريمة كاستخدام جهاز الكمبيوتر لتخزين البيانات التي تم الحصول عليها بشكل غير قانوني.

[1] McCusker, R.,**Transnational organised crime: Distinguishing threat from reality**, Crime Law and Social Change 46, 2006, p. 258.

وتعرف اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية الجريمة الإلكترونية على أنها مجموعة واسعة من الأنشطة الضارة، بما في ذلك الاعتراض غير القانوني للبيانات، والتدخلات في النظام التي تضر بسلامة الشبكة وتوفرها، وانتهاكات حقوق النشر.[1]

كما تعرف الجرائم الإلكترونية بأنها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة (كمبيوتر وانترنت) في أعمال وأنشطة إجرامية، عادة ما ترتكب بهدف تحقيق فوائد مالية عبر أعمال غير شرعية تستخدم عبر شبكة الانترنت.[2]

بينما وضع بعض الباحثين تعريفا إجرائيا للجريمة الإلكترونية أو أي من مرادفاتها بأنها: أي فعل يخالف القانون ويرتكب ضد الأفراد أو المجتمعات، ويهدف إلى إيذاء الغير، أو الحصول على منافع غير مشروعة، باستخدام الانترنت وتقنيات الاتصال الحديثة.[3]

كما أن هناك عدة مسميات للجريمة الإلكترونية بنفس المعنى، من أبرزها: جرائم الحاسوب Computer Crimes، جرائم التقنية العالية Hi-Tech Crimes، الجريمة الإلكترونية E-crime، الجريمة السايبرانية Cybercrime.

أما بالنسبة لعنصر التنظيم، فكما أن النشاط الإجرامي السيبراني العادي يمكن أن يقوم به فرد واحد، فإنه يصبح منظما إذا ارتكبته مجموعة بمهارات تقنية قليلة نسبيا، أو من قبل جماعات إجرامية عالمية عالية التنظيم قد تشمل مطورين مهرة وآخرين من ذوي الخبرة ذات الصلة. وذلك لزيادة تقليل فرص الاكتشاف والمقاضاة، وغالبا ما يختار مجرمو الإنترنت العمل في بلدان ذات قوانين ضعيفة أو غير موجودة بشأن الجرائم الإلكترونية.[4]

ويعتمد تحديد ما إذا كانت بعض الجرائم الإلكترونية على أنها شكل من أشكال الجريمة المنظمة أو مرتبطة بالجريمة المنظمة على التعاريف العملية المستخدمة لـ "الجريمة المنظمة" [5]. وكذلك لا تقدم اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية [6] تعريفا للجريمة المنظمة عموما. وهذا ليس نتيجة عدم وجود

---

[1] Revue internationale de droit pénal, **La cybercriminalité,** Éditeur : Érès, 2006/3-4 (Vol. 77)**,** p. 3**.**

[2] أحمد عبد المحسن بدوي محمد، **مشكلات الإعلام الجديد**، أبحاث المؤتمر الدوني الإعلام الجديد: تكنولوجيا جديدة لعالم جديد، جامعة البحرين، من 7 إلى 9 أفريل 2009، المنامة: منشورات جامعة البحرين، 2009، ص 86.

[3] عبير مجني أبو دية، **الجرائم الإلكترونية –دراسة نظرية**، الملتقى الخامس للرابطة العربية للبحث العلمي وعلوم الاتصال بعنوان: إشكالية المصطلح في علوم الإعلام والاتصال في العالم العربي، بيروت من 29 إلى 1 ديسمبر 2018، ص 6.

[4] Williams, P.,**Organized crime and cyber-crime: Implications for business**, Available at: http://www.cert.org/archive/pdf/cybercrime-business.pdf, 2002, p. 4.

[5] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، **التقرير المال والبيانات المالية المراجعة لفترة السنتين المنتهية في 31 ديسمبر 2013 وتقرير مجلس مراجعي الحسابات**، الوثائق الرسمية للأمم المتحدة، نيويورك، 2014، ص 44-45.

[6] مكتب الأمم المتحدة المعني بالمخدرات والجريمة فيينا، **اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة بها**، الوثائق الرسمية للأمم المتحدة، نيويورك، 2004.

اتفاق بين الدول فحسب، بل هو بالأحرى خيار واعي اتخذه المفاوضون بشأن الاتفاقية، والسبب في ذلك على الأرجح هو احتمالية أن يتضمن أي تعريف قائمة بالأنشطة غير المشروعة التي تقوم بها الجماعات الإجرامية المنظمة، والتي تتغير باستمرار وتتكيف مع التطور الديناميكي للعالم ؛ مما يجعل من هذا التعريف قديما ومتجاوزا. وبدلا من ذلك عرفت الاتفاقية الفاعل بموجب المادة 2 (أ) ، بقولها: "يقصد بتعبير "جماعة إجرامية منظمة" جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الاتفاقية، من أجل الحصول، بشكر مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى".

تجدر الإشارة هنا إلى أن استعمال مصطلح مجموعة منظمة يجعل التعريف واسعا، إذ أنه لا يشترط في المجموعة المنظمة أي تسلسل هرمي أو استمرار في العضوية، بما في ذلك المجموعات ذات الارتباط العفوي غير المحكم دون أية أدوار رسمية محددة لأعضائها وبدون هيكل مطور وثابت.

في حين أن مكتب الشرطة الأوربي اليوروبول فقد حدد أنه ولكي يتم تصنيف أي مجموعة على أنها جريمة منظمة فيجب توافر 6 خصائص على الأقل، أربعة منها إلزامية وهي الأولى والثالثة والخامسة والحادية عشر، وجاءت كما يلي: [1]

1) أن يزيد عدد المشاركين عن فردين، 2) أن يكون لكل فرد مهمة محددة، 3) أن تكون ممتدة لفترة من الوقت أو غير محددة المدة، 4) استخدام بعض من أشكال الانضباط والرقابة، 5) يشتبه في ارتكاب جرائم جنائية جسيمة، 6) تعمل على الصعيد الدولي، 7) تستعمل العنف أو الوسائل الأخرى المناسبة للترهيب، 8) استخدام هياكل تجارية أو نظامية، 9) أن يكون لها صلة بغسل الأموال، 10) ممارسة التأثير على السياسة والإعلام، الإدارة العامة، والسلطات القضائية أو الاقتصاد، 11) يحددها السعي وراء الربح و/أو السلطة.

وعلى الرغم من عدم وجود تعريف متفق عليه عالميا للجريمة المنظمة، يمكننا القول أن الجريمة الإلكترونية المنظمة مصطلح يستخدم لوصف الأنشطة المنظمة غير المشروعة في الفضاء السرايبراني.

المطلب الثاني: الفاعلون في الجريمة الإلكترونية المنظمة

تتطلب العديد من أفعال الجريمة الإلكترونية درجة عالية من التنظيم والتخصص، إذ يرجح ارتفاع ضلوع الجماعات الإجرامية المنظمة التقليدية في ارتكاب جرائم إلكترونية، على الأقل بدوافع مالية مثل استخدام الحاسوب في الاحتيال والتزوير والاعتداء على الهوية. وقد أوضحت إحدى الدراسات الحديثة والتي أجرت استعراضا لعينة من 500 جريمة سيبرانية مسجلة لدى أجهزة الشرطة، أن أكثر من 80 في المائة من

[1] Europol (2021), **Internet Organized Crime Threat Assessment (IOCTA)** 2021, Publications Office of the European Union, Luxembourg.

الجريمة الرقمية تستلزم الآن بعضا من أشكال النشاط المنظم، وبلغت نسبة الجريمة المنظمة التي تحتوي على جريمة إلكترونية 90 بالمائة كتقدير أعلى[1].

وهذا يؤكد ما انتهى إليه مكتب الأمم المتحدة المعني بالمخدرات والجريمة في خلاصة لقضايا الجريمة المنظمة، أن وجود جماعة إجرامية منظمة يعتبر عاملا متأصلا في جميع قضايا الجريمة السيبرانية التي تناولتها الخلاصة، حيث أن دور القراصنة المنفردين باعتبارهم اللاعبين الأساسيين في الجريمة السيبرانية أصبح محدودا. كما أشارت الخلاصة أيضا إلى أن طبيعة الجريمة السيبرانية تتطلب بالضرورة تنظيم العديد من الوسائل والموارد البشرية.[2]

سنعرض فيما يلي إلى التصنيفات المرجحة للفاعلين في الجريمة الإلكترونية المنظمة، وكذا مختلف الأسواق التي ينشطون فيها:

الفرع الأول: تصنيف المجموعات في الجريمة الإلكترونية المنظمة

لا يزال مدى تنظيم الجريمة الإلكترونية المنظمة غير معروف إلى حد كبير ، ومع ذلك فقد تم إنشاء نموذج بناء على البيانات المتاحة المتعلقة بالروابط بين الجريمة المنظمة والجرائم الإلكترونية على أساس درجة مشاركة المجموعات في الأنشطة عبر الإنترنت (مقابل الأنشطة غير المتصلة بالإنترنت) وهيكل الجمعيات داخل المجموعة.[3]

وعلى وجه الخصوص، تم تحديد ثلاثة أنواع عامة من المجموعات:

النوع الأول : المجموعات التي تعمل في الغالب عبر الإنترنت وترتكب جرائم الإنترنت ، وتضطلع هذه المجموعة بنشاطات واسعة تركز على البيئات الرقمية أو توجه هذه النشاطات نحوها. ويمكن تقسيمها أيضا إلى قسمين: أسراب متمحورة على الانترنت لكن هياكلها معزولة مثل القراصنة، وموزعين مركزيين متمحورين على الانترنت لكن هياكلهم مرتبطة.[4]

ويكمن الفرق بين القسمين، أن الطبيعة غير المترابطة للأسراب وانحرافها عن المركز في ظل عدم وجود قيادة واضحة، تشكل عائقا أمام حفظ الأمن والنظام العام في كشفها. ورغم ذلك يسهل اختراقها بسبب ضوابط الالتحاق بها التي تعد ضعيفة لأنها مشكلة غالبا من هواة. وعلى العكس من ذلك، تواجه هيئات حفظ الأمن صعوبة بالغة في اختراق الموزعين المركزيين، بسبب هيكلتها القيادية الواضحة.[5]

[1] Smith M.c.v., and Paul Jck., **Organized crime in digital a**ge, Winstly magazine for legal research, London, T (3) 32, 2020, p 514.

[2] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، خلاصة سنة 2013، ص 65.

[3] BAE Systems Detica and London Metropolitan University (2012). **Organised Crime in the Digital Age**. *Norton Cybercrime Report 2011.*

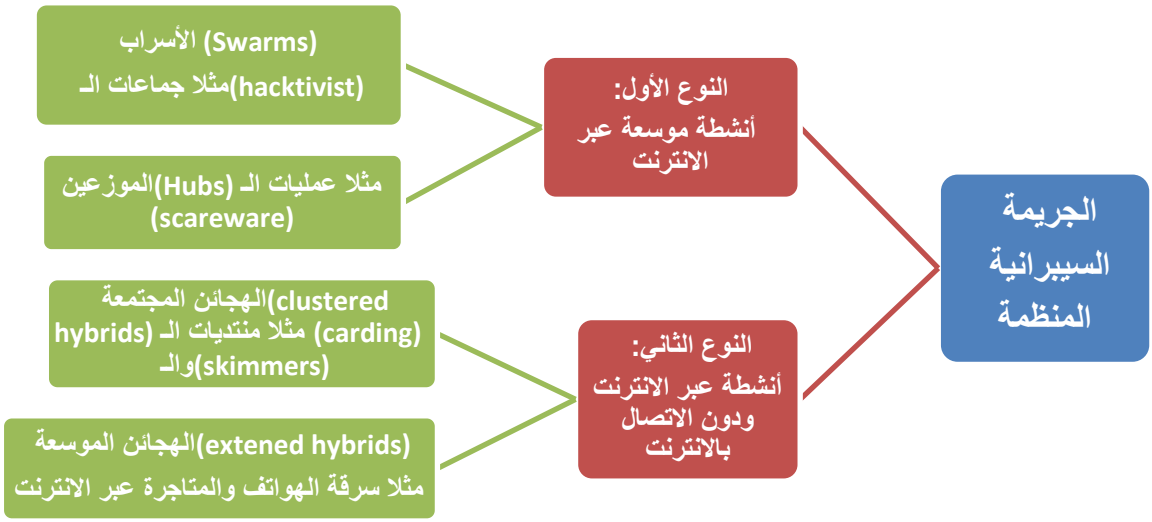
[4] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، خلاصة سنة 2013، ص 66.

[5] نفس المرجع، ص 66.

النوع الثاني: تلك التي تعمل خارج الإنترنت وعبر الإنترنت وتنخرط في الجرائم والجرائم الإلكترونية ، وتباشر أنشطة تنتقل بين برامج على الشبكة وأخرى دون الاتصال بها. وهذا النمط من الجماعات الإجرامية يكون منسقا بعض الشيء، لأنها في الأساس شبكات تقليدية يمتد جزء من نشاطها عبر الشبكة.

وهاذين النوعين مبينين في الشكل المرفق أدناه.

النوع الثالث : وأولئك الذين يستخدمون تكنولوجيا المعلومات والاتصالات فقط لتسهيل الجرائم غير المتصلة بالإنترنت.



هياكل الجماعات في الجريمة الإلكترونية المنظمة، المصدر: BAE DETICA/LMU

الفرع الثاني: أسواق الجريمة الإلكترونية المنظمة

إن تحليل الهياكل التنظيمية للجرائم ذات الدافع المالي مثل سرقة بيانات البطاقات المصرفية وبطاقات الإئتمان يمكننا من تحديد خصائص السوق السوداء للجريمة السيبرانية المنظمة، حيث يؤدي فيها أفراد الجماعة أدوارا مختلفة وقد تكون متعددة من بينهم:

- المبرمجون programmers
- الموزعون distributers
- الخبراء التقنيون technical experts
- القراصنة hackers
- المحتالون fraudsters
- المستضيفون hosters
- الصرافون cashers

- نقلة الأموال money mules
- والزعماء leaders [1]

كما تتفاعل هذه الجماعات مع عدة مجالات أخرى، كإعداد البرمجيات الخبيثة والتحكم في شبكات حاسوب مصابة برسائل التصيد الاحتيالي، وإدارة شبكات الروبوت، والحصول على البيانات الشخصية والمالية والمتاجرة بالبيانات المالية.[2]

كما تعتبر البيانات السرية أحد الأساليب التي تستخدمها الجماعات المنظمة لتبادل المعلومات والتوسط في بيع الخدمات الاستشارية وخدمات الانتشار والفيروس، وتأجير شبكة الروبوت وخدمات البريد الإلكتروني الطفيلي والاستضافة والتفاصيل المالية. وعلاوة على ذلك، يمكن لمثل هذه الأسواق أن تضم عددا كبيرا من الأفراد والمنظمات العابرة للدول، لا سيما في حالة مهربي الأموال والأعمال والمعاملات التجارية المشبوهة مثل استئجار الروبوتات لارتكاب الهجمات ضد نظم المعلومات وسرقة البيانات والتي تعرض بتكلفة منخفضة نسبيا لا تتجاوز الألف دولار شهريا وتعد تكلفة بسيطة مقارنة مع المكاسب المالية المحتملة التي قد تصل إلى عشرات الملايين من الدولارات.[3]

المبحث الثاني: مكافحة أنشطة الجريمة الإلكترونية المنظمة

المطلب الأول: أنشطة الجريمة الإلكترونية المنظمة

تتعدد وتتنوع الأنشطة التي يمارسها الفاعلون في الجرائم الإلكترونية المنظمة ، بما في ذلك الاحتيال، والقرصنة، وإنشاء البرامج الضارة وتوزيعها، وهجمات DDoS، والابتزاز، وجرائم الملكية الفكرية مثل بيع المنتجات المقلدة أو المزيفة ذات العلامات التجارية الرائجة (مثل الملابس والإكسسوارات والأحذية والإلكترونيات والمنتجات الطبية وقطع غيار السيارات وما إلى ذلك) والملصقات والحزم وأي تصميمات أخرى لتحديد هذه المنتجات.[4] ومن نافلة القول أن هذه الجرائم تسبب ضررا نفسيا وماليا واقتصاديا وحتى جسمانيا لا سيما الأجهزة الإلكترونية المقلدة وقطع غيار السيارات، وخصوصا المنتجات الطبية المزيفة، وقد تستعمل العائدات في تمويل أنشطة إجرامية أخرى كالإرهاب مثلا.

يمكننا عرض مجمل الأنشطة الإجرامية في النقاط التالية:

---

[1] Haysom, Simone (2018). **Digitally Enhanced Responses: New horizons for combating online illegal wildlife trade**. *Global Initiative Against Transnational Organized Crime*, p. 11

[2] Fortinet, 2013. Fortinet 2013 **Cybercrime Report**; Panda Security, 2010. **The Cybercrime Black Market:** Uncovered; and Group IB, 2011. **State and Trends of the Russian Digital Crime Market**.

[3] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، خلاصة سنة 2013، ص 69.

[4] Albanese, Jay (2018**). Cybercrime as an Essential Element in Transnational Counterfeiting Schemes**. Presentation at *International Academic Conference: Linking Organized Crime and Cybercrime.* A conference hosted by Hallym University and sponsored by the United Nations Office on Drugs and Crime (UNODC), 8 June 2018, p. 13.

1. تقديم خدمات تسهل الجرائم والجرائم الإلكترونية للآخرين: (الجريمة كخدمة)

تقدم الجماعات الإجرامية التي تشارك في الجريمة الإلكترونية المنظمة خدمات تسهل الجرائم والجرائم الإلكترونية، مثل البيانات ووثائق الهوية (مثل البيانات المالية والصحية وجوازات السفر وهويات تسجيل الناخبين)؛ البرامج الضارة (على سبيل المثال، المصممة حسب الطلب أو البرامج الضارة مثل زيوس وحصان طروادة المصرفي والمصمم لالتقاط التفاصيل المصرفية للمستخدمين وغيرها من المعلومات اللازمة لتسجيل الدخول إلى الحسابات عبر الإنترنت)، هجمات رفض الخدمة الموزعة (DDoS) وخدمات الروبوتات، أدوات التصيد ودروس القرصنة ومعلومات حول نقاط الضعف واستغلال الثغرات وإرشادات حول كيفية الاستفادة منها.[1]

وكمثال على ذلك، تم طرح للبيع البرنامج الضار الشهير Butterfly Bot عبر الإنترنت باعتباره قادرا على التحكم في أجهزة الكمبيوتر التي تعمل بنظام Windows و Linux، والذي أدى في النهاية إلى إصابة 12.7 مليون جهاز كمبيوتر حول العالم.[2]

2. تقديم خدمات الاستضافة: [3]

يوفر المجرمون الإلكترونيون المنظمون خدمات الاستضافة المضادة للرصاص، والتي تمكن المجرمين من استخدام الخوادم لارتكاب جرائم الإنترنت ولا تزيل المحتوى الإجرامي من هذه الخوادم . والسبب هو انخفاض الثقة في المعاملات الإجرامية عبر الإنترنت ووجود محتالين، فإن الطلب على خدمات الضمان التي تقدمها الجماعات الإجرامية المنظمة عبر الإنترنت مرتفع. تتيح خدمات الضمان هذه إرسال الأموال التي يدفعها العملاء المجرمون مقابل سلع وخدمات غير مشروعة فقط بعد تأكيدهم أن السلع أو الخدمات التي دفعوا مقابلها قد تم استلامها في حالة جيدة.

3. تشفير عملات الدفع:

يتم شراء السلع والخدمات غير المشروعة أساسا باستخدام العملة الرقمية المشفرة لأسباب أمنية، فهناك العديد من العملات المشفرة في السوق (مثل Bitcoin و Litecoin و Dogecoin و Ethereum و Monero). بينما تستخدم معظم أسواق الشبكة المظلمة Bitcoin بشكل أساسي، حيث تستخدم بعض مواقع الويب المظلمة ما يعرف باسم "البهلوان" ، والذي يرسل جميع المدفوعات من خلال سلسلة معقدة وشبه عشوائية من المعاملات الوهمية مما يجعل من المستحيل تقريبا تتبع الدفع بأية عملة مشفرة تغادر الموقع.[4]

---

[1] Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab and Steve Chon (2014). **Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime**; *International Journal of Cyber Criminology*, Vol 8(1), pp. 1-20.

[2] *Ibid.*

[3] National Cyber Security Centre (2017). ***Cyber crime: Understanding the online business model***., p.8.

[4] Albanese, Jay., *Op. Cit., p*. 25.

4. غسيل الأموال:

علاوة على ذلك، يوفر مجرمو الإنترنت المنظمون أيضا غسيل الأموال كخدمة ، حيث ينطوي غسل الأموال على ثلاث مراحل: وضع العائدات غير المشروعة في النظام المالي (الإيداع)، وإخفاء مصدر الأموال غير المشروعة، وإعادة إدخال الأموال في الاقتصاد مع إخفاء المنشأ (التكامل) . لكن، يتم غسل الأموال باستخدام العملة الرقمية (أي العملة غير المنظمة المتاحة فعليا فقط) ، وكذلك باستخدام بطاقات الائتمان والخصم المدفوعة مسبقا (حتى البطاقات القائمة على Bitcoin)، بطاقات الهدايا ، الحسابات المصرفية الخاضعة للسرية المصرفية، أو بلسم مزيف أو حسابات مصرفية لشركة وهمية، حسابات PayPal، مواقع الألعاب عبر الإنترنت (عبر عملة الألعاب الافتراضية)، ومواقع المقامرة غير المشروعة.

وحسب تقرير Europol يستخدم المجرمون الإلكترونيون عمليات تبادل العملات المشفرة شبه الآلية (المعروفة باسم المبادلات) والتبادلات اللامركزية (نظير إلى نظير)، والتي لا تتطلب تحديد هوية المستخدمين والتحقق منها لغسل العائدات الإجرامية . كما وجد المجرمون الإلكترونيون المنظمون طرقا جديدة ومبتكرة لغسيل الأموال، مثل "رحلات الأشباح" الخاصة بأوبر (أي يتلقى السائقون أموالا من مبييض الأموال لقبول طلبات الركوب من حسابات أوبر بسعر محدد مسبقا دون استخدام الغاسلين للخدمة فعليا) ، والإيجارات المزيفة عبر Airbnb (على سبيل المثال، يدفع مبيضو الأموال لمالكي Airbnb دون الإقامة في ممتلكاتهم). وزيادة على ذلك ينخرط المجرمون الإلكترونيون المنظمون في عمليات غسيل متناهية الصغر "وهي عملية يقوم بموجبها المجرمون بغسل مبالغ كبيرة من الأموال من خلال الانخراط في العديد من المعاملات الصغيرة" عبر الإنترنت، ويمكن أن تحدث هذه الأنواع من المعاملات على المواقع التجارية ومواقع المزادات وحتى مواقع التوظيف. [1]

5. تسهيل أنشطة الجريمة المنظمة غير التقليدية:

يستخدم المجرمون الإلكترونيون المنظمون تكنولوجيا المعلومات والاتصالات (ICT) لتسهيل أشكال مختلفة من أنشطة الجريمة المنظمة التقليدية غير المتصلة بالإنترنت، مثل تهريب المهاجرين والاتجار بالأشخاص والحياة البرية والمخدرات والأسلحة النارية والاتجار بالسجائر والقطع الأثرية المهربة.

كما يتم استخدام تكنولوجيا المعلومات والاتصالات من قبل المتاجرين بالبشر لتحديد الضحايا وتجنيدهم باستخدام وعود كاذبة بالعمل والشهرة والحب، والإعلان عن الضحايا، والتواصل مع العملاء والمتاجرين الآخرين، وتخطيط وتنظيم وترتيب الاجتماعات بين العملاء والضحايا، ومراقبة أماكن وجود الضحايا والتحكم فيهم. [2]

المطلب الثاني: سبل منع الجريمة الإلكترونية المنظمة

[1] Europol, *Op. Cit.p. 8.*

[2] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، خلاصة سنة 2013، ص 79.

قصد مكافحة الجرائم الإلكترونية المنظمة يجب أن توزع الجهود على عدة مستويات، بدء بتعزيز التدابير والجهود على مستوى سلطات إنفاذ القانون والتشريع والقضاء، ثم الحلول التقنية، وأخيرا ما يتعلق بالحملات التثقيفية والتوعوية.

الفرع الأول: تدابير على مستوى العدالة الجنائية

1. يجب أن لا تكتفي تدابير التصدي للجريمة السيبرانية بالبلاغات التي يقدمها الضحايا فقط، بل بتحقيقات استباقية سرية استراتيجية على المدى المتوسط والبعيد، تركز على أسواق الجريمة ومدبري المخططات الإجرامية. وكمثال على ذلك، فإن سلطات إنفاذ القانون في الدول المتقدمة قد شاركت في تحقيقات متوسطة وطويلة الأجل، عن طريق وحدات سرية تستهدف المجرمين على مواقع التواصل الاجتماعي وغرف المحادثة والرسائل الفورية وخدمات النظراء P2P. حيث تم اختراق منتديات قرصنة بطاقات الائتمان عبر الانترنت، واستخدام البحث الجنائي لفحص المنتديات المتخصصة في استغلال القصر في المواد الإباحية، وفحص خوادم القيادة والسيطرة للبرمجيات الخبيثة.

2. تحيين التشريعات والأطر القانونية التي تعزز من صلاحيات الاختراق والتنكر والتحقيق في الجريمة السيبرانية، بما يشمل طرائق التفتيش والمصادرة والأوامر القضائية للحصول على البيانات الحاسوبية وجمع البيانات والتحفظ عليها في الوقت الحقيقي.[1]

3. رفع مستوى التخصصات القضائية في الجريمة السيبرانية، إذ أظهر تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن أكثر من 40 في المائة من بلدان العالم يتولى فيها قضاة و مدعون لا يتمتعون بمهارات أساسية في تكنولوجيا المعلومات والمعدات الحاسوبية متوسطة، النظر في أغلب قضايا الجريمة السيبرانية.[2]

4. تعزيز التعاون الدولي في قضايا الجريمة المنظمة عبر الانترنت: وذلك في شكل تدريب وتبادل المعرفة فيما يتعلق بالتحقيقات المتعلقة بالجرائم الإلكترونية المنظمة . ومن الأمثلة على ذلك عمليات إنفاذ القانون المشتركة بين الولايات المتحدة وهولندا (عملية Bayonet) عندما تم الاستيلاء على AlphaBay، هاجر المستخدمون (البائعون والمشترين) للمنصات إلى سوق تشفير آخر Hansa، والتي كانت تحت سيطرة الشرطة الهولندية التي كانت تجري عملية سرية لتحديد وتعطيل الأنشطة غير المشروعة المرتكبة على موقع darknet فمكنت هذه الهجرة السلطات الهولندية من تحديد هؤلاء الأفراد والتحقيق معهم قبل إغلاق المنصة في يوليو 2017.[3]

5. ضرب البنية التحتية للمجرمين الإلكترونيين المنظمين: فعلاوة على ترصد الأسواق الإجرامية لهم، ينبغي على هيئات إنفاذ القانون عدم إغفال أولئك الذين يقدمون تسهيلات لمجرمي الانترنت كي لا يفلتوا من

[1] نفس المرجع، ص 190-192.
[2] نفس المرجع، ص 248.
[3] Europol, 2018, *Op. Cit*. p. 36.

العقاب. مثل المواقع المستضيفة، ومنشئي حاجب المواقع VPN، وتجار العملات المشفرة غير المشروعة، ومنصات غسيل الأموال، وتطبيقات الدردشة المشفرة التي يستخدمها مجرمو الانترنت المنظمون.[1]

الفرع الثاني: الحلول التقنية

1. استخدام بعض الحلول التكنولوجية لمواجهة الجريمة الإلكترونية المنظمة. كاستخدام برامج الإنذار اللغوي لاكتشاف اللغة في الاتصالات والمحادثات والرسائل التي تشير إلى بعض الجرائم . على سبيل المثال، يستخدم تجار البشر الرموز التعبيرية (على سبيل المثال ، القلب المتنامي) لتصوير قاصر يتم الإعلان عنه. أو استخدام كلمات إبداعية لبضائعهم، على سبيل المثال، بالنسبة لكلمة" عاج "، قد يستخدم البائع كلمة" ivoree، ivori"" أو " i v o ry" أو " iv * ry" أو استخدام بعض المصطلحات مثل "البلاستيك الأبيض" للإشارة إلى العاج أو "البلاستيك الأسود" للإشارة إلى قرن وحيد القرن.

كما يمكن استعمال تقنية التعرف على الوجوه لتحديد الأشخاص المتجر بهم، والأطفال الذين تم استغلالهم جنسيا، أو يمكن أيضا استخدام برامج التعرف على الصور للتعرف على الحيوانات البرية والسلع غير المشروعة، مثل المخدرات أو الأسلحة النارية. يمكن لهذا البرنامج تسريع تحديد البضائع غير المشروعة عبر الإنترنت والإبلاغ عن المحتوى غير المشروع لمراجعته من قبل المشرفين على المنصات عبر الإنترنت.[2]

2. تدريب فنيين متخصصين: فبسبب التطور المتسارع في تكنولوجيات الاتصال تبدو الحاجة ملحة لفنيين أكثر مهارة في تحليل البيانات، وتتبع العملات المشفرة، وفك التشفير.

3. اقتراح تدابير عملية للأمن السيبراني مصممة لتحديد نقاط الضعف ومنع استغلال الثغرات الأمنية على مستوى أجهزة الأفراد والمؤسسات الحكومية والخاصة ، مثل تدابير المصادقة القوية واكتشاف التسلل وحماية التطفل على الأنظمة.

الفرع الثالث: حملات التثقيف والتوعية

1. تكثيف الحملات التثقيفية كأداة لزيادة الوعي بالجريمة الإلكترونية المنظمة، من قبيل إعلام الجمهور بالطرق التي يمكن للأفراد من خلالها حماية أنفسهم من الجرائم الإلكترونية، مثل الاحتيال والبرامج الضارة (أحصنة طروادة، وبرامج التجسس، وبرامج التحكم عن بعد).

2. تكثيف حملات التوعية بالآثار السلبية للجريمة المنظمة عبر الإنترنت ، لتحذير الأفراد من الترويج أو التعامل مع الأسواق المظلمة، كشراء السلع المقلدة عبر الانترنت أو استعمال برمجيات مقرصنة أو أكواد مسروقة.

3. توعية الأفراد بضرورة الالتزام بالتدابير الروتينية للسلامة الإلكترونية، خصوصا:

[1] *Ibid*., p. 40.
[2] European Commission (2016). **The Use of Social Media in the Fight Against Migrant Smuggling.** *European Migration Network (EMN) Inform.*

– إتلاف أية معدات تتعلق بالحواسيب قبل التخلص منها، لأنها عادة تحتوى على معلومات مهمة قد تصل إلى أشخاص غير مصرح لهم الاطلاع عليها.

– عدم ترك الأجهزة الالكترونية مفتوحة وفصل الانترنت عنه في حال عدم الاستخدام.

– تغيير كلمات السر باستمرار، والتأكد من درجة صعوبتها.

– استخدام وسائل الأمان والحماية الحديثة على الأجهزة الإلكترونية كبصمات العين واليد والصوت.

– استخدام وتحيين برامج الكشف عن الفيروسات والجدران النارية.

– تجنب تحميل البرامج مجهولة المصدر.

– تشفير البيانات والملفات المهمة على الحواسيب والهواتف الذكية.[1]

خاتمة

نخلص من خلال هذه الورقة البحثية إلى أن تكتيكات الجماعات الإجرامية المنظمة قد تطورت لتشمل الجرائم الإلكترونية أو لتستخدم تكنولوجيا المعلومات والاتصالات لتسهيل أشكال مختلفة من الجريمة المنظمة. ترتكب تلك الجماعات مجموعة متنوعة من الأنشطة غير المشروعة عبر الشبكة، وتعرف بمواقع الأسواق المظلمة والأسواق المشفرة ، وهي لا توفر السلع والخدمات غير المشروعة فحسب، بل تتيح أيضا لبقية المجرمين التفاعل مع بعضهم البعض، ومشاركة المعرفة والموارد، وتطوير الاتصالات، وبناء العلاقات والحفاظ عليها، وتجنيد الأفراد لارتكاب أعمال غير مشروعة، وغسل الأموال ، وتعلم تقنيات ارتكاب الجرائم والجرائم الإلكترونية، وتشفير العملات والتهرب من سلطات إنفاذ القانون.

النتائج:

- الجريمة الإلكترونية المنظمة مصطلح يستخدم لوصف الأنشطة المنظمة غير المشروعة في الفضاء السرايبراني.
- تتطلب العديد من أفعال الجريمة الإلكترونية درجة عالية من التنظيم والتخصص، إذ يرجح ارتفاع ضلوع الجماعات الإجرامية المنظمة التقليدية في ارتكاب جرائم إلكترونية، على الأقل بدوافع مالية مثل استخدام الحاسوب في الاحتيال والتزوير والاعتداء على الهوية. وقد أوضحت إحدى الدراسات الحديثة والتي أجرت استعراضا لعينة من 500 جريمة سيبرانية مسجلة لدى أجهزة الشرطة، أن أكثر من 80 في المائة من الجريمة الرقمية تستلزم الآن بعضا من أشكال النشاط المنظم، وبلغت نسبة الجريمة المنظمة التي تحتوي على جريمة إلكترونية 90 بالمائة كتقدير أعلى.

[1] عبير أبو دية، مرجع سابق، ص: 18.

- يمكن تقسيم المجرمين الإلكترونيين المنظمين إلى أسراب متمحورة على الانترنت لكن هياكلها معزولة مثل القراصنة، وموزعين مركزيين متمحورين على الانترنت لكن هياكلهم مرتبطة.
- تتضمن الهيكلية التنظيمية للجرائم السيبرانية المنظمة ذات الطابع المالي أدوارا متعددة مثل: المبرمجون، الموزعون، الخبراء التقنيون، القراصنة، المحتالون، المستضيفون، الصرافون، نقلة الأموال والزعماء.
- تتفاعل هذه الجماعات مع عدة مجالات أخرى، كإعداد البرمجيات الخبيثة والتحكم في شبكات حاسوب مصابة برسائل التصيد الاحتيالي، وإدارة شبكات الروبوت، والحصول على البيانات الشخصية والمالية والمتاجرة بالبيانات المالية.
- كما تعتبر البيانات السرية أحد الأساليب التي تستخدمها الجماعات المنظمة لتبادل المعلومات والتوسط في بيع الخدمات الاستشارية وخدمات الانتشار والفيروس، وتأجير شبكة الروبوت وخدمات البريد الإلكتروني الطفيلي والاستضافة والتفاصيل المالية.
- تتعدد وتتنوع الأنشطة التي يمارسها الفاعلون في الجرائم الإلكترونية المنظمة ، بما في ذلك الاحتيال، والقرصنة، وإنشاء البرامج الضارة وتوزيعها، وهجمات DDoS، والابتزاز، وجرائم الملكية الفكرية مثل بيع المنتجات المقلدة أو المزيفة ذات العلامات التجارية الرائجة (مثل الملابس والإكسسوارات والأحذية والإلكترونيات والمنتجات الطبية وقطع غيار السيارات وما إلى ذلك) والملصقات والحزم وأي تصميمات أخرى لتحديد هذه المنتجات. وقد تستعمل العائدات في تمويل أنشطة إجرامية أخرى كالإرهاب مثلا.
- تمتد الأنشطة الإلكترونية المنظمة لتشمل: تقديم خدمات تسهل الجرائم والجرائم الإلكترونية للآخرين/ الجريمة كخدمة – تقديم خدمات الاستضافة – تشفير عملات الدفع – غسيل الأموال – تسهيل أنشطة الجريمة المنظمة غير التقليدية –
- قصد مكافحة الجرائم الإلكترونية المنظمة يجب أن توزع الجهود على عدة مستويات، بدء بتعزيز التدابير والجهود على مستوى سلطات إنفاذ القانون والتشريع والقضاء، ثم الحلول التقنية، وأخيرا ما يتعلق بالحملات التثقيفية والتوعوية.

التوصيات:

– تكثيف البحوث المنهجية حول طبيعة نشاط المنظمات الإجرامية في الفضاء الإلكتروني.
– دعم منع الجريمة وتدابير العدالة الجنائية في مجال الجريمة الإلكترونية السيبرانية المنظمة، لاسيما تحميل مؤسسة حكومية رائدة مسؤولية القيادة وتنسيق المبادرات وتعزيز الموارد لمكافحة الجريمة السيبرانية المنظمة.

- تحيين التشريعات والأطر القانونية التي تعزز من صلاحيات الاختراق والتنكر والتحقيق في الجريمة السيبرانية، بما يشمل طرائق التفتيش والمصادرة والأوامر القضائية للحصول على البيانات الحاسوبية وجمع البيانات والتحفظ عليها في الوقت الحقيقي.
- تشكيل فرق التصدي للطوارئ الحاسوبية، مهمتها تحديد نقاط ضعف أنظمة الاتصالات وكذا التصدي لحوادث الأمن الحاسوبي.
- تمكين التعاون بين الدول في المسائل الجنائية التي تنطوي على جرائم سيبرانية وأدلة إلكترونية.

المراجع:

1) *Steve Morgan, Special Report:* ***Cyberwarfare In The C-Suite****, – Nov. 13, 2020,* Cybercrime Magazine on cybersecurityventures.com.
2) McCusker, R.,**Transnational organised crime: Distinguishing threat from reality**, Crime Law and Social Change 46, 2006.
3) Revue internationale de droit pénal, **La cybercriminalité,** Éditeur : Érès, 2006/3-4 (Vol. 77).
4) أحمد عبد المحسن بدوي محمد، **مشكلات الإعلام الجديد** ، أبحاث المؤتمر الدوني الإعلام الجديد: تكنولوجيا جديدة لعالم جديد، جامعة البحرين، من 7 إلى 9 أفريل 2009، المنامة: منشورات جامعة البحرين، 2009.
5) عبير مجني أبو دية، **الجرائم الإلكترونية –دراسة نظرية** ، الملتقى الخامس للرابطة العربية للبحث العلمي وعلوم الاتصال بعنوان: إشكالية المصطلح في علوم الإعلام والاتصال في العالم العربي، بيروت من 29 إلى 1 ديسمبر 2018.
6) Williams, P.,**Organized crime and cyber-crime: Implications for business**, Available at: http://www.cert.org/archive/pdf/cybercrime-business.pdf, 2002.
7) مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، **التقرير المال والبيانات المالية المراجعة لفترة السنتين المنتهية في 31 ديسمبر 2013 وتقرير مجلس مراجعي الحسابات،** الوثائق الرسمية للأمم المتحدة، نيويورك، 2014.
8) مكتب الأمم المتحدة المعني بالمخدرات والجريمة فيينا، **اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة بها،** الوثائق الرسمية للأمم المتحدة، نيويورك، 2004.
9) Europol (2021), **Internet Organized Crime Threat Assessment (IOCTA)** 2021, Publications Office of the European Union, Luxembourg.

10) Smith M.c.v., and Paul Jck., **Organized crime in digital a**ge, Winstly magazine for legal research, London, T (3) 32, 2020.

11) BAE Systems Detica and London Metropolitan University (2012). **Organised Crime in the Digital Age**. *Norton Cybercrime Report 2011.*

12) Haysom, Simone (2018). **Digitally Enhanced Responses: New horizons for combating online illegal wildlife trade**. *Global Initiative Against Transnational Organized Crime.*

13) Fortinet, 2013. Fortinet 2013 **Cybercrime Report**; Panda Security, 2010. **The Cybercrime Black Market:** Uncovered; and Group IB, 2011. **State and Trends of the Russian Digital Crime Market**.

14) Albanese, Jay (2018). **Cybercrime as an Essential Element in Transnational Counterfeiting Schemes**. Presentation at *International Academic Conference: Linking Organized Crime and Cybercrime.* A conference hosted by Hallym University and sponsored by the United Nations Office on Drugs and Crime (UNODC), 8 June 2018.

15) Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab and Steve Chon (2014). **Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime**; *International Journal of Cyber Criminology*, Vol 8(1).

16) National Cyber Security Centre (2017). ***Cyber crime: Understanding the online business model.***

17) European Commission (2016). **The Use of Social Media in the Fight Against Migrant Smuggling**. *European Migration Network (EMN) Inform.*

فراقة رمضان
fraga.ramdane@gmail.com
جامعة 08 ماي 1945 قالمة

رقطي منيرة
mounirarogti24@gmail.com
جامعة 08 ماي 1945 قالمة

جرائم الاحتيال على وسائل الدفع الالكتروني
وتأثيرها على كل من التجارة الالكترونية والتنمية الاقتصادية

ملخص:

إذا كان النمو السريع في انتشار استخدام وسائل الدفع الالكترونية عبر الإنترنت وأجهزة الاتصال الحديثة لديه القدرة على المساهمة في التنمية الاقتصادية والاجتماعية للدول، فإنه من ناحية أخرى منح فرصًا للمجرمين لاستغلال الثغرات الأمنية في البيئة المعلوماتية، فأصبحوا يهددون التجارة الالكترونية عن طريق اساليب الاحتيال التي تأخذ منحى متصاعدا، بالرغم من محاولات تطوير الأساليب والآليات الأمنية لحماية بيانات وبطاقات دفع المستخدمين، فأصبح مستخدمو بطاقات الدفع الإلكترونية عرضة للاحتيال من طرف قراصنة الانترنت، عن طريق سرقة بياناتهم واستخدامها في تحويل أموالهم ، أو استخدام تلك البيانات لشراء أغراض لصالحهم عن طريقها.

Abstract:

If the rapid growth in the spread of the use of electronic means of payment via the Internet and modern communication devices has the potential to contribute to the economic and social development of countries, on the other hand it has given opportunities to criminals to exploit security gaps in the information environment, and they have become a threat to electronic commerce through fraudulent methods that take an escalating trend, despite attempts to develop security methods and mechanisms to protect users' data and payment cards. Users of electronic payment cards have become vulnerable to fraud by hackers, by stealing their data and using it to transfer their money, or using that data to buy items for their own benefit.

مقدمة

عرفت الوسائل التكنولوجية والتقنية تطورا كبيرا في العقود الأخيرة، وقد دفعت هذه الطفرة العلمية في الوسائل التقنية إلى ضرورة الاستفادة منها في شتى المجالات التي تمس حياة الإنسان، بل أنها أرغمته على ضرورة استغلالها والاستفادة من خدماتها لما تقدمه من تسهيلات وما تتيحه من إمكانيات، سواء من حيث

سرعة المعاملات أو من حيث جودتها، بسبب ما توفره من وقت ومال باعتبارهما أهم العناصر المؤثرة والفاعلة في الاقتصاد.

ولا شك أن المؤسسات الحكومية وغير الحكومية إلى جانب الأفراد، كلها تسعى إلى توفير الوقت والمال من أجل إحداث فعالية أكبر وتحقيق عوائد مالية أفضل، ما دفعها لاستغلال كل الوسائل التقنية للوصول إلى غاياتها، وهذا مهد لظهور التجارة الإلكترونية وانتشارها في كل دول العالم، تزامنا مع التطورات التي حصلت في النظم المصرفية التي واكبت هي الأخرى التطورات التقنية وادخالها في تسيير أجهزتها المالية ، وهذا ما يساهم في إحداث التنمية في شتى المجالات الاقتصادية والاجتماعية .

ف الثورة التكنولوجية الحديثة في مجال الأجهزة والبرمجيات والاتصالات، فرض ت أشكالا جديدة من المعاملات المرتبطة بالاقتصاد والمعلومات، ومن أبرز هذه الأشكال التجارة الإلكترونية المتعلقة بتنفيذ كل ما يتصل بعمليات شراء وبيع السلع والخدمات والمعلومات عبر شبكة الانترنت والشبكات التجارية الأخرى التي تعتمد اساسا على استعمال وسائل الدفع الالكترونية التي أصبحت تتيحها أغلب البنوك الوطنية والدولية ، ومن خلال تبادل البيانات إلكترونيا دون ضرورة التنقل الشخصي أو التبادل التقليدي للوثائق والعملات النقدية.

غير أنه وإذا كان النمو السريع في انتشار استخدام وسائل الدفع الالكترونية عبر الإنترنت وأجهزة الاتصال الحديثة لديه القدرة على المساهمة في التنمية الاقتصادية والاجتماعية للدول، فإنه من ناحية أخرى منح فرصًا للمجرمين لاستغلال الثغرات الأمنية في البيئة المعلوماتية، ليجعل من الجرائم الالكترونية الواقعة نتيجة الاستغلال الغير شرعي لهذه الوسائل له من التأثير على الجانب الاقتصادي، خاصة نتيجة ما يمر به الاقتصاد العالمي نتيجة العولمة وتحرير التجارة الدولية وتحول الاقتصاد العالمي من مرحلة الاقتصاد التقليدي إلى مرحلة الاقتصاد الرقمي ، مما أدى إلى تصاعد خطورة الجرائم الإلكترونية واتساع حجمها ، فلقد أصبحت تسبب هذه الاخيرة تهديدا حقيقيا للأمن المجتمعي والاقتصاد من خلال عمليات الاحتيال والسرقة والقرصنة التي تتم من خلال شبكة الانترانت[1].

من هذا المنطلق وأمام ما تحمله هذه الوسائل كأدوات لممارسة التجارية الكترونية من أهمية قصوى من جهة، وما يقابلها من خطورة وجب تسليط الضوء عليها من جهة أخرى، تتبادر لأذهاننا إشكالية تطرح نفسها في هذا المجال، تمت صياغتها على النحو التالي:

– ما مدى تأثير الاستخدام الغير شرعي والاحتيالي لوسائل الدفع الالكترونية على فعالية الممارسات التجارية الالكترونية، وتأثير ذلك على مدى سيرورة عجلة التنمية الاقتصادية؟

تتفرع عن هذه الاشكالية العديد من التساؤلات الفرعية نذكر منها:

– ما المقصود بوسائل الدفع الالكتروني؟ وماهي أهم الجرائم الواقعة عند الاستخدام الغير شرعي لهذه الوسائل ؟

[1]- صراع كريمة ، دقيش جمال، الأبعاد الاقتصادية للجريمة الإلكترونية، مجلة الدراسات التسويقية وإدارة الأعمال، المجلد2-العدد1 ، جانفي 2018، ص 35.

- ماهي أهم الانعكاسات السلبية لهذه التجاوزات على كل من التجارة الالكترونية كضرورة حتمية فرضتها معطيات وتطورات الثورة الصناعية والتكنولوجية عبر العالم؟
- وكيف أثرت هذه الجرائم بالتوازي على سيرورة عجلة التنمية الاقتصادية الوطنية من جهة والعالمية من جهة أخرى؟
- وكيف يمكن مواجهة هذه الجرائم ومكافحتها سعيا للحد من تأثيراتها؟

للاجابة على هذه التساؤلات ارتأينا تقسيم دراستها إلى محورين اثنين:

المحور الأول: تجريم المساس بوسائل الدفع الالكتروني

أولا: مفهوم وأدوات نظام الدفع الإلكتروني.

ثانيا: الجرائم الواقعة على وسائل الدفع الالكتروني .

المحور الثاني: انعكاسات الاستخدام الاحتيالي لوسائل الدفع الالكتروني على الممارسات التجارية وعجلة التنمية الاقتصادية.

أولا: الأبعاد الاقتصادية لجرائم الدفع الالكتروني وتأثيرها على فعالية العملية التجارية الالكترونية وانعكاس ذلك على التنمية الاقتصادية .

ثانيا: أساليب وآليات مكافحة الجرائم الواقعة على وسائل الدفع الالكترونية .

المحور الأول: تجريم المساس بوسائل الدفع الالكتروني

أصبح العالم اليوم أكثر ارتباطًا رقميًا من أي وقت مضى ، وهذا ما مكن المجرمين من الاستفادة من هذا التحول باستهداف نقاط الضعف في الأنظمة والشبكات والبنية التحتية عبر الإنترنت ، ما يشكل تهديدا اقتصاديا واجتماعيا هائلا على الحكومات والشركات والأفراد في جميع أنحاء العالم.

و يعد التصيد الاحتيالي وبرامج الفدية وخروقات البيانات مجرد أمثلة قليلة على التهديدات الإلكترونية الحالية، بينما تظهر أنواع جديدة من الجرائم الإلكترونية في كل وقت ، فإن مجرمي الإنترنت يتسمون بالمرونة والتنظيم بشكل متزايد ويستغلون التقنيات الجديدة ويخصصون هجماتهم ويتعاونون بطرق جديدة[2].

وبينما لا تعرف الجرائم الإلكترونية حدودًا وطنية ، يمتد خطر المجرمين والضحايا والبنية التحتية التقنية إلى ولايات قضائية متعددة ، مما يثير العديد من التحديات بالنسبة للتحقيقات والملاحقات القضائية.

أولا: مفهوم وأدوات نظام الدفع الإلكتروني

تعمل المصارف الالكترونية على مواكبة التطورات والمستجدات لضمان النجاح والاستمرار، وهي تسعى إلى اكتشاف طرق جديدة أكثر فعالية من تلك المستعملة، كتطوير أنظمة الدفع من أنظمة تقليدية إلى

[2] https://www.interpol.int/Crimes/Cybercrime date of viewing 10/9/2022 at 18 :50

أنظمة دفع إلكترونية، وبذلك فهي تحقق الانتقال السريع من اقتصاد الموجودات إلى اقتصاد المعلومات والأرقام .

1- مفهوم نظام الدفع الإلكتروني

تتضمن العمليات المصرفية تلقي الأموال من الج مهور وعمليات القرض وكذا وضع وسائل الدفع تحت تصرف الزبائن وإدارة هذه الوسائل[3].

ويقصد بنظام الدفع الإلكتروني عمليات التحويل الالكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر بالبنك الذي يوجد به حسابه، وذلك من خلال شبكة التسوية الإلكترونية[4].

ومن بعض التشريعات المقارنة نجد أن المجلس الاقتصادي الفرنسي قد عرف الدفع الالكتروني بأنه:« مجموعة التقنيات الاعلامية، المغناطيسية أو ا لالكترونية ...الخ تسمح بتحويل الاموال دون دعامة ورقية، والتي ينتج عنها علاقة ثلاثية ما بين البنك والبائع والمستهلك»[5].

أما المشرع الجزائري فلم يعرف صراحة نظام الدفع الإلكتروني، لكنه نص صراحة على إمكانية أن يكون الدفع الكترونيا ، كما أعطى بموجب قانون التجارة الالكترونية 18-05 مفهوما لوسيلة الدفع الالكتروني ، حيث جاء فيه:« كل وسيلة دفع مرخص بها طبقا للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد عبر منظومة الكترونية»[6].

فنظام الدفع الإلكتروني هو عبارة عن الصورة أو الوسيلة ا لإلكترونية التقليدية للدفع والتي نستعملها في حياتنا اليومية، أما الفرق الأساسي بين الوسيلتين هو أن وسائل الدفع الالكتروني تتم كل عملياتها وتسير الكترونيا ولا وجود للحوالات ولا للقطع النقدية[7].

2- وسائل نظام الدفع الإلكتروني

---

[3] المادة 66 من القانون 10/90 المتعلق بالنقد والقرض المؤرخ في 1990/4/16 المعدل بموجب الأمر 11/03 المؤرخ في 26/ 2006/6.

[4] د. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، مصر، 2019، ص239

-for further information see also : international chamber of commerce :« Electronic payment services and e-commerce» ISSUES BRIEF Nº 4 , https://iccwbo.org/content/uploads/sites/3/2020/02/icc-issues-brief-4-electronic-payment-services-and-ecommerce.pdf, date of viewing 10/9/2022 at 20 :04

[5] -TOERING Jean Pierre et BRION François , les moyens de paiement ,Edition Presses Universitaires de France - P.U.F 1 ère édition ,Paris , 1999,p32

[6] المادة 5/6 من القانون 18-05 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الالكترونية ، ج ر عدد287 مؤرخة في 16 ماي 2018

[7] عمار لوصيف، استراتيجيات نظام المدفوعات للقرن الحادي و العشرين مع الاشارة للتجربة الجزائرية ، مذكرة ماجستير في العلوم الاقتصادية، جامعة قسنطينة ، 2008-2009 ص 28

- عرف مصطلح «إلكتروني» في قانون المعاملات الالكترونية الاردني بأنه." تقنية استخدام وسائل كهربائية أو مغناطيسية ضوئية أو الكهرومغناطيسية ، أو أي وسائل مشابهة في تبادل المعلومات وتخزينها" المادة 19 من قانون المعاملات الالكترونية الاردني رقم 85 لسنة 2001

وفرت الاجهزة الالكترونية الحديثة وسائل متعددة تستعمل في نظام الدفع الالكتروني نحاول أن نوجزها فيما يلي:

أ- البطاقة الالكترونية

تشمل كل من بطاقة الدفع التي من خلالها يتم تحويل مبلغ من حساب المشتري صاحب البطاقة إلى حساب البائع خلال يوم أو يومين، كما تستخدم في سحب النقود من الحساب ، وكذا بطاقة الصرف التي تقضي بتسديد قيمة المشتريات بمجرد ارسال الفاتورة، أما عن بطاقة الائتمان فهي التي تسمح لحاملها بالحصول على قرض ، حيث من خلالها تقدم تلك البطاقة للتاجر لتسديد ثمن مشترياته، ويقوم التاجر بتحصيل تلك القيمة من الجهة المصدرة التي تقوم بدورها باستيفاء تلك المبالغ من الحامل[8].

ب- البطاقات الذكية

هي بطاقة تحتوي على معالج دقيق يسمح بتخزين الأموال من خلال البرمجة الأمنية، والتأكد من سلامة كل معاملة من الخداع، وهذه البطاقة تستطيع التعامل مع بقية الحواسيب، ولا تتطلب تفويضا أو تأكيدا لصلاحية البطاقة من أجل نقل الأموال من المشتري إلى البائع[9].

ج- الشيكات والتحويلات الالكترونية

يتضمن الشيك امرا من شخص يسمى الساحب إلى البنك المسحوب عليه بأن يدفع مبلغا من النقود لإذن شخص ثالث يسمى المستفيد ، وقد اصبح الشيك الالكتروني هو أكثر الأوراق التجارية التي يمكن الاستفادة منها في مجال التقنيات الالكترونية[10].

والشيك الالكتروني عبارة عن رسالة الكترونية موقعة توقيعا الكترونيا، يرسلها مصدر الشيك إلى المستفيد ليتم تحويل قيمة الشيك إلى حساب المستفيد عن طريق بنك يعمل عبر الانترنت ، والذي يقوم عندئذ بإلغاء الشيك وإعادته إلى الحامل الكترونيا ليتأكد بأنه تم صرف الشيك وتحولت قيمته إلى حسابه[11].

د- النقود الالكترونية

هي العملة التي تخزن إلكترونيًا على مواقع أو أنظمة إلكترونية، أو على قواعد بيانات رقمية خاصة بها، مع العلم بأن قيمة النقود أو العملة الإلكترونية مدعومة بالعملة الإلزامية الورقية، ومن الممكن إجراء التحويل بين العملتين بسهولة، ويطلق على النقود الإلكترونية مسمى النقود الرقمية[12].

---

[8] جلال عابد الشورة، وسائل الدفع الالكتروني، دار الثقافة للنشر والتوزيع ، الأردن، 2008 ،ص 25

– عبد الرحيم وهيبة، إحلال وسائل الدفع المصرفية التقليدية بالإلكترونية دراسة حالة الجزائر، مذكرة لنيل شهادة ماجستير في علوم التسيير، جامعة الجزائر، ص 44

[9] ديمثان المجالي، أسامة عبد المنعم، التجارة الالكترونية، الطبعة 1، دار وائل للنشر، الاردن، 2013 ،ص 215.

[10] عماد الدين بركات، ظ.د/طيبي حوري :« وسائل الدفع الإلكترونية ودورها في تفعيل التجارة الالكترونية» مجلة القانون والتنمية المحلية، العدد 2، 2019 .

[11] كردي نبيلة : «الشيك الالكتروني» مجلة العلوم الاجتماعية والانسانية، مجلد 10، عدد 2، 2017، ص251

ثانيا: الجرائم الواقعة على وسائل الدفع الالكتروني

كشفت آخر الإحصائيات التي تتعلق بتعرض البطاقات البنكية لعمليات القرصنة في جوان 2005 وذلك من طرف شركة ماستر كارد التي صرحت بتعرض أكثر من 40 مليون رقم سري للبطاقات البنكية للاختلاس منها 14 مليون (821000 تعود لأوروبيين و 70000 تعود لفرنسيين) بطاقة تابعة لماستر كارد و20 مليون هي بطاقة تابعة لشركة فيزا كارد، وقد استغل معامل المخترقون ثغرة في نظام الأمان الذي توفره أحد المؤسسات المكلفة بضمان الأمان لمعاملات البطاقة البنكية[13].

من هذه الإحصائيات نلاحظ مدى جسامة الخروقات التي تمس أحد وسائل الدفع الإلكتروني رغم ما توفره المؤسسات التي تقدم الخدمات المتعلقة بهذه البطاقات من أنظمة أمان، وهذا بسب قدرة القراصنة على تكييف مهاراتهم في الاحتيال واختراق أنظمة الأمان باستمرار، باستغلال الوسائل التكنولوجية الاكثر تطورا. ناهيك عن الاستخدام الاحتيالي لوسائل الدفع من قبل بعض أصحابها أنفسهم. لكن للأسف مازالت الكثير من الدول ومنها الجزائر لم تنظم استعمال وسائل الدفع الإلكتروني كما لم تجرم الأعمال غير المشروعة الواقعة عليها، مقابل ما قامت به الدول الأوربية مثلا في هذا الصدد[14].

1- الاستخدام غير الشرعي لوسيلة الدفع من قبل المصدر

تكثر انواع الجرائم التي تمس وسائل الدفع الالكتروني، لذلك سنحاول عرض أهم وأخطر هذه الجرائم والتي تتعلق خاصة بمصدر وسائل الدفع أو التاجر الذي يمكنه سرقة بيانات العميل.

أ- تواطؤ موظف البنك مع العميل

في هذه الحالة يقوم موظف البنك باستخراج بطاقة الدفع الإلكتروني ببيانات مزورة، ويتم منحها لعميل يتواطأ معه على استخراج مبالغ من البنك ، أو يتم استخدامها لفائدة عميل ليس له وجود وتمنح لعميل مع علمه بذلك حتى يستنفذ هو وموظف البنك بالمبالغ التي تنطوي تحت رصيد البطاقة، وتكيف هذه الواقعة علي أنها جريمة للاستيلاء علي أموال البنك دون وجه حق وتزوير للمستندات[15].

ب- تواطؤ موظف البنك مع التاجر

كأن يتفق الموظف مع التاجر فيصرف له قيمة إشعارات البيع وهذا بدافع الاستيلاء علي الأموال، أو

---

[12] أنظر : أ. زكريا مسعودي، ط.د/ الزهرة جقريف :« ماهية النقود الإلكترونية » المجلة الدولية للبحوث القانونية والسياسية، مجلد 2 ، عدد3 ، 2018.

[13] Hélène Puel :« Des milliers de Français victimes du vol de leur numéro de carte bancaire» https://www.01net.com/actualites/ consulter le 11/9/2022 a 22 :55

[14] صليح بونفلة، النظام القانوني للعمليات المصرفية الالكترونية، أطروحة لنيل شهادة الدكتوراه، جامعة قالمة، 2020، ص 325

[15] لبنى عمر سقاوي، المسؤولية المصرفية في الاعتماد المالي، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2006 ،ص252

يقوم موظف البنك باعتماد إشعارات بيع تنسب إلى بطاقة مزورة أو وهمية أو منتهية الصلاحية وهو يعلم بذلك، فيكون بذلك أمام جريمة التزوير[16].

ج- تواطؤ موظف البنك مع الغير

يتفق موظفو البنك مع القراصنة ومنحهم بيانات وسائل الدفع الإلكتروني الصحيحة، وذلك بهدف تقليدها أو صناعتها ولاستعمالها في عمليات السحب والوفاء لدى التجار، أومن خلال أجهزة الصرف الآلي.

2-الاستخدام غير الشرعي للبطاقة من قبل التاجر

تعتبر العلاقة بين التاجر وحامل وسيلة الدفع علاقة تعاقدية، بصفته الجهة التي تقبل البطاقة من حاملها وذلك للدفع بواسطتها مقابل السلع والخدمات المقدمة للعميل، بشرط توقيعه علي إشعارات البيع وشرط وجود تعاقد من أحد المصدرين للبطاقة ، حتى يتم تزويد التاجر بالأجهزة ومستلزمات التشغيل الخاصة بها ، بحيث يقوم التاجر فيما بعد بتحصيل ثمن سندات البيع من المصدر المتعاقد معه[17].

وللتاجر دور كبير في فحص البطاقة والتأكد من صلاحيتها ومن شخصية حاملها وتوقيعه وبالتالي تأكيد الموافقة لإجراء عملية الدفع ، وهذا ما يمنحه مساحة واسعة للتلاعب أو ارتكاب بعض الافعال غير الشرعية كتزوير هذه البطاقات أو التلاعب ببياناتها من خلال استخدام الأجهزة المخصصة لاستعمال وسائل الدفع الإلكتروني.

3- الاستخدام غير الشرعي من قبل الحامل والغير

أ - الاستخدام غير الشرعي من قبل الحامل

تسمح بطاقة الدفع الالكترونية لحاملها الشرعي بسحب النقود لدى الموزعات الآلية أو دفع مقابل المشتريات للتاجر بواسطتها في حدود القيمة المسموح بها من قبل الجهة المصدرة للبطاقة ومن خلال حساب العميل المفتوح لديها. إلا حامل وسيلة الدفع الالكتروني قد يتصرف بسوء نية، فيقوم بسحب مبالغ مالية من أجهزة دفع النقود دون أن يكون له رصيد في حسابه البنكي، أو يقوم بشراء حاجيات تفوق قيمتها قيمة المبلغ المالي لدى البنك المصدر للبطاقة[18]، أو استخدام البطاقة من خارج مدة صلاحيتها.

ب- الاستخدام غير الشرعي من قبل الغير

يعد تزوير وتقليد وسائل الدفع الالكترونية واستعمالها في الاستيلاء على مال الغير من أخطر الاستعمالات غير المشروعة الواقعة عليها، ذلك لأن صاحب وسيلة الدفع يجهل بوقوع التزوير أو التقليد إلا

---

[16] عبد الكريم الردايدة، جرائم بطاقة الإئتمان، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2013 ،ص 61

[17] -أمجد حمدان الجهني ، الاستخدامات الغير مشروعة لبطاقة الدفع الإلكتروني من قبل الغير، مركز الدراسات القضائية، المملكة الأردنية الهاشمية، مقال منشور على الموقع http://www.coiss.com/replay.php ص 148

[18] أمينة بن عميور، البطاقات الالكترونية للدفع والقرض والسحب، مذكرة لنيل شهادة الماجستير في القانون الخاص، كلية الحقوق، جامعة منتوري، قسنطينة، 2005، ص 70

عند نقص رصيده البنكي أو انعدامه، وكذلك الأمر بالنسبة للبنك المصدر، حيث لا يمكن أن ترد البطاقة المزورة على القائمة السوداء نظرا لصعوبة اكتشاف التزوير، كونه جريمة هادئة لا تخلف آثارا تدل عليها، ويرجع ذلك للمهارة العالية لدى مجرمي التقليد، التزوير وقراصنة الانترنت[19].

المحور الثاني: انعكاسات الاستخدام الاحتيالي لوسائل الدفع الالكتروني على الممارسات التجارية وعجلة التنمية الاقتصادية

لا يمكن إنكار المزايا التي قدمتها تكنولوجيا الإعلام والاتصال في كافة مجالات الحياة ، إذ وعلى القدر الذي ساهمت المعلوماتية في النهوض والتقدم والرقي، بقدر ما ساهمت في بروز نوع مستحدث من الإجرام وهو الإجرام المعلوماتي، هذا النوع من الإجرام الذي عرف عدة تسميات ومصطلحات للدلالة عليه ، ومن ذلك الجريمة الإلكترونية، جرائم الحاسوب، جرائم تكنولوجيا الإعلام والاتصال، الجريمة الرقمية، الجريمة السيبرانية ، جريمة الانترنيت.

وبالتالي فالجريمة المعلوماتية تشكل نمط إجرامي مستحدث فرض نفسه على الواقع ، وتعرف على أنها كل سلوك إيجابي أو سلبي تقدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة من أجل تنفيذ فعل إجرامي، ومن هنا فالجريمة تتسم بالحركية والسرعة فهي جريمة عبارة للقارات ، وغير عنيفة[20].

وبعد توضيح أهم الوسائل المعتمدة في عملية الدفع عند ممارسة التجارة الالكترونية ضمن المحور الأول من مداخلنا، وكذا تعداد أهم الجرائم التي قد ترتكب عند الاستخدام الاحتيالي والغير قانوني لهذا الوسائل بصفتها أليات جديدة تعتمد في حركيتها على ضرورة توافر عنصر الائتمان والثقة بين المتعاملين، سنحاول ضمن هذا المحور تسليط الضوء على الانعكاسات السلبية لهذا الاستخدام على التجارة الالكترونية بكل أطرافها (المتسوق والمورد الالكترونين) من جهة ، وتأثير ذلك بالتوازي على سيرورة ومتطلبات التنمية الاقتصادية على المستويين الداخلية والخارجي .

أولا: .الأبعاد الاقتصادية لجرائم الدفع الالكتروني وتأثيرها على فعالية العملية التجارية الالكترونية وانعكاس ذلك على التنمية الاقتصادية :

إن الجرائم والهجمات الالكترونية من أخطر التهديدات التي تواجه معظم دول العالم، ولاشك أنه مع ظهور العولمة واستخدام الشبكة المعلوماتية في النشاطات الاقتصادية والتي أصبحت تدار إلكترونيا ومع إمكانية تحويل الإلكتروني للأموال بسرعة هائلة عبر شبكة الانترنت بين جميع الدول دون تحديد هوية المرسل وعدم وجود قيود وضوابط جمركية لتدفق رؤوس الاموال والأفراد أدى إلى ظهور أشكال وأنماط جديد

[19] عبد الصمد حوالف، النظام القانوني لوسائل الدفع الالكتروني، أطروحة دكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2015/2014 ، ص 551ال

[20]–مؤلف جماعي، الجريمة المعلوماتية وأثرها على التنمية الإقتصادية، الطبعة الأولى " 2020"، عن المركز الديمقراطي برلين ألمانيا منشور عبر الرابط ، https://democraticac.de/?p=67302 ، 2022/09/12، 8:15.

للإجرام وبذلك امتدت الجريمة الإلكترونية إلى المنظمات والقطاعات الاقتصادية والمالية التي أصبحت تكبد ها خسائر مالية كبيرة مما يؤثر سلبا على الاقتصاد.

من هذا المنطلق تتحدد لنا ثلاث مستويات يمكن من خلالها حصر مجال وتأثير الاستخدام الاحتيالي للوسائل الدفع الالكترونية على كل من أطراف العملية التجارية الالكترونية، وتأثير ذلك بالتوازي على سيرورة عجلة التنمية الاقتصادية ، حيث أنها جرائم عابرة للحدود ومتعددة الجهات ، قد يتعرض لها الأفراد والشركات والبنوك وحتى الدولة من طرف أشخاص أو منظمات محترفة هدفها الرئيس ي الربح والتأثير املادي عليها وزعزعة أمن والاستقرار الاقتصادي للدول[21].

نحاول فيما يلي تسليط الضوء على أهم الانعكاسات السلبية الناتجة عن المساس والاستخدام الغير قانوني لوسائل الدفع الالكتروني على كل من التجارة الإلكترونية من جهة، وعلى تأثير ذلك التنمية الاقتصادية ككل، وقبل ذلك، سنحاول تحديد أهم الأطراف المتضررة من الاستخدام الاجرامي لوسائل الدفع الالكترونية أولا، نذكرها فيما يلي:

1/ اتساع دائرة المتضررين من الاستخدام الاحتيال لوسائل الدفع الالكترونية(المتعاملين ، المستهلك والمورد الالكتروني، الشركات والبنوك والاجهزة الحكومية)

تتعدد الجهات المتأثرة بالاستخدام الاحتيالي لوسائل الدفع الالكتروني بتعدد أطراف النشاط التجاري المبرم، حيث يتضح لنا جليا مدى خطورة هذه الجرائم على العمليات التجارية الالكترونية وتأثير ذلك على مدى فعاليتها كممارسات حتمتها العديد من التغييرات والتطورات في عالم الصناعة والتجارة العالمية والتطور التكنولوجي، وما يقابله من تسارع في التطورات على المستوى الوطني والدولي سعيا لتحقيق أكبر قدر من الفائدة، حيث أنه يتم تقييم نجاح النظام المصرفي لأي دولة في تطوير التجارة الإلكترونية ولا بد من إبراز أهم دعائم التجارة الإلكترونية في مجال النظام المصرفي من خلال العديد من المظاهر أهمها :

تكريس منظومة قانونية خاصة بوسائل الدفع الإلكترونية، والمتصفح في النصوص القانونية الجزائرية في هذا الصدد يجد العديد من النصوص نذكر منها : النظام رقم (06/05) المتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى بعد تعديل الأمر (59/75)[22] المتعلق بالقانون التجاري الجزائري بموجب القانون رقم (02/05) المتضمن تعديل القانون التجاري ، وكذا الأمر (11/03) المتعلق بالنقد والقرض[23]، لنجد أنه من بين أهم مظاهر فشل النظام المصرفي في تطوير التجارة الإلكترونية غياب أجهزة الدفع الإلكتروني (TPE) لدى أغلب التجار رغم تكريس المشرع الجزائري لمنظومة قانونية خاصة بالسندات

[21]– صراع كريمة ، دقيش جمال، المرجع السابق، ص 42.

[22]- الأمر رقم 59/75 ، المتضمن القانون التجاري الجزائري،

[23]- صراع كريمة ، دقيش جمال، المرجع السابق، ص 42.

التجارية الحديثة وتحديدا وسائل الدفع الإلكترونية، إلا أن هذا التكريس قد واكبه تقصير كبير من بنك الجزائر ،وكذا البنوك والمؤسسات المالية التي يخول لها القانون إدارة وسائل الدفع الإلكترونية، فنجد أن الإحصائيات المقدمة من الموقع الإلكتروني لشركة النقد الآلي والعلاقات التلقائية بين البنوك(SATIM) قد أكدت أن عدد عمليات السحب من أجهزة الصرف الآلي أكبر بكثير من عمليات الدفع سواء باستعمال بطاقات الدفع الإلكترونية أو باستعمال طريقة الدفع عبر مواقع الأنترنت، حيث تشير أغلب الإحصائيات أن السبب الرئيسي يعود إلى عاملين هما عدم ثقة المستهلك بوسائل الدفع الإلكترونية ، وكذا إلى غياب أجهزة الدفع الإلكتروني(TPE [24]) ، من هنا نجد أن تأثير أي عملية احتيال عند استعمال هذه البطاقات له من التأثير ما يمس العديد من الأطراف نوضح ذلك في ما يلي :

أ – **تأثير جرائم الدفع الالكتروني على الأفراد :**

لقد سمحت الانترنت للأفراد بالتواصل مع العالم الخارجي بحيث أصبح بإمكانه إجراء معاملات الشراء والبيع وإدارة أعماله إلكترونيا الجرائم الالكترونية التي قد يتعرض لها الفرد والتي تؤثر على الجانب املادي لديه• :سرقة الهوية الشخصية •سرقة بطاقة الائتمان الخاصة به •الابتزاز والتهديد •عمليات احتيال •تحويل أو نقل حسابه المصرفي •نقل ملكية ألاسهم •زيادة الفواتير بتحويل فواتير المجرم للضحية[25].

ب – **تأثير جرائم الدفع الالكتروني على الشركات** : تتمثل في : الاطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منها •العبث بمخازن المعلومات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول إليها •سرقة الأموال وتحويل حسابات مصرفية الخاصة بالشركة •الغش في المعاملات الالكترونية كالتغيير في المبيعات •عمليات الاحتيال •التهديد والابتزاز •اختراق الموقع الإلكتروني الخاص بالشركة.

ت – **تأثير جرائم الدفع الالكتروني على مستوى البنوك:** • السطو الإلكتروني •العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها •تعطيل النظام نقل ملكية ألاسهم •اختراق الموقع الإلكتروني الخاص بالبنك.

ث – **تأثير جرائم الدفع الالكتروني على المنظمات والمؤسسات** نذكر منها:

الاطلاع على معلومات سرية والاستفادة منها •العبث بمخازن المعلومات الخاصة بالمنظمة أو المؤسسة بحذفها أو تعديلها أو تعطيل الوصول إليها •سرقة الأموال وتحويل حسابات مصرفية الخاصة بالمنظمة أو المؤسس •عمليات الاحتيال •الابتزاز والتهديد •اختراق الموقع الإلكتروني الخاص بالمنظمة أو المؤسسة.

[24] - مهدي رضا، بطاقات الدفع الإلكترونية وترقية التجارة الإلكترونية، مجلة الدراسات والبحوث القانونية ، المجلد 5 / العـــدد: 2/ جوان 2020 ،ص 163 -175 .

[25] صراع كريمة ، دقيش جمال، المرجع السابق، ص 42.

ج – **تأثير جرائم الدفع الالكتروني على الجهات والأجهزة الحكومية:**

• الوصول إلى المعلومات سرية و الاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم. • دعم الإرهاب والأفكار المتطرفة ونشر الإشاعات •تعطيل وتخريب الخوادم الموفرة للمعلومات • تعطيل أنظمة قطاعات حكومية وحيوية • تعطيل الانترنت بالكامل •سرقة الأموال بواسطة وسائل الدفع المختلفة، وغيرها من الطرق الاحتيالية.[26]

2/ الخسائر المالية الباهضة لجرائم الدفع الالكتروني وانعكاس ذلك على فعالية الممارسات التجارية وعلى التمية الاقتصادية :

إن تحول الاقتصاد العالمي من مرحلة الاقتصاد التقليدي إلى مرحلة الاقتصاد الرقمي وتحول التعاملات التجارية والمالية إلى شكل إلكتروني زاد من خطورة الجريمة الإلكترونية والتي أصبحت في تصاعد مستمر ومن المتوقع أن يتزايد حجم الخسائر التي يتكبدها العالم بسبب الجريمة الإلكترونية في العقود القليلة المقبلة، نتيجة تزايد عدد الشركات التي تعتمد على الأنترنت في ممارسة نشاطها.

فبحسب أخر الإحصائيات فإن الاقتصاد العالمي يتضرر جراء الجرائم المتعلقة بوسائل الدفع ككل تقدر بتريليون دولار سنويا، غير أن الخطورة الحقيقية لا تنبع من ضخامة حجم الخسائر فقط، وإنما من القبول سنويا المتزايد لخسائر الجريمة الإلكترونية باعتبارها ضريبة لا مفر منها لممارسة الأعمال في مختلف أنحاء العالم.

2/1 الخسارة المالية بسبب الابتزاز:

تمت في مصر عملية ابتزاز عن طريق الشبكة العنكبوتية و ذلك بتهديد شركة مياه غازية بنشر صورة لأحد منتجاتها و بداخلها حشرة، ولكن لم ترضخ الشركة إلى التهديد ونشر المبتزون الصورة وشاهدها 3700 شخص و تم التعرف على المبتزين و اعترفوا بجرمهم.

2/2 .الخسارة المالية بسبب بعض الموظفين المطرودين:

بسبب سرية العمل في البنوك والشركات سواء العامة أو الخاصة وغيرها من الجهات والاجهزة الرامية لتحقيق الربح ، ونظرا لأهمية توفر عامل الامان في مثل هذه المعاملات ، فإن العامل البشري يعتبر مهما جدا في هذه المهمة ، وبالتالي فإن أي تغيير في المراكز والمناصب داخل هذه المؤسسات من شأنه أن يشكل خطرا على أموال الشركة ، حيث أنه قد يتسبب طرد أي من هؤلاء الموظفين داخلها سيؤدي إلى العديد من الخسائر المتعددة تنتهي كلها في قالب الخسائر المالية، فمثلا المدعو " تيموثي ألن ليود" وهو مصمم

[26]– صراع كريمة أ.دقيش جمال، المرجع السابق، ص 44.

ومبرمج فصل من عمله، فما كان منه إلا أن أطلق قنبلة إلكترونية ألغت كافة التصاميم وبرامج الإنتاج لأحد أكبر مصانع التقنية العالية في نيوجرسي التي تعمل لحساب وكالة الفضاء NASA والبحرية الأمريكية.[27].

وتتضح فكرة الخسارة المالية بسبب بعض الموظفين المطرودين في تأثير الجرائم المتعلقة بوسائل الدفع في كون الموظفين في المؤسسات المالية والشركات الضخمة وفي حالة طردهم، يمكنهم بحكم الخبرة المتوفرة لديهم من استغلال هذه الوسائل من أجل النصب والاحتيال على مؤسساتهم أو غيرها بطريقة تسبب العديد من الخسائر المالية الباهضة.

2/3 .الخسارة المالية بسبب سرقة المعلومات الشخصية:

تحمل وسائل الدفع الالكترونية العديد من المعلومات الشخصية والسرية جدا في نفس الوقت ، وهذا بالنظر لما تتطلبه المعاملات المالية من أمن وسرية في نفس الوقت ، ويشكل العبث بهذه الأخيرة خطورة جد صعبة على صاحب البطاقة ذاته وكذا على بقية الاطراف المتعاملة معه ، حيث يتم من خلال هذه المعلومات اختراق الحساب وسرقة الأموال عن طريق الاستعمال الغير قانوني لهذه الوسائل كونها تعتمد على الجانب الالكتروني الذي وإن كان يتسم بالسرعة والفعالية من جهة إلا أنه في نفس الوقت يجعل منها وسيلة سهلة الاحتيال فيها من قبل العديد من المختصين أنفسهم في المجال ، فمثلا في بنك لويدز في أمستردام تم تحويل مبلغ 8.4 مليون دولار الى بنك في سويسرا من قبل شاب عمره 26 عام ، وفي عام 2000م ، جرى السطو على 33 ألف جهاز صرف الي ATM في بريطانيا ، وقد كانت الخسارة المالية كبيرة قدرت بنحو 15 مليون جنيه إسترليني ذلك بالاعتماد على المعلومات الشخصية المتضمنة داخل بطاقات الائتمان وغيرها من وسائل الدفع.[28]

3/خلق أزمة الثقة في المعاملات التجارية الالكترونية مما يؤدي إلى شل عجلة التنمية الاقتصادية:

إن مثل هذه الجرائم له تأثير واسع النطاق نتيجة عالمية الممارسات التجارية الإلكترونية وتعدد أطرافها، حيث يتضح هذا التأثير على فعالية المعاملة التجارية (المتسوق والمورد الالكترونيين.....)، ليمتد تأثير ذلك على متطلبات التنمية الاقتصادية على المستوى الوطني والعالمي، ومن بين أهم المخلفات الناتجة عن هذه التجاوزات وعلى رأسها خلق أزمة ثقة بين المتعاملين في التجارة الالكترونية على أكثر من مستوى.

---

[27]- فصل مصمم ومبرمج حاسوب، ورئيس سابق لشركة أوميغا ، ويدعى "تيموثي ألين لويد" (35 عاما) تم اعتقاله في 1998/2/17م، بسبب إطلاقه قنبلة إلكترونية في عام 1996م، استطاعت ان تلغي كافة التصاميم وبرامج الإنتاج في أكبر مصانع التقنية العالية في نيوجرسي، والمرتبطة والمؤثرة على نظم تحكم مستخدمة في وكالة الفضاء الأمريكية(ناسا)، والبحرية الأمريكية، ملحقا خسائر بلغت 10 مليون دولار، وتعتبر هذه الحادثة اكثر جرائم تخريب الكمبيوتر خطورة للتوسع أكثر في القضية.انظر الرابط : http://www.lawjo.net/vb/archive/index.php/t-22328.html ، 2022/09/20، 00:05.

[28]–سكيورتي العرب، تأثير الجرائم الالكترونية على النواحي الاقتصادية، http://www.secarab.com/thread–3339.html/ 2022/09/18.

حيث أن من بين أهم الركائز التي تقوم عليها العملية لتجارية الالكترونية هي عامل الثقة المتبادلة خاصة وقت الدفع سواء بالنسبة للمستهلك أو الموزع والمورد الالكتروني أو أي واسط بين الطرفين ، كونها تكتسي من الأهمية ما يجعل للثقة أهمية جد كبيرة في عمليات التبادل سواء بالنسبة للمؤسسة أو للعميل نستخلصها كما يلي :

توفير الارتياح في العمل والقرارات – .تجعل علاقة التبادل مع الشريك طويلة ودائمة – .الثقة مفتاح نجاح العلاقات التجارية لا سيما تلك التي تتميز بدرجة عالية من المخاطر ، حيث يمكن اعتبارها كشبكة أمان – .الفائدة الرئيسية من الثقة هي رضا العميل ومن ثم ولائه الذي يؤدي بدوره إلى علاقة بعيدة المدى– . من غير الممكن تقييم الخدمة قبل الاستهلاك الفعلي وهذا ما يجعل الثقة عامل قرار ذو قيمة[29].

وبالمقابل لهذا نجد أن من عوائق تطور التجارة الإلكترونية ذلك المتعلق بحماية عمليات الدفع، إذ يمتنع العديد من المستهلكين عن استعمال بطاقة الدفع عبر الأنترنت بسبب المخاطر المنجرة عن عمليات الاحتيال الموجودة ويتخذ الاستعمال الاحتيالي لبطاقة الدفع ثالثة صور تم توضيحها ضمن المحور الأول بالتفصيل.[30]

كل هذه الصور تجعل من استعمال هذه الوسائل استعمال يشوبه نوع من نقص في الثقة إن لم نقل انعدامها في بعض الاحيان، وهذا من شأنه أن يؤثر على فعالية المعاملة التجارية من جهة وما يؤدي اليه من انعكاسات سلبية على التنمية الاقتصادية ككل بسبب عدم ايجاد الدافع والمبرر لاستعمال هذه البطاقات، مما يؤدي إلى شل عجلة التنمية ونقص فعالية المعاملة التجارية الالكترونية.

مما سبق نستنتج أن الانعكاسات الاقتصادية للجريمة الإليكترونية والجرائم المعلوماتية مهما اختلف نوعها ومهما تزايد حجمها تمس النظام المالي والاقتصادي ككل ؛ أي قد تقع على النظام المعلوماتي أو تقع بواسطته سواء بقت ذلك في مرحلة إدخال الأثر الاقتصادي المرتب عنها يختلف حسب البيانات أم في مرحلة إخراجها أم في مرحلة جمع البيانات، الا أن نوع الجريمة ونوع الأنظمة المعلوماتية أو حسب أهمية البيانات المستهدفة، ولهذا تتنوع وتتفاوت الخسائر الاقتصادية الناجمة عن الجرائم المعلوماتية، وقد تكون هذه الخسائر مباشرة أو غ ير مباشرة، أي يكون ضررها اقتصادي مباشر يرتبط بقيمة التجهيزات والبرمجيات موضوع الجريمة، وهو أقلها من حيث الأثر وقد يرتبط بالأثر الاقتصادي الناجم عن ن توقف هذه المنظومات عن العمل مثال: اختراق وتعطيل منظومة شركة الطيران رغم عدم وجود أثر غير مباشر، الا أن توقف المنظومة

[29]– بوداود بومدين ، دحو سليمان وأخرون ، النمذجة البنائية لمساهمة أبعاد الأمن السيبراني للبيانات في تحقيق رضا المستهلك الإلكتروني من خلال تعزيز الثقة كمتغير وسيط دراسة ميدانية لعينة من مستخدمي بطاقات الدفع الالكتروني لبنك التنمية المحلية BDL بولاية غرداية، مجلة إدارة الأعمال والدراسات الاقتصادية ، المجلد (7) ،العدد (01) 2021 ، ص 839.

[30]– حجاج يمينة ، الاستعمال الاحتيالي لبطاقة الدفع وتأثيره على حماية المستهلك الإلكتروني/ المجلد 7 العدد 02 ، 2022، ص 493:

عن العمل تؤدي إلى خسائر تقدر بالألاف الدولارات، أو تعطيل منظومة سوق الأوراق المالية لمدة دقائق قد ينجم عنه خسائر تقدر بعشرات الدولارات أيضا، ... وغيرها من الجرائم المتعددة [31].

ثانيا: أساليب وآليات مكافحة الجرائم الواقعة على وسائل الدفع الالكترونية

تعتبر الانترنت بيئة خصبة لنمو الجرائم الالكترونية وذلك لعدد من الأسباب أهمها العدد الهائل من أجهزة الكمبيوتر المتصلة بشبكة الانترنت مما يعطي الجاني حرية الاختيار بين مجموعة واسعة من الأهداف، بالإضافة إلى أن الانترنت هو وسيلة فعالة لتشغيل البرامج والأنظمة الآلية التي توفر الكثير من الوقت والجهد المطلوبين في العمل الإجرامي، كما أن طبيعة الانترنت تجعل من الصعب إدارة محتواه وكذلك انتقال البيانات خلال الشبكة وبالتالي صعوبة مكافحة البرمجيات الضارة والاحتيال من خلاله.

وأمام هذا التطور وما قد يتنج عنه من خسائر ومخاطر تم الحديث عنها في المداخلة أعلاها، كان لزوما على كل الدول العمل على خلق بعض الحلول المقترحة لمواجهة العقبات التي تواجهها، فهناك العديد من الحلول الممكنة لمحاربة الجرائم الالكترونية عامة والجرائم الواقعة على وسائل الدفع الإلكتروني خاصة، حيث أن هناك بعض الحلول التقنية (مثل تقنية التشفير) التي تستخدم للحد من الجرائم يمكن أن يستخدمها المجرمون أيضا لأغراضهم الاجرامية ، كما أن هناك أيضا بعض الحلول التي تتعرض للخصوصية خصوصا إذا كانت بين أكثر من دولة.

سنحاول وضع توضيح مختصر لهذه الحلول ، مع تبيان ما يقابلها من صعوبات في التنفيذ أو فيها ما يجعل منها تعرضا للخصوصية:

1 .الاحتفاظ بالبيانات المتنقلة عبر الشبكة الالكترونية:

حيث يتم حفظ جميع البيانات والمعلومات الخاصة و صفحات الويب التي تم زيارتها و كذلك البريد الالكتروني وهذا كله لغرض التحقيق في الجرائم وحفظ هذه المعلومات كأدلة رقمية ويمكن أن يساهم هذا الحل على تعقب عودة المجرمين الذين عادوا إلى إجرامهم بعد كشفهم، يواجه هذا الحل بعض الصعوبات في التطبيق منها:

أ. الكم الهائل من البيانات التي سوف يتم حفظها و تراكمها.

ب. بالرغم من أن تكلفة التخزين أصبحت منخفضة في الأعوام السابقة إلا أنها ما زالت تعتبر عائق.

ت. يوجد اعتراض كبير حول أخلاقية هذا الفعل و اتهامه بخرق الخصوصية.

2/ .التشفير: الهدف من التشفير هو جعل المعلومات السرية القابلة للسرقة مثل رقم بطاقة الائتمان غير قابلة للقراءة و الفهم ، فالشخص المخول بالدخول على هذه المعلومات هو الوحيد القادر على فك تشفيرها و من ثم قراءتها و فهمها.

[31]- http://www.secarab.com/thread-3339.html ،2022/09/18 13:00

عيوب التشفير: كما ذكرنا سابقا يمكن للمجرمين الاستفادة من هذه التقنية و ذلك بتشفير خططهم الإجرامية وجعلها سرية بحيث لا يمكن قراءتها و فهمها من قبل السلطات.[32]

3/التعاون الدولي: للجرائم الالكترونية أبعادا دولية تتزايد باطراد . علينا إذا أن ندرك الحاجة إلى التعاون بين مختلف الدول من اجل مكافحة هذه الجرائم على نحو فعال. وعلاوة على ذلك، هناك حاجة إلى إطار قانوني يضم جميع البلدان ويطبق فيها.

أما على مستوى الشرق الأوسط وبالتحديد دول الخليج العربي فقد أعلنت المملكة العربية السعودية سن قوانين لمحاربة القرصنة و وضع عقوبة لها كالحبس لمدة عام واحد و غرامة لا تزيد عن 500 ألف ريال[33].

وتتضح المجهودات الدولية الرامية للتصدي لجريمة الإلكترونية مع تزايد خطورة الجريمة الإلكترونية على المستوى العالمي انصبت الجهود الدولية والإقليمية من أجل خلق أليات قانونية للحماية من أخطارها و برزت في هذا المجال العديد من المنظمات الدولية والإقليمية، نذكر منها:

الأجهزة الشرطية الدولية القائمة على مكافحة جرائم الكمبيوتر والانترانت مثل : المنظمة الدولية للشرطة الجنائية(INTERPOL)، الشرطة الدولية للويب (IWP).، مركز الشرطة الاوروبية .....و الأورجست وهو جهاز يوجد على المستوى الأوروبي يساعد على التعاون القضائي والشرطي في مواجهة مكافحة جميع أنواع الجرائم الخطيرة للإنترنت[34].

ومن أساليب مكافحة الجريمة الإلكترونية أيضا:

- صياغة نصوص وتنظيمات تشريعية لحماية الملكية الفكرية: حيث تعتبر الإبداعات الفكرية والفنية المتعلقة بمجال الحواسيب والبرامج ، أعمال محمية بواسطة القانون[35].
- فرض عقوبات صارمة على مرتكبي جرائم الانترنت وتأسيس منظمات خاصة لمكافحة الجريمة والحد منها .وذلك بتعزيز التعاون والتنسيق مع المؤسسات الدولية للتصدي لها .
- تشريع قوانين دولية من أجل محاكمة مرتكبي جرائم الأنترنت في أي دولة وذلك نظرا للطبيعة لكافة أشكال الجريمة الإلكترونية عبر العالم.

-استخدام أحدث التقنيات والعمل على تطويرها من أجل كشف هوية مرتكبي الجريمة بأسرع وقت ممكن.

-توعية الأفراد والمؤسسات بشكل دائم بخطورة الجرائم الإلكترونية وذلك بنشر خطورتها وأضرارها عبر وسائل الإعلام أو عبر تنظيم ملتقيات وأيام دراسية.

---

[32]- – تأثير الجرائم الالكترونية على النواحي الاقتصادية، –http://www.secarab.com/thread 2022/09/18، 12:00.

[33]– تأثير الجرائم الالكترونية على النواحي الاقتصادية، –http://www.secarab.com/thread 2022/09/18، 12:00.

[34]- للتوسع في الفكرة أكثر أنظر بوحليط يزيد ، المرجع السابق ، ص 500.

[35]- وهيبة بشريف ، أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي، جامعة باتنة 1(الحاج لخضر) / مقال منشور https://www.asjp.cerist.dz/en/article/76418، 2022/09/20 .

-الحفاظ على كلمة السر وتغييرها بشكل مستمر مع المحافظة على سرية المعلومات الشخصية وذلك بعدم نشر ها في مواقع غير موثوق ، والعمل على تشديد الرقابة على عملية التوقيع والتصديق الالكتروني عند عملية الدفع بأي وسيلة كانت[36].

- وضع رقم سري بشكل مطابق للمواصفات الجيدة التي تضع هذه المواصفات بأن يحتوي على أكثر من ثمانية أحرف أن يكون متنوع الحروف والرموز.
- عدم تحميل برامج مجهولة المصدر مع استمرارية تحديث البرامج الأمن الخاصة بأجهزة الحاسوب.
- استخدام برمجيات أمنة و خالية من الثغرات.
- الإبلاغ الفوري في حالة تعرض لجريمة إلكترونية وأخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.[37]

خاتمة :

من خلال ما تم التطرق له ضمن هذه الدراسة اتضح لنا جليا مدى أهمية كل من وسائل الدفع الإلكترونية في تأكيد فعالية الممارسات التجارية الالكترونية كضرورة حتمية فرضتها متطلبات الثورة التكنولوجية هذا من جهة، ومن جهة أخرى نجد أنه بقدر ما تنجلي هذه الأهمية بقدر ما تتضح لنا مدى خطورة العبث بمثل هذه الوسائل عند الاستخدام الغير شرعي لها وانعكاسها السلبي على مدى فعالية هذه الممارسات مؤثرة في ذات الوقت وبطريقة موازية وأكثر خطورة على سيرورة عجلة التنمية الاقتصادية سواء على المستوى الوطني أو العالمي، حيث أنه و من ابرز الجرائم الالكترونية التي تهدد الاقتصاد :

أ. التلاعب بالتجارة الالكترونية حيث يتم عرض أسهم واستثمارات مزورة وبيعها.

ب. اختراق البنوك وسرقة معلومات العملاء وكذلك سرقة الأرصدة وتحويلها إلى بنوك أخرى.

لنستخلص من خلال ما تمت معالجته ضمن هذه المداخلة العديد من النتائج نحاول حصر أهمها في النقاط التالية:

1 - تعدد وسائل الدفع الالكترونية وطرق استعمالها أدى لتعدد صور الاحتيال عليها وعدم القدرة على ضمها ضمن اطار قانوني موحد، الأمر الذي أدى لتشعب النصوص القانونية المتعلقة بها وتفرعها على العديد من النصوص الخاصة والمتفرقة.

2 - محاولة المشرع الجزائري لمواكبة التطورات العالمية كون هذه الجرائم تتصف بالجرائم العابرة للحدود، حتم على المشرع الجزائري وإن كان بوتيرة محتشمة وبطيئة العمل جاهدا للسعي نحو مكافحة هذه الجرائم وما

[36]- غزالي نزيهة، الأليات القانونية لحماية وسائل الدفع الإلكتروني في التشريع الجزائري، جملة البحوث السياسية والإدارية، العدد العاشر، ص 287.

[37]- صراع كريمة، دقيش جمال، المرجع السابق، ص ص 35، 53.

قد تسببه من مخاطر على عجلة التنمية الاقتصادية للدولة، نتيجة اتساع دائرة المتضررين جراء هذه التجاوزات كون العملية التجارية الالكترونية متعددة الأطراف والجوانب.

3 – كثرة انتشار الجرائم المتعلقة بوسائل الدفع أدى لانعدام الثقة من قبل المتعاملين عند الاعتماد على هذه الوسائل عند الدفع، نتيجة التخوف من الاضرار بمصالحهم، الأمر الذي يساهم بطريقة عكسية وسلبية على سيرورة عجلة التنمية الاقتصادية ككل.

بناء على هذه النتائج حاولنا وضع بعض التوصيات المتواضعة والمقترحة كالتالي:

– على المشرع الجزائري ضرورة العمل والاسراع من أجل صياغة قانون خاص بالجرائم الالكترونية ضمن النصوص الداخلية بما يتماشى مع مضامين الاتفاقيات الدولية من أجل بسط المراقبة على مثل هذه المعاملات الالكترونية، وتخصيص البعض من نصوصه للإلمام بالأحكام المتعلقة باستعمالات وسائل الدفع الالكترونية كونها الوسائل الأكثر انتشارا لتنظيم الجانب المالي الالكتروني.

– ضرورة وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهياكل التنظيمية متعلقة بجرائم الانترنتّ والسياسات المتعلقة بالموضوع.

– ضرورة وضع استراتيجية لتحديد الحد الأدنى المقبول لعاملي البرامج والأنظمة في موضوع معايير الأمن ونظم تطبيقاتها، والعمل على تعزيز ثقة الشعب من أجل الاستخدام الأمان والفعال لوسائل الدفع الالكترونية لما لها من فوائد على كل من التجارة الالكترونية والتنمية الاقتصادية الوطنية والعالمية.

– ضرورة وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود .

– ضرورة وضع استراتيجيات لإنشاء نظام هوية رقمي وطني وعالمي وتطبيقه وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

– تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي جميع المجالات المعلوماتية.

– تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية إلى تعزيز القدرة على إنفاذ سياسات التقنية المعلوماتية والأمن المعلوماتي لضمان فاعلية تطبيق الخطط المنبثقة عن تلك الاتفاقيات.

قائمة المراجع: المرجع باللغة العربية:

أولا : النصوص القانونية:

1 +الأمر رقم 59/75 ، المتضمن القانون التجاري الجزائري.

2 –القانون 10/90 المتعلق بالنقد والقرض المؤرخ في 1990/4/16 المعدل بموجب الأمر 11/03 المؤرخ في 26/ 2006/6.

3 – القانون 18–05 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الالكترونية ، ج ر عدد 287 مؤرخة في 16 ماي 2018

الكتب والمؤلفات :

1 – جلال عابد الشورة، وسائل الدفع الالكتروني، دار الثقافة للنشر والتوزيع ، الأردن، 2008 .

2 – ديمثان المجالي، أسامة عبد المنعم، التجارة الالكترونية، الطبعة 1، دار وائل للنشر، الاردن، 2013

3 – لبنى عمر سقاوي، المسؤولية المصرفية في الاعتماد المالي، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2006

4 – عبد الكريم الردايدة، جرائم بطاقة الإئتمان، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، 2013

5 – يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، مصر، 2019.

المقالات والمجلات العلمية:

1 –بوداود بومدين ، دحو سليمان وأخرون، النمذجة البنائية لمساهمة أبعاد الأمن السيبراني للبيانات في تحقيق رضا المستهلك الإلكتروني من خلال تعزيز الثقة كمتغير وسيط دراسة ميدانية لعينة من مستخدمي بطاقات الدفع الالكتروني لبنك التنمية المحلية BDL بولاية غرداية، مجلة إدارة الأعمال والدراسات الاقتصادية ، المجلد (7) ،العدد (01) 2021.

2 –صراع كريمة ، دقيش جمال، الأبعاد الاقتصادية للجريمة الإلكترونية، مجلة الدراسات التسويقية وإدارة الأعمال، المجلد2–العدد1 ، جانفي 2018.

3 –عماد الدين بركات، ظ.د/طيبي حوري:« وسائل الدفع الإلكترونية ودورها في تفعيل التجارة الالكترونية» مجلة القانون والتنمية المحلية، العدد 2، 2019.

4 – كردي نبيلة : «الشيك الالكتروني» مجلة العلوم الاجتماعية والانسانية، مجلد 10، عدد 2، 2017، زكريا مسعودي، ط.د/ الزهرة جقريف :« ماهية النقود الإلكترونية » المجلة الدولية للبحوث القانونية والسياسية، مجلد 2 ، عدد3 ، 2018.

5 –مهدي رضا، بطاقات الدفع الإلكترونية وترقية التجارة الإلكترونية، مجلة الدراسات والبحوث القانونية، المجلد 5 / العدد: 2/ جوان 2020 .

6 – حجاج يمينة ، الاستعمال الاحتيالي لبطاقة الدفع وتأثيره على حماية المستهلك الإلكتروني/ المجلد 7 العدد 02 ، 2022.

7 – وهيبة بشريف ، أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي، جامعة باتنة 1 https://www.asjp.cerist.dz/en/article/76418، 2022/09/20، 14:00.

8 – غزالي نزيهة، الأليات القانونية لحماية وسائل الدفع الإلكتروني في التشريع الجزائري، جملة البحوث السياسية والإدارية، العدد العاشر.

المذكرات والرسائل الجامعية :

1 – بونفلة صليح ، النظام القانوني للعمليات المصرفية الالكترونية، أطروحة لنيل شهادة الدكتوراه، جامعة قالمة، 2020.

2 –عبد الصمد حوالف، النظام القانوني لوسائل الدفع الالكتروني، أطروحة دكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2015/2014.

3 –أمينة بن عميور، البطاقات الالكترونية للدفع والقرض والسحب، مذكرة لنيل شهادة الماجستير في القانون الخاص، كلية الحقوق، جامعة منتوري، قسنطينة، 2005،

4 – عبد الرحيم وهيبة، إحلال وسائل الدفع المصرفية التقليدية بالإلكترونية دراسة حالة الجزائر، مذكرة لنيل شهادة ماجستير في علوم التسيير، جامعة الجزائر،

5 –عمار لوصيف، استراتيجيات نظام المدفوعات للقرن الحادي و العشرين مع الاشارة للتجربة الجزائرية ، مذكرة ماجستير في العلوم الاقتصادية، جامعة قسنطينة ، 2008–2009 .

المواقع الالكترونية :

1- https://www.interpol.int/Crimes/Cybercrime date of viewing 10/9/2022 at 18 :50

2- Hélène Puel :« Des milliers de Français victimes du vol de leur numéro de carte bancaire» https://www.01net.com/actualites/ consulter le 11/9/2022 a 22 :55

3 –أمجد حمدان الجهني، الاستخدامات الغير مشروعة لبطاقة الدفع الإلكتروني من قبل الغير، مركز الدراسات القضائية، المملكة الأردنية الهاشمية، مقال منشور على الموقعhttp://www.coiss.com/replay.php

4 – مؤلف جماعي، الجريمة المعلوماتية وأثرها على التنمية الإقتصادية، الطبعة الأولى "2020"، عن المركز الديمقراطي برلين ألمانيا منشور عبر الرابط ، https://democraticac.de/?p=67302 ، 12/09/2022، 8:15.

5 -تأثير الجرائم الالكترونية على النواحي الاقتصادية، http://www.secarab.com/thread-3339.html/ .2022/09/18

ثانيا : المراجع بالغة الاجنبية :

-1-for further information see also : international chamber of commerce :« Electronic payment services and e-commerce» ISSUES BRIEF Nº 4 , https://iccwbo.org/content/uploads/sites/3/2020/02/icc-issues-brief-4-electronic-payment-services-and-ecommerce.pdf, date of viewing 10/9/2022 at 20 :04

2 -TOERING Jean Pierre et BRION François , les moyens de paiement ,Edition Presses Universitaires de France - P.U.F 1 ère édition ,Paris , 1999,p32

نجـاة حمــلاوي
nadjettehamlaoui@gmail.com
المركز الجامعي ايليزي

مصطفى سلالي
mostaphasellali@gmail.com
جامعة محمد خيضر بسكرة

أثار الجرائم الالكترونية على الجانب الاقتصادي

ملخص

تشكل الجرائم الالكترونية تهديدا حقيقيا للتنمية الاقتصادية في مختلف دول العالم، من خلال تزايد عمليات الاحتيال و السرقة والقرصنة التي يعرض لها الأفراد والمؤسسات والبنوك والتي تتم عبر شبكة الانترنت، حيث أثبتت الإحصائيات التزايد المستمر لهذه الجرائم على الجانب الاقتصادي نتيجة التوجه المتسارع نحو التجارة الالكترونية وتحول العالم من الاقتصاد التقليدي إلى الاقتصاد الرقمي، الأمر الذي يستدعي تضافر جهود دول العالم وتعزيز مختلف الآليات قصد التصدي لخطر هذه الجرائم على التنمية الاقتصادية فيها.

Summary

Cybercrime poses a real threat to economic development in various countries of the world, through the increase in fraud, theft and piracy to which individuals, institutions and banks are exposed, and which are carried out via the Internet. Statistics have proven the continuous increase of these crimes on the economic side as a result of the accelerating trend towards electronic commerce and the transformation of the world From the traditional economy to the digital economy, which calls for the concerted efforts of the countries of the world and the strengthening of various mechanisms in order to address the threat of these crimes to their economic development.

مقدمة

أدى التطور التكنولوجي في مجال الاتصال و المعلوماتية وظهور تقنية الانترنت إلى التحول من الاقتصاد التقليدي إلى الاقتصاد الرقمي عن طريق الاعتماد على التجارة الالكترونية، حيث لا يمكن إنكار ما تقدمه تكنولوجيا الإعلام والاتصال من مزايا في جميع مناحي الحياة ومنها الاقتصادية، ولكن بقدر ما ساهمت المعلوماتية في نهوض كافة القطاعات وتقدمها ورقيها ، بقدر ما أسهمت في ظهور نوع جدد من الجرائم، وهو ما الإجرام المعلوماتي ، أو ما يسمى بالجريمة الالكترونية، أو جرائم الحاسوب، أو الجرائم الرقمية، أو جرائم تكنولوجيا الإعلام والاتصال إلى غير ذلك من التسميات.

فقد أصبحت أجهزة الحاسوب من أهم وسائل الاتصال بين الأفراد والمؤسسات حيث ازداد التوجه لاستخدام شبكات المعلومات الإلكترونية في الفترة الأخيرة بصفتها أداة اتصال دولية في مختلف المجالات ونظرا لعديد المزايا التي تختص بها من سرعة انتقال المعلومة وتوفير الوقت والجهد واختصار المسافات ولكن لم يمنع الانتشار الكبير لهذه الشبكات الإلكترونية ظهور العديد من المشاكل والمخاطر، والتي قدمت أصنافاً من الجرائم لم تكن متداولة سابقاً، سميت بالجرائم الإلكترونية

وتتجلى خطورة هذا النوع من الجرائم في الآثار السلبية والخطيرة على الجانب الاقتصادي، وأثارها المدمرة على التنمية الاقتصادية في المجتمعات النامية وكذا المتقدمة.

وتكمن أهمية هذا الموضوع في كون الجرائم الالكترونية في أن الأخيرة تشكل نمطا إجراميا مستحدثا أصبح يهدد سلامة وأمن الأفراد والمؤسسات على حد سواء، الأمر الذي تثبته في كل مرة الإحصائيات والتي تؤكد أن الجرائم الالكترونية ترهق كاهل الدول في الجانب الاقتصادي جراء الخسائر الكبيرة التي تقدر بتريليونات الدولارات سنويا.

ومنه فإن الإشكالية التي تعالجها هذه الدراسة هي: **ما هي الآثار السلبية للجرائم الالكترونية على الجانب الاقتصادي؟**

حيث تتم الإجابة وفقا للخطة المقترحة التالية :

المحور الأول: المقصود بالجرائم الالكترونية وخصوصيتها.

المحور الثاني: أثار الجرائم الالكترونية على التنمية الاقتصادية والحلول المتخذة لمجابهتها

المحور الأول: المقصود بالجرائم الالكترونية وخصوصيتها.

فى ظل الإنتشار السريع للتكنولوجيا خاصة في زمن الكورونا وزمن "العادي الجديد "أصبحت معظم التعاملات الاجتماعية والتجارية والسياسية تتم عن طريق الشبكة المعلوماتية (الإنترنت)، وأصبح الإنسان أكثر عُرّضه للوقوع كضحية لتلك لجرائم الإلكترونية أو المعلوماتية ، تشكل الجريمة الالكترونية نمطا إجراميا مستحدثا، فرض نفسه على الواقع له العديد من الآثار السلبية على الأفراد والمؤسسات وكذا البنوك والمصارف، ومن هذا المنطلق وجب في هذا المقام من الدراسة ناول الإطار المفا هيمي لهذا الموضوع كالأتي:

أولا : تعريف الجريمة الالكترونية:

لا يوجد تعريف واحد للجريمة الالكترونية حيث يمكن ايجاد العديد من هذه التعريف والتي رغم اختلافها الا أنها تتفق على احتوائها على نفس الخصائص التي تخص هذه الظاهرة ، وعلى ذلك يمكن القول أنها "

كل نشاط غير قانوني باستخدام الكمبيوتر أو الحوسبة مثل الهواتف الذكية والأجهزة اللوحية والمساعد الرقمي الشخصي لوحدها أو باستخدام شبكة الانترنت لتنفيذ الجريمة الماسة بالجانب الاقتصادي"[1]
وهناك تعريف أخر هو أنها :"كل عمل غير مشروع صادر عن إرادة أثمة يحدث لها عقوبة أو تدبير وقائي أي بمعنى أنها الفعل أو الترك المعاقب عليه جنائيا، فالجريمة قانونا هي الفعل أو الترك الذي نص عليه القانون بعقوبة مقدرة له[2].

والجريمة الإلكترونية تتمثل في اعتداء معلوماتي يقوم فيه الجاني باستخدام وسائل اتصال حديثة بهدف ابتزاز الضحية أو تشويه سمعتها وما إلى ذلك، سواء بغرض تحقيق مكاسب مادية أو أهداف سياسية .علي الصعيد الآخر، يتحمل المستخدمون من المواطنون، بل الشركات والحكومات أنفسهم كل تلك المخاطر، وذلك نظرًا إلى أن الإنترنت أصبح بلا منافس في شتى التعاملات وبات من الصعب على مستخدميه تجنبه وذلك لأنه أكثر الوسائل سُرعة وتوفيرًا للوقت والجهد، خاصَة في ظل تحديد الحركة وفي ظل "المنافسة "التي تجيد استخدامه في شتى بقاع الأرض.

وتعد الجريمة المعلوماتية و الالكترونية إفرازا لتقنية المعلومات، فهي ترتبط بها وتقوم عليها إذ كلما زادت هذه التقنية ازداد حجم الجرائم المتصلة بها، حيث أحاط في تعريف الجريمة الالكترونية الكثير من الغموض إذ لا يوجد تعريف جامع لها وموحد، إلا أن غالبية الفقة رأت عدم وضع تعريف لها لأنها ما هي إلا جريمة تقليدية في شكل الكتروني.[3]

كما يمكن القول أن الجريمة الالكترونية هي نشاط إجرامي إما يستهدف أو يستخدم جهاز كمبيوتر أو شبكة كمبيوتر أو جهازًا متصلاً بالشبكة، ويرتكب معظم الجرائم الالكترونية، وليس كلها، مجرمون الكترونيون أو متسللون يريدون جني المال وتحقيق الربح كما قد ينفّذها الأفراد أو منظمات الجرائم الالكترونية.

ثانيا: خصائص الجرائم الإلكترونية :

تتميز الجريمة الالكترونية عن غيرها منن الجرائم التقليدية بمجموعة من الخصائص والي تتحدد وفقا لطبيعة هذه الجريمة وتجعلها ذات خصوصية معينة، حيث تتسم بالحركية و السرعة وأنها جريمة عابرة للقارات ، ولا ترتكب باستعمال القوة والعنف وغيرها من الخصائص التي نشرحها في الاتيّ:

أ –عالمية الجريمة الالكترونية

---

[2] ألاء محمد رحيم حمادي، **الجريمة السبيرانية ومخاطرها على الأفراد** (الإشكاليات و الحلول)(دراسة تحليلية في ضوء الإحصائيات الدولية والعربية والوطنية)، مجلة كلية التربية للبنات، جامعة بغداد، مجلد 28، عدد04، 2017، ص1106.

3 حسان سعاد، **إثبات التعاملات الالكترونية وفقا للقانون الجزائري والتشريعات المقارنة** ، الطبعة الأولى، دار الوفاء للطباعة والنشر، الإسكندرية، 2019، ص 34

بمعنى انها " **جرائم عابرة للقارات** " لا تعترف بالحدود الجغرافية للدول وحتى بين القارات، وبفضل شبكة الانترنت أصبح مجتمع المعلومات مجتمع منفتح لا يخضع لحرس الحدود وأصبحت الجريمة المرتبكة على الانترنت تعتبر جريمة لا حدود لها وظهرت مشاكل حول تحديد القانون الواجب تطبيقه وتحديد الدولة صاحبة الاختصاص القضائي.

ب – جرائم بدون عنف

أطلقت على الجرائم التي تحدث عبر الانترنت بأنها الجرائم الناعمة إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة، فالجرائم الالكترونية لا تتطلب أدنى مجهود عضلي ممكن، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة، على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكيد لتحقيق مصلحة ما".

ج **صعوبة إثبات الجرائم الالكترونية:**

بحيث يتميز الجاني المجرم المعلوماتي بالذكاء والاحترافية الأمر الذي يصعب تتبع أثره إضافة إلى عدم وجود دليل مادي كالبصمة كما يستطيع أن يمحي أثره عن طريق استخدام برامج أو كلمات سرية ورموز ويلجأ إلى التشفير لمنع أي دليل يقود إلى إدانته، كما أن المجني عليهم وهم غالبا مؤسسات عامة أو خاصة يحجمون عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة، فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية وتعد جرائم صعبة الإثبات لكونها ، جريمة لا تترك أثرا بعد ارتكابها ، وصعوبة الاحتفاظ بآثارها أن وجدت، كما أنها تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها، كونها تعتمد على الخداع والتضليل في ارتكابها.

ثالثا: **طرق ارتكاب الجريمة الإلكترونية الماسة بالجانب الاقتصادي:**

ترتكب الجريمة الالكترونية عن طريق مجموعة من الطرق والأساليب والتي تعد اهمها هي انتهاك الخصوصية من خلال سرقة حسابات الأفراد ونشر معلومات سرية عنهم بهدف إفشاء أسرارهم.

إضافة إلى سرقة وتخريب وتزوير المعلومات وإساءة استخدامها ويشمل ذلك قواعد المعلومات المكتبات تمزيق الكتب تحريف المعلومات والدراسات الهامة الخاصة بالتطوير التقني والصناعي أو العسكري والتصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف. التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.

كذلك التشهير ويشمل استخدام المعلومات الخاصة أوذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة و السرقة العلمية الكتب والبحوث العلمية الأكاديمية

وخاصة ذات الطبيعة التجريبية والتطبيقية ، إضافة إلى سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.

ونجد من جانب أخر أن قرصنة البرمجيات التي يشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى يعد أحد أهم الأساليب التي ترتكب عن طريقها هذه الجرائم، إضافة إلى قرصنة البيانات والمعلومات والتي تشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

كما تمثل خلاعة الأطفال صورة أخرى من صور هذه الجرائم والتي تشمل نشر صور خاصة للأطفال " الجنس السياحي " للأطفال خاصة وللإناث على الشبكات بشكل عام.

إرسال فيروسات على شكل رسائل إلكترونية بهدف تدمير البيانات مثل فيروسات الفدية والتي ارتكبت من طرف مجموعة تسمى شادو بروكرز، وهو عبارة عن برمجيات خبيثة طالت أكثر من 156 دولة عام 2017 وأصابت أكثر من 300.000 جهاز حاسب ألي، حيث يقوم هذا الفيروس بإقفال ملفات المستخدمين وتعطيل نظام التشغيل ويرغمهم على دفع مبلغ من المال يتراوح بين 300 و 600 دولار مقابل اعادة فتح الجهاز[4].

سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.

ويعد ذلك كله نتاج الثورة التكنولوجية التي أدت إلى ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التي نعرفها من حيث البيئة التي تتم فيها هذه المعاملات فقد سمحت المعلوماتية والانترنت في تداول الأنشطة التجارية عبر الشبكة مما أتاح للأنشطة الإجرامية بتحقيق عوائد مالية عن طريق وسائل غير مشروعة ناتجه عن عمليات التزوير والاحتيال وغيرها من الجرائم الإلكترونية التي سبقت الإشارة إليها.

المحور الثاني: أثار الجرائم الالكترونية على التنمية الاقتصادية والحلول المتخذة لمجابهتها

إن الجرائم والهجمات الالكترونية من أخطر التهديدات التي تواجه معظم دول العالم، ولاشك مع ظهور العولمة واستخدام الشبكة المعلوماتية في النشاطات الاقتصادية والتي أصبحت تدار إلكترونيا ومع إمكانية تحويل الإلكتروني للأموال بسرعة هائلة عبر شبكة الانترنت بين جميع الدول دون تحديد هوية المرسل وعدم وجود قيود وضوابط جمركية لتدفق رؤوس الأموال والأفراد أدى إلى ظهور أشكال وأنماط جديد للإجرام وبذلك امتدت الجريمة الإلكترونية إلى المنظمات والقطاعات الاقتصادية والمالية التي أصبحت تكبد ها خسائر مالية كبيرة مما يؤثر سلبا على الاقتصاد.

[4] صراع كريمة، دقيش جمال، **الأبعاد الاقتصادية للجريمة الالكترونية** ، مجلة الدراسات التسويقية وإدارة الأعمال، المجلد 02، العدد01، جانفي 2018، ص 47.

إن الجرائم الالكترونية التي قد يتعرض لها الأفراد والشركات والبنوك وحتى الدولة من طرف أشخاص أو منظمات محترفة هدفها الرئيسي الربح والتأثير المادي عليها وزعزعة أمن والاستقرار الاقتصادي للدول وفي الآتي نذكر أهم الجرائم الإلكترونية التي تتعرض لها القطاعات الاقتصادية والتي تؤثر عليها سلبا في الجانب المادي، ومنه فإننا نتطرق في هذا المقام الى أثر الجرائم الالكترونية على الجانب الاقتصادي في نقطة أولى ثم إلى مختلف الجهود الدولية والوطنية المبذولة للتصدي لهذه الظاهرة كالأتي:

أولا: الآثار السلبية للجريمة الالكترونية على التنمية الاقتصادية:

بداية يمكن القول أن الجريمة الالكترونية لها أثار خطيرة على الجانب الاقتصادي والتنمية كما تؤثر الأفراد والبنوك والمؤسسات والهيئات الحكومية فلقد سمحت الانترنت للأفراد بالتواصل مع العالم الخارجي بحيث أصبح بإمكانهم إجراء معاملات الشراء أو البيع وإدارة أعماله م إلكترونيا، الأمر الذي يجعلهم عرضة للجرائم الالكترونية التي قد يتعرضون لها والتي تؤثر على الجانب المادي لديه م كسرقة الهوية الشخصية و سرقة بطاقة الائتمان الخاصة به ، والابتزاز والتهديد وعمليات الاحتيال، وكذا تحويل أو نقل حساب اتهم المصرفية، ونقل ملكية الأسهم وزيادة الفواتير بتحويل فواتير المجرم للضحية.

أما الجرائم الالكترونية التي تتعرض لها الشركات: فتتعلق أساسا بالإطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منها، وكذا العبث بمخازن المعلومات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول إليها ، وسرقة الأموال وتحويل حسابات مصرفية الخاصة بالشركة، والغش في المعاملات الالكترونية كالتغيير في المبيعات .

ومن جانب أخر تعد البنوك والمصارف المالية الأكثر عرضة ل لجرائم الالكترونية من خلال السطو الإلكتروني و العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها ، وتعطيل الأنظمة ونقل ملكية الأسهم، وكذا اختراق المواقع الإلكترونية الخاصة بهذه البنوك.

وتتعرض المنظمات والمؤسسات والجهات والأجهزة الحكومية كذلك للجرائم الالكترونية من خلال الإطلاع على معلومات سرية والاستفادة منها والعبث بمخازن المعلومات الخاصة بالمنظمة أو المؤسسة بحذفها أو تعديلها أو تعطيل الوصول إليها ، ناهيك عن سرقة الأموال وتحويل الحسابات المصرفية الخاصة بالمنظمة أو المؤسرة، واختراق الموقع الإلكتروني الخاص بالمنظمة أو المؤسسة[5] .

كما يمكن أن تساهم الجريمة الالكترونية في دعم الإرهاب والأفكار المتطرفة ونشر الإشاعات ، وتعطيل وتخريب الخوادم الموفرة للمعلومات ، وأنظمة القطاعات الحكومية الحيوية، وتعطيل الانترنت بالكامل ، سرقة الأموال ب'تبارها كل فقعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية ويكون ناتجا بطريقة

[5] صراع كريمة، دقيش جمال، **الأبعاد الاقتصادية للجريمة الالكترونية**، المرجع السابق، ص 44.

مباشرة أو غير مباشرة عن استعمال التقنية المعلوماتية التي تسهل ارتكاب الجرائم الالكترونية كما سلف توضيحها.[6]

وبالتالي فإن تحول الاقتصاد العالمي من مرحلة الاقتصاد التقليدي إلى مرحلة الاقتصاد الرقمي وتحول التعاملات التجارية والمالية إلى شكل إلكتروني زاد من خطورة الجريمة الإلكترونية والتي أصبحت في تصاعد مستمر ومن المتوقع أن يتزايد حجم الخسائر التي يتكبدها العالم بسبب الجريمة الإلكترونية في العقود القليلة المقبلة، نتيجة تزايد عدد الشركات التي تعتمد على الإنترنت في ممارسة نشاطها.

فبحسب أخر الإحصائيات فإن الاقتصاد العالمي يتضرر جراء الجريمة الإلكترونية تريليون دولار سنوياً، غير أن الخطورة الحقيقية لا تنبع من ضخامة حجم الخسائر فقط، وإنما تنبع كذلك من القبول المتزايد لخسائر الجريمة الإلكترونية باعتبارها ضريبة لا مفر منها لممارسة الأعمال في مختلف أنحاء العالم، كما تشير التقديرات إلى أن الاقتصاد العالمي المستند إلى الإنترنت يولد سنوياً نحو ثلاثة تريليونات دولار، وهذا الرقم مرشح للنمو بقوة في العقود المقبلة، وتطال الجريمة الإلكترونية نسبة تتراوح بين 15 و20 في المائة من حجم هذا الاقتصاد العالمي المستند إلى الإنترنت.

وقد تم الإبلاغ عام 2019 عن ما يعادل 3800 حالة اختراق للبيانات مما أدى إلى اختراق أكثر من أربعة مليارات قاعدة بيانات الى الجرائم الالكترونية أدت للكثير من الخسائر.[7]

وقد تجاوزت التكلفة الإجمالية للتهديدات والجرائم الإلكترونية على مستوى العالم، عام 2021 ستتجاوز 6 تريليونات دولار، ويكون بذلك معدل الجريمة قد سجل ارتفاعا بنحو ثلاثة تريليونات دولار عما سجله في عام 2015.

و بحسب المنتدى الاقتصادي العالمي فإن ممارسات التزوير والقرصنة قد كلفت حوالي 1.77 تريليونات دولار في سنة 2015 ما يمثل قرابة 10 % من التجارة العالمية الإجمالية[8].

ولم تبق منطقة الشرق الأوسط بمنأى عن أخطار وتهديدات الجريمة الالكترونية ، حيث تعد من بين الأكثر تضررا في العالم، فما يعادل 56 % من شركات المنطقة التي تعرضت لهجوم إلكتروني خسرت ما يتجاوز 500 ألف دولار سنويا.[9]

---

[6] معاشي سميرة، **الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)**، مجلة المفكر المجلد 13، العدد 01، الصادرة في 2018/06/19، ص403.

[7] بن جدو بن علية، درار عياش، **الآثار الاقتصادية للجريمة الاقتصادية**، مجلة أبحاث اقتصادية معاصرة ، المجلد05، العدد01، الصادرة في 2022 ، ص 567.

[8] صراع كريمة، دقيش جمال، **الأبعاد الاقتصادية للجريمة الالكترونية**، المرجع السابق، ص 44.

[9] صراع كريمة، دقيش جمال، **الأبعاد الاقتصادية للجريمة الالكترونية**، المرجع نفسه، ص 44.

ففي الوقت الذي يخسر فيه الاقتصاد العالمي 0.8 في المائة من إجمالي الناتج المحلي العالمي نتيجة الجريمة الإلكترونية، فإن النسبة تقل عن 0.2 في المائة نتيجة القرصنة البحرية، أي إن الجريمة الإلكترونية تكبد الاقتصاد العالمي أربعة أمثال الخسائر التي تكبدها الاقتصاد العالمي نتيجة القرصنة البحرية ، وتتضح خطورة الجريمة الإلكترونية على الاقتصاد العالمي، عبر مقارنة الخسائر التي يتكبدها الاقتصاد العالمي من الجريمة الإلكترونية بحجم الخسائر التي يتكبدها الاقتصاد العالمي من مصادر تهديد أخرى ، وهي تجارة مربحة منخفضة التكلفة قليلة المخاطر تدر أرباحاً طائلة، تزيد على إجمالي الدخل القومي للكثير من الدول.[10]

ولا تقتصر خسائر الجريمة الإلكترونية فقط على الخسائر المباشرة، وإنما تشمل أيضاً الخسائر غير المباشرة مثل حقوق الملكية الفكرية [11]، وسرقة الأصول المالية والمعلومات التجارية الحساسة، وتكلفة استعادة البيانات وتكلفة الفرص البديلة وبطبيعة الحال لا يمكن تجاهل تأثير الجريمة الإلكترونية على الاقتصاد الوطني، وعلى أداء الشركات وعلى حركة التجارة العالمية، وعلى القدرة التنافسية والابتكار.

ثانيا: الجهود الدولية والوطنية للتصدي للجريمة الالكترونية:

انصبت الجهود الدولية والإقليمية على وضع أطر قانونية للحماية من الجريمة الالكترونية، حيث وفي هذا المجال أنعقد مؤتمر القمة العالمي المعني بمجتمع المعلومات بجنيف عام 2003، ثم بتونس عام 2005، حيث توصل المجتمعون من خلال هذا المؤتمر إلى ضرورة تعزيز الثقة و الأمن بمجتمع المعلومات ووضع الأطر اللازمة لتحقيق ذلك، وقد تمت المصادقة على نتائج هذا المؤتمر أكثر من 174 دولة حول العالم.

كذلك يمكن في هذا المقام الإشارة إلى اتفاقية مجلس أوروبا بشأن الجريمة الالكترونية أو ما يعرف باتفاقية بودابست لعام 2001، والتي دخلت حيز النفاذ عام 2004، والتي ترمي إلى توحيد السياسة الجنائية للدول الأعضاء في مجال الجريمة المعلوماتية، كما سهلت التنسيق بين مختلف السلطات الوطنية في مجال مكافحة الإجرام المعلوماتي والحد منه ، إضافة إلى إرساء قواعد إجرائية للتعاون الدولي تتميز بالسرعة والفاعلية وتعزيز التعاون الإقليمي في هذا الخصوص بين الدول الأوروبية.

[10] صراع كريمة، دقيش جمال، **الأبعاد الاقتصادية للجريمة الالكترونية**، المرجع نفسه، ص 45.

[11] عاقلي فضيلة، **حماية حقوق الملكية الفكرية والصناعية من الجريمة المعلوماتية**، مجلة الاقتصاد الصناعي، مجلد 07 ، العدد 02، ص ص 231-251.

دون أن ننسى في هذا الصدد جهود منظمة الأمم المتحدة لمحاربة الجريمة الالكترونية [12]، وكذا الجهود العربية التي أسفرت عن توقيع اتفاقية لمكافحة جرائم تقنية المعلومات بمقر جامعة الدول العربية عام 2010، وذلك بهدف تعزيز التعاون العربي لمكافحة الجرائم الالكترونية.

كما أنه وعلى المستوى الوطني فرغم تضرر الجزائر من الجرائم الالكترونية على غرار باقي دول العالم والدول العربية إلا أنها لم تبادر إلى سن قوانين في هذا المجال إلا حديثا ويتعلق الأمر أساسا بتعديل قانون العقوبات الجزائري بموجب القانون 15/04 المؤرخ في 2004/11/10 حيث تمت معالجة هذا الموضوع بالقسم السابع تحت عنون" المساس بأنظمة المعالجة الآلية للمعطيات " ضمن المواد 394 إلى غاية المادة 394 مكرر 6 معالجا بذلك أنواع الجرائم الالكترونية وعقوباتها[13].

لإضافة للقانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والذي يهدف إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[14].

وبناء على ما سبق فإن التصدي للجرائم الاقتصادية الماسة بالجانب الاقتصادي يتطلب بذل المزيد من الجهود الدولية والإقليمية والوطنية بغية التخفيف من أثارها السلبية وتهديدها للتنمية الاقتصادية والتي تتزايد يوما بعد يوم، الأمر الذي تعكسه الإحصاءات الصادرة عن مختلف الجهات المهتمة بهذه الظاهرة، خاصة أمام التزايد الملحوظ في اللجوء إلى ممارسة مختلف الأنشطة التجارية عبر شبكات الانترنت.

خاتمة :

إن التطور المتسارع لتكنولوجيا المعلومات أدت الى لاستحداث أشكال جديدة من الجرائم لم تكن معروفة قبلا، شكلت تهديدا على الجانب الاقتصادي من خلال أثارها المادية وغير المادية والتي قد تصل إلى حد المساس بالأمن للدول.

بالإضافة إلى أن الأفراد يعانون من انتهاك الخصوصية أو سرقة المعلومات وتعرضهم للابتزاز وتعطيل الحواسب الشخصية وسرقة معلومات بطاقات الائتمان، كما تكون الخسائر أكبر بالنسبة للمؤسسات المالية والبنوك، ناهيك عن السرقات المتعلقة بالملكية الفكرية.

---

[12] للاستزادة في هذا الموضوع أنظر، بيدي أمال، **جهود الأمم المتحدة لمكافحة الجريمة السيبرانية**، مجلة البحوث في الحقوق و العلوم السياسية ، الصادرة في جوان 2022، المجلد 08، العدد 01 ، ص ص 299-316.

[13] **القانون رقم 15/04 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004** المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات الجزائري، ج ر عدد 71 الصادرة في : 2004/11/10.

[14] **القانون 04/09 المؤرخ في 2009/08/05**، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47، الصادرة في : 2009/08/16

ومن خلال النتائج المتوصل إليها من خلال هذه الدراسة فإننا نوصي بما يلي:

- ضرورة سن قوانين وفرض عقوبات صارمة على مرتكبي الجرائم الالكترونية على مختلف أنواعها وأثارها.
- تعزيز التعاون الدولي والإقليمي للتصدي الفعال لهذه الجرائم.
- توعية المؤسسات والأفراد بخطورة الآثار الناتجة عن التعرض للجرائم الالكترونية و العمل على تدريبهم وتأهيلهم بأحدث الوسائل والتقنيات.
- تطوير برمجيات الأمن بكل دوري، وتأمين وسائل التحويل الالكتروني والبطاقات الائتمانية وبرامج وأجهزة البنوك والمؤسسات المالية والاقتصادية باعتبارها الأكثر عرضة لهذه الجرائم كل ذلك لغرض تحقيق غرض هام وهو حماية اقتصاديات الدول من الآثار السلبية للجرائم الالكترونية المتزايدة يوما بعد يوم.

قائمة المصادر والمراجع:

- **القانون رقم 15/04 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004** المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات الجزائري، ج ر عدد 71 الصادرة في : 2004/11/10.

- **القانون 04/09 المؤرخ في 2009/08/05**، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47، الصادرة في : 2009/08/16
- ألاء محمد رحيم حمادي، **الجريمة السبيرانية ومخاطرها على الأفراد** (الإشكاليات و الحلول)(دراسة تحليلية في ضوء الإحصائيات الدولية والعربية والوطنية)، مجلة كلية التربية للبنات، جامعة بغداد، مجلد 28، عدد04، 2017.
- بيدي أمال، **جهود الأمم المتحدة لمكافحة الجريمة السبيرانية** ، مجلة البحوث في الحقوق و العلوم السياسية ، الصادرة في جوان 2022، المجلد 08، العدد 01.

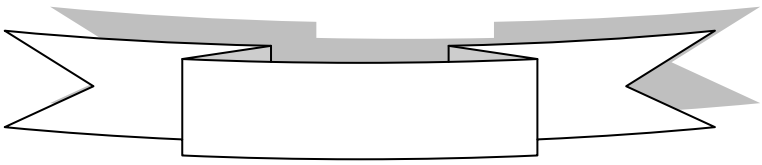
- عاقلي فضيلة، **حماية حقوق الملكية الفكرية والصناعية من الجريمة المعلوماتية** ، مجلة الاقتصاد الصناعي، مجلد 07 ، العدد 02.

- بن جدو بن علية، درار عياش، **الآثار الاقتصادية للجريمة الاقتصادية** ، مجلة أبحاث اقتصادية معاصرة ، المجلد05، العدد01، الصادرة في 2022 .

- معاشي سميرة، **الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)** ، مجلة المفكر المجلد 13، العدد 01، الصادرة في 2018/06/19.

- صراع كريمة، دقيش جمال، **الأبعاد الاقتصادية للجريمة الالكترونية** ، مجلة الدراسات التسويقية وإدارة الأعمال، المجلد02، العدد01، جانفي 2018.

- حسان سعاد، **إثبات التعاملات الالكترونية وفقا للقانون الجزائري والتشريعات المقارنة** ، الطبعة الأولى، دار الوفاء للطباعة والنشر، الإسكندرية، 2019.



موشارة حنان
mouchara.hanane@gmail.com
جامعة 08 ماي 1945 قالمة

الجرائم الإلكترونية الاقتصادية
وآثارها على جباية التجارة الإلكترونية

الملخص:

تعد التجارة الإلكترونية عاملا مؤثرا في نمو اقتصاديات الدول وتعزيز تجارتها الخارجية ، كما أنها أصبحت مصطلحا شائعا يفضله المتعاملون الاقتصاديون كونها أسرع وأسهل وأقل تكلفة. وهو ما انعكس إيجابا على حجم المعاملات الإلكترونية التي حققت أرقاما قياسية خاصة في الدول المتقدمة، لذلك حاولت الحكومات استغلال ذلك في زيادة مداخيلها الضريبية.

إلا أنه على الرغم من المزايا التي تحققها التجارة الإلكترونية خاصة الجبائية منها ، فإن تطور الوسائل المستخدمة فيها واتساع نطاقها أدى إلى ظهور مشاكل عديدة تهدد انتشارها، والتي تعد الجرائم الإلكترونية في مقدمتها على اعتبار أنها ستؤثر سلبا على انتشار استخدام التجارة الإلكترونية وهو ما يؤدي إلى تراجع حجم التعاملات والمبادلات المالية وبالتالي يترتب عنه نقصان حجم المعاملات الخاضعة للضريبة

الكلمات المفتاحية: تجارة إلكترونية-جريمة إلكترونية- جباية التجارة الإلكترونية

***Abstract*:**

E-commerce is an influential factor in growing the economies of countries and promoting their foreign trade, it has also become a common term preferred by economic traders as it is faster, easier and cheaper. This reflected positively in the volume of electronic transactions which reached record figures, especially in developed countries, so governments tried to take advantage of this to increase their tax revenues.

However, despite the advantages provided by e-commerce, especially fiscal ones, the development of the means used in it and the widening of its field of action have brought to light many problems threatening its spread, which is at the forefront of cybercrime on the grounds that it will adversely affect the spread of e-commerce usage, resulting in a decrease in the volume of financial transactions and trade, and consequently, a decrease in the volume of taxable transactions

***Keywords**: Electronic commerce-Electronic crime- Electronic commerce taxation.*

المقدمة"

شهد العالم تطورات عديدة نتيجة ثورة تكنولوجيا الاتصالات الحديثة. ففي ظل انتشار الانترنيت شاع مفهوم التجارة الإلكترونية التي تتيح العديد من المزايا. حيث تكمن أهمية التجارة الإلكترونية في أنها أصبحت عاملا مؤثرا في نمو اقتصاديات الدول وتعزيز تجارتها الخارجية، وقد غدت وسيلة هامة في زيادة المقدرة

التنافسية من تسويق للمنتجات وتوفير المعلومات والخدمات الفورية للمتعاملين، إضافة إلى تمكين المستهلك أينما كان من الطلب الفوري للسلع والخدمات.

فالتجارة الإلكترونية أصبحت مصطلحا شائعا يفضله المتعاملون الاقتصاديون كونها أسرع وأسهل وأقل تكلفة. وهو ما أنعكس إيجابا على حجم المعاملات الإلكترونية التي حققت أرقاما قياسية خاصة في الدول المتقدمة، لذلك حاولت الحكومات استغلال ذلك في زيادة مداخيلها الضريبية.

إلا أنه على الرغم من المزايا التي تحققها التجارة الإلكترونية، فإن تطور الوسائل المستخدمة فيها وإتساع نطاقها أدى إلى ظهور مشاكل عديدة تهدد إنتشارها. فعلى الرغم من أهمية الوسائل الإلكترونية إلا أن الاستخدام غير المشروع لها أدى لظهور نوع جديد من الجرائم مرتبطة بالشبكة الإلكترونية تسمى الجرائم الإلكترونية فتفاقم الاعتداءات على الأنظمة المعلوماتية استدعى تدخلا تشريعياخاصة وأن اللجوء إلى التجارة الإلكترونية أصبح أمرا حتميا، فهي تساهم في تصريف المنتجات للحد من ظاهرة الركود الاقتصادي التي تسبب فيها وباء كورونا.

وبالتالي فإن الجرائم الإلكترونية ستؤثر سلبا على انتشار استخدام التجارة الإلكترونية وهو ما يؤدي إلى تراجع حجم التعاملات والمبادلات المالية وبالتالي يترتب عنه نقصان حجم المعاملات الخاضعة للضريبة. ففيما تتمثل الجرائم الإلكترونية وما هي آثراها على الجباية الإلكترونية؟

للإجابة على هذه الإشكالية ستقسم المداخلة كما يلي:

المبحث الأول: النظام القانوني لجباية التجارة الإلكترونية

المطلب الأول: مدخل مفاهيمي.

المطلب الثاني: متطلبات فرض الجباية على التجارة الإلكترونية

المبحث الثاني: انعكاسات الجرائم الإلكترونية على الجباية الإلكترونية

المطلب الأول: تعريف الجريمة الإلكترونية

المطلب الثاني: مكافحة الجريمة الإلكترونية في التشريع الجزائري

المبحث الأول: النظام القانوني لجباية التجارة الإلكترونية

المطلب الأول: مدخل مفاهيمي.

الفرع الأول: مفهوم التجارة الإلكترونية

تعد التجارة الإلكترونية من أصعب المفاهيم التي تناولها الفقه لارتباطها بأمور تقنية بحتة، لذلك سيتم تعريفها ثم بيان أشكالها وأخيرا التعرض لخصائصها

أولا: تعريف التجارة الإلكترونية.

ظهر عدة تعريفات يحاول كل منها أن يصف ويحدد طبيعة هذه التجارة الإلكترونية وما يتعلق بها من ممارسات وأنشطة. وربما يرجع تعدد هذه التعريفات إلى أن تطبيقات التجارة الإلكترونية تشتمل على عدة مكونات أساسية لابد من توفرها لتنفيذ عمليات التجارة الإلكترونية، مثل استخدام الحواسب الآلية وتقنية

الاتصالات ونظم المعلومات والبرمجيات وغيرها. ومفهوم التجارة الإلكترونية بعامة يندرج تحت مفهوم أوسع يسمى بالاقتصاد الرقمي (Digital Economy) حيث يشمل الأخير التجارة الإلكترونية والقطاعات المنتجة والمستخدمة لتقنية المعلومات، وأجهزة الاتصالات، وقطاعات خدمات الاتصالات.

لكن بالرغم من هذا فإنه يجب أن ننظر إلى تعبير التجارة الإلكترونية من خلال تقسيمه إلى قسمين، القسم الأول: التجارة، هي مصطلح يعبر عن نشاط إقتصادي يتم من خلاله تداول السلع و الخدمات بين الحكومات و المؤسسات و الأفراد في إطار نظم و قواعد متفق عليها . أما القسم الثاني: الإلكترونية، هي مجال أداء النشاط المحدد في المقطع الأول أي التجارة و يقصد به أداء النشاط التجاري باستخدام الوسائط و الأساليب الإلكترونية و التي تدخل كواحدة من أهم هذه الوسائط[1] .

ثانيا: أشكال التجارة التجارة الإلكترونية.

سنحاول أن نختصر الحديث عن اشكال التجارة الإلكترونية[2] في العناصر التالية :

1-بين مؤسسة ومؤسسة أخرى Business to Business :

أو ما يرمز إليه بـ B to B حيث تمرر مؤسسة من خلال شبكة الأنترنيت طلبات شراء أو عروض بيع لمؤسسات أخرى وما يتبعها من عناصر متعلقة بالمعاملة التجارية من فواتير ودفع وغيرها .

2-بين المؤسسة والمستهلكconsumer Business to :

أو ما يرمز له بـ B to C ، وذلك من خلال العروض المختلفة التي تقدمها المؤسسات للمستهلكين على ما يسمى مراكز التسوق على الأنترنيت ، حيث تعرض كل أنواع السلع والخدمات ويتم أيضا هنا تنفيذ عمليات الشراء والبيع بأسس وتقنيات حديثة كالدفع عن طريق بطاقات الإئتمان أو الشيكات الإلكترونية ....إلخ .

3-بين المؤسسة والإدارةAdministration Business to:

أو ما يرمز له بـ B to A ، حيث يمكن للمؤسسة أن تجري معاملاتها – أو إلتزاماتها – أمام مختلف الإدارات الخاضعة لها ، كإدارة الضرائب والجمارك ، والتأمين وغيرها ، كأن تقوم بعمليات الدفع لمختلف المستحقات ، وأيضا تقديم التصريحات اللازمة مما يوفر الجهد والوقت .

4-بين المستهلكين والإدارة Administration to Consumer :

أو ما يرمز له بـ A to C ، وذلك من خلال ممارسات يلتزم بها المستهلك تجاه إدارته، كدفع الضرائب والرسوم ، وتقديم التصريحات إلى مختلف الهيئات الإدارية المعنية .

---

[1] **أحمد أمداح**، التجارة الإلكترونية من منظور الفقه الإسلامي، مذكرة ماجستير، تخصص فقه وأصوله، قسم الشريعة، كلية العلوم الاجتماعية والعلوم الإسلامية، جامعة الحاج لخضر-باتنة، 2005-2006، ص 7 وما يليها.

راجع أيضا:

-**مدحت رمضان**، الحماية الجنائية للتجارة الإلكترونية-دراسة مقارنة-، دار النهضة العربية، القاهرة، 2001، ص 12.

- **رأفت رضوان**، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، القاهرة، 1999، ص 13.

[2] راجع في تفصيل أشكال التجارة الإلكترونية: **أحمد أمداح**، المرجع السابق، ص 16 وما يليها.

ثالثا: خصائص التجارة الإلكترونية.

تتميز التجارة الإلكترونية بمجموعة من الخصائص تميزها عن التجارة التقليدية، تتمثل فيمايلي:

-عدم وجود علاقة مباشرة بين طرفي العملية التجارية حيث يتم التلاقي بينهما عن طريق شبكة الاتصالات ، ويتميز هذا الأسلوب بوجود درجة عالية من التفاعل بغض النظر عن وجود الطرفين في نفس الوقت على الشبكة.

-عدم وجود أي وثائق ورقية متبادلة في إجراء وتنفيذ المعاملات ، حيث كافة عمليات التفاعل تتم بطريقة إلكترونية ، ودون استخدام أي أوراق.

-إمكانية التفاعل مع أكثر من مصدر في الوقت نفسه، حيث يستطيع أحد الأطراف إرسال رسالة إلكترونية إلى عدد لا نهائي من المستقبلين في نفس الوقت، وبذلك تتوفر إمكانات بلا حدود للتفاعل الجمعي أو المتوازي وهو شئ غير مسبوق.

-إمكانية تنفيذ كل مكونات العملية التجارية. بما فيها تسليم السلع غير المادية على الشبكة وذلك بخلاف أي من وسائل الاتصال السابقة.

-توفر في النفقات الإدارية ونفقات الاتصال وغيرها، حيث تعتبر بديلاً عن تخصيص جزء كبير من رأس المال في إقامة علاقات مستمرة بين البائعين والمشترين، كما أنها تسمح بإتمام عملية التوزيع رأساً للمستهلك.

-تعتبر ذات أهمية خاصة لكل من المنتجين والمستهلكين في الدول النامية حيث تمكن من التغلب على الحواجز التقليدية للمسافة ونقص المعلومات.

الفرع الثاني: مفهوم الجباية الإلكترونية

بشكل عام يقصد بالجباية كل القوانين والقواعد المتعلقة بتحديد وتحصيل الضرائب.كما تعرف على أنها نظام من المساهمات الإلزامية المفروضة من قبل الدولة، وتأتي معظمها في شكل ضرائب تفرض على الأشخاص وعلى المؤسسات والممتلكات. ومن جهة أخرى عرفت الجباية باعتبارها مشتق اقتصادي هام يعكس الهيكل الاقتصادي والاجتماعي لتطوير المجتمع، لكونها أداة مالية وتدخلية لها أثارها المتعددة على المستوى الكلي أو الجزئي.وبالتالي فإن الجباية تعتبر بمثابة مجموعة من القواعد القانونية والإدارية التي تنظم مختلف الضرائب والرسوم، التي تحصلها لصالح الدولة والجماعات المحلية. وتعد بمثابة الوسيلة الضرورية لتحقيق للسياسة الاقتصادية والاجتماعية للدول[3]

المطلب الثاني: متطلبات فرض الجباية على التجارة الإلكترونية

الفرع الأول: الأساس القانوني لفرض الجباية على التجارة الإلكترونية

[3] **بوعزة عبد القادر وحميمش نرجس** ، "نحو حل مشاكل جباية التجارة الإلكترونية في إطار الجهود الدولية "، مجلة الإقتصاد وإدارة الأعمال، مجلد 1، عدد 2، 2017، ص 116.

بداية لم ينص المشرع الجزائري ضمن القانون 18-05 المتعلق بالتجارة الإلكترونية [4] على إلزامية تسجيل المورد الإلكتروني لدى مصالح الضرائب إلا أنه بالرجوع إلى المادة 11 من نفس القانون نجدها تضمنت أنه يجب أن يتضمن العرض التجاري الإلكتروني التعريف الجبائي. وبالتالي فإن نشاط التجارة الإلكترونية يخضع أيضا مثله مثل الأنشطة التجارية الإلكترونية للتسجيل لدى مصلحة الضرائب للحصول على رقم التعريف الجبائي[5].

وقد اتجهت الجزائر [6] إلى فرض ضريبة على التجارة الإلكترونية، حيث نصت المادة 10 من قانون المالية لسنة 2019[7] على فرض ضريبة جزافية بمعدل 5% على التجارة الإلكترونية والتي تنص على: "تحدث ضمن القسم الرابع من الباب الثاني من قانون الضرائب المباشرة والرسوم المماثلة، مادتان 282 مكرر 4أ، 282مكرر 5أ، تحرران كما يأتي:

"المادة 282 مكرر 4أ: استثناء لأحكام المواد 282مكرر إلى 282مكرر 4، فان الأشخاص الطبيعيين، مهما كانت وضعيتهم إزاء الفئات الأخرى من المداخيل، الذين ينشطون في إطار دائرة توزيع السلع والخدمات عبر منصات رقمية أو باللجوء إلى البيع المباشر على الشبكة، يخضعون لاقتطاع من المصدر محرر من الضريبة بمعدل % 5 بعنوان الضريبة الجزافية الوحيدة، يطبق على مبلغ الفاتورة مع احتساب كل الرسوم. ويطبق هذا الاقتطاع، حسب الحالة، من طرف مؤسسات إنتاج السلع والخدمات أومن طرف المؤسسات التي تنشط في مجال الشراء/ إعادة البيع.

كما يجب على المؤسسات المذكورة أعلاه، أن تطبق هذا الاقتطاع من المصدر بالنسبة للأشخاص غير المسجلين لحد الآن لدى الإدارة الجبائية والذين يحققون عمليات إنتاج للسلع والخدمات أو المؤسسات الناشطة في الشراء/ إعادة البيع.

---

[4] القانون رقم 18-05 المؤرخ في 24 شعبان 1439 الموافق 10 مايو 2018 المتعلق بالتجارة الإلكترونية، جريدة رسمية عدد 28 بتاريخ 30 شعبان 1439 الموافق 16 مايو 2018، ص 4

[5] راجع بالنسبة لمسألة إجراءات الحصول على رقم التعريف الجبائي:

عديد أمينة، "ضبط التجارة الإلكترونية آلية للحد من هدر الموارد الضريبية"، حوليات جامعة الجزائر 1، المجلد 35، العدد 1، 2021، ص 126.

[6] علما أن مسألة فرض ضريبة على التجارة الإلكترونية كانت محل العديد من النقاشات، فهناك من يرى ضرورة الإعفاء الضريبي على المبادلات التجارية الإلكترونية لضمان إنتشار هذا النوع من التجارة، في حين يرى آخرون ضرورة فرض ضريبة على عمليات التجارة الإلكترونية أسوة بالتجارة التقليدية.

راجع في تفصيل الإتجاهين:

العمري هاشمي وصالح بزة، "التجارة الإلكترونية في الجزائر واقعها وتحدياتها الضريبية"، مجلة أبحاث ودراسات التنمية، المجلد 8، العدد 2، ديسمبر 2021، ص 384 وما يليها.

بوعزة عبد القادر وحميمش نرجس، المرجع السابق، ص 117 وما يليها.

[7] قانون رقم 18-18 مؤرخ في 27 ديسمبر 2018يتضمن قانون المالية لسنة 2019 جريدة رسمية عدد 79 بتاريخ 30 ديسمبر 2018

تتم إعادة صب هذا الاقتطاع من طرف المؤسسات في العشرين من الشهر الذي يلي الفوترة، على الأكثر، لا تطبق أحكام المادة 282مكرر 3 على هذه الفئة من المكلفين بالضريبة"".

"المادة 212مكرر 5أ: طبقا لأحكام المادة 212مكرر 4أ أعلاه، يعاد صب ناتج الضريبة الجزافية الوحيدة المقتطع على شكل اقتطاع من المصدر، لفائدة ميزانية الدولة".

من جهة أخرى نصت المادتين 39 و 41 من قانون المالية لسنة 2020[8] على إخضاع معاملات التجارة الإلكترونية لأول مرة في الجزائر إلى الرسم على القيمة المضافة TVA.

الفرع الثاني: إجراءات فرض الجباية على التجارة الإلكترونية وتحدياتها

أولا: إجراءات فرض الجباية على التجارة الإلكترونية

تتم ممارسة التجارة الإلكترونية من طرف المورد الإلكتروني سواء كان شخص طبيعي أو معنوي(شركة)، وتعتبر الشركات الحالة الأكثر شيوعا ومن ثم تلزم بالقيام بجميع الالتزامات التصريحية التي تخضع لها الشركات الخاضعة للضريبة. ومع أن المشرع الجزائري لم ينص صراحة ضمن قوانين الضرائب المختلفة عن كيفية الإخضاع الضريبي لنشاط التجارة الإلكترونية إلا أن الأشخاص التي تمارس نشاط التجارة الإلكترونية (المورد الإلكتروني) تلتزم بتقديم التصريح بالوجود ويعد هذا التصريح إلتزام تبعي لعملية التسجيل على مستوى إدارة الضرائب ويخص التصريح بالوجود جميع المكلفين بالضريبة الجدد. بالإضافة إلى التصريح بالوجود يلتزم المورد الإلكتروني بالتصريح بالأرباح المحققة من معاملات التجارة الإلكترونية بتقديم ما يفيد رقم أعماله في المدة الزمنية المحددة[9].

وفي سبيل الإطلاع على حجم المعاملات التجارية الإلكترونية ونوعها وعائداتها يعتبر العقد الإلكتروني وسيلة تسهل لإدارة الضرائب بسط رقابتها على نشاطات التجارة الإلكترونية. حيث نص المشرع الجزائري في المادة 10 من القانون 18-05 المتعلق بالتجارة الإلكترونية على وجوب توثيق جميع المعاملات التجارية الإلكترونية بموجب عقد إلكتروني الذي يجب أن يتضمن حد أدنى من البيانات الواجب إدراجها فيها حددها المادة 13 من نفس القانون.

وحتى يكون للعقد الإلكتروني حجية بما يتضمنه في مواجهة إدارة الضرائب خلال عمليات الرقابة والتحقيقات التي تجريها من أجل التقدير الفعلي للمبلغ الضريبي الواجب التحصيل فإنه يتعين أن يكون المحرر الكتابي المعد للإثبات مقروءا حيث يتم التدوين بحروف أو رموز معروفة ومفهومة للشخص الذي يراد الإحتجاج عليه بهذا المحرر تعبيرا عن محتواه، كما يتعين أن تتوافر استمرارية الكتابة بمعنى ثبات الكتابة بحيث يمكن الرجوع إليها وقت الحاجة ويتحقق هذا الشرط باستخدام وسائط إلكترونية متطور تحقق فيها عنصر الثبات والاستمرارية بالنسبة لما دون عليها، كما يشترط لإسباغ حجية الإثبات على المحرر

[8] القانون رقم 19-14 المتضمن قانون المالية لسنة 2020 مؤرخ في 11 ديسمبر 2019جريدة رسمية عدد 81 بتاريخ 30 ديسمبر 2019.

[9] **عديد أمينة**،المرجع السابق، ص 128.

الإلكتروني أن يكون غير قابل للتعديل أي أن يكون ظاهرا فلا يتم هذا التعديل إلا بإتلاف المحرر أو يترك أثرا واضحا عليه، وعلة هذا الشـرط هو إضفاء عنـصر الثقة على ما هو مدون بالمحرر الإلكتروني[10].

وفي سـبيل تقدير المادة الخاضعة للضـريبة على ممارسي التـجارة الإلكترونـية تسـتعين إدارة الضرائب بكافة الوسائل التي تمكنها من تقدير قيمة الضـريبة ومن بين هذه الوسائل الفواتيـر المحررة من طرف الموردين الإلكترونين. كما يمكن لإدارة الضرائب الوقوف على طبيعة المعاملات المبرمة وعددها من خلال سجـل المعاملات الإلكـترونية الممـسوك من طرف المورد الإلكـتروني، غير أن المشرع لم يحدد طبيعة الملفات الواجب مسكها من طرف المورد الإلكتروني هل ينبغي أن تكون ملفات ورقية أم إلكترونية واكتفى بالنص على إلزامية إرسالها إلكترونيا فقط، ومما لاشك فيه أن للسجلات الإلكترونية دور كبير في الوقوف على حجم المعاملات الإلكترونية وطبيعتها، ويستمد هذا السجل الإلكتروني أثره القانوني إذا توافرت فيه الشروط معينة[11]

ثانيا: تحديات تطبيق جباية التجارة الإلكترونية

تواجه جباية التجارة الإلكترونية العديد من التحديات ترتبط بخصائص المعاملات التجارية الإلكترونية التي تميزها عن تلك التقليدية، حيث تتمثل أهم الخصائص التي تمتاز بها المعاملات التجارية الإلكترونية في[12]:

-إختفاء الوثائق الورقية، فالرسائل الإلكترونية هي الأثر الوحيد في مثل هذه التعاملات مما يسبب إشكالية إثبات المعاملة قانوناً.

-التوسع عبر العالم، فالمؤسسات التي تعتمد على التجارة الإلكترونية مهما كان حجمها تستفيد من التوسع الجغرافي لمعاملاتها عبر العالم، وهو ما يوقعها أمام تعارض مصالحها ومصالح حكومات الدول.

-الإنفصال المكاني، فشبكة الإنترنت تتيح للمؤسسات إدارة تعاملاتها من أي موقع جغرافي، ويمكن لمقر المؤسسة أن يكون في أي مكان دون أن يؤثر على أداء المؤسسة، وتعتمد المؤسسات في هذا السياق على عدة مقرات في عدة دول لتسهيل الاتصال بالعملاء.

-عدم إمكانية تحديد الهوية، فلا يملك الطرفان المتعاملان كل المعلومات الأساسية عن بعضهما، وهو ما يقيد استكمال البائع للملفات الضريبية المطلوبة منه قانوناً، كما أنه قد يستخدم هذا كحجة للتهرب من الضريبة.

-المنتجات الرقمية، فشبكة الإنترنت تتيح تبادل منتجات رقمية(غير منظورة) كالبرمجيات، الملفات الموسيقية وغيرها، ويجدر الإشارة لأنه هذه المنتجات تشكل تحدياً نظرا لعدم وجود آليات متفق عليها لإخضاعها للضريبة؛

---

[10] **عديد أمينة**،المرجع السابق، ص 129.

[11] راجع في تفصيل هذه الشروط:

ناهد فتحي الحموري، الأوراق التجارية الإلكترونية -دراسة تحليلية مقارنة-، دار الثقافة، الأردن، 2009، ص 78 وما يليها.

[12] **بوعزة عبد القادر وحميمش نرجس**، المرجع السابق، ص 118.

-سرعة تغير القواعد المطبقة، فلا بد من صياغة إطار تشريعي يتسم بالمرونة ليواكب التغيرات الناتجة عن التقدم التكنولوجي

تتمثل أهم التحديات التي تواجه جباية التجارة الإلكترونية في[13]:

-**التواجد المكاني:** حيث أن المؤسسات ومزودي الخدمات والسلع المتداولة عبر المنصات الرقمية تتنوع بين مؤسسات جزائرية وأخرى أجنبية، وبين المستقرة في الجزائر ولها هويتها الجبائية ومقرها المعلوم، وتلك المتواجدة خارج الجزائر، سواء معلومة او مجهولة، وهو ما ينشئ عنه الكثير من العقبات من خلال تحديد الدولة التي لديها الحق في فرض الضرائب، وكذلك حتى بعد اقتطاعها من المصدر بالنسبة للمؤسسات الغير مستوطنة في الجزائر ما هي سبل ووسائل تحويل الأموال، وهل هناك اتفاقيات ثنائية بن الدولة المقر والجزائر.

-**طبيعة التعاملات والسلع والخدمات المتداولة:** كما هو الحال عليه في التجارة التقليدية حيث هناك صعوبات كبيرة لمراقبة وتحديد قيمة التعاملات المتداولة بن الأطراف، وبالتالي تحديد الوعاء الضريبي وقيمة الضريبة، فالحال أكثر تعقيدا في نشاط التجارة الالكترونية المتسم بعالمية النشاط وتداول السلع والخدمات غير الملموسة، وبتحويل للأموال والعوائد بدون وثائق وأوراق رسمية ملموسة، بل عبر منصات رقمية يصعب إثباتها ومراقبتها،

-**المؤهل البشري:** نقص الكادر البشري المؤهل والمتخصص في مجال المعلوماتية في إدارة الضرائب، لمواكبة التطور التقني المتسارع لتنكولوجيا الاتصال المستخدمة في التجارة الالكترونية والمبادلات الرقمية.

-**البنية التقنية:** الافتقار للوسائل والتقنيات الحديثة المتطورة لمراقبة ومسايرة الوسائل التقنية المستخدمة في التجارة الالكترونية والمبادلات الالكترونية.

المبحث الثاني: إنعكاسات الجرائم الإلكترونية على الجباية الإلكترونية

المطلب الأول: تعريف الجريمة الإلكترونية

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية، ويعود ذلك للإختلاف حول تحدي نطاق هذه الجريمة، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق، والبعض الآخر ينظر إليها بمفهوم موسع.

فبالنسبة للإتجاه المضيق لتعريف الجريمة الإلكترونية يرى أنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لإرتكابه من ناحية، لملاحقته وتحقيقه من ناحية أخرى"[14].

على عكس الإتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الأنترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الإجتماعية، بهدف إلحاق الضرر.

---

[13] **العمري هاشمي وصالح بزة**، المرجع السابق، ص 388

[14] **حمزة بن عقون** ، السلوك الإجرامي للمجرم المعلوماتي، شهادة ماجستير، تخصص علم الإجرام والعقاب، جامعة باتنة، 2012، ص 13.

أما المشرع الجزائري فقد تطرق للجريمة الإلكترونية تحت مسمى الجرائم المتصلة بتكنولوجيا الإعلام والإتصال والتي عرفتها المادة 2 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها [15] على أنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية".

المطلب الثاني: مكافحة الجريمة الإلكترونية في التشريع الجزائري

إن تفاقم الإعتداءات على الانظمة المعلوماتية خاصة مع ضعف الحماية الفنية استدعى تدخلا تشريعيا لذلك استدرك المشرع الجزائري الفراغ القانوني بتعديل قانون العقوبات بموجب القانون 04-15[16] باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات" فأدرجت بذلك المواد من 394 مكرر إلى 394 مكرر 7.

حيث تعد الجرائم الإلكترونية [17] من الجرائم المستحدثة نظرا لإرتباطها بالتقنيات الحديثة من أجهزة كمبيوتر وشبكات أنترنيت.

عرف المشرع الجزائري نظام المعالجة الآلية للمعطيات بأنه: "كل نظام أو مجموعة من الانظمة منفصلة كانت أم متصلة بعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[18] . حيث يمكن أن تتخذ الجريمة هنا إحدى الصور[19] التالية:

---

[15]القانون 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 يتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، جريدة رسمية عدد 47 صادرة بتاريخ 2009/08/16.

[16]قانون 04-15 مؤرخ في 2004/11/10 يعدل ويتمم الامر 66-156 يتضمن قانون العقوبات الجزائري، جريدة رسمية عدد 71 بتاريخ 2004/11/10.

[17]راجع في تفصيل تعريف الجريمة الإلكترونية:

-**برناوي راضية وزعيطي آمنة** ، " مكافحة الجرائم الإلكترونية في ضوء قانون العقوبات الجزائري دراسة مقارنة "، مجلة حقوق الإنسان والحريات العامة، جامعة مستغانم، مجلد 4، عدد 7، جوان 2019.

-**ونوغي نبيل وزيوش عبد الرؤوف**، "الجريمة المعلوماتية في التشريع الجزائري"، مجلة العلوم القانونية والإجتماعية جامعة زيان عاشور الجلفة-الجزائر، المجلد 4، العدد 3، سبتمبر 2019، ص 127 إلى ص 139

[18]المادة 2 من القانون 09-04 يتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

راجع في تفصيل مفهوم أنظمة المعالجة الآلية للمعطيات:

-**رابحي عزيزة**، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه ، قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان-الجزائر، ص 56 وما يليها.

-**بوبرقيق عبد الرحيم**، "مفهوم أنظمة المعالجة الآلية للمعطيات في الجرائم المحددة في المواد 394 مكرر إلى 394 مكرر 2 من قانون العقوبات الجزائري"، مجلة الدراسات والبحوث القانونية، المجلد 4، العدد 1، جوان 2019.

[19]راجع في تفصيل هذه الصور:

قسيمة محمد وخضري حمزة، "مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في قانون العقوبات الجزائري"، مجلة صوت القانون، المجلد 7، العدد 2، نوفمبر 2020، ص 126 إلى ص 150.

1-تجريم الإعتداء على نظظام المعالجة الآلية للمعطيات

حيث يأخذ الإعتداء على نظام المعالجة الآلية للمعطيات صورتين، الأولى بسيطة والثانية مشددة.

أ-الصورة البسيطة لجريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات : نصت عليها المادة 394 مكرر فقرة 1 من قانون العقوبات الجزائري، إذ يشترط لقيام هذه الجريمة توفر الركنين المادي والمعنوي[20] لتكون العقوبة المقررة هي الحبس من 3 أشهر إلى سنة حبس و 50000 دج إلى 100000 دج غرامة.

ب-الصورة المشددة لجريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات: نصت عليها المادة 394 مكرر فقرة 2،3 من قانون العقوبات الجزائري والتي تضمنت ظرفين مشددين لعقوبة الدخول أو البقاء داخل النظام لتصبح العقوبة المقررة هي الحبس من 6 أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج ، حيث يتمثل الظرفان في[21]:

-إذا ما نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحويها النظام

- إذا ما نتج عن الدخول أو البقاء غير المشروع عدم قدرة النظام على تأدية وظيفته.

علما أنه يكفي لتطبيق الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، فالمشرع الجزائري إعتبر النتيجة ذاتها ظرفا مشددا في الجريمة.

2-الإعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام.

فالإعتداء هنا يهف إلى الإضرار بمعلومات الكمبيوتر أو وظائفه سواء بالمساس بسريتها أو المساس بسلامة محتوياتها، وتكون عقوبته الحبس من 6 أشهر إلى 3 سنوات وغرامة من 500000 دج إلى 2000000 دج. ويتخذ الإعتداء ثلاث صور، إما فعل الإدخال أو المحو أو التعديل[22].

3-المساس العمدي بالمعطيات خارج النظام.

فنص المادة 394 مكرر 2 قانون عقوبات جزائري يستهدف حماية المعطيات في حد ذاتها لأنها لم تشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم برمجتها آليا فمحل الجريمة هو المعطيات سواء كانت مخزنة أم لا. ويتخذ الفعل المادي لهذه الجريمة إحدى الصورتين:

-تصميم أو بحث او تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية.

---

[20]راجع في تفصيل ذلك:

رابحي عزيزة،المرجع السابق، ص 154 وما يليها.

[21]**أمجدي بوزينة آمنة** ، "خصوصية قواعد التجريم عن الإعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري"، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، العدد 5، مارس 2020، ص 79.

[22]راجع في تفصيل هذه الصور:

نبيل صقر، جرائم الكمبيوتر والانترنيت-موسوعة الفكر القانوني-، دار الهلال للخدمات الإعلامية، الجزائر، 2005، ص 141 وما يليها.

-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها.

وتكون العقوبة في هذه الحالة الحبس من شهرين إلى 3 سنوات وغرامة من 1000000 دج إلى 5000000 دج.

الخاتمة

في الاخير يمكن القول أنه على الرغم من إيجابيات التجارة الإلكترونية ودورها في دعم الإقتصاد الوطني إلا أنها إرتباطها بنظم الحاسب الآلي جعلها مهددة بالعديد من الجرائم المستحدثة، وهو ما قد يعيد إنتشارها. لذلك حاول المشرع الجزائري من خلال قانون العقوبات والقوانين الخاصة الأخرى التصدي لمثل هذا الإجرام.

إلا أن الملاحظ أن المشرع الجزائري لم يوفق كثيرا في التصدي لذلك لوجود جملة من النقائص إعترت تلك النصوص خاصة تلك المنصوص عليها في قانون العقوبات والذي يحكمه مبدأ أساس أنه لاجريمة ولا عقوبة إلا بنص. فمن بين تلك النقائص عدم شمول النصوص القانونية لمختلف الجرائم المعلوماتية إضافة إلى عدم التركيز على مسألة الشروع في تلك الجرائم.

لذلك لابد من تعديل هذه النصوص لتتلاءم مع طبيعة جرائم الانترنيت وتطورها المستمر، إضافة إلى النص على ضرورة التكوين لكافة الأشخاص المكلفين بالكشف عن هذه الجرائم بإخضاهم لدورات تكوينية، خاصة فيما يتعلق بموظفي إدارة الضرائب لتطوير مهاراتهم في مجال تكنولوجيا الإعلام بما يسهل عليهم التقدير السليم للضرائب المستحقة وكذا كشف أي تلاعب أو تدليس مرتكب من قبل ممارسي التجارة الإلكترونية

قائمة المراجع

أولا: القوانين

1. قانون 04-15 مؤرخ في 2004/11/10 يعدل ويتمم الامر 66-156 يتضمن قانون العقوبات الجزائري، جريدة رسمية عدد 71 بتاريخ 2004/11/10
2. القانون 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 يتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، جريدة رسمية عدد 47 صادرة بتاريخ 2009/08/16
3. القانون رقم 18-05 المؤرخ في 24 شعبان 1439 الموافق 10 مايو 2018 المتعلق بالتجارة الإلكترونية، جريدة رسمية عدد 28 بتاريخ 30 شعبان 1439 الموافق 16 مايو 2018، ص 4
4. القانون رقم 18-18 مؤرخ في 27 ديسمبر 2018يتضمن قانون المالية لسنة 2019 جريدة رسمية عدد 79 بتاريخ 30 ديسمبر 2018

5. القانون رقم 19-14 المتضمن قانون المالية لسنة 2020 مؤرخ في 11 ديسمبر 2019، جريدة رسمية عدد 81 بتاريخ 30 ديسمبر 2019.

ثانيا: الكتب

1. **رأفت رضوان**، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، القاهرة، 1999.
2. **مدحت رمضان**، الحماية الجنائية للتجارة الإلكترونية-دراسة مقارنة-، دار النهضة العربية، القاهرة، 2001.
3. **ناهد فتحي الحموري** ، الأوراق التجارية الإلكترونية -دراسة تحليلية مقارنة-، دار الثقافة، الأردن، 2009
4. **نبيل صقر**، جرائم الكمبيوتر والانترنيت-موسوعة الفكر القانوني-، دار الهلال للخدمات الإعلامية، الجزائر، 2005

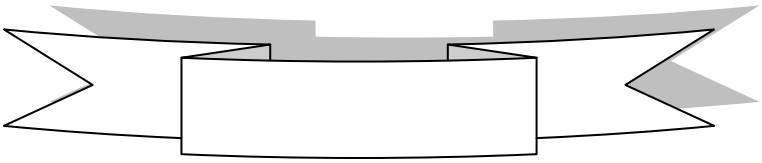
ثالثا: الرسائل

1. **أحمد أمداح**، التجارة الإلكترونيةمن منظور الفقه الإسلامي، مذكرة ماجستير، تخصص فقه وأصوله، قسم الشريعة، كلية العلوم الإجتماعية والعلوم الإسلامية، جامعة الحاج لخضر-باتنة، 2005-2006.
2. **حمزة بن عقون** ، السلوك الإجرامي للمجرم المعلوماتي، شهادة ماجستير، تخصص علم الإجرام والعقاب، جامعة باتنة، 2012
3. **رابحي عزيزة**، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه ، قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان-الجزائر.

رابعا: المقالات

1. **أمجدي بوزينة آمنة**، "خصوصية قواعد التجريم عن الإعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري"، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، العدد 5، مارس 2020
2. **برناوي راضية وزعيطي آمنة** ، " مكافحة الجرائم الإلكترونية في ضوء قانون العقوبات الجزائري دراسة مقارنة"، مجلة حقوق الإنسان والحريات العامة، جامعة مستغانم، مجلد 4، عدد 7، جوان 2019.
3. **بوعزة عبد القادر وحميمش نرجس** ، "نحو حل مشاكل جباية التجارة الإلكترونية في إطار الجهود الدولية"، مجلة الإقتصاد وإدارة الأعمال، مجلد 1، عدد 2، 2017
4. **عديد أمينة**، "ضبط التجارة الإلكترونية آلية للحد من هدر الموارد الضريبية"، حوليات جامعة الجزائر 1، المجلد 35، العدد 1، 2021
5. **العمري هاشمي وصالح بزة** ، "التجارة الإلكترونية في الجزائر واقعها وتحدياتها الضريبية"، مجلة أبحاث ودراسات التنمية، المجلد 8، العدد 2، ديسمبر 2021.

6. **قسيمة محمد وخضري حمزة** ، "مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في قانون العقوبات الجزائري"، مجلة صوت القانون، المجلد 7، العدد 2، نوفمبر 2020.
7. **–وبرقيق عبد الرحيم**، "مفهوم أنظمة المعالجة الآلية للمعطيات في الجرائم المحددة في المواد 394 مكرر إلى 394 مكرر 2 من قانون العقوبات الجزائري"، مجلة الدراسات والبحوث القانونية، المجلد 4، العدد 1، جوان 2019.
8. **ونوغي نبيل وزيوش عبد الرؤوف** ، " الجريمة المعلوماتية في التشريع الجزائري "، مجلة العلوم القانونية والإجتماعية جامعة زيان عاشور الجلفة–الجزائر، المجلد 4، العدد 3، سبتمبر 2019.



مـــــامـــــي هاجر
hadjer.droitpriv2018@gmail.com
جامعة الجزائر -1-

أشكال الجريمة الالكترونية الاقتصادية وآثارها على المتعاملين الاقتصاديين

الملخص:

خصصت هذه الورقة البحثية لدراسة جانب من جوانب موضوع يتسم بالحداثة والعمق، يتعلق بالجريمة الالكترونية الاقتصادية وما مدى تأثيرها على التنمية، خاصة وما يعرفه العالم من سرعة في التقدم العلمي ،التقني و التكنولوجي ،حيث تكمن أهمية هذه الورقة البحثية كونها تناولت موضوعا حديثا، سريعا ومتجددا، لاسيما في ظل ارتفاع نسبة الجريمة الالكترونية الاقتصادية، تعدد أشكالها، صورها و أنماطها.

تتنوع أشكال وصور هذه الجرائم الماسة بالاقتصاد في البيئة الرقمية من تلك المتعلقة بالملكية الفكرية، تبييض الأموال وبجرائم المصارف، والتي تتمّ من خلال برامج الفيروسات و التجسس، الاختراق و قرصنة البيانات و التصيد. وتتميز باختلاف مراحلها وذكاء مرتكبيها وانعكاساتها الخطيرة و المكلّفة على المتعاملين الاقتصادية و بالتالي التأثير السلبي على التنمية الاقتصادية للدول.

Abstract :

This research paper is devoted to studying an aspect of a topic characterized by modernity and depth, related to economic electronic crime and its impact on development, especially what the world knows about the speed of scientific, technical and technological progress, where the importance of this research paper lies in the fact that it dealt with a recent, rapid and renewed topic, especially in light of the high rate of economic cybercrime, in its many forms, forms and patterns.

The forms and forms of these crimes affecting the economy in the digital environment vary, including those related to intellectual property, money laundering and banking crimes, which are carried out through virus and spyware programs, hacking, data piracy and phishing. It is characterized by its different stages, the intelligence of its perpetrators; it's dangerous and costly repercussions on economic operators, and consequently the negative impact on the economic development of countries.

المقدمة:

في ظل الانفتاح المعلوماتي ،التكنولوجي والعولمة الرقمية وبروز تقنيات الثورة الصناعية الخامسة والذكاء الاصطناعي، في مختلف القطاعات الأمر الذي أسهم في زيادة تفشي الجرائم الالكترونية بضرب الأمن المعلوماتي للبنية الحيوية للدول، وتعددت هذه الجرائم المستحدثة أبرزها الجريمة الاقتصادية الالكترونية، هذه الجرائم التي يصعب تكييفها ولها تحدياتها القانونية والأمنية والتقنية لخطورتها على البنية الحيوية والتنموية والمؤسسات الاقتصادية للدول، سواء تلك التي تهدف إلى الإطاحة و المساس بالاقتصاد أو تلك التي تهدف إلى تدمير المؤسسات المالية على رأسها المصرفية، و التي تمتد أثارها إلى التنمية الاقتصادية المستدامة للدول.

يعرف الإجرام الاقتصادي والمالي الرقمي على أنه جملة المخالفات التي تصبوا إلى تحقيق أرباح على حساب الاقتصاد، من طرف أشخاص لهم حنكة ودراية بالإجرام المعلوماتي عن طريق استغلال التقدم التكنولوجي والعولمة الاقتصادية وحرية المبادلات، دون مراعاة القوانين و بطرق وأساليب غير شرعية بهدف تحقيق أرباح تلحق أضرار بالنظم الاقتصادية العالمية [1]. كما تعرف الجريمة الالكترونية الاقتصادية على أنها سلوك إيجابي أو سلبي يرمي بموجبه المجرم المعلوماتي إلى تحصيل عائد مادي و تحقيق أرباح من جراء ارتكاب جريمة تمس بالاقتصاد الوطني[2].

تعتبر الجريمة الاقتصادية الالكترونية من أخطر الجرائم الواقعة على المؤسسات الاقتصادية في مختلف دول العالم التي تكلف الاقتصاد العالمي خسائر بنسبة 1% من إجمالي الناتج الخام المحلي، الأمر الذي يؤثر على النمو الاقتصادي والاستثمارات في سوق العمل، حيث أن شركة Kaspersky المختصة في محاربة الجريمة الالكترونية أحبطت 95000 هجمة الكترونية ضدّ الجزائر خلال سنة 2020، حيث تصدرت الجزائر قائمة الدول العربية في خطورة الهجمات الالكترونية [3]. و من هذا المنطلق فقد خصصنا هذه الورقة البحثية التي نهدف إلى إثرائها خاصة بالنتائج والتوصيات التقنية والقانونية التي من شأنها الحدّ و مكافحة هذا النوع من الجرائم التي تعمل مرتكبيها على تحطيم التنمية الاقتصادية للدول عامة و الجزائر خاصة. لتكون الإشكالية القانونية التي نعمل على الإجابة عليها من خلال هذه الورقة البحثية : **ما هي أشكال الجريمة الالكترونية الاقتصادية وكيف يكون تأثيرها على المتعاملين الاقتصاديين في البيئة الرقمية ؟**

لنجيب عن هذه الإشكالية القانونية من خلال محورين أساسيين :

المحور الأول: أشكال الجرائم الالكترونية الاقتصادية في البيئة الرقمية.

أولا/ الجرائم الالكترونية الماسة بالملكية الفكرية و تبييض الأموال.

ثانيا/ الجرائم الإلكترونية الماسة بالقطاع المصرفي.

المحور الثاني: تأثيرات الجريمة الالكترونية الاقتصادية على المتعاملين الاقتصاديين.

أولا/ تأثيرات الجريمة الالكترونية على الشخص الطبيعي.
ثانيا/ تأثيرات الجريمة الالكترونية على الشخص المعنوي.

المحور الأول: أشكال الجرائم الالكترونية الاقتصادية في البيئة الرقمية.

تأخذ الجريمة الالكترونية الاقتصادية في بيئتها الرقمية، حيّزا مهما في إطار الإشكاليات المعاصرة لجهة تهديدها الفعلي للأمن القومي والاجتماعي بعد تنامي استخدام التكنولوجيا الحديثة والشبكة العنكبوتية، وتمكين تلك الوسائل من مسح آثار المجرم الرقمي بشكل سهل وباحترافية. يُطلَق على المجرم الرقمي اسم المخترق Hacker[4]، وهو الذي يمارس جريمته السيبرانيّة (الالكترونية/المعلوماتية)، من خلال أجهزة الكومبيوتر بهدف القرصنة والتصيّد الاحتيالي والإضرار بالأشخاص أو الشركات، وبالتالي الوصول إلى معلومات شخصية أو تجارية يتمّ بيعها واستثمارها من خلال التهديد وقبول الرشوة[5] . حيث تتنوع أشكال و صور هذه الجرائم من تلك المتعلقة بالملكية الفكرية، تبييض الأموال وبجرائم المصارف، والتي تتمّ من خلال برامج الفيروسات و التجسس، الاختراق و قرصنة البيانات و التصيد.

أولا- الجرائم الالكترونية المتعلقة بالملكية الفكرية و تبييض الأموال:

تشمل تكاليف الجرائم الالكترونية تلف وتدمير البيانات وسرقة الأموال وفقدان الإنتاجية وسرقة الملكية الفكرية وسرقة البيانات الشخصية والمالية والاختلاس والاحتيال وتعطيل الأعمال وتكلفة التحقيق الجنائي واستعادة وحذف البيانات والأنظمة المقرصنة والإضرار بالسمعة [6]. فإذا تمّ قياس حجم خسائر الجرائم الالكترونية بناتج دولة فإن الخسائر التي تكبدها العالم في 2021 تقارب 6 تريليون دولار، أي أصبحت ثالث أكبر اقتصاد في العالم بعد الولايات المتحدة والصين[7].

1- الجرائم المتعلقة بانتهاك الملكية الفكرية. INTELECTUAL PROPERTY THEFP

ظهرت أشكال عديدة من جرائم القرصنة الالكترونية سواء في مجل المصنفات الفكرية أو الإنتاجية، وشكل ذلك تحدي كبيرا لأجهزة مكافحة الجرائم الاقتصادية، أثبتت الملكية الفكرية أنها محرك للابتكار و القدرة التنافسية و التنمية الاقتصادية و هي من أكثر المجالات تكلفة بالنسبة للجرائم الالكترونية هو سرقة الملكية الفكرية و المعلومات السرية للأعمال وتتمثل إحدى طرق قياس تكلفة سرقة الملكية الفكرية في البحث عن المنتجات المنافسة التي تحصل على حصة في السوق من أصحابها الشرعيين، إذ يسرق المتسللون الملكية الفكرية مثل تصميمات المنتجات من الشركات الكبرى أو المؤسسات المصغرة. حيث سجلت الجزائر 25 قضية احتيال عولجت منها 17 قضية أي بنسبة 68 %.[8]

2- -جريمة تبييض الأموال في البيئة الرقمية:

اعتمدت أغلب التشريعات العربية مصطلح غسيل الأموال ضمن قوانينها، أما المشرع الجزائري استعمل مصطلح "تبييض الأموال" بالدلالة على تحويل النقد الناتج من عمليات غير قانونية إلى أصول أو نقد سائل يأخذ الصيغة القانونية و الشرعية عبر القطاع العقاري أو عبر المصارف و البنوك و قد ازدادت هذه الجريمة نتيجة التطورات التكنولوجية و عولمة الاتصالات و المؤسسات المالية والتحرر المالي ورفق القيود وإزالة الحواجز، كلها عوامل أدت إلى انتظار هذه الظاهرة[9].

ففي الوقت الذي تتصاعد فيه جهود الدول ضدّ عمليات تبييض وغسل الأموال ظهرت العملات الرقمية المشفرة بشكل واسع، لتدخل كل دول العالم في أزمة جديدة، لصعوبة مراقبة هذه الأموال وأسواقها ومتداوليها، حيث لا تخضع العملات الرقمية لأية رقابة ولا إشراف من أية جهة على مستوى العالم، على عكس الرسمية تتم مراقبتها من خلال الحكومات والبنوك المركزية، وهو ما صعد في وتيرة التداول الرقمي للعملات باعتبارها أداة سهلة لغسيل الأموال، حيث قامت بريطانيا والولايات المتحدة الأمريكية بحضر العديد من شركات تداول العملات المشفرة.

ثانيا: الجرائم الماسة بالقطاع المصرفي. Financial cybercrime

تعتبر البنوك الهدف المفضل لمجرمي الانترنت المحترفين، حيث تفرض الجرائم الالكترونية تكلفة باهظة على الموارد المالية للمؤسسات المالية و المصرفية، كأن يتم نسخ البيانات الالكترونية لبطاقة الصراف الآلي واستخدامها لصرف أموال الضحية أو أن ينشئ المجرم الالكتروني صفحة web مماثلة جدا لموقع أحد البنوك أو المؤسسات المالية لتطلب من العميل إدخال بياناته ومنها تتم سرقته حيث تشير آخر التقارير أن المخترقين سرقوا ما يقرب ثلاثة مليارات من بيانات اعتماد الانترنت وغيرها من معلومات تحديد الهوية الشخصية، ومن أمثلة ذلك خرق وكالة التقارير الائتمانية في أمريكا " EQUISAX"، التي كشفت البيانات الشخصية لـ143 مليون مستهلك أمريكي في سبتمبر 2011، ومنها تكبدت شركة " EQUISAX" رسوما جملة واحدة تتعلق بحادث الأمن السيبراني بقيمة 87,5 مليون دولار و انخفض صافي دخلها بنسبة 27 %[10].

كما تساعد سرقة الهوية مجرمي الانترنت على إرسال رسائل بريد الكتروني تمنح شخصية الرئيس التنفيذي أو المدير المالي للشركة تطلب منهم إجراء تحويلات مالية ضخمة، حيث يصعب على البنوك اكتشاف و منع اختراق البريد الالكتروني لأن المعاملة يتم تقديمها من قبل موظف شرعي و معتم من العميل، كما هو الحال في جريمة سرقة أموال البنوك عن طريق سرقة المعلومات الشخصية للمستخدمين و الاستخدام غير الشرعي لمعلوماتهم للسطو على أموال البنوك بطريقة متخفية أو عن طريق قرصنة حسابات البنوك و المؤسسات المالية و تحويل الأموال من حساب إلى حساب آخر[11].

كما ظهرت فئة سرقة الهوية " BEC" تستهدف مخططاتها قسم الموارد البشرية في الشركة أو قسم الرواتب، ويشكل هذا النوع من الاحتيال تحديات خاصة للبنوك حيث يبدوا أن طلب التحويل البنكي قد تمّ تقديمه من عميل شرعي، في حين أنه مجرم ينتحل صفة هذا العميل أو المورد.

و التي تتمّ عن طريق استخدام أحدث البرامج التكنولوجيا المتوفرة أهمها:

1 -البرامج الفيروسية و برامج التجسس. Malwar and spywar

تعرف برامج التجسس بوجه عام على أنها برامج مصممة لجمع البيانات من حاسوب أو جهاز آخر و إعادة توجيهها إلى طرف آخر من دون موافقة المستخدم أو معرفته، ويتضمن هذا عادة جمع بيانات سرية مثل كلمات المرور و رموز PIN . وأرقام بطاقات الائتمان ومراقبة ضغطات لوحة المفاتيح وتعقب عادات الاستعراض وجمع عناوين البريد الالكتروني.

وتؤثر هذه الأنشطة في أداء الشبكة و إبطاء النظام فضلا عن الإضرار بالعمليات التجارية وتنقسم برامج التجسس بوجه عام إلى فئات أساسية:

- ✓ الفيروسات VERUS،
- ✓ أحصنة طروادة /TROJANS،
- ✓ الديدان WARMS،
- ✓ القنبلة المعلوماتية INFORMATION BOMBS،
- ✓ تراب TRAPP،
- ✓ برامج الإعلانات المتسللة وملفات تعريف الارتباط للتعقب،
- ✓ برامج مراقبة النظام.

و تتسبب هذه البرامج الضارة في سرقة المعلومات الشخصية و الهوية وحسابات البريد الالكتروني وكلمات المرور المحفوظة للتسوق والخدمات المصرفية عبر الانترنت.

2 -اختراق و قرصنة البيانات DATA BREACHERS:

على الحواسيب و كل الأجهزة الالكترونية المتصلة بالانترنت لأن أغلب الأجهزة و الحواسيب مرتبطة عبر هذه الشبكة أو حتى شبكات داخلية ويقوم بهذه العملية شخص أو عدّة أشخاص متمكنين من برامج الحاسوب وطرق إدارتها ومبرمجين ذوي مستوى عالي يلقبون بـ"هاكرس"Hackers و"كراكرس" CraCkers ، حيث سجلت الجزائر للسنة الجارية 2022، 23 قضية قرصنة عولجت منها 21 قضية، أي بنسبة معالجة 92 %.[12]

يقسم خبراء التكنولوجيا المعلومات و أخبارها قراصنة الانترنت إلى قسمين:

-القراصنة الأخلاقيين (القبعات البيض).

القراصنة المجرمين (القبعات السود).

ويضاف إليهم قسم ثالث هم أصحاب القبعات الرمادية.

- **القبعات البيض** : هم قراصنة يعملون في المؤسسات الحكومية وشركات أمن المعلومات أو منفردين، لاكتشاف ثغرات البرامج والأجهزة والشبكات والإبلاغ عنها لسدها ومنع استغلالها من المحترفين المجرمين.
- **القبعات السود** : وهو النوع الشائع والأكثر خطورة، يخترقون أمن الحاسوب من أجل مكاسب شخصية، مثل سرقة بيانات، بطاقات الائتمان أو البيانات الشخصية من أجل بيعها.
- **القبعات الرمادية** : قراصنة يقومون بأعمال قانونية أحيانا أو بمساعدة أمنية، كما يملي عليهم ضميرهم أحيانا أو باختراق في أحيان أخرى. وهم بذلك مزيج بين القراصنة ذوي القبعات البيض وذوي القبعات السود، وهم عادة يخترقون لزيادة خبراتهم في الاختراق[13].

3 التصيد PHISHING:

وفقا لمجموعة عمل مكافحة التصيد الاحتيالي (APWG) تم تسجيل أكثر من 165 ألف موقع للتصيد الاحتيالي من عام 2020، حيث ظهرت عروض التصيد كخدمة في أسواق الجرائم الالكترونية أغنت مجرمي الانترنت عن حاجتهم للخبرة في تصميم البنية التحتية للتصيد الاحتيالي قبل إرسال حملاتهم، حيث يمكن للمجرمين الشراء من البائعين لتلك المجموعات الخاصة والتركيز على الضحايا الذين تتوفر فيهم تفاصيل الاتصال بهم بسهولة من نفس الأسواق [14]. وهذا النوع من الجرائم لا يقل خطورة عن بقية الجرائم الالكترونية فهي تستنزف الموارد البشرية و المادية للدولة وتلحق الأضرار الاجتماعية والنفسية بالضحايا والشباب ممن يقعون في فخّ الابتزاز الالكتروني والتصيد عبر مواقع التواصل الاجتماعي. حيث سجلت الجزائر للسنة الجارية 2022 حوالي 430 قضية تمسّ بالأشخاص عبر الانترنت عولجت منها 289 قضية، أي بنسبة 98 %.[15]

المحور الثاني: تأثيرات الجريمة الالكترونية الاقتصادية على المتعاملين الاقتصاديين.

إن التأثير الأساسي للجريمة الالكترونية هو الآثار المالية، حيث تعتبر المخاطر الاقتصادية للجريمة الالكترونية على درجة بالغة من الخطورة نظرا لوقوعها في معظم الأحوال على معلومات وبرامج ذات قيمة اقتصادية عالية سواء في ذاتها أو لارتباطها بأموال قيّمة، مما يؤدي في الغالب إلى خسائر مالية فادحة إذ أنه وبمجرد حصول المجرم المعلوماتي على الوقت و الوسيلة الكافيتين لتنفيذ جريمة [16].فإنه لا يتردد في القضاء على أكبر المتعاملين الاقتصاديين و الذين يشكلون حجر الأساس لأي اقتصاد منهم المستثمرون ورجال الأعمال سواء كانوا أشخاص طبيعيين أو معنويين، و كذلك الشركات والمؤسسات المالية و أهمها أيضا المصارف و التي تشكل مجتمعة عماد الاقتصاد ، حيث يعتبر تعرضهم لمثل هذه الجرائم تهديدا لاستقرار التنمية الاقتصادية لأية دولة.

مع تزايد نسبة الجرائم الإلكترونية وتنوع طرقها لا شك أنها تلحق خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات وهذا بالطبع يؤثر بشكل سلب على الاقتصاد .

ما نواجهه هو هجوم شرس من أشخاص أو مجموعات أو منظمات محترفة هدفها الرئيسي تحقيق ربح مادي بالإضافة إلى أهداف أخرى وذلك بالاستفادة من توسع استخدام الكمبيوتر والانترنت ويمكن إجمالهم في عدّة مستويات هي:

أولا- تأثيرات الجريمة الالكترونية على الشخص الطبيعي:

أدى اتساع استخدام الأفراد للحاسب الآلي والهواتف الذكية للتواصل مع العالم الخارجي بحيث أصبح بإمكان الفرد إجراء معاملات الشراء أو البيع وإدارة أعماله إلكترونيا، وهنا لا يجد المجرم الالكتروني عناء كبيرا في اصطياد ضحاياه من خلال[17]:

- ✓ سرقة الهوية الشخصية،
- ✓ سرقة بطاقة الائتمان الخاصة به،
- ✓ الابتزاز والتهديد،
- ✓ عمليات احتيال،
- ✓ تحويل أو نقل حسابه المصرفي.
- ✓ نقل ملكية الأسهم،
- ✓ زيادة الفواتير بتحويل فواتير المجرم للضحية[18] .

والملاحظ أنه في كثير من الحالات لا يبادر الضحايا إلى الإبلاغ عن هذه الجرائم خشية على سمعتهم داخل الأسرة و المجتمع، الأمر الذي لا يساعد على مكافحة الجريمة الالكترونية. ويجعل الجنات في منئ عن المتابعة، بل أن عزوف الضحايا عن التبليغ يشجع الجنات على مواصلة نشاطهم الإجرامي من خلال استمرارهم في تصيد الضحايا[19]، خاصة إذا استعمل الجاني أسلوب الابتزاز و التهديد عن الكشف عن معلومات لها علاقة بالحياة الشخصية للأفراد.

ثانيا: تأثيرات الجريمة الالكترونية على الشخص المعنوي.

تشكل الجرائم الالكترونية التي تستهدف الأشخاص المعنوية خطرا أكبر، سواء تعلق الأمر بالأشخاص المعنوية الحكومية أو الخاصة وذلك أنها تستهدف عددا كبيرا من الضحايا دفعة واحدة ، أو تمس بمصلحة من المصالح الحيوية لاقتصاد الدولة كالشركات و البنوك.

- ✓ **تستهدف الشركات من خلال:**

- ✓ الإطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منها ،
- ✓ العبث بمخازن المعلومات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول إليها،
- ✓ سرقة الأموال وتحويل حسابات مصرفية الخاصة بالشركة،
- ✓ الغش في المعاملات الالكترونية كالتغيير في المبيعات،
- ✓ عمليات الاحتيال،
- ✓ التهديد والابتزاز،
- ✓ اختراق الموقع الإلكتروني الخاص بالشركة[20].

بالإضافة إلى احتمال انخفاض أسعار الأسهم قد تواجه الشركات أيضا زيادة تكاليف الاقتراض وصعوبة أكبر في جمع المزيد من رأس المال نتيجة الهجوم الالكتروني.

- ✓ **تستهدف البنوك من خلال:**
- ✓ السطو الإلكتروني،
- ✓ العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها،
- ✓ تعطيل النظام،
- ✓ نقل ملكية الأسهم،
- ✓ اختراق الموقع الإلكتروني الخاص بالبنك[21].

كما تتعرض البنوك لقرصن بطاقات الائتمان البنكية عن طريق التوصل إلى معرفة الأرقام السرية لهذه البطاقات، كما تعرف سهولة الجرائم الالكترونية على بنوك الانترنت التي تعتبر وسيط في انجاز بعض العمليات المالية عن طريق إدراج العميل للرقم السري في الكمبيوتر ، كما أن ظهروا أنظمة التحويل الالكترونية مهمتها تحويل الأموال بين البنوك العالمية أبرزها SWIFT/ CHIPS[22]. كلها عوامل زادت من حدوث الجرائم الالكترونية الاقتصادية.

وعلى غرار إحجام الأفراد عن التبليغ نجد الأشخاص المعنوية كالمؤسسات المالية و البنوك كأكثر الأشخاص عزوفا عن الإبلاغ عن الجرائم الالكترونية، وذلك خيفة فقدان ثقة العملاء و الزبائن بها، فتفقد سمعتها و قيمتها بين المنافسين لذلك تعمد الكثير من البنوك إلى التفتح على تلك العمليات التي تمس أمنها السيبراني من قرصنة و إتلاف و تجسس و غيرها من الجرائم الالكترونية[23].

من خلال التطور العالمي الحاصل على مستوى الأمن السيبراني للبنوك العالمية و رغم ما تمّ استحداثه في المنظومة البنكية الجزائرية إلا أن الكثير من التقارير تأكد على أن هذه البنوك مازالت متخلفة فهي إلى حدّ الآن تعمل بالنظام الكلاسيكي القائم على الأوراق ،وأما البنك الجزائري يدفع أموال باهظة لشراء منظومة الكترونية دون شراء برمجيات التي تسير تلك المنظومة [24].

الخاتمة:

تشهد التقنية والتكنولوجيا تطورات كثيرة واستحداث لأمور جديدة، هذا الأمر ينذر بتطور أدوات وسبل الجريمة الإلكترونية بشكل أكثر تعقيدا و أشد ضراوة من قبل ، حيث أوضحت أحدث الأبحاث التي أجرت شركة الأبحاث عن الأمن السيبراني MCACEE مدى الضرر المالي الذي أحدثته جرائم الانترنت على مستوى العالم التي كلفت الاقتصاد العالمي تريليون دولار منذ عام 2018، أي ما يعادل 1% من الناتج المحلي الإجمالي، بالإضافة إلى الضرر الذي يلحق بالعلامة التجارية و السمعة له آثار طويلة المدى على العديد من الشركات، ووفقا لتقرير MCAC أن 56% من المؤسسات التي يشملها الاستطلاع لا تملك خطّة لمنع الحوادث الالكترونية. واجمع خبراء الأمن السيبراني على مستوى العالم أنه لا يمكن تحقيق الأمن السيبراني بنسبة 100%. حيث أن التكاليف ليست مجرد نتيجة ولكنها تشمل أيضا تخفيظات كبيرة في كل من الإنتاجية و ساعات العمل الضائعة على قول آدم سيلبوت رئيس MCAC، في حين تكبد العالم سنة 2021 خسائر تقرب 6 تريليون دولار، كما توقعت شركة VENTUES CYBERSECURITY بلوغ الخسائر الناتجة عن الجرائم الالكترونية الاقتصادية العالمية بحلول 2025 نحو 10,5 ترليون دولار، أي أن تزداد تكاليف الجرائم الالكترونية العالمية بنسبة 15% سنويا، الأمر الذي يلزم الدول لتطوير آليات مكافحة هذه الجرائم وتتبع كل تطوراتها واستحداث خطوط دفاع قوية وسنّ قوانين وتشريعات وتوعية الناس بمستحدثات هذه الجرائم وتشجعيهم للإبلاغ عنها بهدف الحد وتقليل من مقدار الخسائر قدر الإمكان على المستوى الفرد والمنظمة والدولة والذي سينعكس بالتأكيد على الجانب الاقتصادي . و استناداً إلى ما ورد من معطيات وتحذيرات على مستوى الاستخدام السلبي للشبكة العنكبوتيّة ورواج الجريمة الرقمية في المجتمع المعاصر، **نضع توصيات تحفيزية للجهات المعنيّة بهدف السيطرة على هذه الآفة المستحدثة، ونعددها كالآتي:**

- ✓ العمل على زيادة تطبيقات الأمن الالكتروني القائم على الذكاء الاصطناعي لتحديد العمليات غير الطبيعية خاصة في القطاع المصرفي و التجزئة و التسويق.
- ✓ تنفيذ شبكة الكترونية اتحادية تسمح بالتوصيل البيني و تبادل البيانات بين الجهات المحلية و الدولية.
- ✓ الدعم المالي و اللوجيستية و التقني من أحدث الأجهزة و المعدات لرصد الجريمة، للشركات و المؤسسات المالية و المصرفية وتزويدها بنخبة متميزة من الخبراء و العلماء في الأمن المعلوماتي، و دعمها بأحدث شبكات تقنية المعلومات والاتصالات للتواصل الدائم و المستمر مع شبكة القيادة المركزية الوطنية لتلقي التقارير وإصدار التوجيهات وتبادل المعلومات لتحقيق سرعة الاستجابة لمحاصرة الجريمة و الحدّ من انتشارها.
- ✓ اعتماد الترميز متعدد البروتوكولات "MPLS" التي تتيح الربط الآمن للانترنت لكافة الجهات الحكومية عبر مزود مزدوج لخدمة الانترنت يسمح بتحقيق إنتاجية أعلى و تقليل الثغرات.

- ✓ اعتبار الأمن المعلوماتي التكنولوجي محورا رئيسيا في استراتيجيات الدولة الجزائرية مع زيادة اعتماد على التكنولوجيا الحديثة، مع الأخذ بعين الاعتبار التجربة السعودية في القطاع المصرفي في اعتماد نظام المدفوعات الفورية الرقمية "سريع" في التعاملات المالية و الحوالات البنكية.
- ✓ تنمية قدرات الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية بهدف مواكبة الأحداث والتطورات التكنولوجيّة، ووضع استراتيجيّات وسياسات وإجراءات تنفيذيّة وجدّية على مستوى الدولة بهدف مواجهة هذه الجرائم، وبناء منظومة قانونيّة تساير تنزيل الأنظمة المعلوماتيّة المشروعة.
- ✓ تأهيل العنصر البشري والتحسيس بمخاطر الجرائم الرقمية من خلال نشر الوعي بين صفوف المواطنين حول أخطار التعامل مع الحسابات الوهمية والمواقع السيئة على شبكة الإنترنت، والآثار الاقتصادية والاجتماعية الناجمة عنها في حالة الابتزاز والتصيد.
- ✓ إتاحة الفرصة أمام المواطنين للمشاركة في مكافحة الجرائم الرقمية، وذلك من خلال تأسيس خط ساخن يتلقى البلاغات المتعلقة بهذه الجرائم.
- ✓ استحداث بعد أمني لمجابهة الهجمات الالكترونية و تطوير أنظمة الأمان على غرار الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية و المركز المصري للاستجابة للطوارئ المعلوماتية و مركز تكامل استخبارات التهديد السيبراني "CTIIC"للولايات المتحدة الأمريكية.
- ✓ تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية، وخصوصا الإنتربول. وفي هذا المقام من الممكن أن تنضم الجزائر إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الانترنت وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والانترنت والعمل على دراسة ومتابعة المستجدات العالمية.
- ✓ –وضع خطط التعافي من الكوارث Disaster Recovery Plan والخسائر المترتبة عن الجرائم الالكترونية الاقتصادية.

❖ المراجع و المصادر حسب ترتيبها في الورقة البحثية.

[11]- نبيلة لعريد،" دراسة تحليلية حول الآثار الاقتصادية و المالية الدولية الناتجة عن جرائم نظم المعلومات " ، المجلة الجزائرية للاقتصاد و المالية، المجلد 06، العدد 11، السنة 2021، الصفحة 193.

[2]- سفيان بوقطاية/ كريمة حاجي،" أسباب و تداعيات تصاعد الجريمة الاقتصادية في الدول العربية"، مجلة الدراسات الاقتصادية، العدد 02، ماي 2018، الصفحة 144.

[3]- موقع شركة Kaspersky https://me.kaspersky.com/ تمّ الاطلاع يوم 2022/07/25.

[4]- **تعريف الجرائم السيبرانية** : هي كل عمل أو امتناع عن عمل يأتيه الإنسان إضرارا بمكونات الحاسب المادية و المعنوية، وشبكات الاتصال الخاصة به، باعتبارها من المصالح و القيم المتطورة التي يحميها القانون، مهدي رضا،"الجرائم السيبرانية و طرق مكافحتها في التشريع الجزائري"، مجلة إيليزا للبحوث و الدراسات، المجلد 06، العدد 02 لسنة 2021. و عرّفها القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، في نص المادة الأولى منه، على أنها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الاتصالات الالكترونية".

[5]- البروفيسورة وديعة الأميوني، مقال بعنوان "الجريمة الرقمية كيف نكافحها" تمّ نشره بتاريخ 2021/10/29 ، بالمرقع الالكتروني: https://www.annahar.com/arabic/section/ تمّ الاطلاع على الموقع بتاريخ 2022/07/26.

[7]- جريدة البيان الالكترونية، مقال للدكتور وائل اللبابيدي،،"خسائر الجرائم الالكترونية "، نشر بتاريخ 2022/03/13.
[8]- الموقع الالكتروني لمديرية العامة للأمن الوطني. https://www.algeriepolice.dz / تمّ الاطلاع يوم 2022/07/25.

[9]- نادية عبد الرحيم، "تطور الخدمات المصرفية و دورها في تفعيل النشاط الاقتصادي –دراسة حالة الجزائر-"، رسالة ماجستير، جامعة الجزائر -3-، كلية العلوم الاقتصادية و التجارية وعلوم التسيير، 2011/2010، الصفحة 120.
[10] - Centre for Strategic and International Studies, CSIS, www.csis.org , le 28/07/2022.
[11]- بد الفتاح مراد،" شرح جرائم الكمبيوتر و الانترنت"، دار الكتب و الوثائق المصرية، بدون سنة نشر، الصفحة 37.
[12]- الصفحة الرسمية للمديرية العامة للأمن الوطني. https://www.algeriepolice.dz / تمّ الاطلاع يوم 2022/07/25.
[13]- محاضرة في القرصنة الالكترونية والأمن الشخصي، كلية التربية البدنية وعلوم الرياضة، جامعة بغداد، م م، بان أونيد رشيد.
[14] - Centre for Strategic and International Studies, CSIS, www.csis.org , le 29/07/2022.
[15]- الصفحة الرسمية لمديرية العامة للأمن الوطني.
[16]- محمد حماد مرهج الهيسي،" التكنولوجيا الحديثة و القانون الجنائي"، دار الثقافة، عمان ، الأردن، 2004 ، الصفحة 155.
[17]- حورية قويقح،" الأبعاد الاقتصادية للجريمة الالكترونية"، revue des réformes économiques et intégration en économie mondial، حجم 14، رقم 1 مكرر، 2020، الصفحة 240 -250.
[18]- أ. صراع كريمة/ أ.دقيش جمال،" الأبعاد الاقتصادية للجريمة"، مجلة الدراسات التسويقية و إدارة الأعمال، المجلد 2، العدد 01، جانفي 2018، الصفحة 43.
[19]- بن يحيى إسماعيل،" التحقيق الجنائي في الجرائم الالكترونية"، أطروحة لنيل شهادة دكتوراه علون في القانون الخاص، جامعة أبي بكر بلقايد، تلمسان، كلية الحقوق و العلوم السياسية ، قسم الحقوق، السنة الجامعية 2021/2020، الصفحة 35.
[20]- أ. صراع كريمة/ أ.دقيش جمال، المرجع السابق، الصفحة 43.
[21]. أ. صراع كريمة/ أ.دقيش جمال، المرجع السابق، الصفحة 43 و 44.
[22]- د. قارة ملاك، "الجريمة المعلوماتية في القطاع البنكي و أساليب مكافحتها –إشارة لحالة الجزائر-"، جامعة قسنطينة، الصفحة 421.
[23]- بن يحيى إسماعيل،" التحقيق الجنائي في الجرائم الالكترونية"، الصفحة 35 و 36.
[24]- تقرير الخارجية الأمريكية، جرائم تبييض الأموال في الجزائر تجري خارج القطاع المصرفي، الموقع الالكتروني www.nilenetonline ، تمّ الاطلاع عليه بتاريخ 2022/07/27.

عبد المالك درعي
abdemalekdera@gmail.com
جامعة مولود معمري، تيزي وزو

النظام القانوني للجريمة الإلكترونية الماسة بحقوق الملكية الفكرية

ملخّص:

الجريمة الإلكترونية الاقتصادية يمكن أن تعرّف بأنّها الاستخدام غير المشروع لمختلف وسائل الاتصالات الإلكترونية من أجل المساس بالمصالح الاقتصادية، المالية والتجارية للدول، الأشخاص والمتعاملين الاقتصاديين.

هذه المداخلة تحاول الإجابة عن الاشكالية التي تثيرها الجريمة الإلكترونية في مجال المساس بحقوق الملكية الفكرية بمختلف مجالاتها، الأدبية أو الصناعية أو التجارية منها، والعقاب عليها، باعتبارها من أهم مقوّمات التنمية الاقتصادية، سواء بالنسبة للتجارة الدولية أو بالنسبة للتجارة داخل الدولة.

Abstract :

Economic cybercrime is defined as the illegal activities of electronic means of communication that seek to prejudice the economic, financial and commercial interests of stats and economic operators.

This intervention attempts to answer the problem of violating intellectual property rights, one of the most important areas of economic development, in the field of international trade or internal trade.

مقدّمة

الجريمة الالكترونية جريمة قائمة بذاتها، تتميّز من حيث الأركان عن الجريمة التقليدية، خاصة من حيث الركن المادي ووسائل الاتصالات الإلكترونية المستخدمة لارتكابها، وهي مجال واسع من مجالات الأنشطة الإجرامية المعقّدة، كالتجسس، الإرهاب، تبييض الأموال، الاتجار بالبشر...، لكنها قد ترتبط أيضا وبشكل وثيق وتهدد أهداف التنمية الاقتصادية للدول، حينئذ تسمى بالجريمة الإلكترونية الاقتصادية.

تُعرّف الجرائم الالكترونية الاقتصادية بأنّها تلكم النشاطات الناشئة عن الاستخدام غير المشروع لوسائل الاتصالات التكنولوجية الحديثة عن طريق شبكة الانترنت، والتي تهدف إلى المساس والتعدّي على المصالح الاقتصادية، المالية والتجارية للدول، الأشخاص والمتعاملين الاقتصاديين. ولقد ساعد في ارتكاب الجريمة الاقتصادية كجريمة مستحدثة [1]، التطور الذي حصل في مجال المعلوماتية والتطور العلمي والتكنولوجي في التجارة والصناعة.

[1]– بلقاسم محمد، الجرائم الاقتصادية المستحدثة، مجلة البحوث والدراسات القانونية والسياسية، العدد الخامس، ص.137

لا ريب أنّ التطور التكنولوجي الذي شهده الإنسان في السنوات الأخيرة قد ضاعف بشكل مضطرد جميع أشكال السرقة والتقليد والقرصنة للابتكارات والمنتجات وبراءات الاختراع باستخدام وسائل الاتصالات التكنولوجية عبر شبكة النترنت.

لكن وبالمقابل، أدّى ذلك بالدول في الوقت نفسه، إلى مسايرة هذه الوتيرة المتصاعدة من الجرائم الإلكترونية والاهتمام بمجال حماية الملكية الفكرية للمصنعين والمنتجين أصحاب الحق، سواء كانوا أشخاصا طبيعيين أم اعتباريين عن طريق نظام قانوني متعدد، من حيث الاتفاقيات الدولية التي تهتم بحماية الملكية الفكرية[2]، حيث تشكل اتفاقية التجارة الدولية المتصلة بحقوق الملكية الفكرية (TRIPS) النظام القانوني الذي يحقق توحيد قواعد التجارة الدولية التي تغطي جميع المجالات المتعلقة بالملكية الفكرية [3]، أو عن طريق التشريعات الداخلية للدول من أجل تجريم والعقاب عن المساس بالملكية الفكرية.

وفي هذا السياق، جاء مضمون المادة 3 المتعلق بقانون التجارة الإلكترونية [4] في الجزائر ليحظر كلّ معاملة عن طريق الاتصالات الإلكترونية تتعلق، لاسيما، بالمنتجات التي تمسّ بحقوق الملكية الفكرية أو الصناعية أو التجارية، حيث قالت:" تمارس التجارة الالكترونية في إطار التشريع والتنظيم المعمول بهما. غير أنّه، تمنع كلُّ معاملة عن طريق الاتصالات الإلكترونية تتعلق بما يأتي:- المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية".

تشمل حقوق الملكية الفكرية عموما جميع الابتكارات والاختراعات محلّ إبداع العقل البشري، سواء في المجال الفكري، الصناعي أو في المجال التجاري. غير أنّ مضمون المداخلة لن يتناول تفاصيل هذه المجالات، إنّما سنعمد إلى تحديد النظام القانوني للجريمة الالكترونية التي تمس بحقوق الملكية الفكرية وحمايتها والعقاب عليها، دون التفصيل في مضمونها ولا في تعريفها وأنواعها.

في هذا الإطار، ورغم أنّ الدول النامية لم يكن مرحبا بها، باعتبار أنّ كل الاختراعات والابتكارات المراد حمايتها تعود للدول المتقدمة تكنولوجيا [5]، إلّا أنّ المادة 7 من اتفاقية المنظمة العالمية للتجارة المتصلة بالتجارة في الملكية الفكرية (TRIPS) أبرزت الأهداف الرئيسية من وراء إنفاذ وتوفير الحماية القانونية الفعّالة للملكية الفكرية، من ذلك تشجيع روح الابتكار وتحقيق الرفاهية الاجتماعية والاقتصادية للمجتمعات، بنصها:" تسهم حماية وإنفاذ حقوق الملكية الفكرية في تشجيع روح الابتكار التكنولوجي ونقل وتعميم التكنولوجيا، بما

---

[2]- نذكر منها اتفاقية المنظمة العالمية للتجارة المتصلة بالتجارة في الملكية الفكرية (TRIPS)، وكذا اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 1883 المعدلة مرارا، دون إغفال الدور المهم الذي تلعبه المنظمة العالمية للملكية الفكرية في المجال الاتفاقي الدولي.

[3]- عمر سعد الله، قانون التجارة الدولية، النظرية المعاصرة، دار هومه، الطبعة الثانية 2009، ص.65

[4]- قانون رقم 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يتعلّق بالتجارة الإلكترونية، ج ر: عدد 28

[5]- زقان خوخة، سعدون صباح، تطور الآليات الدولية لحماية الملكية الصناعية، مذكرة ماستر في الحقوق، تخصص القانون العام للأعمال، جامعة عبد الرحمن ميرة، 2013، ص.55

يحقق المنفعة المشتركة لمنتجي المعرفة التكنولوجية ومستخدميها بالأسلوب الذي يحقق الرفاهية الاجتماعية والاقتصادية..."

فللجريمة الالكترونية عرّفها المشرع الجزائري من خلال مفهوم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بقوله في المادة 2/ فقرة أ من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها [6]:" يقصد في مفهوم هذا القانون...أ- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأيّ جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلومات أو نظام للاتصالات الالكترونية".

وبما أنّ الجريمة الالكترونية الاقتصادية هي بالأساس جريمة عبر وطنية تجتاز حدود الدولة الواحدة، فبذلك تصبح التجارة الدولية مجالا خصبا لتهديدها بما لا يسمح بحرية التجارة الدولية وتعريض التنمية الاقتصادية للخطر، خاصة بالنسبة للدول النامية.

الخطر الذي تتعرض له التجارة الدولية هو ذاته الذي يصيب الدول المتقدمة تكنولوجيا في مجال السرقات والقرصنة للبرامج المعلوماتية وبراءات الاختراع وغيرها من المنتجات السلعية المزيفة والخدماتية الذي تتعرض لها، وهذا إنّما يخلق حربا تجارية غير متكافئة ويعرّض كبريات الشركات التجارية والصناعية العالمية لخسائر مالية كبيرة[7]، بل ويؤدي ببعضها في الكثير من الأحيان إلى حافة الإفلاس.

وقد أدّى هذا التطور التكنولوجي إلى ظهور مجال حديث ومتطور من التجارة الإلكترونية، من جهة باقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك إلكتروني عن طريق الاتصالات الإلكترونية، ومن جهة أخرى انتشار وتوفير وسائط الدفع الإلكتروني [8] مما يساعد على التحويل الإلكتروني للأموال من رصيد لآخر ومن بنك لآخر عبر شبكة الأنترنت، خاصة وأنّ المعاملات التجارية العابرة للحدود تتم حصريا عبر الاتصالات الإلكترونية[9]، مع صعوبة وجود قيود وضوابط جمركية على حركة رؤوس الأموال نحو الخارج[10].

---

[6]- القانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر: ع 47

[7]- بلقاسم محمد، مرجع سابق، ص.138

[8]- عرفت المادة 6 من القانون 18-05 وسيلة الدفع الالكتروني أنها: "كل وسيلة دفع مرخص بها طبقا للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد عبر منظومة إلكترونية".

[9]- المادة 27/ فقرة 3 من القانون 18- 05، مرجع سايق

كما عرّفت المادة 10 القسم الثاني: الاتصالات الإلكترونية، من قانون 18-04 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية. ج و: عدد 27، :" يقصد في مفهوم هذا القانون بما يأتي: 1- اتصالات إلكترونية: كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية".

[10]- صراع كريمة، دقيش جمال، الأبعاد الاقتصادية للجريمة الإلكترونية، مجلة الدراسات التسويقية وإدارة الأعمال، المجلد 2، العدد 1، 2018، ص.42

اشكالية المداخلة تحاول تحديد الإطار القانوني الذي يضبط من حيث الأساس القانوني للتجريم والعقاب على الجرائم الماسة بحقوق الملكية الفكرية التي تهدد الاقتصاد الوطني عن طريق الاستخدام غير المشروع لوسائل الاتصالات الالكترونية؟

- **المحور الأول: مضمون الجريمة الالكترونية الماسة بحقوق الملكية الفكرية**

أولا: الأساس القانوني لتجريم المساس بالملكية الفكرية عبر الاتصالات الالكترونية

ثانيا: الاختصاص القضائي للمحاكم الجزائرية

ثالثا: الممارسات غير المشروعة الماسة بالملكية الفكرية

- **المحور الثاني: العقوبات المقرّرة للجريمة الإلكترونية الماسة بالملكية الفكرية**

أولا: تحديد المسؤولية الجزائية ضد الأشخاص

ثانيا: تحديد العقوبات

المحور الأول: مضمون الجريمة الالكترونية الماسة بحقوق الملكية الفكرية

ينصب المحور الأول من هذه المداخلة إلى وضع بعض، بل أهم النصوص القانونية التي تضبط وتربط مفهوم الجريمة الإلكترونية وعلاقتها بحماية حقوق الملكية الفكرية في التشريع الجزائري (**أولا**)، وكذا الاختصاص القضائي للمحاكم الجزائرية للنظر في تلكم الجرائم باعتبارها جرائم كثيرا ما تُقترف عن بعد عن طريق الاتصال الالكتروني، أو بفعل الاستيراد غير المطابق للقوانين الجزائرية (**ثانيا**)، وسنقف عند بعض الممارسات غير المشروعة التي تمس بالملكية الفكرية **(ثالثا)**.

أولا: الأساس القانوني لتجريم المساس بالملكية الفكرية عبر الاتصالات الالكترونية

مع أنّ بعض المواد المتعلقة بتجريم المساس حقوق الملكية الفكرية قد أُلغيت ضمن قانون العقوبات[11]، غير أنّ هذا استتبع اهتمام المشرع الجزائري بإصدار قوانين خاصة بذلك [12] تتناول بالتفصيل حماية الملكية الفكرية بمختلف مجالاتها، بالإضافة إلى القوانين المتعلقة بالتجارة الالكترونية والجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ووضعَ نصوصًا قانونية في جميع هذه المجالات تعنى بتجريم المساس بحقوق الملكية الفكرية المقترفة عبر الوسائل الالكترونية.

---

[11]– إلغاء المواد من 390 إلى 394 في قانون العقوبات، بعنوان القسم السابع: التعدي على الملكية الأدبية والفنية، بموجب الأمر رقم 97–10، بتاريخ 6 مارس 1997، المتعلق حقوق المؤلف والحقوق المجاورة، الملغى بدوره بموجب المادة 163 من الأمر رقم 03–05 مؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر: ع 44

[12]– أمر رقم 03–05 مؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر: ع 44

أمر رقم 03–06 ، يتعلق بالعلامات

أمر رقم 03–07 ، يتعلق ببراءات الاختراع

أمر رقم 03–08، يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة. وغيرها من النصوص القانونية ذات الصلة

لقد واكبت الجزائر تطوير ممارسة التجارة الإلكترونية وفق التشريع والتنظيم المعمول به، ولكنّها منعت ضمن نص المادة 3 المتعلق بقانون التجارة الإلكترونية كلّ معاملة عن طريق الاتصالات الإلكترونية تتعلق، لاسيما، بالمنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية حيث نصت على ما يأتي:" تمارس التجارة الإلكترونية في إطار التشريع والتنظيم المعمول بهما. غير أنّه، تمنع كل معاملة عن طريق الاتصالات الإلكترونية تتعلق بما يأتي:- المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية".

كما يُعدّ مرتكبا لجنحة التقليد وفق التشريع الجزائري، كلّ من يقوم بالأعمال المرتبطة باستيراد أو تصدير نسخ مقلدة من مصنف[13] مشمول بالحماية القانونية.

إنّ المشرع الجزائري قد ألزم المتعاملين الاقتصاديين الذين ينشطون في مجال الاتصالات الالكترونية بضرورة التقيّد الصارم بقواعد المنافسة، لكنه أيضا قد ألزمهم بضرورة احترام الشروط المحددة في دفتر الشروط، ومنها على الأخص إلزامية احترام الملكية الفكرية وحقوق المؤلف والحقوق المجاورة، وكذا إلزامية احترام الاتفاقات والاتفاقيات الدولية التي تكون الجزائر مصادقة عليها.

وفي هذا الصدد، أكدت المادة 123/ الفقرتين 23 و25 من القانون 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية [14] أنّه:"...ويلتزم (المتعامل الاقتصادي في مجال الاتصالات الإلكترونية) باحترام الشروط المحددة في دفتر الشروط. ...على الخصوص بما يأتي:

- إلزامية احترام الاتفاقات والاتفاقيات الدولية التي تصادق عليها الدولة،
- إلزامية احترام الملكية الفكرية وحقوق المؤلف والحقوق المجاورة،".

وقد ذكر الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة في مادته الأولى أنّ هذا الأمر يهدف إلى التعريف بحقوق المؤلف...وتحديد العقوبات الناجمة عن المساس بها.

ليس هذا فحسب، بل إنّ المشرع الجزائري ورغبة منه في توفير الأسس القانونية والمساهمة في حماية الاقتصاد الوطني وضمان مناخ ملائم للتنمية، ضمّن القانون 17-04 المعدل والمتمم، المتضمن قانون الجمارك[15] ونص في المادة 2 منه المُعدِّلة للمادة 3 (من قانون الجمارك لسنة 1979) على:" تتمثل مهمة إدارة الجمارك على الخصوص فيما يأتي:- مكافحة المساس بحقوق الملكية الفكرية والاستيراد والتصدير غير المشروعين للممتلكات الثقافية،"

ثانيا: الاختصاص القضائي في الجرائم الالكترونية الماسة بالملكية الفكرية

---

[13]- المادة 151/ فقرة 4 من الأمر رقم 03-05 يتعلق بحقوق المؤلف والحقوق المجاورة.

[14]- قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر: عدد 27

[15]- قانون رقم 17-04 مؤرخ في 19 جمادى الأولى عام 1438 الموافق 16 فبراير سنة 2017، يعدل ويتمم القانون رقم 79-07 المؤرخ في 26 شعبان عام 1399 الموافق 21 يوليو سنة 1979 والمتضمن قانون الجمارك، ج ر: عدد 11

بالإضافة إلى النصوص القانونية التي تحظر وتمنع المساس بحقوق الملكية الفكرية في مجال الاتصالات الالكترونية، التجارة الالكترونية وفي مجال التصدير والاستيراد، فقد أقرّ التشريع الجزائري أيضا اختصاص الجهات القضائية الجزائرية، وغيرها من المؤسسات الأخرى [16]، بالفصل في الجرائم المرتبطة بتكنولوجيات الاتصال الحديثة التي تستهدف المصالح الاستراتيجية للاقتصاد الوطني والمساس بمكانة الجزائر في التجارة الدولية، حتى بالنسبة للجرائم المرتكبة خارج الاقليم الوطني وحتى ولو كان مرتكبها من جنسية أجنبية.

وفي هذا الصدد، نصت المادة 15 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها أنّه:" زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف...المصالح الاستراتيجية للاقتصاد الوطني".

هذا، وبالنسبة للتعويض المدني عن الضرر، فتكون الدعوى القضائية لتعويض الضرر الناتج عن الاستغلال غير المرخّص به لمصنف لمالك الحقوق... من اختصاص القضاء المدني [17]، بغض النظر عن المسرى الجزائي الذي قد تتخذه المتابعات القضائية، لاسيما منها الجرائم الالكترونية الماسة بالمصالح الاقتصادية ومكانة الجزائر التجارية أو تلك التي تهدد الاختراعات التي تهمّ الدفاع الوطني[18].

ثالثا: الممارسات غير المشروعة الماسة بالملكية الفكرية

تتعدد الممارسات غير المشروعة التي تسهدف الاضرار بالاقتصاد الوطني عبر الجريمة الالكترونية، كما تهدف إلى خلق منافسة غير مشروعة [19]، وهي كلّ تقليد أو قرصنة أو سرقة أو استيراد أو تصدير للمنتجات والعلامات التجارية والاختراعات وبراءات الاختراع الصناعية، وغيرها كثير لا يمكن حصره. لكن هذه الممارسات الماسة بالملكية الفكرية تصبح كذلك عندما تستغل بغير إذن أصحابها أو إذا لم يسمح بذلك القانون، بغض النظر عن الضرر المادي الذي قد تحدثه.

إلى ذلك نصت المادة 27 من القانون رقم 04-02 المحدد للقواعد المطبقة على الممارسات التجارية[20] بنصها:" تعتبر ممارسات تجارية غير نزيهة...لاسيما منها الممارسات التي...:

---

[16]- المادة 9/ فقرة 9 من تنص على:" يختار الشعب لنفسه مؤسسات، غايتها... حماية الاقتصاد الوطني من أيّ شكل من أشكال التجارة غير المشروعة".

[17]- المادة 143 من الأمر رقم 03-04 المتعلق بحقوق المؤلف والحقوق المجاورة

[18]- أنظر لاحقا في التفريع الثاني بعنوان: تحديد العقوبات، من المحور الثاني، ص.11

[19]- نصت المادة 10 (ثانيا) من اتفاقية باريس لحماية حقوق الملكية الصناعية على:" (1)- تلزم دول الاتحاد ...حماية فعّالة ضد المنافسة غير المشروعة. (3)- ويكون محظورا بصفة خاصة ما يلي: 1- كافة الأعمال التي من طبيعتها أن توجد بأيّة وسيلة كانت لبسا مع منشأ أحد المنافسين أو منتجاته أو نشاطه الصناعي أو التجاري".

[20]- القانون رقم 04-02 مؤرخ في 5 جمادي الأولى عام 1425 الموافق 23 يونيو سنة 2004، يحدد القواعد المطبقة على الممارسات التجارية، المعدل والمتمم، ج ر: عدد 41

2- تقليد العلامات المميزة لعون اقتصادي منافس أو تقليد منتوجاته أو خدماته أو الاشهار الذي يقوم به...

3- استغلال مهارة تقنية أو تجارية مميزة دون ترخيص من صاحبها،"

6- إحداث خلل في تنظيم عون اقتصادي منافس وتحويل زبائنه باستعمال طرق غير نزيهة كتبديد أو تخريب وسائله الإشهارية واختلاس البطاقيات أو الطلبيات والسمسرة غير القانونية وإحداث اضطرابات بشبكته بالبيع".

ذلك أنّ الوسائل الإشهارية، بما فيها الإشهار الالكتروني [21] التي يستخدمها العون الاقتصادي تتضمن كلّ إعلان يهدف إلى الترويج للسلع أو الخدمات التي يعرضها مهما كانت وسائل الاتصال المستعملة [22]، حيث يتم الاعتماد الآن بشكل متزايد من قبل جميع المتعاملين الاقتصاديين على وسائل الاتصالات الإلكترونية، بحيث تقدّم التقنيات الحديثة للعون الاقتصادي إمكانية الإشهار الالكتروني لمنتوجاته، ويتم التعدّي على هذه الوسائط خاصة عن طريق قرصنة موقعه الالكتروني، أو قرصنة اسم النطاق المسجل لدى المركز الوطني للسجل التجاري، بحيث يسمح بالتعرف والولوج إلى الموقع الالكتروني للعون الاقتصادي، أو أن يتم استغلال المحطات اللّاسلكية التي تستعملها المؤسسات ذات الطابع الاقتصادي الخاضعة للقانون العام أو القانون الخاص [23] والنفاذ إليها من متعامل اقتصادي آخر منافس له بطرق غير مشروعة رغبة في الإضرار به.

من جهة أخرى، تمتد الجريمة الاقتصادية أيضا إلى المساس بالسوق المرتبطة بالاتصالات الالكترونية، وهي السوق التي تحتوي على كل المنتوجات والخدمات التي تعدّ نسبيا قابلة للتبادل والتداول من طرف المستهلك، بفعل المنافسة بين المتعاملين الاقتصاديين بسبب خصائص تلك المنتجات وسعرها واستعمالاتها[24]، ومن جهة ثانية المساس بشروط حماية حقوق مشتركي خدمات الاتصالات الإلكترونية [25]، لاسيما المتعاملين الاقتصاديين منهم الذين يستفيدون بدورهم من الخدمات التي يوفرها متعاملي الاتصالات الالكترونية الذين تجب عليهم حمايتهم ضد كل مساس بمنظومة المعلوماتية خاصتهم.

المحور الثاني: العقوبات المقرّرة للجريمة الإلكترونية الماسة بالملكية الفكرية

---

[21]- عرّفت المادة 6/ فقرة 6 من القانون 18-05 المتعلق بالتجارة الالكترونية، عرّفت الاشهار الإلكتروني أنّه:" كل إعلان يهدف...إلى ترويج بيع سلع أو خدمات عن طريق الاتصالات الإلكترونية".

[22]- المادة 3 من ذات القانون يقصد في مفهوم هذا القانون بما يأتي: 3- إشهار: كل إعلان يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع السلع أو الخدمات مهما كان المكان أو وسائل الاتصال المستعملة".

[23]- المادة 10/ فقرة23 من القانون 18-04 ، مرجع سابق

[24]- المادة 10/ فقرة 19 من القانون 18-04 ، مرجع نفسه.

[25]- المادة 97/ فقرة 6 من القانون 18-04 بنصها:" يخضع إنشاء واستغلال شبكات الاتصالات الإلكترونية المفتوحة للجمهور وتقديم خدمات الاتصالات الالكترونية للجمهور إلى احترام ما يأتي:- شروط حماية حقوق مشتركي خدمات الاتصالات الإلكترونية".

حتى تنطبق الجريمة الالكترونية في ما يتعلق بالجرائم المنصبة على حقوق الملكية الفكرية، ونظرا لكون الوسائل التكنولوجية المستخدمة تجعل من عمل السلطات الأمنية المختصة معقدة في كثير من الأحيان، بالإضافة إلى أنّها جريمة يتم ارتكابها عن بعد، لذلك لابد من تحديد صفة الأشخاص الذين قد يتهمون بارتكابها **(أولا)**، وكذا تحديد العقوبات المقررة ضدهم **(ثانيا)**.

أولا: تحديد المسؤولية الجزائية ضد الأشخاص

يدخل من الأشخاص في طائفة الذين بوسعهم ارتكاب الجريمة الاقتصادية عن طريق الاتصالات اللكترونية، وأدى سوء استخدامها بالمساس بحقوق الملكية الفكرية لأصحابها، سواء كان تاجرا أو متعاملا اقتصاديا أو شخصا لا يكتسب صفة التاجر[26]. وقد ذكرت المادة 25 من القانون رقم 04-02 المحدد للقواعد المطبقة على الممارسات التجارية أنّه:" يمنع على التجار حيازة: - منتوجات مستوردة أو مصنعة بصفة غير شرعية".

أضف إلى ذلك أنّه قد يكون مرتكبًا الجريمة الإلكترونية المتعلقة بالتعدي على حقوق الملكية الفكرية المتعامل الاقتصادي الذي ينشط في مجال خدمات الاتصالات الإلكترونية وتوفيرها للجمهور، بموجب القانون رقم 18-04 المتعلق بالبريد والاتصالات الإلكترونية، سواء كان متعاملا اقتصاديا خاضعا للقانون العام وللقانون الخاص.

من جهة أخرى، قد يتعلّق الأمر بصفته مجرما إلكترونيا معتديا على حقوق الملكية ضد المتعامل الاقتصادي إذا كان شخصا طبيعيا مُستخدَما لدى شركة الاتصالات الإلكترونية وأدى نتيجة منصبه الوظيفي إلى المساس بالمعطيات الإلكترونية ملحقا بها ضررا بالمصالح الاقتصادية للمتعاملين الاقتصاديين الآخرين أو بالشركة ذاتها التي تُوّظفه.

ثانيا: تحديد العقوبات

بغض النظر عن القواعد المشتركة بين جميع الجرائم المرتبطة بالمساس بمنظومة المعلوماتية [27]، فإنّ مخالفة مضمون ما جاءت به المادة 3 من القانون 18-05 المنظم للتجارة الالكترونية، لاسيما منه كلّ معاملة عن طريق الاتصالات الإلكترونية تتعلق ببيع المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية، من شأنه أن يُعرّض صاحبه للعقوبة بغرامة من 200.000 دج إلى 1.000.000 دج، كما يمكن للقاضي أن يأمر بغلق الموقع الإلكتروني لمدة تصل إلى 6 أشهر[28].

---

[26]- حيث نصت المادة 14 من قانون رقم 04-02 مؤرخ في 5 جمادى الأولى عام 1425 الموافق 23 يونيو سنة 2004، يحدد القواعد المطبقة على الممارسات التجارية، ج ر، عدد 41، المعدل والمتمم، عرفت الممارسات التجارية أنّه:" يمنع على أيّ شخص ممارسة الأعمال التجارية دون اكتساب الصفة التي تحددها القوانين المعمول بها".

[27]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجرائم الاقتصادية وبعض الجرائم الخاصة، الجزء الثاني، دار هومه، الطبعة الثانية 2006، ص ص.406-407

[28]- المادة 37 من القانون 18-05، مرجع سابق.

وما دامت الاتصالات الالكترونية كثيرة الاستخدام من طرف المجرم الإلكتروني بقصد سرقة وتقليد المنتوجات المشمولة بحماية الملكية الفكرية لأصحابها، فإنّ المادة 152 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة قد عدّت مرتكبا لجنحة التقليد كلّ من ينتهك الحقوق المحمية بموجب هذا الأمر باستخدام أيّ وسيلة كانت أو بأيّ منظومة معالجة معلوماتية.

أمّا المادة 164 من القانون 18-04، في الباب الرابع المتضمن الأحكام الجزائية فقد نصت على:" يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، كل شخص ينتهك سرية المراسلات المرسلة عن طريق...الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه...".

كما أنّ المادة 165/ فقرة 2 من نفس القانون (18-04) فجاءت بالعقوبة التالية:" تسري نفس العقوبة على كلِّ متعامل للاتصالات الإلكترونية يحوّل، بأيّ طريقة كانت، المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية أو أمر أو ساعد في ارتكاب هذه الأفعال".

من جانب آخر، إذا تمّ الاعتداء على حقوق الملكية الفكرية للمتعامل الاقتصادي الذي ينشط في مجال الاتصالات الإلكترونية من طرف شخص ما، بحيث قام بتوفير خدمات الاتصالات الإلكترونية المفتوحة للجمهور من دون الحصول على الترخيص العام، أو أنشأ أو استغل شبكة خاصة من دون ترخيص، فقد ألزمت المادة 172 (18-04) الشخص بعقوبة بالحبس من ستة (6) أشهر إلى سنتين (2)، وبغرامة من 500.000 دج إلى 1.000.000 دج أو باحدى العقوبتين..."

وهو نفس المنحى الذي انتهجته المادة 65 من قانون العقوبات الجزائري [29] حين جرّمت وعاقبت بالسجن المؤبد كل من يجمع معلومات أو أشياء أو تصميمات بغرض تسليمها إلى دولة أجنبية، حيث يؤدي جمعها واستغلالها من أجل محاولة الإضرار بالمصالح الاقتصادية الوطنية، بما فيها محاولة الإضرار بالدفاع الوطني. نصت المادة 394 مكرر 2 من قانون العقوبات الجزائري أنّه:" يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كلّ من يقوم عمدا وعن طريق الغشّ بما يلي:

1 -تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكبها الجرائم المنصوص عليها في هذا القسم.

2 -حيازة أو إفشاء أو نشر أو استعمال لأيّ غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

بل إنّ قانون العقوبات الجزائري لم يغفل تجريم والعقاب عن المساس بالاختراعات أو الدراسات أو طرق تصنيع تلكم الاختراعات التي تهمّ الدفاع الوطني، خاصة وأنّ من طبيعة الجرائم الماسة بالأمن الوطني أنّها تعتمد تقنيات الاتصالات التكنولوجية لمحاولة التجسس.

[29]- ورد نص المادة 65 من قانون العقوبات وما يليها ضمن القسم الثاني بعنوان: جرائم التعدي الأخرى على الدفاع الوطني أو الاقتصاد الوطني.

وفي هذا الإطار، أي حماية الملكية الفكرية للاختراعات التي تهمّ الأمن الوطني ضد الجريمة الالكترونية الماسة بها، أكّدت المادة 68 من قانون العقوبات على:" يعاقب بالسجن المؤقت من عشر سنوات إلى عشرين سنة كل من يسلّم بغير إذن سابق من السلطة المختصة إلى شخص يعمل لحساب دولة أو مؤسسة أجنبية اختراعا يهمّ الدفاع الوطني أو معلومات أو دراسات أو طريقة صنع تتصل باختراعٍ من هذا النوع أو بتطبيقات صناعية تهمّ الدفاع الوطني...".

الخاتمة:

أيّا كانت العقوبات أو القيود التي قد تفرضها الدول من أجل حماية حقوق الملكية الفكرية ضد كل أشكال الاستخدام غير المشروع لوسائل الاتصالات الالكترونية، إلّا أنّ هذه العقوبات أو القيود لا ينبغي أن تشكل عائقا أمام التجارة الدولية المشروعة وأن توفر ضمانات ضد إساءة استعمالها [30]، وهذا ما اتجهت إلى تأكيده اتفاقية المنظمة العالمية للتجارة المتصلة بحقوق الملكية الفكرية في ديباجتها بقولها:" ضرورة أن لا تصبح التدابير المتخذة لإنفاذ حماية الملكية الفكرية حواجز في حدّ ذاتها أمام التجارة المشروعة".

من جهة أخرى، لا يجب أن تكون الممارسات التقييدية لأصحاب حقوق الملكية الفكرية بدورهم عائقا أمام تشجيع مناهج البحث العلمي وتطوير التقنيات الحديثة ودعم الابتكارات الجديدة والاستثمارات الأجنبية المباشرة في مجال التكنولوجيا ونقلها إلى البلدان النامية، أو أن تكون عاملا سلبيا أمام النقل الدولي للتكنولوجيا[31]، خاصة بالنسبة للدول النامية أو الأقل نموا.

أخيرّا، يمكن الخروج بمجموعة من التوصيات المهمة نختصرها فيما يأتي:

- الاهتمام بتدعيم الإطار القانوني الموجود، كما هو الأمر بالنسبة للتشريع الجزائري، في مجال حماية حقوق الملكية الفكرية، خاصة بالنسبة للجرائم الالكترونية التي يرتكبها المتعاملون الاقتصاديون ضد متعاملين اقتصاديين آخرين منافسين لهم، قصد توفير مناخ اقتصادي ملائم تحقيقا للتنمية
- تشجيع مجالات التصنيع والاختراع بفضل الحماية القانونية الصارمة، لاسيما في ميدان الاتصالات الالكترونية والتحكم فيها بشكل جيّد مواكبة للتطور التكنولوجي عبر العالم، وفي هذا الصدد، دعم المؤسسات الناشئة المهتمة بالاتصالات الالكترونية
- ضرورة تحقيق الربط الفعلي بين الجامعة وبين العالم الاقتصادي،كما هو الأمر بالنسبة للمجلس الوطني للبحث العلمي والتكنولوجي باعتباره هيئة دستورية [32] تعنى بترقية البحث العلمي في مجال الابتكار التكنولوجي، من جهة بتشجيع والاهتمام بتدريس قانون الملكية الفكرية نظرا لارتباطه الوثيق بالاعتبارات

---

[30]– عمر سعد الله، مرجع سابق، ص.73.

[31]– المادة 8/ فقرة 2 من اتفاقية (TRIPS):" قد تكون هناك حاجة لاتخاذ تدابير، يشترط اتساقها مع أحكام الاتفاق الحالي، لمنع حائزي حقوق الملكية الفكرية من إساءة استخدامها، أو منع اللّجوء إلى ممارسات تسفر عن تقييد غير معقول للتجارة أو تؤثر سلبا على النقل الدولي للتكنولوجيا".

[32]– نص المادة 216 وَ 217 من الدستور الجزائري.

الاقتصادية، ومن جهة ثانية نقل وترقية الأبحاث العلمية والاختراعات من مخابر الجامعات إلى التجسيد الحقيقي في الميدان الاقتصادي وتحرير روح الابتكار

المراجع:

- **الكتب، المقالات والمذكرات:**
  - عمر سعد الله، قانون التجارة الدولية، النظرية المعاصرة، دار هومه، الطبعة الثانية 2009
  - أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجرائم الاقتصادية وبعض الجرائم الخاصة، الجزء الثاني، دار هومه، الطبعة الثانية 2006
  - زقان خوخة، سعدون صباح، تطور الآليات الدولية لحماية الملكية الصناعية، مذكرة ماستر في الحقوق، تخصص القانون العام للأعمال، جامعة عبد الرحمن ميرة، 2013
  - صراع كريمة، دقيش جمال، الأبعاد الاقتصادية للجريمة الإلكترونية، مجلة الدراسات التسويقية وإدارة الأعمال، المجلد 2، العدد 1، 2018www.asjp.cerist.dz
  - بلقاسم محمد، الجرائم الاقتصادية المستحدثة، مجلة البحوث والدراسات القانونية والسياسية، العدد الخامس www.asjp.cerist.dz
- **النصوص القانونية:**
  - دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر 2020، ج ر: عدد 82
  - قانون العقوبات الجزائري، المعدل والمتمم
  - قانون رقم 04-02 مؤرخ في 5 جمادى الأولى عام 1425 الموافق 23 يونيو سنة 2004، يحدد القواعد المطبقة على الممارسات التجارية، ج ر، عدد 41، المعدل والمتمم.
  - قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر: ع 47
  - قانون رقم 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يتعلّق بالتجارة الإلكترونية، ج ر: عدد 28
  - قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر: عدد 27
  - قانون رقم 17-04 مؤرخ في 19 جمادى الأولى عام 1438 الموافق 16 فبراير سنة 2017، يعدل ويتمم القانون رقم 79-07 المؤرخ في 26 شعبان عام 1399 الموافق 21 يوليو سنة 1979 والمتضمن قانون الجمارك، ج ر: عدد 11
  - أمر رقم 03-05 مؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر: ع 44

- أمر رقم 03-06 ، يتعلق بالعلامات، مؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، ج ر: ع 44
- أمر رقم 03-07 ، يتعلق ببراءات الاختراع، مؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، ج ر: ع 44
- أمر رقم 03-08، يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة. وغيرها من النصوص القانونية ذات الصلة، مؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، ج ر: ع 44

- **الاتفاقيات الدولية**
  - اتفاقية المنظمة العالمية للتجارة المتصلة بالتجارة في الملكية الفكرية TRIPS
  - اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 1883 المعدلة

بوترفاس حفيظة
hachemi.ha2010@yahoo.fr
جامعة تلمسان

القرصنة الإلكترونية للعلامات التجارية

Trademark Cybersquatting

الملخص:

تعتبر العلامات من أكثر حقوق الملكية الفكرية المتضررة نتيجة التعدي عليها من طرف مسجلي العناوين الالكترونية، حيث فوجئت أغلب الشركات عند إقدامها على تسجيل علامتها كعناوين بسبق تسجيلها من طرف الغير، ما نتج عنه خلافات ونزاعات لا تزال محاولة حلها دائرة في المحاكم حول العالم.إذ تشير الإحصائيات إلى أن 40% من أكبر 500 شركة في العالم لم تمتلك سنة 1994 العناوين الخاصة بها على شبكة الانترنت، حيث قدمت أكثر من 700 قضية للمطالبة بالتعويض وشطب العناوين التي تنتهك حقوق أصحاب العلامات التجارية ؛وظاهرة القرصنة الإلكترونيةِ هي أبعد من أن تكون في انخفاض، إذ تلقى مركز التحكيم والوساطة للويبو ما بين عامي 2000 و2010 أكثر من 20 ألف نزاعا بشأن العناوين الإلكترونية الدولية والوطنية.

أهم ما ساعد على انتشار القرصنة الالكترونيةِ أو التسجيل التعسفي للعلامات كعناوين مبدأ الأسبقية في التسجيل الذي نتج عنه وحدة العناوين الالكترونية، إضافة لغياب مبدأي التخصيص والإقليمية مما جعل مفارقة بينه وبين نظام العلامات. لابد من التصدي لهذه الجريمة لأنها تهدد الوضعية التنافسية للمؤسسات والشركات مالكة هذه العلامات ما يمس بأمن واستقرار المعاملات التجارية الالكترونية وثقة المستهلك الالكتروني، كما أن حمايتها مرتبط بحماية المستهلك الذي أصبح يعتمد في الحصول على الكثير من السلع والخدمات طريق التعاقد عبر شبكة الانترنت.

Abstract

Trademarksare considered one of the most affected intellectual property rights because of infringement by domains names registrants, as most companies were surprised when they registered their mark as domains namespreviously registered by others, which resulted in disputes and disputes that are still being resolved in courts around the world.Statistics indicate that 40% of the world's 500 largest companies did not have their own domains nameson the Internet in 1994. More than 700 cases were submitted to claim compensation and delete domains names that infringe the rights of trademark owners;Cybersquatting is far from declining. Between 2000 and 2010, the WIPO Arbitration and Mediation Center received more than 20,000 disputes over international and national domains names.

The most important thing that helped spread Cybersquatting or the arbitrary registration of marks as was the principle of precedence in registration, which resulted in the unit of electronic domains names, in addition to the absence of the principles of privatization and territoriality, which made a paradox between it and the marks system.This crime must be addressed because it threatens the competitive position of the institutions and companies that own these trademarks, which affects the security and stability of electronic commercial transactions and the confidence of the electronic consumer, and its protection is linked to the protection of the consumer, who has become dependent on obtaining many goods and services through contracting via the Internet.

مقدمة:

نتيجة تزايد الأهمية التجارية والمالية للعناوين الإلكترونية [1] أدركت الشركات ضرورة حجز موقع إلكتروني لها على شبكة الانترنت للاستفادة من المزايا التي تقدمها هذه الأخيرة من سرعة الإعلان عن منتجاتها والوصول إلى أكبر عدد من المستهلكين والمتعاملين معها ،وبواسطة هذا العنوان يستطيع مستخدم الانترنت الدخول إلى موقع معين لشركة أو مشروع وبدونه يستحيل عليه ذلك، فالعنوان الإلكتروني يحدد موقع الشركة ويميزها عن منافسيها ضمن المجال الافتراضي.[2]

وقد عمدت أغلب الشركات إلى تسجيل عنوان إلكتروني يطابق اسمها أو علامتها التجارية،[3] فلختيار مثل هذا العنوان يسمح بالاستنتاج المنطقي ويسهل البحث عن موقع لا يعرف المستخدم عنوانه.[4]

وتجب الإشارة لأهمية العلامات التجارية ودورها في التنمية الاقتصادية للشركات والمؤسسات، حيث تعتبر أداة لتسويق المنتجات بتمييزها عن غيرها، وزيادة الأرباح من خلال جذب أكبر عدد من المستهلكين خاصة إذا كانت مشهورة مما يجعلها أكثر وسائل المنافسة فعالية في الاقتصاد الحالي الذي يقوم على كثرة الإنتاج وتوفر أنواع كثيرة من المنتجات والخدمات في السوق.

أستغل البعض من الأفراد والشركات تلك الأهمية وسارعوا إلى تسجيل عناوين مواقع إلكترونية بأسماء مطابقة أو مشابهة لعلامات تجارية مملوكة للغير بقصد إعادة بيعها لأصحابها الشرعيين بمبالغ باهضة، وهو ما أدى إلى نشوء ما يعرف بالسطو أو القرصنة الإلكترونية كأبرز صورة من صور اعتداء عناوين المواقع الإلكترونية على العلامات التجارية. وقد حاول أصحاب هذه العلاماترفع دعاوى أمام القضاء لحماية حقوقهم، حيث قدمت أكثر من 700 قضية أمام القضاء للمطالبة بالتعويض وشطب العناوين التي تنتهك حقوق أصحاب العلامات التجارية ،كما تلقى مركز التحكيم والوساطة للويبو– المنظمة العالمية للملكية الفكرية– [5]أكثر

---

[1]–يسمى أيضا، إسم النطاق، اسم الدومين، ايضا عنوان الموقع الكتروني، وأصل الكلمة انجليزي Domain Name.

أما المشرع الجزائري فاستعمل مصطلح "إسم النطاق" وعرفه في المادة 6/ف8 من القانون رقم 18–05 المؤرخ في 10 مايو 2018، المتعلق بالتجارة الالكترونية، ج.ر.ج.ج، ع.28، الصادرة في 16 مايو2018، ص.4:التي تنص:"إسم النطاق: عبارة عن أحرف و/أو أرقام مقيسة ومسجلة لدى السجل الوطني لأسماء النطاق وتسمح بالتعرف والولوج إلى الموقع الإلكتروني."؛ الملاحظ أن المشرع إستند في تعريفه على مكونات ووظيفة اسم النطاق.

[2]– محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، الاسكندرية، 2003،ص.244.

[3]–عرف المشرع الجزائري العلامة التجارية في المادة 2/ف1 من الأمر رقم 03–06 المؤرخفي 19 يوليو 2003،يتعلقبالعلامات،ج.ر.ج.ج،ع.44، الصادرة في 23 يوليو 2003،ص.22، التي تنص: "كل رمز قابل للتمثيل الخطي، لاسيما الكلمات بما فيها أسماء الأشخاص والأحرف والأرقام، والرسومات أو الصور والأشكال المميزة للسلع أو توضيبها، والألوان بمفردها أو المركبة التي تستعمل كلها لتمييز سلع أو خدمات شخص طبيعي أو معنوي من سلع أو خدمات غيره."

[4]–حسن عبد الباسط جميعي وسمير حمزة، الحماية القانونية لمواقع الانترنت وأسماء الدومين، بحث مقدم في مؤتمر" التجارة الإلكترونية والإعسار عبر الحدود"، مركز القاهرة الإقليمي للتحكيم الدولي، 20–22 نوفمبر 2000، ص.4.

[5]– ظهرت الويبو في سنة 1967 وتأسست سنة 1970، لتشجيع النشاط الابداعي وتعزيز حماية حقوق الملكية الفكرية عبر العالم ، ويقع مقرها في جنيف السويسرية وهي وكالة متخصصة من وكالات الأمم المتحدة، مكرسة لتطوير نظام دولي متوازن بشأن الملكية الفكرية.
http://www.wipo.int/treaties/ar/convention

من 4 آلاف قضية تحكيم عن طريق التسوية الودية لأكثر من 7 آلاف عنوان إلكتروني لغاية سنة 2000، وما بين عامي 2000 و2010 أكثر من 20 ألف نزاعا بشأن العناوين الإلكترونية الدولية والوطنية.

انطلاقا من ذلك، ما هي أسباب نشوء القرصنة الالكترونية على العلامات التجارية؟ ما مفهومها؟وما موقف القضاء الفرنسي والمنظمة العالمية للملكية الفكرية منالقضايا المتعلقة بالقرصنة الالكترونية؟

لدراسة هذا الموضوع تم اعتماد المنهج الوصفي لضبط مفاهيم المصطلحات محل الدراسة، أيضا المنهج التحليلي من خلال التفصيل في أسباب نشوء القرصنة الالكترونية وتحليل الأحكام القضائية الفرنسية وقرارات مركز التحكيم والوساطة للويبوبشأنها.

وإجابة على هذه الإشكاليات، سيتم التطرق لأسباب نشوء القرصنة الالكترونية على العلامات التجارية (المبحثالأول)، ثم لمفهوم القرصنة الالكترونية وموقف القضاء الفرنسيوالويبومنها (المبحث الثاني)

المبحث الأول: أسباب نشوء القرصنة الالكترونية على العلامات التجارية

لقد ارتبط ظهور وانتشار القرصنة الإلكترونية على العلامات التجارية بظهورشبكة الانترنت على المستوى الشخصي والتجاري في بداية التسعينات، خاصة في ظل عدم وضوح الرؤيا والفهم القانوني لطبيعة الانترنت.وتشير الإحصائيات إلى أن 40 بالمائة من أكبر 500 شركة في العالم لم تمتلك سنة 1994 العناوين الإلكترونية الخاصة بها على شبكة الانترنت، بحيث قدمت أكثر من 700 قضية أمام القضاء للمطالبة بالتعويض وشطب العناوين التي تنتهك حقوق أصحاب العلامات التجارية، وأكثر من 4 آلاف قضية تحكيم أمام مركز التحكيم والوساطة للويبولأكثر من 7 آلاف عنوان إلكتروني لغاية سنة 2000.[6] وظاهرة القرصنة أو السطو الإلكتروني هي أبعد من أن تكون في إنخفاض، إذ تلقى مركز التحكيم والوساطة للويبوما بين عامي 2000 و2010 أكثر من 20 ألف نزاعا بشأن العناوين الإلكترونية الدولية والوطنية.[7]

وتجدر الإشارة في هذا المقام إلى أهم الأ سباب أو العوامل التي أدت إلى نشأة القرصنة الإلكترونية والتي شجعت في نفس الوقت على انتشارها، والتي يعود أساسها إلى اختلاف وخصوصية المبادئ التي يقوم عليها كل من نظام العناوين الإلكترونية ونظام العلامات إضافة لتداخلهما نتيجة تسجيل هذه الأخيرة كعنوان إلكتروني.

المطلب الأول:الأسباب المتعلقة بنظام العناوين الالكترونية

أهم المبادئ التي يقوم عليها نظام تسجيل العنوان الالكتروني عبر شبكة الانترنت والتي كانت سببا في تشجيع القرصنة وانتشارها مبدأ الأسبقية في التسجيل، حيث أن طالب التسجيل الأوليستأثربالعنوان الإلكتروني

[6]–مصطفى موسى العطيات، الجوانب القانونية لتعاملات التجارة الالكترونية، ط.1، دار وائل للنشر والتوزيع، عمان، الاردن، 2011، ص.182.

[7]- N. DREYFUS, Marques et Internet : protection, valorisation, défense, Lamy, Paris, 2011, p.101.

للموقع الخاص به أو المشروع الذي يمارسه في المجال الذي يتم فيه تسجيل هذا العنوان سواء كان المجال دوليا أم وطنيا.[8]

وبعبارة أخرى إذا تم تسجيل أحد العناوين الإلكترونية فيمنع بشكل مطلق تسجيل نفس العنوان في نفس المجال، بغض النظر عن إختلاف النشاط الذي يرتبط به العنوانين الإلكترونين، ومفاد ذلك أن حق صاحب العنوان الإلكتروني هو حق مطلق، [9]بسبب مبدأ الأسبقية الذي يقوم عليه تسجيل العنوان الالكتروني (الفرع أول).

وتجدر الاشارة أن العناوين الالكترونيةتنقسم إلى نوعين، عناوين المواقع العامة أو الدولية أو النوعية (gTLDs)[10] وعناوين المواقع الوطنية أو الخاصة بالدول (ccTLDs).[11] و تسعى أكثر المشروعات والشركات نظرا للطبيعة التجارية لأعمالها إلى تسجيل عناوينها في المجال الدولي، خاصة تحت العنوان الرئيسي (com.)، لأنه يساعد على إنتشار علامتها وتسويق منتجاتها بصورة أفضل ما أدى إلى زيادة الاقبال على العناوين المسجلة في المجالات الدولية التي تعتبر محدودة العدد(الفرع الثاني).

الفرع الأول: مبدأ الأسبقية في التسجيل

يقوم مبدأ تسجيل عناوين المواقع الإلكترونية على اعتبار أساسي، وهو أن كل شخص أو شركة يتقدم بطلب للحصول على عنوان موقع إلكتروني، فإنه سيتم تسجيل العنوان باسمه متى كان أول من يقوم بتقديم طلب الحصول على هذا العنوان قبل غيره من الأشخاص أو الشركات (premier arrivé premier servi) أي (من يصل أولا يخدم أولا)، فالعبرة هنا بأسبقية طلب التسجيل من حيث التاريخ دون اعتبار للطلبات اللاحقة.[12]

لقد شجع هذا المبدأ على استخدامه كوسيلة للكسب غير المشروع على حساب أصحاب العلامات التجارية من قبل الغير، فقد أدى تطبيق هذا المبدأ مع غياب الرقابة من جانب الجهات المختصة بتسجيله إلى إثارة نزاعات متعددة بين مالكي العلامات التجارية ومسجلي العناوين الإلكترونية، [13] حيث قام بعض الأشخاص والشركات باستغلال هذا المبدأ والإسراع إلى تسجيل عدد من العناوين الإلكترونية –خاصة وأنه كان يسمح لأي مشروع أو شخص عادي بتسجيل العنوان الإلكتروني في المجال الدولي إضافة إلى قلة تكاليف التسجيل

---

[8]– شريف محمد غنام، حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني، مجلة الحقوق الكويتية، جامعة الكويت، ع. 2، 2004، ص.326،327.

[9]– هادي مسلم يونس، أسماء النطاق على الانترنت وطبيعتها القانونية، مجلة الرافدين للحقوق، ع. 25، مجلد 12، السنة العاشرة، العراق، 2005، ص.178.

[10]– Les noms de domaine génériques ou gTLDs (Generic Top Level Domain)

[11]– Les noms de domaines territoriaux ou ccTLDs (Country Code Top Level Domain)

[12]- S. PORLON, La lutte contre le cybersquatting (France, OMP, Etats-Unis), Mémoire du DEA Informatique et droit, faculté de droit, Université de Montpellier 1, 2000-2001, p.5.

[13]– كوثر ماركي، الحماية القانونية للعلامة التجارية عبر الشبكة الرقمية، المجلة الجزائرية للعلوم القانونية، الاقتصادية والسياسية، كلية الحقوق، جامعة الجزائر، ع.3، 2003، ص.305.

نسبيا–، ثم القيام بعد ذلك بمساومة الأصحاب الشرعيين لهذه العلامات، والحقيقة أن أغلب الشركات فوجئت عند إقدامها على تسجيل علاماتها كعنوان موقع إلكتروني بسبق تسجيلها من قبل الغير.[14]

وتجدر الاشارة، أن الجهات المختصة بالتسجيل لا تتأكد فيما إذا كان طالب تسجيل العنوان مالكا لهذه التسمية –خاصة إذا كانت علامة– عند تسجيله لهذا العنوان، وأيضا الهدف من التسجيل هل هو الاستخدام الفعلي للموقع الالكتروني الذي يحمل العنوان والذيي عبر عن نشاطه المهني أو التجاري، أو تسجيله بقصد الاستفادة منه لاحقا في أمور لا علاقة لها بالاستخدام الفعلي لهذا العنوان، كالتسجيل بهدف البيع لاحقا؛ فكل ما يجب التأكد منه لإتمام التسجيل أن يكون طالب التسجيل هو أول من تقدم للحصول على العنوان الإلكتروني وأنه قد دفع المقابل اللازم لإتمام التسجيل.[15]

وبالتالي فإن سياسة الأسبقية في التسجيل لا تأخذ في الاعتبار حقوق الأطراف الأخرى التي قد تضار من تسجيل العنوان الإلكتروني لطالب التسجيل، وبما قد يتضمنه ذلك من اعتداء على أصحاب العلامات التجارية وغيرهم،[16] أي منع هؤلاء من استخدام علاماتهم كعناوين مواقع لهم عبر الانترنت لأنه بتسجيل عنوان الموقع الإلكتروني يصبح مسجله مالكا له ولا يستطيع أحد تسجيله بعد ذلك.[17]

وقد حاولت بعض الجهات الخاصة بالتسجيل أن تتطلب شروطا معينة للتسجيل والتي قد تخفف من حدة هذا المبدأ كاشتراط تقديم ما يثبت أن تسجيل هذا العنوان متعلق بعمل تجاري قائم، مثلا يشترط النظام الخاص بتسجيل العناوين الإلكترونية تحت النطاق الوطني الجزائري (.dz)، والفرنسي (.fr)،والمصري(.eg) إلى ضرورة أن يقدم طالب التسجيل نسخة من السجل التجاري أو نسخة من طلب تسجيل العلامة التجارية لدى المصلحة المختصة. [18] كذلك قامت بعض الشركات الخاصة بتسجيل عناوين المواقع العامة عند بدء تسجيل عناوين المواقع الجديدة بوضع شروط خاصة كإعطاء الأفضلية لمالكي العلامات التجارية عند تسجيل هذه العناوين.

مثلا شركة Neulevel ا لمسؤولة عن التسجيل تحت العنوان الرئيسي (biz) أعطت معاملة تفضيلية لأصحاب العلامات المسجلة وذلك بأن سمحت لهم بالاعتراض على طلب تسجيل أي عنوان يتطابق أو يتشابه مع علاماتهم خلال 30 يوما،فإذا لم يقم صاحب العلامة خلال هذه المدة بتقديم طلب الإعتراض وطلب التسجيل، ففي هذه الحالة تستمر عملية تسجيل عنوان الموقع بإسم الشخص الذي طالب بتسجيله.[19]

---

[14]– كوثر سعيد عدنان خالد، حماية المستهلك الالكتروني، دار الجامعة الجديدة، ا الاسكندرية، 2012، ص.240.

[15]- V. SEDALLIAN, Droit de l'internet: Réglementation, Responsabilité, Contrats, Éditions Net Press, Collection AUI, 1997, p.35.

[16]– كوثر سعيد عدنان خالد، المرجع السابق، ص.234.

[17]–محمد سعيد أحمد اسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين الشمس، 2005، ص.318.

[18]- Organe d'Enregistrement pour le domaine DZ, Charte de nommage du .DZ, Mars 2010, p.5 : www.nic.dz; Guide des Noms de Domaines, p.10 ; www.arsys.fr

[19]– مصطفى موسى العطيات، المرجع السابق، ص.81.

كما وضعت مؤسسة (AFNIC)–الهيئة المسؤولة عن إدارة وتسيير عناوين المواقع في فرنسا (.fr)- لنفسها قواعد خاصة أو ميثاق، يقوم على منطق حماية حقوق الغير عند تخصيص وتسجيل العناوين الإلكترونية في المنطقة الخاصة بفرنسا (.fr).

تتولى هذه المؤسسة قبل تخصيص العنوان، التحقق من أن يكون هذا العنوان المختار على علاقة بمن يطلبه، إذ يتم التأكد من الأساس الذي تقوم عليه الأحقية في طلب منح هذا العنوان دون غيره. فالشركات غالبا ما تلجأ إلى اختيار علامتها التجارية أو اسمها التجاري كعنوان لموقعها الالكتروني بدلا من الاختيار العشوائي الذي قد يؤدي إلى المساس بحقوق الملكية الفكرية للغير. لذلك هناك من يرى بأنه من الأحسن أن تعتمد كل دولة على قواعد بيانات للعلامات المميزة، يمكن الرجوع إليه لمنع تسجيل عناوين إلكترونية سبق اتخاذها كعلامات تجارية في حالة ما إذا كانت هذه الأخيرة لا تعود ملكيتها إلى طالب التسجيل.[20]

إضافة لذلك، التحقق من أن يكون العنوان المختار مرتبط بخدمة فعلية ويمكن الوصول إليه بشكل دائم من قبل كل المشتركين على شبكة الانترنت، وعليه لا يجوز الحجز المسبق لعناوين المواقع منعا لجريمة القرصنة الإلكترونية (Cybersquatting).[21] وإذا كان عنوان الموقع الالكتروني يتكون من علامة مسجلة، فاشترطت مؤسسة (AFNIC)منذ مارس 1998 أن يكون إسم العلامة مسبوقا بصيغة تكميلية (.tm) بما يسمح للشركات بتسجيل عناوين إلكترونية من علامات متطابقة في أكثر من مجال.[22]

إن مبدأ أسبقية التسجيل يقوم على قاعدة عدم وجود عنوان إلكتروني مسجل مطابق للعنوان المراد تسجيله، أما إذا كانت هناك عناوين مسجلة مشابهة له فلا عبرة لذلك، إذ يعتد بالتطابق ولا يعتد بالتشابه في العناوين.[23] فالقاعدة العامة في تسجيل العناوين الإلكترونية هي عدم فحص طلبات التسجيل لتحديد ما إذا كانت تتشابه مع غيرها من العناوين المسجلة سابقا، والتي قد تؤدي إلى إثارة الخلط في أذهان الجمهور بين العنوان الجديد والعناوين الإلكترونية المسجلة سابقا خاصة إذا ما كانت هذه العناوين تميز مواقع مرتبطة بأنشطة تجارية مماثلة أو مشابهة؛ في حين أن القوانين المنظمة للعلامات التجارية تمنع تسجيل علامات تجارية مطابقة أو مشابهة إذا كانت تتعلق بمنتجات مماثلة أو مشابهة حماية للمستهلك من الوقوع في اللبس والخلط.[24]

---

[20]- N. BEAURAIN et E. JEZ, Les noms de domaine de l'interne, Litec, Paris, 2001, p.17.

[21]- F. CHARLET,La protection des raisons de commerce sur internet, DESS Propriété industrielle, Droit commerce, l'Université de Lausanne, 2009-2010, p.7.

[22]- N. DREYFUS, op.cit, p.55.

[23]– كوثر سعيد عدنان خالد، المرجع السابق، ص.234.

[24]– حيث تنص المادة 7/ف9من الأمر رقم 03–06 المشار اليه سابقا :" يستثنى من التسجيل:... 9– الرموز المطابقة أو المشابهة لعلامة كانت محل طلب تسجيل أو تسجيل يشمل سلعا أو خدمات مطابقة أو مشابهة لتلك التي سجلت من أجلها علامة الصنع أو العلامة التجارية إذا كان هذا الاستعمال يحدث لبسا". كما نص قانون الملكية الفكرية الفرنسي على منع نسخ أو استعمال أو وضع أية علامة دون موافقة صاحبها على سلع أو خدمات مطابقة أو مشابهة لتلك المبينة في التسجيل طبقا للمادتين(L713- 3) ،(L713-2) من قانون الملكية الفكرية الفرنسي.

الفرع الثاني: نظام العناوين الإلكترونية العامة

يعتبر النظام الحالي في تقسيم العناوين العامة إلى مجالات محددة من العوامل التي ساعدت بصورة كبيرة على السطو الإلكتروني، فالعنوان الرئيسي (.com)ومن بعده (.net) هي أكثر العناوين العليا العامة إنتشارا،[25] حيث تسعى أكثر المشروعات والشركات نظرا للطبيعة التجارية لأعمالها إلى تسجيل عناوينها تحت العنوان الرئيسي (.com)والذي يساعد على إنتشار علامتها وتسويق منتجاتها بصورة أفضل، كما أن هذه العناوين هي الأكثر شهرة ومعرفة لدى جمهور المتعاملين مع شبكة الانترنت.[26]

وبما أن الأسبقية في التسجيل وعدم التطابق في العناوين تقتضي تسجيل العنوان الإلكتروني مرة واحدة، فإن قيام شركة للنقل مثلا بتسجيل العنوان الإلكتروني (trans.com) سيمنع جميع الشركات المتعلقة بالنقل في جميع أنحاء العالم من تسجيل هذا العنوان والبحث عن عنوان آخر وهو ما يعطي القيمة النادرة للعناوين الإلكترونية، نظرا لكونها تعبر عن نشاط تجاري بأسره أو متعلقة بعلامة تجارية معينة.[27]

المطلب الثاني: الأسباب المتعلقة بنظام العلامات التجارية

إن تطبيق مبدأ الأسبقية في تسجيل العنوان الإلكتروني والذي ينتج عنه وحدة العناوين، يتعارض مع مبدأ التخصيص الذي يخضع له الحق في العلامة التجارية، ف طبقالهذا ال مبدأ لاتتمتعالعلامةبالحمايةإلافيحدودالمنتجاتأوالخدماتالمحددة في طلب التسجيل ،إذيجوزاتخاذعلامة مطابقةلتمييزمنتجاتمختلفة،[28] هذا ما يثير صعوبة تطبيق مبدأ التخصيص في حالة تسجيل العلامة من طرف الغير كعنوان إلكتروني(الفرع الأول).

يستتبع ذلك اختلاف آخر بين العلامة التجارية والعنوان الإلكتروني من حيث النطاق الجغرافي بشأن الحماية المقررة لكل منهما، فإذا كانت حماية العلامة التجارية تقوم على مبدأ الإقليمية، فإن حماية العنوان الإلكتروني على شبكة الانترنت ذات بعد عالمي، وهذاما يثير صعوبة تطبيق مبدأ الإقليمية (الفرع الثاني)

ومن الأسباب المشجعة على القرصنة الإلكترونية أيضا شهرة العلامة التجارية والتي تتميز بسمعتها وقيمتها المالية الباهضة(الفرع الثالث).

الفرع الأول: صعوبة تطبيق مبدأ التخصيص

طبقا للقواعد العامة التي تحكم تسجيل العلامات التجارية، فإنه يمكن تسجيل علامات تجارية متطابقة أو متشابهة ما دامت تعبر عن منتجات أو خدمات مختلفة، فالأصل أن يتم حماية الحق في العلامة في إطار

[25]- S. PORLON, op.cit, p.5.

[26]– شريف محمد غنام، المرجع السابق، ص.410.

[27]- Y. EL SHAZLY, L'application du principe de spécialité aux noms de domaine: Un regard croisé entre la voie judiciaire et extrajudiciaire, p.2 ;http://www.droit-technologie.org/upload/dossier/doc/160-1.pdf

[28]–راشديسعيدة، النظامالقانونيللعلاماتالتجارية،مذكرةماجستيرفيالحقوق،فرعقانونالأعمال،كليةالعلومالقانونيةوالادارية،جامعةالجزائر ، الجزائر ،2001 – 2002،ص. 45.

مبدأ التخصيص أي بالنسبة للسلع والخدمات المبينة في طلب التسجيل، ومن تم يجوز لمالك العلامة منع الغير من استعمال علامته فقط إذا كانت السلع أو الخدمات متطابقة أو متشابهة، في حين لا يمكنه ذلك إذا كانت المنتجات أو الخدمات مختلفة لأن هذا الاختلاف يمنع إيقاع الجمهور في اللبس.[29] ونتيجة لذلك يمكن أن تتعايش علامتان متطابقتان إذا اختلفاختصاصهما، ومثال ذلك العلامة (Mazda) الخاصة بالسيارات ونفسها للبطاريات الكهربائية.[30]

إن أصحاب العلامات المتطابقة أو المتشابهة قد يتزاحمون في تسجيل العنوان الإلكتروني نفسه والذي يعبر عن العلامة التجارية التي يمتلكونها. ولكن مبدأ الأسبقية في التسجيل لا يعطي الحق في تسجيل عنوان إلكتروني باسم هذه العلامة إلا لمن قدم طلب التسجيل أولا دون غيره من أصحاب العلامات التجارية الأخرى، هذا ما قد يترتب عليه نزاعات بين أصحاب هذه العلامة التجارية حول ملكية العنوان الإلكتروني، بالرغم من أن تسجيل عنوان الموقع باسم هذه العلامة هو حق مشروع لكل منهم ورغم حسن نية المسجل الأول للموقع الإلكتروني أي انتفاء سوء النية في هذه الحالة.

ومن أمثلة ذلك، الحكم الصادر عن القضاء الفرنسي،[31] بشأن الدعوى التي أقامتها شركة (SA Recif) التي سجلت العلامة (Recif) في 12 جويلية 1988 المتخصصة في نشاط الهندسة والتدريب على استخدام الحاسوب، ضد شركة (SARL Recif) التي سجلت نفس العلامة في 19 نوفمبر 1997 والمتخصصة في تقديم خدمة الاتصالبالأنترنت، كما قامت بتسجيل عنوان إلكتروني باسم العلامة في المجالين (.com)، (.fr).

قضت المحكمة أن العلامتين المتطابقتين يمكن أن تتعايشا مادام ليس هناك تماثل في الخدمات المقدمة من الشركتين أي ليس لهما نفس التخصص، وبالتالي يستبعد احتمال الخلط بينهما. كما قضت بأنه لا يجوز أن تمنع الشركة (SARL Recif) من استعمال العناوين الإلكترونية المطابقة لعلامتها مادامت كانت هي الأسبق في التسجيل.

الفرع الثاني: صعوبة تطبيق مبدأ الاقليمية

تخضع العلامات في نظامها القانوني إلى مبدأ الإقليمية، حيث يقتصر نطاق حمايتها القانونيعلى إقليم الدولة التي سجلت فيه إلا إذا تم تسجيلها دوليا أو كانت العلامة مشهورة.[32]

في حين يتصف العنوان الالكتروني المسجل على شبكة الانترنت بالعالمية الذي لا يعترف بالحدود الإقليمية، ومن تم لا يخضع لمبدأ الإقليمية لأن شبكة الانترنت بطبيعتها لا تعرف الحدود، لذلك فإن العنوان يأخذ مداه

[29]– عدنان غسان برانبو،التنظيم القانوني للعلامة التجارية، دراسة مقارنة، ط. 1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012، ص. 360.

[30]-D. FOREST, Droit des marques et Noms de domaine, Gualino, Paris, 2012, p.60.

[31]- TGI Créteil, 29 mai 2001, cité par, Droit des marques et nom de domaine : application du principe de spécialité ; https://www.Legalis.net

[32]– المادة 7/ف8 والمادة 9/ف3من الأمر رقم 03–06، المتعلق بالعلامات، المشار إليه سابقا.

على النطاق العالمي أيا كان المجال الذي سجل فيه سواء كان دوليا أم وطنيا، [33] وبذلك يجوز لأي مشروع أو شخص أن يسجل عنوانا في النطاقالعام حتى ولو لم تكن له أنشطة خارج الإقليم الذي يعيش فيه، هذا ما شجع بعض الأشخاص والمشروعات إلى تسجيل عناوين على حساب حقوق أصحاب العلامات ثم بيعها لهم بمقابل باهض.

مثلا، لو سجل العنوان الالكتروني (trans.com) لحساب شركة للنقل في جهة من العالم، فإن ذلك يمنع التسجيل اللاحق لنفس العنوان في المستوى العالي (com.) على الإطلاق.[34]

الفرع الثالث: شهرة العلامة التجارية

تكتسي العلامات التجارية المشهورة قيمة مالية عالية وانتشارا واسعا بين جمهور المستهلكين مما أدى إلى ازدياد أهميتها عبر شبكة الانترنت، وسببا مشجعا للاعتداء عليها عن طريق القرصنة الإلكترونية. [35] فالعديد من الأحكام الصادرة بإدانة القرصنة صدرت بمناسبة الإعتداء على علامات تجارية تحظى بشهرة عالمية ومعروفة لدى جمهور كبير من المستهلكين مثلا، Lancôme،McDonalds،Vichy،... .

لقد أدانت محكمة نانتر، الشركة التي قامت بتسجيل العنوانين (Lankome.com) و(Lankom.com) المشابهة للعلامة المشهورة (Lancôme)، بالرغم من أنه لم يتم تفعيل هذين الموقعين.[36]

أيضا، الحكم الصادر عن القضاء الفرنسي [37] في قضية ترجع وقائعها إلى قيام لجنة المهنيين للخمر والشامبانيا (CIVC)[38] بمقاضاة شركة سويسرية (Cornu) تنتج بسكويت فاتح للشهية تسوق له في فرنسا تحت العلامة (Champagne)من خلال فرع للشركة في فرنسا وتم إنشاء موقع إلكتروني بعنوان (Champagne.ch). طلبت اللجنة من المحكمة منع استعمال(Champagne) لأنه يعد استيلاء غير مشروع لعلامة تجارية مشهورة وإضعافا للاسم الأصلي المسجل كعلامة ، الأمر الذي يوقع المستهلك في الالتباس حول مصدر المنتجات ويَعقد مسؤولية الشركة المدعى عليها. وقد أكدت المحكمة ذلك كما قررت بأن عنوان الموقع المختار باللغة الفرنسية لا يذكر اسم الشركة السويسرية كمنتج تجاري، كما يمكن الوصول إليه من الإقليم الفرنسي؛ وعليه منعت محكمة باريس كل من الشركة السويسرية وفرعها الشركة الفرنسية من

[33]-J. MORLEC, Le cybersquatting,Mémoire préparé dans le cadre de la Maîtrise de droit des affaires de la Faculté de droit de Nantes,Université d'Ottawa, 2004, p.6.

[34]–عدنان إبراهيم سرحان، أسماء النطاق على الشبكة العالمية للمعلوماتية، المفهوم والنظام القانوني، دراسة مقارنة، مجلة الشريعة والقانون، دولة الإمارات العربية المتحدة، يناير 2006، ص.326.

[35]– عبد الله حميد سليمان الغويري، العلامة المشهورة وحمايتها ضمن اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تربس) وقانون العلامات الأردني، رسالة دكتوراه في القانون الخاص، جامعة القاهرة، القاهرة، 2005–2006، ص.176.

[36]-TGI Nanterre ,10 janvier 2000 ; S. PORLON, op.cit, p.13.

[37]- TGI Paris, 9 avril 2008, chambre civil, n° RD 05/10372;

مشار اليه، كوثر سعيد عدنان خالد، المرجع السابق، ص.245،244.

[38]– وهي اختصار لـ: Comité interprofessionnel du vin de champagne

استعمال تسمية (Champagne)، كما أمرت الشركة السويسرية بإجراء شطب لعنوان الموقع الإلكتروني تحت غرامة تهديدية 150 يورو عن كل يوم تأخير.

ومن القضايا التي عرضت على مركز التحكيم والوساطة للويبو، قضية العلامة المشهورة (Adidas) التي سجلت من قبل شخص كعنوان (adidas.com)، وقد قامت الشركة الألمانية بمطالبة مسجل العنوان الإلكتروني بنقله إليها إلا أنه لم يرد على طلب الشركة. وقد أقر مركز التحكيم بأحقية الشركة بالعنوان مع أن المسجل للعنوان الإلكتروني لم يستخدم هذا الأخير تجاريا ولم يبد أي نية للبيع، ولكن المركز اعتمد على شهرة العلامة كقرينة على سوء نية المسجل باعتبارها من العلامات المعروفة في مجال الملابس والمعدات الرياضية على مستوى العالم.[39]

أما شركة ماكدونالدز للوجبات السريعة العملاقة فوجدت نفسها في مواجهة عقبة غير متوقعة عندما أرادت إنشاء عنوان موقع إلكتروني على شبكة الانترنت (www.mcdonalds.com) ولحسن الحظ كان قد تم تسجيله من أحد الصحفيين في دورية متخصصة بالمعلوماتية (Wired Magazine)والذي كان دافعه من هذا التسجيل إظهار مشاكل النظام الحالي لعناوين المواقع الإلكترونية القائم على مبدأ الأسبقية في التسجيل ، وعلى إثر الصلح بين الطرفين قبل الصحفي التنازل عن العنوان الإلكتروني مقابل مبلغ زهيد قدره 35 ألف دولار ذهب لصالح إحدى المدارس في نيويورك.[40]

المبحث الثاني: مفهوم القرصنة الالكترونية وموقف القضاء الفرنسي والويبومنها

لقد سمحت قاعدة مبدأ الأسبقية في التسجيل التي تحكم تسجيل العناوين الإلكترونية بظهور مبكر للنزاعات في بداية تطبيق نظام هذه العناوين. وقد ظهرت هذه النزاعات لأول مرة في الولايات المتحدة الأمريكية باعتبارهاالمصدر الأول لشبكة الانترنت، وتركزت هذه النزاعات على وجه التحديد في حالات تسجيل عناوين مطابقة أو مشابهة مع علامات تجارية مملوكة للغير. فشبكة الانترنت لم تستقطب فقط المشاريع التي تهتم بالتجارة الإلكترونية وتريد تطوير علاقتها بالجمهور، بل استقطبت أيضا ما يعرف بالقراصنة الذين وجدوا في تسجيل العناوين الإلكترونية وإعادة بيعها تجارة مربحة وهو ما عرف بالقرصنة الإلكترونية.

تبعا لذلك سيتم التطرق إلى مفهومها (الفرع الأول)، ثم لموقف القضاء الفرنسي من هذه الجريمة الإلكترونيةخاصة وأن هناك قضايا كثيرة رفعت من طرف أصحاب هذه العلامات التي تم الاعتداء عليها(الفرع الثاني).

الفرع الاول: مفهوم القرصنة الإلكترونية

[39]– قرار مركز التحكيم والوساطة التابع للويبو،قضية رقم (D 2002 –0107)، لسنة 2002 ، مشار اليه؛ مصطفى موسى العطيات، المرجع السابق، ص.197.

[40] - R. GOLA, Droit du commerce électronique, Guide pratique du e-commerce, Gualino, Paris, 2013, p.2.

يتجسد الإعتداء على العلامات التجارية من قبل قراصنة الانترنت بالعديد من الأساليب، ويبدو بأن الشكل الأكثر شيوعا هو ما يعرف بالقرصنة أو السطو الإلكتروني والذي عرف بأنه قيام بعض الأشخاص بتسجيل عناوين مواقع إلكترونية بشكل قانوني لدى الجهة المختصة بالتسجيل، [41] وتضمين عنوان الموقع إحدى العلامات التجارية المسجلة بإسم شخص أو شركة أخرى، وذلك بقصد الإضرار بمالك العلامة، أو بقصد إعادة بيع العنوان الإلكتروني إلى المالك الأصلي للعلامة التجارية أو إلى أحد منافسيه أو حتى فقط مجرد منع المالك من إجراء هذا التسجيل وحرمانه من ميزات الاستفادة من علامته التجارية عبر شبكة الانترنت.[42]

وبعبارة أخرى يقصد به، أن يقوم شخص أو مشروع لا يمتلك أي حق على علامة تجارية بتسجيلها في صورة عنوان موقع على شبكة الانترنت، وذلك بقصد الإضرار بمالك هذه العلامة أو بقصد المضاربة.[43]

وعرفت المنظمة العالمية للملكية الفكرية القرصنة الإلكترونية بأنها: "تسجيل إسم مجال بسوء نية."[44]

وهناك من وصفها بالقرصنة الإلكترونية لأنها تمثل إستيلاء غير مشروع لحقوق الغير،[45] حيث يتم تسجيل عنوان إلكتروني مطابق تماما لعلامة تجارية مملوكة للغير.

أما محكمة باريس فوصفت هذه الممارسة "بالابتزاز المنظم"، وقد أشارت إلى معيارين أساسين في تحديد السطو الإلكتروني هما سوء نية مسجل العنوان الإلكتروني والقيام بأعمال تؤدي إلى خلق الإلتباس لدى الجمهور.[46]

يؤدي السطو الإلكتروني بصورة مباشرة إلى تضليل جمهور المستهلكين، لأن أغلب هؤلاء يتوقعون الوصول إلى الموقع الإلكتروني للشركة صاحبة العلامة التجارية عن طريق افتراض أن العنوان الإلكتروني مطابق لعلامتها التجارية. وبالتالي فإن منع المستخدم من الوصول إلى موقع الشركة صاحبة العلامة التجارية المطلوبة بتحويله إلى موقع شركة أخرى سيؤدي إلى تضليل الجمهور والإضرار بمصالح الشركة مالكة العلامة وهو ما سيؤدي حتما إلى محاولة هذه الأخيرة الحصول على عنوان الموقع المطابق لعلامتها.[47]

الفرع الثاني: موقف القضاء الفرنسيوالويبومن القرصنة الالكترونية

تعتبر جريمة القرصنة الالكترونية تهديدالمستقبل العمل التجاري عبر شبكة الانترنت، حيث يضعف ثقة التجار والزبائن بما يهدد التنمية الاقتصادية للشركات مالكة العلامات التجارية التي تريد توسيع نشاطها أوالتعامل في اطار التجارة الالكترونية.

[41]–خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2009، ص.345.

[42]- R. GOLA, op.cit, p.37.

[43]-J. MORLEC, op.cit, p.4.

[44]– عدنان غسان برانبو، المرجع السابق،ص. 611.

[45]– كوثر سعيد عدنان خالد، المرجع السابق، ص.242.

[46]- TGI Paris, 25 avril 1997, affaire « Framatome » ; cité par, J. MORLEC, op.cit, p.11.

[47]–خالد ممدوح ابراهيم، حقوق الملكية الفكرية، الدار الجامعية، الإسكندرية، 2010، ص.98.

ولمواجهة هذه الجريمة الالكترونية، حاول القضاء الفرنسي تطبيق القواعد التقليدية العامةبشأن القضايا المرفوعة من أصحاب العلامات للدفاع عن حقوقهم، أما المنظمة العالمية للملكية الفكرية فوضعت قواعد خاصة لتسوية النزاعات بين أصحاب العلامات والعناوين الالكترونية.

أولا– موقف القضاء الفرنسي من القرصنة الالكترونية

حاول القضاء الفرنسي البحث في العوامل الأساسية التي تساعد في تحديد وقوع القرصنة الإلكترونيةلأجل تسهيل إثباتها والحد منها حماية لحقوق أصحاب العلامات التجارية، والعامل الأهمهو سوء نية مسجل العناوين الإلكترونيةكركن معنوي لهذه الجريمة الالكترونية، وقد كان القضاء يستشف سوء النية من عدة مؤشرات:

أولا– إعادة بيع العنوان الالكتروني

يعتبر بيع العنوان الإلكتروني بعد تسجيله من أهم المؤشرات التي تدل على سوء نية مسجله، خاصة إذا قام بإعادة بيعه إلى صاحب العلامة التجارية أو لأحد منافسيه بثمن مغالى فيه يتجاوز نفقات التسجيل، كما يوضح نية المتاجرة لدى مسجل هذا العنوان.[48]

والواقع أن ظاهرة تسجيل العناوين الإلكترونية ثم إعادة بيعها باتت تجارة لها مقوماتها من حيث القيمة المالية العالية للعناوين الإلكترونية، مثلا تم إعادة بيع العنوان الإلكتروني (buissiness.com) سنة 2005 بـ 150 مليون دولار. [49] وتم بيع العنوان الإلكتروني (drugs.com) بمبلغ 823456 دولار أمريكي لشركة متخصصة بالحقل الصيدلاني.[50] كما تم بيع العنوان (porn.com) سنة 2007 بما يعادل 9.5 مليون دولار، وفي بداية 2011 تم إقتناء العنوان (realestate.com) بمبلغ 8.25 مليون دولار.[51]

وقد نشأت فئة من التجار المختصين ببيع وشراء عناوين المواقع الإلكترونية، يطلق عليهم (Domaines) وهم فئة المحترفين الذين يتعاملون في بيع وشراء العناوين الإلكترونية. كما أن هناك العديد من المواقع عبر شبكة الانترنت مختصة ببيع العناوين الإلكترونية، بحيث يكتب العنوان وملحقا به ثمنه.[52]

العبرة في هذه الحالة بالعمل غير الأخلاقي الذي يقوم به ممارسوا القرصنة الإلكترونية، فالقضاء يدين القرصنة بسبب إستغلال هؤلاء لمبدأ الأسبقية في التسجيل الذي يحكم تسجيل العناوين الإلكترونية، حيث يقومون بتسجيل عدد كبير منها للمتاجرة فيها دون أن يكون لهم أي حق أو مصلحة مشروعة في هذه العناوين.

---

[48]- TGI Nanterre, 18 janvier 1999, PIBD 1999, N°673, p.147, cité par, J-F. BOURQUE et autre, Guide juridiques du commerçant électronique, Montréal, 2001, p.42, 43.

[49]– ايهاب السنباطي، الموسوعة القانونية للتجارة الالكترونية، دار الجامعة الجديدة، الاسكندرية، 2008، ص.170.

[50]– عدنان ابراهيم سرحان، المرجع السابق، ص.311.

[51]- N. DREYFUS, op.cit, p.99.

[52]– بسام مصطفى عبد الرحمن طبيشات، الحماية القانونية للعلامات التجارية في ظل القانون الاردني والقانون المصري والاتفاقيات الدولية، طبع بدعم من وزارة الثقافة، مصر، 2009، ص.277.

إن الاعتداء على حقوق الغير المشروعة وإعادة بيعها لهم مرة أخرى، أمر يرفضه القانون والأخلاق كما يختل به أمن المعاملات عبر شبكة الانترنت.[53]

ولهذا السبب اعتبر القضاء أن مجرد عرض العنوان الإلكتروني للبيع يمثل سطوا إلكترونيا ويسأل من يقوم به حتى ولو لم يتم البيع بالفعل، لأن ذلك يكشف عن سوء نية مسجل العنوان الإلكتروني في الاستفادة من المتاجرة في عنوان الموقع.[54]

ومن أهم القضايا المشهورة في السطو الإلكتروني قضية (Panavision/Toppen)وهي أول قضيةترفع أمام المحاكم الأمريكية، ووقائعها أن الشركة (Panavision international) تمتلك العلامتان المشهورتان(Panavision,Panaflex) وقد إستخدمتابالإرتباط مع عمل الشركة بالتصوير الفوتوغرافي، وفي 1995 سجل المدعو (Dennis Toeppen) عنوان الموقع (Panavison.com)،وذلك قبل أن تبادر الشركة إلى تسجيل هاتين العلامتين كعنوان للموقع الإلكتروني على شبكة الانترنت. كان (Dennis) مدركا لأهمية التجارة الإلكترونية بالكامل، حيث لم يقم بإستعمال عناوين المواقع التي قام بتسجيلها، وقد طالب الشركة بمبلغ 1300 دولار كمقابل للتنازل عن هذه العناوين.

رفعت الشركة دعوى عليه لمنع الاعتداء على علامتها التجارية، فقررت المحكمة أن سلوك المدعي عليه يتضمن إضرارا بالشركة بعدم تمكينها من استخدام الانترنت بصورة مشروعة للإعلان عن العلامة التجارية المسجلة باسمها، ومطالبته بالمقابل ينطوي على سوء نيته عند التسجيل. [55] وتجدر الإشارة بأن (Dennis) قام بتسجيل أكثر من 100 عنوان إلكتروني تضمن العديد من العلامات التجارية المشهورة.[56]

ثانيا– نية الإضرار بمالك العلامة التجارية

تكون سوء النية متوافرة لدى مسجل العنوان الإلكتروني إذا سجل هذا العنوان بهدف الإضرار بمالك العلامة التجارية، وذلك بمنعه من تسجيل عناوين تمثل علامته على شبكة الانترنت. وتتضح سوء نية الإضرار إذا قام المسجل بتسجيل العنوان الإلكتروني في أكثر من مجال لمنع ظهور مالك العلامة التجارية على شبكة الانترنت؛ مثلا تسجيل العناوين الإلكترونية ، (samsung.com)، (samsung.org) ، (samsung.net)، يترجم بوضوح سوء نية المسجل في منع مالك هذه العلامة من أي ظهور على شبكة الانترنت، ورغبته في دفع صاحبها للتفاوض معه حول هذه العناوين.[57]

تجدر الإشارة، بأن شهرة العلامة التجارية المعتدى عليها قد تعد دليلا على وجود سوء نية المسجل لعنوان إلكتروني مطابق لها، إذ لا يستطيع مسجل العنوان الإلكتروني إثبات حسن نيته بعدم علمه بأن العنوان يعود

[53]– بسام مصطفى عبد الرحمن طبيشات، المرجع نفسه، ص.278.

[54]–خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص. 349.

[55]–محمد سعيد أحمد اسماعيل، المرجع السابق، ص. 321،320.

[56]–خالد ممدوح ابراهيم، حقوق الملكية الفكرية، المرجع السابق، ص. 638.

[57]–خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص. 351،550.

لعلامة مشهورة.[58] كما وأن أغلب الشركات التي لها علامة تجارية مشهورة يهمها أن يكون عنوان موقعها الإلكتروني بذات العلامة، فمثلا لا يمكنأن تتنازل شركة كوكاكولا العالمية على أن يكون موقعها الإلكتروني هو(www.cocacola.com) وهو الأمر الحاصل فعلا، ويكاد يكون هو الحال لكل الشركات الضخمة التي لها فروع في شتى أنحاء العالم.[59]

ومن تطبيقات ذلك، الحكم الصادر عن محكمة باريس الذي توصلت فيه المحكمة أن القيام بتسجيل العلامة التجارية المشهورة (Celio) كعنوان إلكتروني (Celio.com) يعد دليلا على سوء نية المسجل مما يشكل اعتداء على هذه العلامة.[60]

أيضا الحكم الصادر عن محكمة نانتر، بشأن قرصنة علامات مشهورة عالميا منها، (La source,Suisses, Chouchou, la rodute, Helline)، وقد جاء فيه:"البيع بالمزاد العلني لعناوين إلكترونية مقلدة لعلامات تجارية مشهورة يشكل عملا من أعمال القرصنة توجب مسؤولية من اشترك فيها."[61]

وتجب الإشارة، أن القضاء الفرنسي أكد بأن القرصنة الالكترونية تعد جريمة تقليد، منها قضية (L'Oréal)، حيث جاء في الحكم وفي عبارات واضحة بأنه: "من الثابت أن هذا الإستحواذ على عناوين المواقع الإلكترونية على شبكة الانترنت يشكل نسخا وتقليدا للعلامات المودعة."[62]

أيضا، ما قضت به محكمة نانتر في قضية (SFR)،[63]بقولها تعليقا على مجرد تسجيل عنوان موقع إلكتروني "إن قيام شركة(W3 SystemsInc)باستعمال عنوان الموقع (sfr.com) على شبكة الانترنت يعد تقليدا، ويقوم هذا الأخير بمجرد تسجيل عنوان الموقع الذي ينسخ العلامة".[64]

لقد تبنى المشرع الجزائري [65] على غرار نظيره الفرنسي [66] مفهوما موحدا وواسعا لجنحة التقليد،ويقصد بها كل التصرفات التي يقوم بها الغير وتمس بحقوق صاحب العلامة، أي كل الأعمال التي ترتكب مخالفة لحقوقه الشرعية.[67]

---

[58]–عبد الله حميد سليمان الغويري، المرجع السابق، ص. 183.

[59]– ايهاب السنباطي، المرجع السابق، ص.170.

[60]- TGI Paris, 19 octobre 1999;

عبد الله حميد سليمان الغويري، المرجع السابق، ص. 177.

[61]- TGI Nanterre, 31 janvier 2000 ;

مشار إليهأيضا، شريف محمد غنام، المرجع السابق، ص. 404.

[62]-TGI Nanterre, Ord. réf, 30 juin 1999 ;

مشار إليه، عبد الراضي محمود كيلاني، المشكلات العملية الناتجة عن استعمال العلامات التجارية كأسماء للمواقع على الانترنت، دراسة مقارنة، ع. 30، مجلة الدراسات القانونية، كلية الحقوق، جامعة اسيوط، مصر، سبتمبر 2011، ص.532.

[63]– وهي اختصار لـ:Société Française du Radiotéléphone

[64]- TGI Nanterre, Ord. réf, 18 Janvier 1999, PIBD 1999, N°673, p.147, cité par, J-F. BOURQUE et autre, op.cit, p.42, 43.

[65]– تنص المادة26/ف1منالامررقم 03-06 المشار إليه سابقا: "مع مراعاة أحكام المادة 10 أعلاه، يعد جنحة تقليد لعلامة مسجلة كل عمل يمس بالحقوق الإستئثارية لعلامة قام به الغير خرقا لحقوق صاحب العلامة."

وتقوم جنحة التقليد على ركنين، ركن مادي يتمثل في اصطناع واستعمال علامة مطابقة أو مشابهة للعلامة الأصلية والركن المعنوي المتمثل في القصد الجنائي وهو سوء نية المقلد.

ثانيا- موقفالويبو من القرصنة الالكترونية

تناولت المنظمة العالمية للملكية الفكرية–الويبو– حماية العلامات عبر شبكة الانترنت من خلال العديد من التقارير[68]والتوصيات،[69] وأهم ما ترتب عن ذلك تكريس القواعد الموحدة لتسوية النزاعات ما بين العلامات والعناوين(UDRP)،[70] أصدرتها منظمة الايكان (ICANN)،[71]حيث تطبق على النزاع بموجب شرط أو بند يدرج في عقد تسجيل العنوان، يقبل بمقتضاه المسجل الخضوع للقواعد في حل نشوب نزاع يتعلق بالعنوان، والأصل أن تنطبق هذه القواعد على العناوين العامة وأيضا الوطنية إذا اعتمدتها الهيئات المسؤولة عن التسجيل.

وقد حددت المادة الرابعة في فقرتها (b) من هذه القواعد،[72]أربع حالات تثبت فيها سوء نية المسجل وهي:

– أن يسجل العنوان الإلكتروني بقصد بيعه لمالك العلامة التجارية أو أحد منافسيه بثمن مبالغ فيه يتجاوز بكثير نفقات تسجيله.

---

[66]- Art. L716-1 C.fr. propr. intell :« L'atteinte portée au droit du propriétaire de la marque constitue une contrefaçon engageant la responsabilité civile de son auteur. Constitue une atteinte aux droits de la marque la violation des interdictions prévues aux articles L. 713-2, L. 713-3 et L. 713-4.»

المادة L.716-1 ق.م.ف.ف:" يعد تقليدا كل اعتداء على حق مالك العلامة ويؤدي إلى مسؤولية مرتكبها مدنيا. وتشكل أفعال اعتداء تلك المنصوص عليها في المواد L. 713-2, L. 713-3 et L. 713-4"

[67]– فرحة زراوي صالح، الكامل في القانون التجاري، الحقوق الفكرية، ابن خلدون للنشر والتوزيع، EDIK، وهران، 2006، ص.259.

[68]– التقرير الأول بشأن إدارة الأسماء أو العناوين على الانترنت: قضايا الملكية الفكرية، 30أفريل 1999؛ التقرير الثاني حول إقرار الحقوق واستعمال الأسماء في ظل نظام العناوين، 3 سبتمبر 2001.

[69]– التوصية المشتركة بشأن حماية العلامات التجارية وغيرها من حقوق الملكية الصناعية على الانترنت، 2001/10/3، أيضا برنامج الويبو بخصوص العناوين الوطنية في 20 جوان 2001 "أفضل الإجراءات لتفادي منازعات الملكية الفكرية بشأن الحقول العليا المكونة من رموز البلدان وتسويتها".

[70]- Uniform Dispute Resolution Policy (UDRP)

[71]– اختصارا بالانجليزيةInternet Corporation For AssignedNames And Numbers

الايكانهي منظمة تحديد الأسماء والأرقام عبر الانترنت، والتي أوكل إليها مهمة تنظيم وإدارة عناوين المواقع الانترنت على المستوى الدولي.

[72]- Art. 4(b) de Principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine, adoptés le 26 août 1999, Documents d'application approuvés le 24 octobre 1999 **; www.wipo.int/amc/fr /docs/icannpolicy.pdf**

: « **b. Preuve de l'enregistrement et de l'utilisation de mauvaise foi.** Aux fins du paragraphe 4(a) (iii), la preuve de ce que le nom de domaine a été enregistré et est utilisé de mauvaise foi peut être constituée, en particulier, pour autant que leur réalité soit constatée par la commission administrative, par les circonstances ci-après:

i) les faits montrent que vous avez enregistré ou acquis le nom de domaine essentiellement aux fins de vendre, de louer ou de céder d'une autre manière l'enregistrement de ce nom de domaine au requérant qui est le propriétaire de la marque de produits ou de services, ou à un concurrent de celui-ci, à titre onéreux et pour un prix excédant le montant des frais que vous pouvez prouver avoir déboursé en rapport direct avec ce nom de domaine,

ii) vous avez enregistré le nom de domaine en vue d'empêcher le propriétaire de la marque de produits ou de services de reprendre sa marque sous forme de nom de domaine, et vous êtes coutumier d'une telle pratique,

iii) vous avez enregistré le nom de domaine essentiellement en vue de perturber les opérations commerciales d'un concurrent ou

iv) en utilisant ce nom de domaine, vous avez sciemment tenté d'attirer, à des fins lucratives, les utilisateurs de l'Internet sur un site Web ou autre espace en ligne vous appartenant, en créant une probabilité de confusion avec la marque du requérant en ce qui concerne la source, le commanditaire, l'affiliation ou l'approbation de votre site ou espace Web ou d'un produit ou service qui y est proposé.»

– أن يسجل العنوان الإلكتروني بهدف منع مالك العلامة التجارية من امتلاك عنوان إلكتروني يمثل علامته على شبكة الأنترنت.

– إذا تم تسجيل العنوان الإلكتروني بهدف الإخلالبالأعمال التجاريةللمنافسين.

– استخدام العنوان لجذب عملاء مالك العلامة التجارية من مستخدمي الأنترنت عن طريق إحداث التضليل والخلط لدى هؤلاء العملاء، وجعلهم يعتقدون بوجود علاقة تربط مسجل العنوان مع مالك العلامة بهدف تحقيق مكاسب تجارية.

لقد وردت هذه الحالات على سبيل المثال لا الحصر، إذ يمكن استنتاج سوء نية المسجل من مؤشرات أخرى، كشهرة العلامة التجارية التي اعتدي عليها، قيام مسجل العنوان الإلكتروني بتزويد هيئة التسجيل بمعلومات مضللة أو كاذبة عن هويته وشخصيته الحقيقية، كما اعتبر أيضا إهمال المدعى عليه في الرد على ادعاءات المدعى مؤشرا على ضعف حجته وسوء نيته في تسجيل العنوان الإلكتروني.[73]

كما أن تسجيل عنوان إلكتروني مطابق أو مشابه لعلامة تجارية واستخدامه لعرض أو بيع منتجات تحمل علامة مقلدة، دليل على سوء نية المدعى عليه.[74]

وقد استقرت قرارات مركز التحكيم والوساطة على اعتبار مجرد العرض للبيع محققا لسوء نية مسجل العنوان حتى ولو لم يستخدمه تجاريا، مما يستوجب نقله أو إلغاءه حتى ولو تم توجيه العرض للبيع لمالك العلامة أثناء مرحلة التفاوض بينهما على العنوان محل النزاع.[75]

ومن تطبيقات ذلك، القـرار الصادر من مركز التحكيم والوساطة للويبو في 13 مارس 2002 في قضية (Air France)،حيث توصلت اللجنة التي نظرت النزاع وجود نية إعادة بيع العنوان (airfrance-delta.com) من طرف المسجل وهو شركة أمريكية (van wijk) من عبارة أجابت بها الشركة المدعي عليها على الشكوى المقدمة من المدعية، وتتمثل هذه العبارة (please come with a betteridea)أي – يرجى أن تأتي بفكرة أفضل–، فقد وصفت اللجنة هذه العبارة بأنها غامضة ويمكن تفسيرها على الأرجح بأنها دعوة من المدعي عليه إلى المدعي بشراء العنوان الإلكتروني محل النزاع.[76]

أيضا أقر المركز، بنقل العناوين الإلكترونية (nikewoman.com, nikesshop.org, inike.net) التي سجلت من قبل الشركة (Crystal International) إلى شركة(Nike) استنادا إلى شهرة العلامة، وأن استخدام هذه العناوين قد يثير الخلط في أذهان الجمهور حول مصدر هذه المنتجات إضافة إلى سوء نية

---

[73]– قرار مركز التحكيم والوساطة التابع للويبو، قضية (AlcoholicsAnomymous World Service. v. Lauren Raymond) رقم (0007–D2000)؛مصطفى موسى العطيات، المرجع السابق ،ص.383.

[74]- OMP, déc. n° D2010-0068, PandoraJewelry, LLC v. David Lee, (pandora4sale.com), transfert; cité par, N. DREYFUS, op.cit, p.149.

[75]– قرار مركز التحكيم والوساطة التابع للويبو، قضية (GBS Broad Casting. v. GaddoorSaid) رقم (0243– 2000 D)؛ وقرارآخر لمركز التحكيم والوساطة التابع للويبو، قضية (World WrestlingFderal. v. Bosmer) رقم (0001– 99 D)؛ مصطفى موسى العطيات ،المرجع السابق،ص.385.

[76]– بسام مصطفى عبد الرحمن طبيشات، المرجع السابق، ص.278.

المسجل الذي قام بتكرار تسجيل العلامة بصور مختلفة ومتشابهة مع هذه العلامة المشهورة بما يفيد هدفه في الاستفادة المالية من وراء تسجيل هذه العناوين.[77]

رغم ذلك، فإنه قد يصعب إثبات سوء النية المتطلب لحماية العلامات التجارية المسجلة كعنوان إلكتروني أو التي تعرضت للقرصنة الإلكترونية، وذلك في حالةإذا لم تكن العلامة مشهورة، كذلك إذا قام مسجل العنوان الإلكتروني بتسجيله فقط دون استخدامه تجاريا ودون عرضه للبيع لاحقا.

خاتمة

كان لتقنيات المعلومات والاتصالات تأثير كبير على حقوق الملكية الفكرية وبخاصة العلامات التجارية، فمن جهة أدت إلى تسهيل عولمة هذه الأخيرة التي تزايدت قيمتها في إطار التجارة الالكترونية؛ ومن جهة أخرى، كانت العلامات من أكثر هذه الحقوق تضررا نتيجة التعدي عليها من طرف مسجلي العناوين الإلكترونية مستغلين إختلاف نظام تسجيل هذه الأخيرة عن نظام العلامات، وهذا ما سمي بالقرصنة الإلكترونيالتي كانت محل الدراسة، وقد خلصناإلى جملة من النتائج أهمها:

أهم ما ساعد على انتشار القرصنة الالكترونيةِ أو التسجيل التعسفي للعلامات كعناوين ، مبدأ الأسبقية في التسجيل الذي نتج عنه وحدة العناوين الالكترونية ، إضافة لغياب مبدأي التخصيص والإقليمية مما جعل مفارقة بينه وبين نظام العلامات.

يشكل تسجيل عناوين متطابقة أو متشابهة مع العلامات، تعارضا مع حقوق أصحابها، خاصة إذا كانت العلامة المعتدى عليها علامة مشهورة حيث يصبح العنوان بطاقة أعمال في العالم الافتراضي على حد تعبير البعض.[78]

أكد القضاء الفرنسي أن القرصنة الالكترونية تعد جريمة تقليد، وهي تلحق ضررا بأصحاب العلامات بحرمانهم من تسجيلها كعنوان إلكتروني، كما تشكل تهديدا للوضعية التنافسية للمؤسسات والشركات مالكة هذه العلامات ما يمس بأمن واستقرار المعاملات التجارية الالكترونية وثقة المستهلك الالكتروني، كما أن حمايتها مرتبط بحماية المستهلك الذي أصبح يعتمد في الحصول على الكثير من السلع والخدمات طريق التعاقد عبر شبكة الانترنت.

وبناء عليه، فإن أهم التوصيات أو الاقتراحات بشأن الدراسة:

غالبا ما تلجأ الشركات إلى اختيار علامتها التجارية أو اسمها التجاري كعنوان لموقعها الالكتروني بدلا من الاختيار العشوائي الذي قد يؤدي إليه المساس بحقوق الملكية الفكرية للغير. لذلك هناك من يرى، [79] بأنه من

[77]– قضية رقم (0102– 2001 D) الصادر عن مركز التحكيم والوساطة التابع للويبو لسنة 2001. مشار إليها؛ مصطفى موسى العطيات، المرجع السابق، ص.205.

[78]– خليفي مريم، العناوين الالكترونية والعلامات التجارية في مجال التجارة الالكترونية، مجلة دراسات وأبحاث، ع. 2، جامعة الجلفة، الجزائر، 2010، ص.163.

[79]- N. BEAURAIN et E. JEZ, op.cit, p.17.

الأحسن أن تعتمد كل دولة على قواعد بيانات للعلامات التجارية، يمكن الرجوع إليه لمنع تسجيل عناوين إلكترونية سبق اتخاذها كعلامات تجارية في حالة ما إذا كانت هذه الأخيرة لا تعود ملكيتها إلى طالب التسجيل.

أيضا التحقق من أن يكون العنوان المختار مرتبط بخدمة فعلية ويمكن الوصول إليه بشكل دائم من قبل كل المشتركين على شبكة الانترنت، وعليه لا يجوز الحجز المسبق لعناوين المواقع منعا لظاهرة القرصنة الإلكترونية (Cybersquatting).[80]

يتضح مما سبق أن مسألة تسجيل العناوين الالكترونية عبر شبكة الأنترنت كأحد فروع الملكية الفكرية جدير بالتنظيم والحماية حيث قدرت بحوالي 75 مليون عنوان إلكتروني أو إسم نطاق مع حلول عام 2002 وهذا العدد مرشح للزيادة دون حدود، مما يتطلب الأمر وضع سياسة تشريعية تعالج مسألة العناوين من كافة الجوانب على نحو يمنع تداخل المسألة مع فروع الملكية الفكرية الأخرى لا سيما العلامات التجارية.

تجدر الإشارة، أنه رغم صدور قانون التجارة الالكترونية من طرف المشرع الجزائري سنة 2018 إلا أنه اكتفى بتعريف اسم النطاق أي العنوان الالكتروني، لذلك من الأحسن تعديله بوضع تنظيم للعناوين الالكترونية نظرا لأهميتها في معاملات التجارة الالكترونية ما ينعكس على التنمية الاقتصادية للمؤسسات.

قائمة المراجع:

أولا- الكتب

1- باللغة العربية

- ايهاب السنباطي، الموسوعة القانونية للتجارة الالكترونية، دار الجامعة الجديدة، الاسكندرية، 2008.
- بسام مصطفى عبد الرحمن طبيشات، الحماية القانونية للعلامات التجارية في ظل القانون الاردني والقانون المصري والاتفاقيات الدولية، طبع بدعم من وزارة الثقافة، مصر، 2009.
- محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، الاسكندرية، 2003.
- مصطفى موسى العطيات، الجوانب القانونية لتعاملات التجارة الالكترونية، ط. 1، دار وائل للنشر والتوزيع، عمان، الاردن،2011.
- عدنان غسان برانبو،التنظيم القانوني للعلامة التجارية، دراسة مقارنة، ط.1، منشورات الحلبي الحقوقية، بيروت، لبنان،2012.
- خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2009.
- خالد ممدوح ابراهيم، حقوق الملكية الفكرية، الدار الجامعية، الإسكندرية، 2010.
- كوثر سعيد عدنان خالد، حماية المستهلك الالكتروني، دار الجامعة الجديدة، الاسكندرية، 2012.
- فرحة زراوي صالح، الكامل في القانون التجاري، الحقوق الفكرية، ابن خلدون للنشر والتوزيع، EDIK، وهران، 2006، ص.259.

2- باللغة الفرنسية

-D. FOREST, Droit des marques et Noms de domaine, Gualino, Paris, 2012.

[80]- F. CHARLET,La protection des raisons de commerce sur internet, DESS Propriété industrielle, Droit commerce, l'Université de Lausanne, 2009-2010, p.7.

- J-F. BOURQUE et autre, Guide juridiques du commerçant électronique, Montréal, 2001.
- N. BEAURAIN et E. JEZ, Les noms de domaine de l'interne, Litec, Paris, 2001.
- N. DREYFUS, Marques et Internet : protection, valorisation, défense, Lamy, Paris, 2011.
- V. SEDALLIAN, Droit de l'internet: Réglementation, Responsabilité, Contrats, Éditions Net Press, Collection AUI, 1997.
- R. GOLA, Droit du commerce électronique, Guide pratique du e-commerce, Gualino, Paris, 2013.

ثانيا- الرسائل والمذكرات

1- باللغة العربية

- عبد الله حميد سليمان الغويري، العلامة المشهورة وحمايتها ضمن اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تربس) وقانون العلامات الأردني، رسالة دكتوراه في القانون الخاص، جامعة القاهرة، القاهرة، 2005-2006.

-راشديسعيدة،

النظامالقانونيللعلاماتالتجارية،مذكرةماجستيرفيالحقوق،فرعقانونالأعمال،كليةالعلومالقانونيةوالادارية،جامعةالجزائر،الجزائر،2001 – 2002.

2- باللغة الفرنسية

- S. PORLON, La lutte contre le cyersquatting (France, OMP, Etats-Unis), Mémoire du DEA Informatique et droit, faculté de droit, Université de Montpellier 1, 2000-200.
- F. CHARLET,La protection des raisons de commerce sur internet, DESS Propriété industrielle, Droit commerce, l'Université de Lausanne, 2009-2010.
-J. MORLEC, Le cybersquatting,Mémoire préparé dans le cadre de la Maîtrise de droit des affaires de la Faculté de droit de Nantes,Université d'Ottawa, 2004.

ثالثا- المقالات

1- باللغة العربية

- هادي مسلم يونس، أسماء النطاق على الانترنت وطبيعتها القانونية، مجلة الرافدين للحقوق، ع. 25، مجلد 12، السنة العاشرة، العراق، 2005.

- كوثر ماركي، الحماية القانونية للعلامة التجارية عبر الشبكة الرقمية، المجلة الجزائرية للعلوم القانونية، الاقتصادية والسياسية، كلية الحقوق، جامعة الجزائر، ع.3، 2003.

-حسن عبد الباسط جميعي وسمير حمزة، الحماية القانونية لمواقع الانترنت وأسماء الدومين، بحث مقدم في مؤتمر" التجارة الإلكترونية والإعسار عبر الحدود"، مركز القاهرة الإقليمي للتحكيم الدولي، 20-22 نوفمبر 2000.

- خليفي مريم، العناوين الالكترونية والعلامات التجارية في مجال التجارة الالكترونية، مجلة دراسات وأبحاث، ع. 2، جامعة الجلفة، الجزائر، 2010.

-عدنان إبراهيم سرحان، أسماء النطاق على الشبكة العالمية للمعلوماتية، المفهوم والنظام القانوني، دراسة مقارنة، مجلة الشريعة والقانون، دولة الإمارات hالعربية المتحدة، يناير 2006.

- عبد الراضي محمود كيلاني، عبد الراضي محمود كيلاني، المشكلات العملية الناتجة عن استعمال العلامات التجارية كأسماء للمواقع على الانترنت، دراسة مقارنة، ع.30، مجلة الدراسات القانونية، كلية الحقوق، جامعة اسيوط، مصر، سبتمبر 2011.

رابعا- النصوص القانونية

1- باللغة العربية

– الأمر رقم 03-06المؤرخفي 19 يوليو 2003،يتعلقبالعلامات،ج.ر.ج.ج،ع.44، الصادرة في23 يوليو 2003،ص.22.
– القانون رقم 18–05 المؤرخ في 10 مايو2018، المتعلق بالتجارة الالكترونية، ج.ر.ج.ج، ع.28، الصادرة في 16 مايو2018، ص.4

2– باللغة الفرنسية

- Code de la propriété intellectuelle ; https://www.legifrance.gouv.fr

- Principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine, adoptés le 26 août 1999, Documents d'application approuvés le 24 octobre 1999 ; www.wipo.int/amc/fr /docs/icannpolicy.pdf

خامسا– مراجع مواقع الانترنت

- Organe d'Enregistrement pour le domaine DZ, Charte de nommage du .DZ, Mars 2010, p.5 : www.nic.dz; Guide des Noms de Domaines, p.10 ; www.arsys.fr
- TGI Créteil, 29 mai 2001, cité par, Droit des marques et nom de domaine : application du principe de spécialité ; https://www.Legalis.net
- Y. EL SHAZLY, L'application du principe de spécialité aux noms de domaine : Un regard croisé entre la voie judiciaire et extrajudiciaire, p.2 ;
http://www.droit-technologie.org/upload/dossier/doc/160-1.pdf
- http://www.wipo.int/treaties/ar/convention

محمد الحافظ عيشوش
El.hafedh@yahoo.com
جامعة الوادي

زاوي عبد السلام
zaoui-abdesselam@univ-eloued.dz
جامعة الوادي

الجرائم الالكترونية كمحفز لتنمية الكفاءات البشرية

Cybercrime as a catalyst for the development of human competencies

الملخص:

أصبحت الجريمة الإلكترونية تحضى باهتمام المؤسسات والأفراد في ظل الانتشار الواسع لاستخدام تكنلوجيا المعلومات والاتصال، حيث أصحبت تشكل تهديدا صريحا للمؤسسات والأفراد وتكبدهم خسائر مادية ومعنوية كبيرة، لذا تسعى المؤسسات لانتهاج سياسات جديدة في محاربة الجريمة الالكترونية في ظل التطور والانتشار السريع لها، ومن هنا جاء بحثنا هذا للتسليط الضوء على دور الجرائم الالكترونية في دفع المؤسسات إلى بناء وتطوير كفاءاتها البشرية كإستراتيجية جديدة لمحاربة الجريمة الالكترونية.

باستعمال المنهج الاستنباطي الوصفي واستعراض تعريف الجريمة الالكترونية والكفاءة وطرق تنميتها توصلنا إلى أن للجريمة الالكترونية دور في تنمية الكفاءات البشرية من خلال تزويد الموظفين بمعارف ومهارات جديدة كطريقة لمحاربة الجريمة والحد من مخاطرها.

الكلمات المفتاحية: جريمة إلكترونية؛ كفاءات بشرية؛ مهارات ناعمة؛ مهارات صلبة.

Abstract:

Cybercrime has become of interest to institutions and individuals in light of the widespread use of information and communication technology, as it has become an explicit threat to institutions and individuals and incurred great material and moral losses, so institutions seek to adopt new policies in the fight against electronic crime in light of the development and rapid spread of it, hence our research This is to highlight the role of cybercrime in pushing institutions to build and develop their human competencies as a new strategy to fight cybercrime.

Using the descriptive deductive approach and reviewing the definition of cybercrime, efficiency and methods of its development, we concluded that cybercrime has a role in the development of human competencies by providing employees with new knowledge and skills as a way to fight crime and reduce its risks.

Keywords: *Cybercrime; human competencies; soft skills; Solid skills.*

1. المقدمة:

أحدث الإنترنت ثورة في مجال الاتصالات والتجارة في القرن الحادي والعشرين ، لقد أدى إلى عصر غير مسبوق من المعرفة والإبداع ، في الوقت نفسه ، يتزايد عدد الجرائم الإلكترونية بسبب الاستخدام المتزايد لاتصالات الإنترنت في الجرائم ضد الأشخاص والمؤسسات، وتشمل هذه القرصنة والتصيد الاحتيالي وبرامج الفدية والبريد العشوائي والتسويق الفيروسي ،ويمكن أن تؤدي هذه الجرائم إلى خسائر مالية فادحة وتؤثر على الجميع في المجتمع العالمي، مع زيادة قوة أجهزة الكمبيوتر واتصالها بالشبكات ، يواجه خبراء الأمن السيبراني تحديات أكبر لحماية الأنظمة من المتسللين ، فحتى الدول الصغيرة يمكنها أن تقاوم الدول الكبرى إذا كان أمنها السيبراني ضعيفًا.

لقد أصبح العالم متقدمًا تقنيًا بما يكفي للانخراط في جرائم وحروب الإنترنت في وقت واحد. يحتاج الجميع إلى توخي اليقظة عند استخدام الأجهزة الرقمية حتى لا يقع أي شخص ضحية للجريمة أو الحرب عبر الإنترنت ،فالمؤسسات تستثمر الكثير من الأموال في الأمن السيبراني لأنها تعرف مدى أهمية حماية بياناتها من الجرائم الإلكترونية.

إن الجرائم الإلكترونية الاقتصادية أصبحت أكثر شيوعًا وأكثر تعقيدًا ،و أصبحت هذه الجرائم خطيرة للغاية لدرجة أن العديد من الدول أنشأت وحدات جرائم إلكترونية للتعامل معها تمتلك جميع المعدات والأفراد اللازمين للتحقيق في هذه الجرائم وحلها بسرعة وكفاءة ، فقد تشمل بعض الجرائم الإلكترونية الاقتصادية الأكثر شيوعًا السطو على البنوك والاحتيال في تحويل الأموال والاحتيال في التأمين والاحتيال في سوق الأوراق المالية والابتزاز ، و يلجأ الأشخاص إلى الجرائم الإلكترونية الاقتصادية لأنه من الأسهل بكثير سرقة الأموال عبر الإنترنت مقارنةً بسرقة الأموال فعليًا في الشارع.

الجرائم الإلكترونية الاقتصادية متفشية ويمكن أن يرتكبها أي شخص لديه إمكانية الوصول إلى جهاز كمبيوتر أو هاتف ذكي ،فيجب أن تكون المؤسسات والافراد على دراية بكيفية تجنب ارتكاب هذه الجرائم من خلال الاعتماد على كفاءاتها بشرية وتنميتها بشكل مستمر لتشكيل خط دفاع قوي ضد الجرائم الالكترونية.

1.1 الإشكالية الرئيسية:

التهديدات السيبرانية اليوم لا تتعلق فقط بخروقات البيانات أو الفيروسات أو البرامج الضارة أو هجمات برامج الفدية، هناك مجموعة واسعة من الأنشطة الإجرامية الإلكترونية التي تشكل تحديات جديدة للشركات والأفراد في جميع أنحاء العالم ، هذه التهديدات تجبر المؤسسات على تبني طرق جديدة للتفكير والتعاون من أجل بناء ثقافة الأمن في أعمالها، وعليه نطرح الإشكالية التالية:

ما هو دور الجرائم الالكترونية في تنمية الكفاءات البشرية؟

1.2 التساؤلات الفرعية:

- ما هو تعريف الجرائم الالكترونية وأنواعها وطرق محاربتها؟؛
- ما هو تعريف الكفاءات البشرية وماهي أبعادها وطرق تنميتها؟؛
- كيف تساهم الجرائم في دفع المؤسسات لتطوير ككفاءاتها وانتهاج سياسة جديدة في مجال الامن الالكتروني؟

1.3 الفرضيات:

- الجرائم الالكترونية هي كل جريمة تعلقت بتكنلوجيا المعلومات والاتصال.
- للجرائم الالكترونية علاقة بتنمية الكفاءات البشرية.

1.4 أهمية البحث:

تكمن أهمية البحث في النقاط التالية:

- تناول موضوع حديث يتعلق باستخدام تكنولوجيا المعلومات والاتصال؛
- يضيف هذا البحث معرفة جديدة تسهم في معرفة طرق تنمية كفاءات الموارد البشرية؛
- يسلط هدا البحث الضوء على أهمية استغلال طرق محاربة الجرائم الالكترونية.

1.5 أهداف البحث:

يهدف هذا البحث الى:

- تعريف الجرائم الالكترونية وأهم طرق مكافحتها؛
- تعريف الكفاءات البشرية وأبعادها وأهم طرق تنميتها؛
- إيجاد العلاقة بين الجرائم الالكترونية وتنمية الكفاءات البشرية.
- إيجاد حلول وطرق للاستفادة من الجرائم الالكترونية في تعزيز الامن الالكتروني للمؤسسات.

1.6 منهجية البحث:

للإجابة على الإشكالية المطروحة في مقدمة هذا البحث سيتم اتباع المنهج الاستنباطي الوصفي للتطرق لمختلف الفرضيات المطروحة واثبات مدى صحتها من خلال تتبع كتابات وأقوال المختصين للخروج بنتيجة تجيب عن الإشكالية الرئيسية المطروحة من خلال تحليل ردت فعل الموارد البشرية نحو توجه الجرائم الالكترونية ومجارات للتطور السريع في هذا المجال.

2. الجرائم الالكترونية:

مع ظهور الإنترنت والتكنولوجيا الرقمية، ظهر نوع جديد من الجريمة: الجرائم الإلكترونية. تُعرَّف الجريمة الإلكترونية بأنها أي نشاط إجرامي ينطوي على استخدام أجهزة الكمبيوتر أو الإنترنت. يمكن أن

يشمل ذلك أي شيء من سرقة الهوية والاحتيال إلى التسلط عبر الإنترنت والقرصنة وسنحاول فيما يأتي عرض بعض التعريفات للجريمة الالكترونية واهم تصنيفاتها وطرق محاربتها

2.1 تعريف الجرائم الالكترونية:

إن مصطلح «الجريمة الإلكترونية" واسعة جدًا بحيث لا يمكن وصف السلوكيات التي تصنف بانها جرائم الكترونية كثيرة جدا ويبدو أن جميع الجرائم التي تحدث في الفضاء الإلكتروني أو التي لها اتصال بسيط بأجهزة الكمبيوتر أو الإنترنت يمكن تصنيفها تحت مظلة الجرائم الإلكترونية ، ورغم اختلاف المختصين في تعريف الجريمة الالكترونية بين التعاريف الموسعة التفصيلية وبين التعاريف المختصرة نقدم بعضهذه التعاريف:

- اتفاقية بودابست بشأن الجرائم الإلكترونية[1]:
- فتم التوقيع عليهافي عام 2001 ودخلت حيز التنفيذ في عام 2004، ولم تقدم الاتفاقية أي بيان أو وصف واضح للجريمة السيبرانية لكنها أدرجت تسعة أنواع من السلوكيات المحددة التي ينبغي معاملتها كجرائم الكترونية وهي:
- الوصول غير القانوني. اعتراض غير قانوني تدخل البيانات تدخل النظام إساءة استخدام الأجهزة؛ التزوير المرتبط بالحاسوب؛ الاحتيال المرتبط بالحاسوب؛ الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية؛ الجرائم المتعلقة بانتهاكات حقوق النشر والحقوق المجاورة.
- يعتقد كثير من المختصين أن الجريمة الإلكترونية تتمثل في ثلاث سلوكيات هي[2]:
- الجريمة التي تستهدف الكمبيوتر وشبكة الكمبيوتر، على سبيل المثال،القرصنة؛
- (الجريمة التقليدية التي تحدث في عالم الواقع الافتراضي، مثل الاحتيال الإلكتروني؛
- الجريمة التي يلعب فيها الكمبيوتر أو الإنترنت دورًا عرضيًا في ارتكابها

وعرفها Muyiwa Bبانهاجريمة يكون فيها الكمبيوتر هدفًا للجريمة كالقرصنة، التصيد الاحتيالي، البريد العشوائي، أو يتم استخدامه كأداة لإجراءجريمة[3]وتُصنف المواد الإباحية للأطفال وجرائم الكراهية على أنها جرائم إلكترونية [4].

ويرى وول ان الجريمة الالكترونية هيأي انتهاك يتعلق بجهاز كمبيوتر أو جزء منه بأنه جريمة إلكترونية[5].

1 https://rm.coe.int/budapest-convention-in-arabic/1680739173.
2 Clough, J, Cybercrime. Commonwealth Law Bulletin,2011,p: 671-680.
3 Muyiwa B. Afolabi, Gbolahan Ayodamola Raji ،Defeating the 21st century demon “Cybercrime” on corporate ،F1000Research,2022
4 Giuseppe C, Damian AT, Willem-Jan V: Cybercrime Threat Intelligence: ASystematic Multi-Vocal Literature Review, Computers& Security,2021, p:105
5 Wall D,what are Cybercrimes? Criminal Justice Matters, 2004; p:20–21

من خلال ما سبق من تعريفات يمكننا تعريف الجريمة الالكترونية بانها أي نوع من الجرائم يستخدم أو يستهدف تكنلوجيا العلام والاتصال.

2.2 تصنيف الجرائم الإلكترونية:

الجرائم الإلكترونية مصطلح يستخدم لوصف النشاط الإجرامي الذي يحدث عبر الإنترنت. هناك العديد من الأنواع المختلفة للجرائم الإلكترونية، بدءًا من الجرائم البسيطة مثل السرقة عبر الإنترنت إلى الجرائم الأكثر تعقيدًا مثل سرقة الهوية والتسلط عبر الإنترنت وسنسلط الضوء فيما يلي عن بعض تصنيفات الجريمة الالكترونية

2.2.1العنف السيبراني:

وهو يشبه العنف الحقيقي لكن المكونات التي يمكن أن تتضرر هي الأجهزة المتصلة بالإنترنت، والبيانات الموجودة على الخوادم، والمعلومات الموجودة على الإنترنت، وأي فرد أو مؤسسة يمكن أن يمسه العنف السيبراني[1]. فيما يلي أنواع مختلفة من العنف السيبراني التي نناقش منها الأكثر شيوعًا[2]

- حرب الإنترنت:

الهدف من الحرب السيبرانية هو إحداث خلل أو تعطيل أو تدمير البنية التحتية والموارد بناءً على نظام الإنترنت الخاص بالدولة المنافسة أو العدووتستخدم كل أنواع الهجمات الإلكترونية لتحقيق النصر على البلد المستهدف.

- الإرهاب الإليكتروني:

الأشخاص أو الجماعات التي تهدف فقط إلى تدمير الإنسانية والانتصار لدينهم ويستخدمون أي نوع من الهجمات الإلكترونية لتحقيق هدفهم.

المطاردة عبر الإنترنت:

إنه يشبه حلقة for من لغة C حيث يكون شرط الإنهاء هو مضايقة هدفك. في هذا النوع من الهجوم، يستخدم المهاجمون الاتصالات الإلكترونية (البريد الإلكتروني والرسائل الفورية) لمهاجمة هدفهم[3]

- الانتقام السيبراني:

الانتقام يعني إيذاء شخص ما ردًا على فعل سابق له. والهدف من الانتقام السيبراني هو سرقة وتغيير المعلومات السرية للعدو من أجل مصالحه الخاصة.

1 M. Yar, Cybercrime and Society, SAGE Publications, ousandOaks, CA, USA, 2013.
2Harmandeep Singh Brar, Gulshan Kumar, Cybercrimes, A Proposed Taxonomy and Challenges،Journal of Computer Networks and Communications, Volume,2018, p:11
3 April 2017, http://searchsecurity.techtarget.com/definition/cyberstalking

2.2.2 متجول إلكتروني:

المتجول الإلكتروني هو فعل عمل غير قانوني أو سرقة بيانات سرية لشخص ما بمساعدة نظام كمبيوتر متصل بالإنترنت. هناك نوعان أساسيان من الجرائم الإلكترونية في هذه الفئة والتي تمت مناقشتها أدناه.

- الاحتيال الإلكتروني:

الهدف الرئيسي من الاحتيال هو الحصول على مزايا من حيث المال. تتضمن عمليات الاحتيال الإلكتروني هجمات الهندسة الاجتماعية مثل تخمين كلمات المرور تلاعب المتسلل بالمستخدمين للحصول على معلوماتهم السرية ثم يستخدم هذه المعلومات لمصالحه الخاصة.

- النشاط السيبراني:

تُستخدم في هذا النوع التطبيقات الاجتماعية والتواصلية المستندة إلى الإنترنت لإنشاء النشاط وتشغيله وإدارته مثل التواصل الأسرع مع الأشخاص أو توزيع المعلومات على جمهور كبير في بضع ثوانٍ. وتستخدم Twitterو Facebookو YouTubeو LinkedInو Whatsappو Gmailوغيرها؛ في هذا النوع من الجرائمفي الظاهر هي تقنيات جيدة لكنها قد تستعمل لنشر الشائعات للإضرار بصورة المنافسين أو نشر معلومات كاذبة عن منظمتهم أو أفرادهم للحصول على أنواع مختلفة من الفوائد

2.2.3التعدي الإلكتروني:

التعدي الإلكتروني هو الجريمة التي يتم فيها انتهاك القانون الإلكتروني من خلال اختراق نظام مستخدم مرخص وينتهك السرية والنزاهة الأساسية له. أنواعهمختلفة كمها:

- السرقة الإلكترونية:

وهو القيام بالسرقة الإلكترونية في الفضاء الإلكتروني عن طريق اختراق نظام الكمبيوتر الخاص بشخص ما والمتصل بالإنترنت. بهدف سرقةأو إتلاف المعلومات والبيانات لتحقيق مكاسب مالية أو شخصية. هناك نوعان أساسيان من السرقات:

- السطو الإلكتروني الكلاسيكي:

يشبه السطوالإلكتروني، لكن هدفه الحصول على أموال. ثم يقوم ببيع أو حذف اسم المجال الخاص به. لكن بعد تغير القوانين أصبح هذا النوع شبه معدوم[1]

- السطو الإلكتروني المهين:

1 N. S. Sreenivasulu, Law Relating to Intellectual Property, Partridge Publishing, Gurugram, India, 2013.

الهدف الرئيسي له تدمير سمعة هدفه ومكانته في المجتمع. فيقوم المحتال الإلكتروني بذلك بوسائل مختلفة مثل نشر مواد إباحية أو كلام يحض على الكراهية أو محتويات منتهكة على اسم نطاق الهدف

- السطو الإلكتروني المطبعي:

لا يستخدم المهاجم نفس اسم العلامة التجارية بل يستخدم اسم مشابه جدًا لاسم العلامة التجارية الأصلي. على سبيل المثال، إذا قام المهاجم بتسجيل اسم مجال في Gmail مشابه جدًا لـGmail، فقد ينجح في خسارة مالك العلامة التجارية الأصلي

2.3 طرق محاربة الجرائم الالكترونية:

مع ظهور الجرائم الإلكترونية، من المهم أن تكون المؤسسات والافراد على دراية بالطرق التي يمكنك من خلالها حماية أنفسهم وبياناتهم منها، ومحاربة هذه لظاهرة يتطلب جهود وتعاون على مستوى دولي وقاري ومحلي[1]

على المستوى الدولي:

فهناك عدة هيئات دولية تسعى للتعاون وسن قوانين وتنظيمات لمحاربة الجرائم الالكترونية منا:

- الأممالمتحدة؛
- الاتحادالدوليللاتصالات؛
- المنظمةالدوليةللشرطةالجنائيةالإنتربول؛
- المنظمةالعالميةللملكيةالفكرية؛
- منظمة التعاون الاقتصادي والتنمية؛
- الاتحاد الأوروبي؛
- اتفاقية المجلس الأوروبي؛
- مجموعةالدولالثماني.

على المستوى القاري فهناك:

- الاتحاد الإفريقي.

على المستوى العربي:

- الاتفاقيةالعربيةلمكافحةجرائمتقنيةالمعلوماتي؛
- المكتبالإقليميالعربيللاتحادللاتصالات؛
- مجلسوزارالعدلالعرب؛

1فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد الثاني 2015، ص6-21.

أما على المستوى الوطني:

فقد سعت الدولة الى انشاء عدة قوانين لمحاربة الجريمة الالكترونية والحد من خطرها على الافراد والمؤسسات ومنها:

- **المساسبأنظمةالمعالجةالآليةللمعطيات؛**
- الحمايةمنخلالقوانينخاصة كنصوص حمايةالتوقيعالإلكتروني وقانونالملكيةالأدبيةوالفنية؛
- **حمايةحرمةرموزالدولة؛**
- **الحمايةمنخلالقانونالإجراءاتالجزائية؛**

وتذكر Khrystyna VOROBETSعدة نقاط للتصدي للجريمة الالكترونية وفقًا لخطة العمل لعام 2018 بشأن تنفيذ استراتيجية الأمن السيبراني لأوكرانيا، التي وافق عليها مجلس وزراء أوكرانيا اعتبارًا من 11 جوان 2018

يمكن تلخيصها فيمايلي[1]:

1 – تحديد المسؤولية الجنائية عن الجرائم في مجال استخدام الحاسبات (الحاسبات) والأنظمة والشبكات الحاسوبية وشبكات الاتصالات؛

2 – حظر وكالات الدولة والشركات والمؤسسات والمنظمات المملوكة للدولة، باستثناء المؤسسات الدبلوماسية الأجنبية في أوكرانيا، لشراء خدمات بشأن الوصول إلى الإنترنت من مشغلي الاتصالات السلكية واللاسلكية، والتي لا توجد وثائق تؤكد مطابقة نظام حماية المعلومات في مجال حماية المعلومات؛

3 .تحسين التفاعل بين الجهات الفاعلة التي توفر الأمن السيبراني من خلال: إنشاء قاعدة بيانات تفاعلية واحدة لمجرمي الإنترنت لتلبية احتياجات وزارة الدفاع،وSSSU،وSBU، والشرطة الوطنية، والبنك الوطني، ووكالات الاستخبارات؛

4 .التوفيق بين مشاريع البرنامج الوطني للمعلومات، والمتوقع تنفيذه في عام 2018، مع إدارة خدمة الاتصالات الخاصة للدولة والوكالة الحكومية للحوكمة الإلكترونية؛

5 .تحسين الإطار القانوني من خلال: زيادة تنفيذ المعايير الدولية؛

6 .تطوير آلية لجذب الأفراد والكيانات القانونية لأداء مهام الدفاع السيبراني لمصادر المعلومات الإلكترونية للدولة في إطار الشراكة بين القطاعين العام والخاص؛

7 –تطوير الشبكة القومية للاتصالات وتنظيم الأمور المتعلقة بترتيب تقديم الخدمات وتعريفها؛

1 The plan of measures for 2018 on the implementation of theCybersecurity Strategy of Ukraine, approved by the Cabinet of Ministers of Ukraine July 11, 2018, No. 481-p. [accessed 2022 May 22]. Available from: http://zakon.rada.gov.ua/laws/ show/481-2018-%Dl%80

8 .إجراء تحديث للمراكز الظرفية للأمن السيبراني في SSSU وSBU؛

9. ضمان تطوير النموذج التنظيمي والتقني للدفاع السيبراني، ولا سيما إنشاء مركز للاستجابة للتهديدات السيبرانية، فضلاً عن تطوير نظام وصول آمن لسلطات الدولة إلى الإنترنت؛

10 .العمل على إيجاد مركز تدريب إلكتروني لصالح مواضيع توفير الأمن السيبراني؛

11 .تحسين آلية التفاعل مع الأكاديمية الوطنية للعلوم ومؤسساتها المتخصصة لغرض إجراء البحوث العلمية والأعمال العلمية والعملية المشتركة في مجالات الأمن السيبراني والدفاع السيبراني للبنية التحتية الحيوية؛

12 .ضمان أنشطة مركز الدفاع الإلكتروني التابع للبنك الوطني، وتحسين الأمن السيبراني والأمن السيبراني للنظام المصرفي وفي مجال تحويل الأموال؛

13 .تطوير منهجية لتشكيل وتعريف المؤشرات الرئيسية لفعالية استراتيجية الأمن السيبراني، مع الأخذ في الاعتبار تجربة الممارسات الأوروبية والعالمية؛

14 –المشاركة في تدابير تعزيز التعاون الدولي من خلال إنشاء مجموعات ثنائية أو متعددة الأطراف مشتركة لإجراء تحقيقات في جرائم الفضاء الحاسوبي، فضلاً عن العمليات المشتركة وتبادل المعلومات والخبرات؛

15 .تنظيم وعقد المؤتمرات والندوات والمنتديات والموائد المستديرة والتدريب والأمن السيبراني وتمارين الأمن السيبراني على الصعيدين الوطني والدولي؛

16 .تطوير نظام التدريب في مجال الأمن السيبراني، ولا سيما: تدريب المتخصصين على المستوى التكتيكي والتشغيلي؛

17. تصميم مركز بيانات آمن لاحتياجات الجهات الحكومية وخاصة قطاع الأمن والدفاع وقطاعات المال والطاقة والنقل؛

18 .تنفيذ تدابير إنشاء المركز الوطني للعمليات والإدارة الفنية لشبكات الاتصالات السلكية واللاسلكية.

3. الكفاءات البشرية:

3.1 تعريف الكفاءة:

يعد تعريف الكفاءات البشرية محل خلاف بين أهل الاختصاص لارتباطه الوثيق بالعنصر البشري الذي حيث يصعب إيجاد نظرة موحدة للظواهر البشرية لاختلاف زاوية النظر اليها بين مختلف العلوم والتخصصات كلم النفس والاجتماع والاقتصاد والإدارة ولكل منهم وجهة نظر ومقاربة تخدم تخصصه، وسنحاول هنا طرح عدة تعريفات للكفاءات البشرية على أساس إداري:

التعريف الأول (R. Boyatzis1982): هي الخصائص الكامنة للفرد المرتبطة بالأداء العالي الفعال وتتمثل هذه الخصائص في المعرفة والمهارة والدوافع والقيم وغيرها[1].

التعريف الثاني(Gerard Scallon) : هي عبارة عن معرفة التصرف أو تعبئة المعارف والمهارات والسلوك، والمقصود بالتعبئة هو استغلال وتطبيق تلك الموارد فيمواقف مختلفة وسهولة نقلها من موقف لآخر".

التعريف الثالث(Usinor Sacilor) :هي المهارة العلمية الآنية والقصيرة الأجل.

التعريف الرابع Dubois and Rothwell2000:الكفاءات على أنها أدوات يستخدمها العمال بطرق متنوعة لإكمال وحدات العمل أو مهام الوظيفة[2].

التعريف الخامس (David D. Dubois William J. Rothwell) : الكفاءات هي الخصائص التي يمتلكها الأفراد ويستخدمونها بطرق مناسبة ومتسقة من أجل تحقيق الأداء المطلوب،وتشمل هذه الخصائص المعرفة والمهارات وجوانب الصورة الذاتية، الدوافع الاجتماعية والسمات وأنماط التفكير والعقليات وطرق التفكير، الشعور والتمثيل[3].

التعريف السادس (Jean–Marie Peretti): ذكرهالكاتب في قاموسه للموارد البشرية لسنة 2016 عرفها بأنها "القدرة على أداء نشاط متعلق بالوظيفة يساهم في الأداء الفعال عند أداء المهمة[4]"

التعريف السابع (Parry 1996):وهو تعريف تم جمعه من اقتراحات عدة مئات من الخبراء في تنمية الموارد البشرية الذين حضروا مؤتمرًا حول موضوع الكفاءات في جوهانسبرغ في عام 1995، وعرفت الكفاءة على أنها مجموعة من المعارف والمهارات والمواقف ذات الصلة التي تؤثر على جزء كبير من وظيفة الفرد، التي ترتبط بالأداء في الوظيفة، والتي يمكن قياسها مقابل المعايير المقبولة جيدًا والتي يمكن تحسينها من خلال التدريب والتطوير[5].

3.2 أبعاد الكفاءة البشرية:

المعرفة:

1أبو القاسم حمدي. (2004). تنمية كفاءات الأفراد ودورها في دعم الميزة التنافسية للمؤسسات. كلية العلوم التجارية والاقتصادية وعلوم التسيير (مذكرة ماجستير)، الجزائر: جامعة الجزائر.

2David D. Dubois William J. Rothwell, Competency-Based Human Resource Management, Davies-Black Publishing, California, 2004, p:18.

3David D. Dubois William J. Rothwell, Competency-Based Human Resource Management, Davies-Black Publishing, California, 2004, p:16.

4 Marie Peretti, J. DICTIONNAIRE,L'HARMATTAN, Paris,2016, p :159.

5 Seema Sanghi, The HandbookofCompetency Mapping, Response Books, New Delhi, 2007, p: 10.

اختلفت آراء الباحثين حول تعريف المعرفة من عدة مداخل واتجاهات، فليس هناك اتفاق على مفهوم موحد للمعرفة[1] وسنتطرق لبعض هاته التعاريف فيما يلي:

يعرفها ثابت الحبيب وبن عبو الجيلاني بأنها مجموع من المعلومات المستوعبة والمهيكلة والمدمجة في إطار مرجعي يسمح لمؤسسة بقيادة أنشطتها والعمل في إطار خاص [2]، كما تعتبرها حمداوي وسيلة مجموعة من المعلومات المحصل عليها والتي تساعد على فهم أو الإحاطة بمجموعة من الأشياء[3].

المهارة:

وتعرف أيضا بمصطلح المعرفة العملية ويعرفها [4] على أنها القدرة العملية أو وسيلة تطبيق المعرفة، ويعرفها "هي القدرة على تسيير عمل بطريقة ملموسة وفق عملية أو أهداف معروفة مسبقا، والمعارف العملية لا تقصي المعارف النظرية، لكن لا تحتاج إليها بالضرورة، وتتكون المعارف العملية بالتجربة"[5]، وتعرف أيضا أيضا بأنها" المهارة هي استعداد أو موهبة طبيعية أو مكتسبة تنمو بالمعرفة أو بالتعليم وتصقل بالتدريب، وتجعل الفرد قادرا على الأداء جسميا وذهنيا"[6].

السلوك:

عرف (1999) Green السلوك بأنه إجراء يمكن ملاحظته ووصفه والتحقق منه، ويعرفه (شفيق) بأنه مجموع النشاط النفسي الجسمي والحركي والفسيولوجي واللفظي الذي يصدر عن الانسان وهو يتعامل مع بيئته ويتفاعل معها [7]، كما عرفت السلوك أيضًا بأنه مجموعة من الاستجابات التي يصدرها الفرد تجاه الظروف البيئية المختلفة [8]، ويرى سيجمون فرويد أن لكل نمط من أنماط السلوك منشأ فالسلوك ما هـ و الى

1إبراهيم بويحياوي، ونوال بن أحمد. (1 جوان, 2016). أهمية ودور الكفاءات البشرية داخل المنظمة. مجلة التنمية وإدارة الموارد البشرية، الصفحات 9-26.

1 2ثابتي الحبيب ،بن عبو الجيلاني " تطوير الكفاءات و تنمية الموارد البشرية دعائم النجاح الأساسي لمؤسسات الألفية الثالث "، مؤسسة الثقافة الجامعية ،الإسكندرية ،طبعة2009. ص 117

. 3حمداوي وسيلة، ادارة الموارد البشرية«، مديرية النشر لجامعةقالمة، الجزائر،2004، ص 25

4 Clarkson, M. (2001). Developing IT staff: à practical approach. USA : Springerm,

5كمال منصوري، وسماح صولح. (جوان, 2010). تسيير الكفاءات: الإطار المفاهيمي والمجالات الكبرى. مجلة أبحاث اقتصادية وإدارية، الصفحات 48-69.

6رائد عمر الآغا. (2008). المهارات القيادية لدى المسئولين في شركة الاتصالات الخلوية (مذكرة ماجستير). كلية التجارة، غزة: الجامعة الإسلامية 63.

7محمد شفيق. (بلا تاريخ). السلوك الانساني وفن القيادة والتعامل ومهارات الادارة. القاهرة: مصبعة روزالويسف الجديدة.

8سماء منصور. (7 أكتوبر, 2020). تعريف السلوك في علم النفس. تم الاسترداد من مقال: /https://mqaall.com/defining-behavior-psychology

نتيجة للقوى الدافعة والمثيرات والخبرات الكامنة في نفس الانسان [1]،ويعرفهآخرينبأنهأينشاطيصدرعن الإنسانسواءكانأفعالايمكنملاحظتهاوقياسهاكالنشاطات الفسيولوجيةوالحركيةأونشاطاتتتمعلىنحوغيرملحوظكالتفكيروالتذكروالوساوسوغيرها[2]، ويعرفها بأنها ال قدرة الشخص على التصرف الاجتماعي في إطار وظيفته، أي علاقاته مع فريقالعمل ضمن ثقافة المنظمة[3].

يمكن القول إن السلوك هو ردة الفعل لمثير ما فالسلوك لا يمك ن أن يحدث من فراغ وهو يتأثر بالبيئة فيمكن ضبطه وتوجيهه، ولعل أهم مكونات السلوك الدوافع والقيم.

3.3 أهم طرق تنميت الكفاءات البشرية:

تعد الكفاءات البشرية ميزة تنافسية وقيمة مضافة تساعد المؤسسات على التأقلم مع بيئتها سريعة التغير لذا كان لزاما على المؤسسات تنمية كفاءات مواردها البشرية باستمرار واستعمال عدة طرق ووسائل للوصول الى كفاءات متميزة قادرة على دفع المؤسسة الى أداء أفضل وتجنب وقوعها في أزمة كفاءات، ويعرف دافيد ديسونزو وستيفانروبينسوسوزانفيرهولست تنمية الكفاءات بأنها تعني نظرة مستقبلية تجاه الموارد البشرية، تركز بشكلكبير على التعلم، بدل من تدريب الموارد البشرية على ممارسة أنشطة محددة[4]،

ويرى Claude Levy-Leboyأن تنمية الكفاءات عملية تتم بالتوازي مع العمل عكس ما كان متعارف عليه من قبل أن التدريب والتعليم يسبق العمل بل أصبح يرافقه أو أثناء العمل نفسه [5]، فتنمية الكفاءات عملية تسمح بالتكامل الناجح للمعرفة والدراية من أجل بناء كفاءات جديدة.

ويمكن تعريف عملية تنمية الكفاءات البشرية بانها عملية تم التخطيط لها مسبقا للتأثير على ابعاد الكفاءة لتحسين قدرات الموارد البشرية لتستجيب للوظائف المستقبلية

وتتبع المؤسسات عدة طرق ومداخل لتنمية كفاءاتها البشرية،ولضمان نجاح عملية تنمية الكفاءات البشرية لابد من مراعات عدة شروط أساسية تتمثل في[1] :

1[1]روبيرت د. ناى. (2001). السلوك الانساني ثلاث نظريات في فهمه. (احمد إسماعيل صبح، ومنير فوزي، المترجمون) الجيزة: هلا للنشر والتوزيع.

2عبد الجبار أمل. (27 فيفري, 2013). كلية الدراسات القرآنية. تم الاسترداد من جامعة بابل: lcid=34957&http://www.uobabylon.edu.iq/uobcoleges/lecture_file.aspx?fid=19

3حمود حيمر. (2018). تنمية الكفاءات ودورها في تحسين أداء الموارد البشرية بالمنظمة (أطروحة دكتوراه). كلية العلوم الاقتصادية والتجارية وعلوم التسيير، سطيف: جامعة سطيف1.

44حمود حيمر. (2018). تنمية الكفاءات ودورها في تحسين أداء الموارد البشرية بالمنظمة (أطروحة دكتوراه). كلية العلوم الاقتصادية والتجارية وعلوم التسيير، سطيف: جامعة سطيف1.

5 Claude Levy-Leboyer, LA GESTIONDES COMPÉTENCES, Éditions d'OrganisationGroupe Eyrolles, Paris, 2009 : 114, p : 115.

- مطابقة محتوى برنامج التدريب لتنمية الكفاءات والواقع العملي؛
- تجويد الممارسات الوظيفية باستخدام السلوكيات الجديدة والمعارف المكتسبة في عمليةالت نمية خلال العمل؛
- دفع وتحفيز الموارد البشريالى تطبيق الكفاءات الجديدة والمكتسبة من عملية التنمية في أداء وظائفها؛
- تنويع المحتوى التدريبي المقرر بوضعيات عمل مختلفة، وبالتالي تنويع كفاءات الموارد البشرية المكتسبة وتوسيعها؛
- وتعريف الموارد البشرية بمراحل التي ستمر بها عملية التنمية وتعليم النقاط الأساسية؛
- مساعدة الموارد البشرية على أخذ صورة واضحة للأنشطة الضرورية لأداء وظائفهم؛
- التأكد من إدراك وفهم الموارد البشرية للخصائص الهامة للوظيفة ومتطلبات شغلها؛
- التثبت من قدرة البيئة على تشجيع التعلم واكتساب كفاءات جديدة؛
- التأكد من رغبة الموارد البشرية وقبلوها للتعلم واكتساب كفاءات جديدة؛
- إقناع الموارد البشرية على التعلم المستمر وتنمية كفاءاتها لمواجهة تحديات المستقبل.

4. الجرائم الالكترونية كمحفز لتنمية الكفاءات:

التهديدات السيبرانية اليوم لا تتعلق فقط بخرقات البيانات أو الفيروسات أو البرامج الضارة أو هجمات برامج الفدية. هناك مجموعة واسعة من الأنشطة الإجرامية الإلكترونية التي تشكل تحديات جديدة المؤسسات والأفراد في جميع أنحاء العالم ،فتضطر الاقتصادات الصناعية إلى تطوير بنى تحتية تنظيمية للتعامل مع الجرائم الإلكترونية لأنها تواجه المزيد منها .في هذه البلدان، تتطلب بعض القوانين أيضًا من الشركات تعزيز دفاعاتها ضد الجرائم الإلكترونية ،اقترح أحد التقديرات أن البنوك الأمريكية أنفقت 60 مليون دولار في عام 2002 على التكنولوجيا للامتثال لمتطلبات قانون باتريوت، وهذه التهديدات أيضا تجبر المؤسسات على تبني طرق جديدة للتفكير والتعاون من أجل بناء ثقافة الأمن في أعمالها. واستخدام تهديد الجريمة الالكترونية كمحفزلبناء برنامج تطوير الكفاءات البشرية.

فللكفاءات البشرية هي مزيج من المعرفة والمهارات والمواقف،ويمكن للمؤسسات التي تستثمر في تطوير موظفيها جني فوائد هذا الاستثمار من خلال زيادة مشاركة الموظفين وانخفاض معدل دوران الموظفين ،فعندما يأخذ الموظفون الوقت الكافي للتدريب على كيفية تطبيق معارفهم ومهاراتهم الحالية لحل المشكلات واغتنام الفرص ، فإنهيمكنهم من تبني الثقة والمشاركة. الموظفون الذين يشعرون بأن لديهم صوتاويعاملون باحترام هم

1حمود حيمر، تنمية الكفاءات ودورها في تحسين أداء الموارد البشرية بالمنظمة، كلية الاقتصاد، جامعة سطيف1، الجزائر، 2018 م، ص 68.

أكثر عرضة للبقاء منخرطين وملتزمين بالمنظمة، فإذا كان عملك يعتمد بشكل كبير على التكنولوجيا ، فأنت بحاجة إلى موظفين يفهمون التكنولوجيا ، ويعرفون كيفية استخدامها ، ويمكنهم استكشاف الأخطاء وإصلاحها عند تعطلها، لكن التكنولوجيا تتغير بسرعة – وكذلك التهديدات التي تأتي معها ، و يزداد مجرمو الإنترنت تطورا يوما بعد يوم وأصبحوا أكثر إبداعا في الطريقة التي يهاجمون بها المؤسسات،فلا يمكنك فقط توظيف موظفين يمكنهمإجراء اختبار مهارات الكمبيوتر ،فالمؤسسة بحاجة إلى أشخاص يمكنهم التفكير النقدي وقادرين على التكيف مع الظروف المتغيرة والتحديات الجديدة و إلى أشخاص يمكنهم وضع الاستراتيجيات والابتكار وحل المشكلات والتعاون والتواصل بفعالية ، وهناك مهاراتان اساسيتان لمحاربي الجريمة الالكترونية لابد من تمتع الموظفين بهما وهما:

المهارات الناعمة:

في حين أن المهارات الصعبة تحظى بمعظم الاهتمام ، من المهم ملاحظة أن المهارات الناعمة لا تقل أهمية عندما يتعلق الأمر بإعداد الموظفين لمواجهة تهديد الجريمة الإلكترونية، المهارات الناعمة هي المهارات التي تساعد الموظفين على العمل معا وإدارة العلاقات ، بما في ذلك التواصل وحل المشكلات واتخاذ القرارات والذكاء العاطفي القدرة على التعبير عن الأفكار والأفكار بوضوح وفعالية و القدرة على تحديد المشكلات وتحليل الموقف والتوصل إلى حلول منطقية وتنفيذ الحلول بفعالية، القدرة على إصدار أحكام سليمة بناء على المعلومات المتاحة والخبرات السابقة.

المهارات الصعبة:

المهارات الصعبة هي المهارات التقنية المحددة التي يحتاجها الموظفون من أجل أداء وظائفهم، هذه المهارات تساعد الموظف على تنفيذ الوظيفة بفعالية، وهي تشمل مهارات الكمبيوتر ، ومهارات الترميز ، ومهارات الأمان c yber ، و القدرة على استخدام التطبيقات وأنظمة التشغيل مثل Microsoft Office و Adobe Creative Cloudو Salesforce و، Gmail و مهارات الترميز و كتابة التعليمات البرمجية بلغات مثل Pythonو Java و C وما إلى ذلك.، إضافة مهارات الأمن السيبراني كالقدرة على الدفاع ضد التهديدات السيبرانية والتخفيف من نقاط الضعف.

ان تنمية الكفاءات البشرية هي شيء لا يمكن القيام به خلال مرحلة التوظيف فقط بل يمتد لشمل فترة حياة الموظف ، و في حين يمكن اختبار المهارات التقنية ، فإن المهارات الناعمة هي شيء لا يمكنك قياسه إلا من خلال عملية مقابلة شاملة ،و أفضل طريقة لقياس المهارات الناعمة والمهارات الصلبة للموظفين هي من خلال وضعهم في سيناريوهات واقعية تختبر مهاراتهم في حل المشكلات وتساعدهم على تطبيق معارفهم ومهاراتهم الحالية لحل المشكلات الجديدة ، و الجريمة السيبرانية هي واحدة من أكبر المحفزات لتطوير الكفاءات البشرية، لانه تهديد يتطور باستمرار ، وهو معقد بشكل لا يصدق ، ويتغير باستمرار ، فهو يجبر المؤسسات على إعادة التفكير في نهجها تجاه الأمن وإلقاء نظرة جديدة على نقاط ضعفها ، وإعادة تقييم

استراتيجيتها الأمنية وتحديد الثغرات وابتكار طرق لسد هذه الثغرات والتخفيف من نقاط الضعف ، من خلال تنمية كفائتهم البشرية واكسابهم مهارات ومعارف تتماشى مع تطور الجريمة الالكترونية.

وعليه فيمكن للمؤسسات مكافحة الجريمة السيبرانية من خلال تنمية كفاءات الموظفين واكسابهم المهارات اللازمة للحماية من الجرائم الإلكترونية ، ويمكن أن يشمل ذلك تدريب الموظفين على التعرف على تهديدات الجرائم الإلكترونية والاستجابة لها بشكل مناسب. وتزويدهم بالمهارات التي يحتاجونها لتجنب الجرائم الإلكترونية، فوعي الموظفين بالمعلومات يساعد على فهم تهديد الجريمة السيبرانية، مع منحهم المهارات التي يحتاجونها لتجنب الوقوع ضحية لها، يمكن أن يغطي التدريب على التوعية مواضيع مثل التعرف على رسائل البريد الإلكتروني المزيفة ومواقع الويب الضارة وغيرها.

.

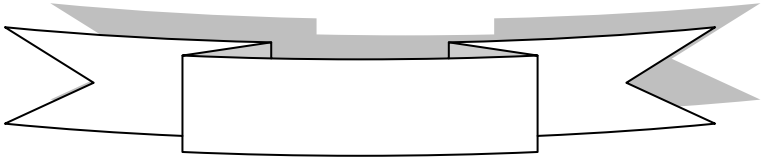
5. الخاتمة:

في ختام هذا البحث يمكننا ملاحظة أن الجرائم الإلكترونية تشكل تهديدا حقيقيا للشركات والأفراد في جميع أنحاء العالم. أفضل طريقة لمكافحة الجريمة السيبرانية هي إعداد تزويد الموظفين بالمعرفة والمهارات التي يحتاجونها للدفاع ضد التهديدات السيبرانية واكتشاف نقاط الضعف وتخفيف المخاطر ، ويمكن تحقيق ذلك باستخدام الجريمة السيبرانية كحافز لتنمية الكفاءات البشرية،ومن بين النتائج التي خرج بها هذا البحث:

- الجرائم الالكترونية في تطور وانتشار مستمر وتتطور ويتطور تكنلوجيا المعلومات والاتصال؛
- الكفاءات البشرية تعتبر حجر الاساس لتطور المؤسسات؛
- تشكل المهارات الصعبة والمهارات الناعمة دورا فعالا في محاربة الجرائم الالكترونية؛
- الجرائم الالكترونية لها علاقة وطيدة بتطور الكفاءات البشرية وتنميتها من خلال التعرف على الاشكال الجديدة للجرائم الإلكتروني ومحاربتها،فالجريمة الإلكتروني وتطورها السريع يدفع المؤسسات لتنمية كفاءاتها البشرية لاستباق المجرمين وإيجاد حلول استباقية.

التوصيات:

- مواكبة تطور التكنلوجي وذالك باستعمال اقوى الاجهزة واخر تدابير الامن السبراني؛
- الالتزام بتدابير الجهات الوصية للحفاظ على أمن البيانات الشخصية؛
- توظيف الكفاءات التي اثبتت قدرات عالية في التحكم في التكنلوجيا؛
- الاطلاع على الابحاث الجديدة في مجال الجرائم الالكترونية لتزويد الموظفين بها.



مريم فلكـــاوي
felkaoui.meryem@univ-guelma.dz
جامعة 8 ماي 1945 قالمة

خصوصية السلوك الإجرامي للمجرم المعلوماتي

مقدمة:

يسود الأحكام الجزائية مبادئ عدة، يعد من أهمها مبدأ الشرعية، والذي مقتضاه ألّا يجرم سلوك أو امتناع، أو تقرر عقوبة أو تدبير أمن إلا بموجب قاعدة قانونية صادرة عن الجهاز التشريعي المختص بالدولة.

هذا المبدأ الذي استقرت على الإعمال به معظم تشريعات العالم الوضعية، والجزائر من بينها، يتجسد في أدق صوره في الأحكام الخاصة للقاعدة الجزائية، أي أن المشرع بعد تحديد الأحكام المشتركة بين جميع الجرائم من حيث الأركان، سيخصص –بناء على الشرعية الجزائية– قواعد تنصص على كل جريمة وفقا لخصوصية أركانها، أو المجال الذي ارتكبت فيه، أو الزمن ...إلى غير ذلك من الظروف التي بتوافرها ستغير لا محالة من طبيعة الجريمة، أو العقوبة المقررة لها، أو ...

انطلاقا من هذا المبدأ، أصبحت القاعدة الجزائية الخاصة محلا للتعديل والتحديث وفقا لما يشهده العالم من تطورات في كل المجالات، وأهم ما يسلط عليه الضوء في هذا المقام هو المجال الرقمي، الذي أصبح تنظيم حركته تحديا للتشريعات بمختلف فروعها، والقاعدة الجزائية الخاصة بصورة أدق، إذ أن الأفعال التي تندرج وفقا للقواعد العامة ضمن مجال التجريم لا يمكن أن تغطي مختلف التجاوزات الحاصلة في المجال المعلوماتي، مما يدع مجالا واسعا لهامش الإفلات من المتابعة والعقاب لأشخاص يعلمون جيدا علم التقنية، ويتمتعون بكل الإمكانيات التي تهيء لهم مجال ارتكاب جرائمهم دون الوصول لهم، أو التعرف عليهم.

فإذا كان يُنظر إلى الجرائم الإلكترونية على أنها هجمات غير منظمة ومنفردة، وتمثلجزءًا صغيرا من المحتالين على الإنترنت، فقد تطورت حاليا بسرعة إلى جريمة منظمة مع منظمات تقودها مستخدمة أسطولًا من المطورين ذوي الخبرة،والذين يصنعون برامج وتكتيكات هجومضارة وأكثر تعقيدًا.

فقد أظهرت نتائج تقرير سنة 2012، لمؤسسة نورتنNORTONالمتخصصة بتوفير برامج الحماية للمعطيات الإلكترونية، أن هناك 556 مليون ضحية من الجرائم الإلكترونية كل عام، أو 18 ضحية في الثانية ،وقدرت أنه كان هناك 1.4 مليون ضحية جرائم الإنترنت كل يوم ،ووضعت الدراسة متوسط الخسارة لكل ضحية عند 197 دولارًا عند القياس عالميًا، لكنها أعلى في الولايات المتحدة، عند 290 دولارًا.

بالإضافة إلى ذلك، أظهرت النتائج أن تكلفة الجرائم الإلكترونية للمستهلكين في حدود 100 مليار دولار في السنة، على الرغم من أن هذا الرقم قد يكون منخفضًا لأن الكثير من الجرائم الإلكترونية لم يتم الإبلاغ عنها. [1]

وقد تفطنت الأجهزة التشريعية لهذه الأزمة، وعملت جاهدة على تطوير القاعدة الجزائية وفقا لما هو حاصل على أرض الواقع، ووجدت نفسها في تحد أمام صعوبة تشريع قاعدة قانونية تتناسب ومتطلبات التقنية الرقمية، وتحتويها.

من هنا كان واجبا الاستعانة بالمختصين في مجال التقنية المعلوماتية لتحسين جودة القاعدة الجزائية، وتحقيق أمن قانوني سيبراني، من شأنه الوصول إلى أعلى مستوى من الفعالية في مواجهة الجرائم المرتكبة على المستوى الرقمي.

هذا المستوى من الأمن القانوني سيتحقق وفقا للمختصين في المجال المعلوماتي عبر آلية وحيدة هي مزامنة أركان الجريمة والواقع الافتراضي، أي بمعنى آخر، أن تخصص القاعدة الجزائية بركنها المادي والمعنوي والمفترض بما يوفره المجال الرقمي من معطيات، تجعل كل فعل أو امتناع من شأنه إحداث نتائج غير مقبولة من ناحية السياسة الجزائية المنتهجة في الدولة، جريمة يعاقب عليها القانون.

وهذا هو محور البحث ضمن هذه الورقة البحثية التي تناولت الخصوصية المرصودة لسلوك المجرم المعلوماتي، وضرورة التصدي لها وفقا لطبيعة هذه الخصوصية، لا وفقا لما هو متعارف عليه من الأحكام التقليدية المادة الجزائية.

وتدور الإشكالية الرئيسية هنا حول سؤال رئيسي هو:

ماهي مقتضيات الخصوصية التي يتسم بها السلوك الإجرامي للمجرم المعلوماتي؟

ويتفرع عن هذه الإشكالية عدة أسئلة فرعية تتجسد في:

فيما تتمثل خصوصية محل السلوك الإجرامي الإلكتروني؟

وماهي صور الخصوصية التي يتسم بها البنيان المادي للسلوك الإجرامي الإلكتروني؟

سيتم الإجابة عن السؤال الرئيس والأسئلة الفرعية المطروحة بناء على تقسيم ثنائي، يتناول العنوان الأول طبيعة محل السلوك الإجرامي على المستوى الرقمي عبر تسليط الضوء على مفهومه، وخصائصه، فيما خصص العنوان الثاني لتوضيح صور الخصوصية التي تفرد بها السلوك الإجرامي الإلكتروني عن باقي السلوكات الإجرامية التقليدية، مع التطرقلمقتضاها في التشريع الجزائي الجزائري، عبر توظيف منهجين بصورة رئيسية، هما منهج تحليل المضمون، والمنهج الوصفي، وفقا للعرض الآتي:

1- According to: **The 2012 Norton Cybercrime Report**, for more details look: Joshua B. Hill, Nancy E.Marion, **Introduction to Cybercrime "computer Crimes, Laws, and Policing in the 21st Century**, PRAEGER, Santa Barbara, CA, 2016, p 13.

أولا: خصوصية محل السلوك الإجرامي المعلوماتي:

تم إنشاء الإنترنت ليكون مصدرًا مجانيًا ومفتوحًا، مع حد أدنى من الرقابة ،غرضهالأصليتبادل البيانات والرسائل بحرية بين عدد محدود من الباحثين ،ومع زيادة الوصول وتطورالإنترنت من أداة بحث إلى أداة أكثراستهلاكيًا واجتماعيًا، فتح توفر حرية الإنترنت وانفتاحه العديد من المزايا للمستخدمين وأيضًا للمجرمين، مثل سهولة الاستخدام والسرعةالوصول والبرامج منخفضة التكلفة، ولكن لهذه السهولة أيضًاعيوبها ،حيث أصبحت البيانات عرضة لمجموعة متنوعة منالهجمات الإلكترونية التي يمكن أن تسبب ضررًا كبيرًا للمستخدمين الخاصين والشركات والحكومات.

وقد أطلق خبراء المعلوماتية الإلكترونية على المجرم المعلوماتي اسم "الهاكر"، وهو الشخص الذي يخترق الحاسب الآلي ويجد متعة في الفحص والاستكشاف عن كثب النظام القابل للبرمجة، ويسعى إلى توسيع معارفه في هذا المجال إلى أقصى حد، وهو يختلف عن مصطلح "كراكر" الذي يطلق على الفئة التي لديها القدرة على الاختراق، وهناك من يعرفهم بمصطلح المحطمون الذي يكون هدفهم الأساسي هو إنشاء أدوات برمجية تسمح بالهجوم على أنظمة معلوماتية أو تحطيم نظم حماية نسخ البرمجيات المدفوعة الثمن. [2]

وتحديد مقتضى السلوك الإجرامي المعلوماتي يحتم علينا التطرق لخصوصية مجاله مقارنة بالسلوك الإجرامي في الجرائم التقليدية، أي محل الجريمة المعلوماتية، كسمة تميز السلوك الإجرامي المعلوماتي دون سواه، ومهما كانت طبيعته، نظرا لارتباط سعة النص التجريمي من عدمها بالمضامين المحمية جزائيا، ما يجعل حصر البيانات المحمية قانونيا عملا دقيقا، وتحديا يقع على عاتق التشريعات، التي ستجد نفسها مضطرة للعمل بالموازاة مع خبراء التقنية حتى لا يتركوا مجالا للغموض، الذي من شأنه ترك هامش للإفلات من المتابعة القانونية للمجرم المعلوماتي.

وفيما يلي سيتم التطرق لتعريف المعلومات محل الاعتداء، ومن ثم تحديد الطبيعة القانونية للهجوم السيبراني وصوره:

1- الطبيعة القانونية المعلومة للرقمية كمحل للاعتداء المعلوماتي:

غالبًا ما يستهدف المجرمون المعلوماتيون أجهزة الكمبيوتر للحصول على معلومات يمكنهم استخدامها لسرقة هوية شخص ما، أو سرقته ،أو الحصول على أموال ، أو الحصول على معلومات من الكمبيوتر تساعدهم في كسب المال على سبيل المثال، أ و قد يحاول المجرم الحصول على معلومات حول الأسهم قبل فتح السوق لتقديم عطاءات معينة من شأنهاتكون مفيدة من الناحية المالية، وهذا النوع من التصرفات غير قانوني بالطبع.

2 - غريبي بشرى، **خصوصية المجرم المعلومات ودوافعه**، مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الثاني، 2021، ص 103.

وعُرِّفت البيانات الرقمية المستهدفة من قبل المجرم المعلوماتي عدّة تعريفات من بينها أنها:" مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا لتبادل واتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل أو أشكال مختلفة".[3]

فيما عرف الأستاذ (CATALA) المعلومة بأنها: "رسالة معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير". [4]

وقد تم تضمين تعريف البيانات بمناسبة تعريف "العمل الأدبي" في قانون حق المؤلف الأمريكي لعام 1976 وتعديلاته، والذي تم التنصيص عليه في عام 1980،بأنها: "مجموعة من البيانات أو التعليمات يتم استخدامها بشكل **مباشر** أو **غير مباشر** في جهاز الكمبيوتر من أجل تحقيق شيء معين أو الوصول لنتيجة ".[5]

أما بالنسبة للمشرع الجزائري، فنجد أنه اهتم بحماية البيانات الرقمية محل الاعتداءات السيبرانية في عدة قوانين، بدءًا بقانون العقوبات [6]، الذي أضاف لأول مرة بموجب القانون 04/15 [7]، قسما خاصا بـ "المساس بأنظمة المعالجة الآلية"، يجرم فيه الاعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات ضمن المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات، غير أنه لم يورد تعريفا واضحا للمقصود بأنظمة معالجة المعطيات الآلية ضمن هذا القانون، مما يحيل إلى البحث عن مفهوم المعطيات الرقمية محل الحماية في قواعد أخرى.

من بين هذه القواعد، ما ورد ضمنالفقرة الأولى من المادة الثانية من القانون 09-04 [8]، بمناسبة تعريف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التي نصت: " **الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:** جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

---

3 - شيخة حسين الزهراني، **الطبيعة القانونية للهجوم السيبراني وخصائصه** ، مجلة جامعة الشارقة للعلوم القانونية ، المجلد 17، العدد الأول، يونيو 2020، ص 786.

4 - حمزة بن عقون، **السلوك الإجرامي للمجرم المعلوماتي**، بحث مكمل لنيل شهادة الماجيستير في العلوم القانونية تخصص: علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر باتنة، 2012، ص 132.

5 - Diane Rowland, Elizabeth Macdonald, **INFORMATION TECHNOLOGY LAW**, CavendishPublishingLimited, Second Edition,London, p 21.

6- الأمر رقم 66-156، المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديموقراطية الشعبية، العدد 48، المؤرخ في 10 يونيو 1966، ص 622.

7 - المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج ر، العدد 71، الصادر بتاريخ 10 نوفمبر 2004، ص 08.

8 - المؤرخ في 5 غشت 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، ج ر العدد 47، المؤرخ في 16 غشت 2006، ص 5.

فيما عرفت الفقرة الثانية المنظومة المعلوماتية بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

والمعطيات المعلوماتية المقصودة من طرف المشرع هي ما تم التنصيص عليه في الفقرة الثالثة من نفس المادة، والتي تنص بأنها: "كل عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

يتضح مما تم عرضه أعلاه من تعاريف خاصة بماهية البيانات المعلوماتية كمحل لارتكاب السلوك الإجرامي، أنه ولاعتبار الركن المادي قائما في الجريمة المعلوماتية، وجب أن يرتكب المجرم فعلا من الأفعال غير المشروعة على بيانات أو معلومات أو برامج، أي باستخدام نظام معالجة آلي، قصد الحصول على مزايا، أو إحداث ضرر غير مشروع.

وغياب هذه الوسيلة يخرج الفعل من صورة الجريمة المعلوماتية، إلى صور أخرى، أو قد يكون فعلا غير مجرم أصلا، وفي هذه المرحلة بالذات، تظهر أهمية تغطية مجال الحماية المبسوطة على بيانات مستخدمي المنظومة المعلوماتية، نظرا لارتباط قيام الجريمة من عدمها بمدى اتساع المجال المحمي من البيانات.

بناء على هذا حاولت المنظمة الأمم المتحدة استحداث تعريف جامع للجريمة الإلكترونية، في مؤتمرها العاشر لمنع الجريمة ومعاقبة المجرمين، موسعة من مجال تطبيقه عبر اعتبار البيانات المستهدفة، عبر اعتبار الجريمة الإلكترونية قائمة متى تم ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.[9]

هذه التعاريف، على اختلاف مضامينها تلخص البيانات المستهدفة إجراميا، والتي تعد محلا للجريمة الإلكترونية، بصفات وخصوصيات تتطلبها تطورات فقهية وقانونية، لتوافر الغطاء الحمائي الجزائي، أي بالمفهوم المغاير، إن عدم توافر بعض الخصوصيات في البيانات الإلكترونية المعتدى عليها سيخرجها من دائرة الحماية المقدمة عبر القاعدة الجزائية، ويمكن حصرها في العنوان الموالي:

2- خصوصية المعطيات المعلوماتية محل الحماية:

القواعد التقليدية، لا تسمح بناء على أحكامها م بإدخال البيانات الرقمية ضمن فئة معينة من الحقوق المادية والمعنوية المحمية في صورتها التقليدية، وهنا وجب استحداث قواعد جديدة تجعل من المواصفات الخاصة التي تنطبق على المعلومة الرقمية الخاصة واضحة ودقيقة، دائما لتحقيق مسعى الأمن القانوني للقاعدة الجزائية، وتحقيق فعاليتها في حماية الحقوق الرقمية والبيانات الإلكترونية للأشخاص الطبيعية والمعنوية.

9 - حمزة بن عقون، المرجع السابق، ص 16.

فمثلا، فيجريمة السرقة التي تتم بما يعرف بـ: "**هجوم الفدية**" على أحد البنوك، المهاجم لا يحتاج إلى مساعدة منالآخرين، فكل ما هو مطلوب هو اتصال الكمبيوتر والشبكة،والسارق الإلكتروني يخترق البنك ويشفر البيانات.

وهنا لا يمكن للبنك إدارة أعماله لأنه لا يمكنه الوصول إلى بياناته، بما في ذلكحسابات العملاء ،فيوسل اللص السيبراني رسالة إلى مدير البنك لإخباره أنه إذا كان البنكيريدون فك تشفير بياناتهم،يجب عليهم دفع فدية قدرها 100000 دولار من عملات البيتكوين (عملة رقمية لا يمكن تعقبهابواسطةتطبيق القانون).

فإذا رفض البنك الدفع، فستبقى البيانات مشفرة ،وعادةً ما يقوم السارق الإلكتروني بتعيين ملفالموعد النهائي للضغط على الضحية،ويمكن للبنك محاولة فك تشفير بياناته الخاصة عن طريق الاستعانة بخبراء أو معبمساعدة تطبيق القانون، ولكن قد لا يكون ذلك ممكنًا.

من هنا تتوضح الاختلافات بين السرقة التقليدية للبنك والهجوم الإلكتروني عليه، كما أنها توضح صعوبة الأمن السيبراني الذي يواجه المتخصصون في القطاع الحكومي والخاص عند التعامل مع الجرائم الإلكترونية.[10]

حيث وجد المشرعون على مستوى العالم صعوبة شديدة في تحديد ما يندرج ضمن البيانات المحمية قانونيا بصفة عامة، وجزائيا بصفة خاصة، وعلى الرغم من اختلاف تشريعات دول العالم في مجال تجريم الاعتداءات السيبرانية، فقد حدد الفقه بعض الخصائص التي في حال توفرها تجعل من البيانات المعلوماتية ذات أهمية تتطلب إدراجها كبيانات محمية، ويمكن حصر هذه الخصائص عبر الآتي:

- **أن تكون المعلومة مبتكرة ومحددة** : إن المعلومة التي تفتقر لصفة التحديد لا يمكن ان تكون معلومة حقيقة، فاذا كانتالمعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ والتبادل عن طريقعلامات أو إشارات مختارة فينبغي أن تكون محددة فالمعلومة المحددة هي التي يمكنحصرها في دائرة خاصة بها وتحديد جوانبها وهو ما يعد ضروريا في حالة الاعتداء علىالأموال؛ لأن هذا الاعتداء يجب أن يكون منصبا على شيء محدد وأن يكون هذا الشيءبدوره محلا لحق محدد.

كذلك يجب أن تنصب صفة الابتكار على الرسالة التي تحملهاالمعلومة فالمعلومة غير المبتكرة هي معلومة عامة متاحة للجميع ولا يمكن نسبتها إلىشخص محدد أو طائفة من الأشخاص.[11]

وهذا الوصف، سيخرج البيانات المشتركة التي تتوفر بشكل عام على العالم الافتراضي من دائرة البيانات المشمولة بدائرة الحماية، إذ تعد من قبيل المتعارف عليه طالما لم يتمسك شخص ما بملكيتها، وابتكاره لها، وإعمال هذه الخاصية يصعب من مهمة المشرع في صياغة النصوص التشريعية التي تحدد مجال الحماية المقترح، وإن كان المثال الذي يذكر في هذه الحالة هو التحديات الفقهية والقانونية التي تعرضت لها التشريعات

10 - Janine KremlingAmanda M. Sharp Parker,**Cyberspace, Cybersecurity, and Cybercrime**,SAGE Publication, United States of America, 2018,p 40.

(11) – شيخة حسين الزهراني، المرجع السابق، ص 791.

الجزائية حال ظهور ما يسمى بالحماية الجزائية للملكية الفكرية، حال مناقشة كيفية تقرير قواعد جزائية تحمي حقوقا غير مادية، لا سيما عند الاعتداء عليها بمختلف صور الجرائم التقليدية، كالسرقة، والتقليد، ...

وفي هذه الحالة، يزداد الأمر تعقيدا عندما يتعلق الأمر بصعوبة تتبع مسار البيانات الرقمية المعتدى عليها، وإثبات ملكيتها، وإيجاد المجرم الذي اعتدى عليها، وهل الفعل المرتكب يدخل ضمن قائمة الاعتداءات الإلكترونية المعترف بها أم لا، هذا بصفة عامة مثال عن التحدي الأول الذي يصطدم به المشرع في المادة الجزائية.

– **أن تكون البيانات الإلكترونية المعتدى عليها مملوكة للغير** : سواء كان هذا الغير شخصا طبيعيا، أو معنويا خاصا، أو عاما.

حيث تعد خاصية الاستئثار بالمعلومة أمرا ضروريا لأنه في مختلف الجرائم التي تنطوي على اعتداء قانوني على الأموال، فان الفاعل يعتدي على حق يخص الغير على سبيلا لاستئثار ويتوافر للمعلومة هذه الصفة إذا كان الوصول اليها غير مصرح به إلا لأشخاصمحددين. [12]

بناء على ما سبق، وبتوفر الركن الافتراضي للجريمة المعلوماتية، ألا وهو البيئة الرقمية، وانطباق وصف البيانات الرقمية المعتدى عليها والمحمية قانونا، تعمد الجهات المختصة، سواء خلال البحث والتحري والتحقيق الإلكتروني، أو خلال المحاكمة، إلى التأكد من توافر أركان الجريمة الإلكترونية، بدءًابركنها المادي، وفيما يلي إلقاء للضوء على أركان السلوك الإجرامي الإلكتروني، مع إعطاء صور للاعتداءات المجرمة وفقا للقانون الجزائري:

ثانيا: خصوصية صور السلوك الإجرامي الإلكتروني:

يكتسي الركن المادي أهمية بالغة، فلا وجود للجريمة دون وجوده، لأنه لن يكون ثمة اعتداء على الحقوق والمصالح التي يحميها القانون، فهو ضروري لحماية أمن الأفراد وحرياتهم، إذ يكفل ألا تحاكمهم السلطات العامة، إلا على ما يصدر عنهم من سلوك مادي محدد.[13]

وكما تتعدد صور السلوك المعتبرة كأفعال يجرمها القانون في أحكامه التقليدية، تتعدد الأفعال المندرجة كاعتداءات إلكترونية يعاقب عليها القانون، والسؤال الذي يطرح في هذا المقام، هو عن مدى خضوع السلوك الإجرامي الإلكتروني للأحكام العامة، وهل يتوجب خصه بقواعد تجريم خاصة بناء على بعض الاعتبارات التي يتميز بها؟

للإجابة عن هذا التساؤل، سيتم تحديد الشروط التي تتطلبها القوانين الجزائية لإدراج فعل ما ضمن السلوكات الإلكترونية المجرمة، وسيتم الحديث عن بعض الصور التجريمية التي نص عليها القانون الجزائي الجزائري،

12 - شيخة حسين الزهراني، المرجع السابق، ص 792.

13–أحمدفتحيسرور،**الوسيطفيشرحقانونالعقوبات،القسمالعام**،دارالنهضةالعربية،الطبعةالسادسة، القاهرة،1996 ،ص271.

وذلك عبر الآتي:

1- مظاهر خصوصية الأفعال الإلكترونية المجرمة:

تتعدد السلوكات الإجرامية الإلكترونية بتعدد أهدافها والغرض منها، وأحكامها العامة تستمد من القواعد التقليدية التي لا غنى عنها من أجل توصيف المقصود العام بالفعل، فالسلوك الإجرامي في جريمة السرقة التقليدية مثلا يتجسد في اختلاس شيء غير مملوك للفاعل، هو نفسه السلوك الإجرامي في جريمة السرقة الإلكترونية، فقط يكمن الاختلاف في محل الجريمة، الذي هو المال النقدي أو العيني في الأولى، والقيم النقدية الرقمية أو الأموال المعنوية الرقمية في الثانية، ووسيلة ارتكابها، وهي الحواسيب، أو الوسائل الإلكترونية التي تخدم أهدافه الإجرامية.

وكما تم التقديم أعلاه، قد يستفيد الجناة من الفراغ التشريعي أو عدم الدقة التي قد تشوب النصوص الجزائية، نتيجة عدم شموليتها واحتوائها لصور تقنية لم يكن المشرع لينتبه لها دون وجود مختصين في المجال، يساعدون في ضبط المفاهيم وتدقيقها.

وقد اختلفت تشريعات العالم الجزائية في تحديد صور السلوك الإجرامي الإلكتروني، فمنها ما تبنى **التوجه العام**، الذي **يوسع من دائرة التجريم** عبر توظيف مصطلحات شاملة، تصب أهدافها أساسا إما لغرض **قرصنة البيانات الرقمية**، أو **إتلافها**، أو **التجسس** على أصحابها، حصرت فيه الاعتداءات في فئات، قسمت تشريعيا وفقهيا بناءً على معايير محددة، فمنها ما اعتبرت اعتداءات مالية، وأخرى على الحياة الشخصية، وأخرى إرهابية، ...

وأغلب الانتقادات التي وجهت لهذه الطريقة من التجريم، هو الصورة العكسية التي حققتها، بسبب تعارضها ومبدأ الشرعية القانونية المتطلب في المادةالجزائية.

في حين ركزت بعض التشريعات على **أهم صور الاعتداءات** التي تقع عبر استعمال التقنية الرقمية، وعرضت تشريعاتها الجزائية لحاجة دائمة للتحيين والتعديل كلما استجدت صور تجريم جديدة تحتاج التغطية القانونية الاستعجالية.

وعموما، فإن كل سلوك إجرامي إلكتروني، سيتحقق **قانونا بارتكاب فعل يجرمه القانون** ، أو **بالامتناععن الإتيان بفعل يأمر به القانون**، يسبب**ضررا للضحية**، وترتبط بين الفعل ونتيجته (الضرر) **علاقة سببية**.

وبغض النظر عن التصنيفات، يمكن حصر طبيعة السلوكات الإجرامية الإلكترونية الأكثر شيوعا وفقا لمختصي التقنية، وبناء على طرق ارتكابها إلى:

- الإصابة بالبرامج الضارة:

يعتبر فيروس الحاسب بمثابة برامج مهاجمة تصيبأنظمة الحاسبات بأسلوب يماثل لحد كبيرأسلوب الفيروساتالحيوية التي تصيب الإنسان، ويمكن تعريفه بأنه برنامجحاسوب يمكنهبصفة مستمرة أو في أي تاريخ أو

زمنمبرمج أن يدخل نسخاً قابلة للتنفيذ من نفسه أو منأجزاء منذاته إلى برامج أخرى أو إليهما معاً، فيصيبهما بالعدوبوتكون البرامج المصابةبالعدوى قابلة للتكاثر، أو تعديل أوحذف أو تلوث أو تلف البرامج أو البيانات الأخرى. (14)

وقد بلغ هذا النوع من الاعتداءات وفق تقرير نورتن لسنة 2012، نسبة 67% من مجموع الهجمات الإلكترونية التي وقعتسنة 2010. (15)

ويتمثل السلوك الإجرامي في هذا النوع في الإرسال العمدي، عن علم وإرادة واضحة للبرنامج الضار، عبر الوسائط الإلكترونية بأنواعها لجهاز أو أجهزة الضحيةالإلكترونية، قصد إحداث ضرر مادي أو معنوي له.

وتستهدف هذه البرامج شغل أكبر نطاق ممكن من سعةالشبكة مما يؤدي إلى التقليل أو الخفض من قدرتها، وقد تتجاوزذلك في بعض الأحيان وتقوم بأعمال تخريب حقيقية للملفاتوالبرامج وأنظمة تشغيل الحاسب ووسائل الاتصال الخاصة به. (16)

- الروبوتات / الزومبي:

في هجوم بسيط ولكنه مدمر، يقوم المجرم المعلوماتي بتجميع قائمة تضم 61 تركيبة من أسماء المستخدمين/كلمات المرور، ويكتب برنامجًا يبحث في شبكة الإنترنت عن منتجات تستخدمها ، وبمجرد الوصول إليها، يُثَبِّت البرنامج نفسه فورًا ويفحص الجهاز، بطريقة خادعة، بحثًا عن برامج خبيثة أخرى معروفة ويمحوها حتى يكون المخترِق الوحيد ، ثم يربط البرنامج الخبيث، الذي أُطلق عليه "ميراي" Mirai، الملايين من هذه الأجهزة المخترَقة معًا في شبكة روبوت –وهي عبارة عنشبكة من أجهزة الكمبيوتر التي تم اختراقها، وعندما تهاجم أعداد ضخمة من هذه الأجهزة " **الزومبي**"، مثل أجهزة مراقبة الأطفال والطابعات والكاميرات، ضحيتها في آنٍ واحد، يصبح الموقع المستهدف مشغولًا ومثقلًا، وبالتالي يتعذر الوصول إليه، ما لم يكن يستخدم وسائل حماية باهظة التكلفة.(17)

ويتألف السلوك الإجرامي في مثل هذا الاعتداء من مجموعة من الأفعال المنظمة، حيث يتجسد السلوك الأول في اختراق كل الأجهزة الإلكترونية الموجودة في حيز مكاني أو جغرافي، أو لشخص معين، مع قرصنة كلمات السر، ومن ثم بناء الروبوت عبر تجميع كل هذه الوسائط، قصد الحصول على أكبر قدر ممكن من المعلومات،

14 - نائل علي المساعدة، **أركان الفعل الضار الإلكتروني في النظام الأردني**، مجلة دراسات، المجلد 32، العدد الأول، 2005، ص 60.

15 - Joshua B. Hill, Nancy E. Marion, op. cit, p12.

16 - نائل علي المساعدة، المرجع السابق، ص 61.

17 - لمزيد من التفصيل، أنظر: **هجوم الزومبي الإلكتروني**، مقال بقلم زينب توفيشكي، بتاريخ 18 أوت 2019، متوفر على موقع Scientific American، على الرابط:

https://www.scientificamerican.com/arabic/articles/from-the-magazine/attack-of-the-zombie-baby-monitors/ أطلع عليه بتاريخ: 20 أوت 2022، على الساعة 22.34

أو الصور، أو الأصوات، ...بهدف الإضرار بالضحية أو الضحايا مهما كانت طبيعتهم، ومهما كانت طبيعة الضرر.

- الاحتيال المصرفي الإلكتروني:

شهدت العمليات المصرفية تطورا ملحوظا خاصة بعد ظهور شبكة الانترنيت والتجارة الالكترونية والتي مكنت العملاء من إجراء معاملاتهم المصرفية من خلال مواقع تلك البنوك على شبكة الانترنيت باستخدام كلمة مرور خاصة، وهو ما سمح بتفشي الاحتيال وذلك باستخدام الآتي:

- بطاقات الائتمان والتي تسمح بسحب النقود سواء من صاحبها أو من شخص آخر أو تزويرها.
- التحويل غير المشروع للأموال.
- الاحتيال عن طريق آلات الصراف الآلي.[18]

ويتلخص سلوك المحتال الإلكتروني الإجرامي في استعمال عدة طرق منها ما يتم عبر قرصنة بيانات الوكيل البنكي، أو بيانات بطاقة الزبون الائتمانية، أو عبر تزوير الروابط والنوافذ الإلكترونية الخاصة بالبنوك الرقمية، ...وذلك لإيهام الزبون أو البنك أنه بصدد القيام بعملياته المصرفية بصورة عادية، في حين هو سيخسر أمواله.

- هجوم قطع الخدمة:

هجمات الحرمان من الخدمات أو هجوم حجب الخدمة (بالإنجليزية: Denial of ServiceAttacks) هي هجمات تتم عن طريق إغراق المواقع بسيل من البيانات غير اللازمة يتم إرسالها عن طريق أجهزة مصابة ببرامج (في هذه الحالة تسمى DDOS Attacks).

تعمل نشر هذه الهجمات بحيث يتحكم فيها القراصنة والعابثين الإلكترونيين لمهاجمة الشبكة (الإنترنت) عن بعد بإرسال تلك البيانات إلى المواقع بشكل كثيف مما يسبب بطء الخدمات أو زحاماً مرورياً بهذه المواقع ويسبب صعوبة وصول المستخدمين لها نظراً لهذا الاكتظاظ، ...، وعلى هذا الأساس فإن هذا النوع من الهجمات يُدعى في بعض الأوساط «بإيدز الإنترنت».

ويتم هذا الهجوم بدون كسر ملفات كلمات السر أو سرقة البيانات السرية، حيث أن هجمات حجب الخدمة تتم ببساطه بان يقوم المهاجم بإطلاق أحد البرامج التي تزحم المرور للموقع الخاص بك وبالتالي تمنع أي مستخدم آخر من الوصول إليه.[19]

18 - رفيق يوسفي، حنان دريد، **دور حوكمة البنوك الإلكترونية في حماية العميل الإلكتروني من الاحتيال المصرفي** ، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، المركز الجامعي عبد الحفيظ بوالصوف ميلة، المنعقد يومي 23 و 24 أفريل 2018، ص 06.

إذا فالسلوك الإجرامي الإلكتروني ضمن هذه الصورة من صور الجرائم الإلكترونية، يتجسد في زرع عوائق إلكترونية لحرمان الجمهور من خدمة الإنترنت.

- تشويه الموقع:

هو هجوم تخترق فيه الأطراف الخبيثة موقع ويب وتستبدل المحتوى الموجود على الموقع برسائلها الخاصة، حيث يمكن أن تنقل الرسائل رسالة سياسية أو دينية أو لغة بذيئة أو أي محتوى آخر غير لائق أو إشعارًا بأن الموقع قد تم اختراقه من قبل مجموعة قراصنة معينة، كما تقوم معظم مواقع الويب وتطبيقات الويب بتخزين البيانات في ملفات البيئة أو التكوين، مما يؤثر على المحتوى المعروض على موقع الويب، أو يحدد مكان وجود القوالب ومحتوى الصفحة، حيث قد تعني التغييرات غير المتوقعة على هذه الملفات اختراقًا أمنيًا وقد تشير إلى هجوم تشويه.[20]

وهذا النوع من السلوك يكثر لدى التنظيمات بمختلف أهدافها، كمنظمة أنونيموس التي تعد من أكثر الجهات ارتكابا لمثل هذه الصورة من الجرائم، آخرها الهجومات المتتابعة على المواقع الرسمية، والإعلامية الروسية، كرد فعل عن مناهضة جزء من أفراد هذه المنظمة لسياسة روسيا تجاه الحرب الأوكرانية.

كماوقد عدّد المختصون في مجال التقنية صورا أخرى للسلوك الإجرامي الإلكتروني، يصعب حصرها في هذا المقام، من بينها:

- إساءة استخدام الوصول إلى الإنترنت أو البريد الإلكتروني من الداخل، على سبيل المثال، المواد الإباحية أو البرامج المقرصنة).
- الوصول غير المصرح به أو امتيازالتصعيد من الداخل.
- اختراق النظام من قبل الخارج.
- السرقة أو الوصول غير المصرح به إلىمعلومات التعريف الشخصية بسببسرقة/فقدانالجهاز المحمول.
- السرقة أو الوصول غير المصرح به إلىالملكية الفكرية بسبب الجهاز المحمول (السرقة/الخسارة).

---

19 - **هجمات الحرمان من الخدمات**، ويكيبيديا الموسوعة الحرة، متوفر على الرابط:
https://ar.wikipedia.org/wiki/%D9%87%D8%AC%D9%85%D8%A7%D8%AA_%D8%A7%D9%84%D8%AD%D8%B1%D9%85%D8%A7%D9%86_%D9%85%D9%86_%D8%A7%D9%84%D8%AE%D8%AF%D9%85%D8%A7%D8%AA
أطلع عليه يوم: 21 أوت 2022 على الساعة: 14.10

20- - آية العضيبات، **ما هو هجوم تشويه موقع الإنترنت**، مقال منشور على موقع "إي عربي E Arabi"، متوفر على الرابط:
https://e3arabi.com/technology/%D9%85%D8%A7-%D9%87%D9%88-%D8%AA%D8%B4%D9%88%D9%8A%D9%87-%D9%85%D9%88%D9%82%D8%B9-%D8%A7%D9%84%D9%88%D9%8A%D8%A8-website-defacement-attack/
أطلع عليه بتاريخ: 21 أوت 2022، على الساعة: 16.54.

مما سبق، يتضح أن تعداد صور السلوك الإجرامي الإلكتروني يعد عملا معقدا، يحتاج في الإحاطة به تكاثف الجهود التشريعية، والخبرة التقنية، والقطاعات المختلفة، والجمهور، والدول على الصعيد الدولي، نظرا لكونه خطرا يمس كل جوانب الحياة.

وقد حاول المشرع الجزائري تغطية مختلف صور الاعتداءات الإلكترونية بالتنصيص على جرائم الاعتداء على المعطيات الرقمية ضمن قانون العقوبات، كما فرضت التطورات في هذا المجال إجراء تعديلات متتالية، وإضافة أحكام جديدة سيتم التطرق إليها عبر الآتي:

2 –التوصيف القانوني للسلوك الإجرامي الإلكتروني في نظر المشرع الجزائري:

إن المصالح المتعلقة بمعطيات الحاسب الآلي تتمثل أساسا في سرية هذه المعطيات وفي سلامتها (أوتكاملها) وفي وفرتها،ورغبة من المشرع الجزائري فيحما يق هذه المصالح فقد استحدث ثلاث جرائم تمس أساسا بها، فقامبتجريم**مجرد الدخول أو البقاء غير المصرح بهما في أنظمة المعالجةالآليةللمعطيات**(حمايق مصلحة السريق)، وشدد العقوبة إذا أدى ذلك إلى **تخريبالنظام**(حمايقمصلحة الوفرة والإتاحة)، أو **تعديل أو إزالة المعطيات التي يتضمنها**(حمايق مصلحة السلامة والتكامل)،وحمايق لسلامة المعطيات وتكاملهافقد قام المشرع بتجريم**التلاعب بها** وذلك **بإدخال معطيات جديدةعليها غيرمصرح** بإدخالها أو **بتعديل أو إزالة غ ير مصرح** بها لمعطيات موجودة داخل نظامالمعالجة الآليق للمعطيات، أي قام بتجريم كل ما يؤدي إلى تغيير حالة المعطياتبغير تصريح. [21]

وفيما يلي، ملخص لأهم الأفعال التي أدرجها المشرع الجزائري ضمن قائمة الجرائم المعلوماتية:

– الدخول أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات:

اعتبر المشرع الجزائري ضمن نص المادة 394 مكرر، كل دخول أو بقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات جريمة يعاقب عليها بالحبس من ثلاثة أشهر إلى سنة، وبالغرامة من 50.000 دج إلى 200.000 دج.

وهذه الصورة من التجريم، تغطي السلوك الإجرامي الذي يتم إما بالدخول المشروع، كالذي يتم من موظف البنك أو المؤسسة المالية، قصد تسيير معاملات مالية للزبون، ومن ثم القيام بتحويل القيم المالية، أو البيانات الرقمية الخاصة دون إذن من صاحبها.

كما تغطي الدخول غير المشروع الذي يتم بقرصنة كلمات السر، أو إرسال نوافذ مزيفة للحصول على بيانات الضحية أو قيم مالية بشكل غير مشروع.

21 - محمد خليفة، **دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطياتفي قانون العقوبات الجزائري** ، المجلة النقدية للقانون والعلوم السياسية، المجلد 13، العدد الأول، جوان 2018، ص 61.

ونص المادة غطى ضمن هذه الجريمة أيضا كل بقاء غير مشروع تم في سبيل تحصيل فوائد غير مشروعة، سواء قصد التجسس أو قصد الاستحواذ على بيانات معينة، ...

فالمشرع الجزائري –من خلال استقراء الأفعال التي يمكن أن تندرج ضمن نص المادة– حذا حذو الاتجاه الموسع، الذي يوظف مصطلحات واسعة تحتوي عدة سلوكات إجرامية معلوماتية.

– التلاعب غير المشروع بالمعطياتأو الغش والإتلاف المعلوماتي:

ورد هذا النوع من السلوك الإجرامي الإلكتروني ضمن نص المادة 394 مكرر 1 من قانون العقوبات، وهو كل إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

وباللغة الرقمية، يمكن أن تندرج ضمن هذه المادة كل أعمال القرصنة، و تعني تمكن الفاعل من البرامجوالبيانات الإلكترونية والحصول عليها دون إرادة مالكها ، ولا يدخلفي نطاق القرصنة الإلكترونية استيلاء الفاعلعلى المكونات المادية المستخدمة في الحاسب والتيقدتحتوي على تلك البرامج والبيانات كاستيلائه على الأقراصالمدمجة مثلاً أو الأشرطة أو الأقراص اللينة فلا يكاد ذلكيخرج عن اعتباره غصباً في مجال الفعل الضار العادي الذييقع على الأشياء المادية.[22]

خاتمة:

السلوك الإجرامي المعلوماتي كفعل أو امتناع غير مشروع، يتم عبر استخدام التقنية المعلوماتية، يتطلب لتفريده بأحكام مجرمة التزاما بخصوصية مجاله، وصوره التي يرتكب بها.

ويقتضي واجب توفير حماية نوعية للبيانات الرقمية للمواطنين والدولة على حد سواء، توفير قواعد قانونية نوعية تتناسب والخصوصية الجرائم الإلكترونية.

وقد اتضح عبر هذه الورقة البحثية أن التحديد الدقيق للبيانات الرقمية المحمية بواسطة القاعدة الجزائية، نظرا لكمها الهائل الذي يتدفق عبر الشبكة العنكبوتية كل ثانية، وقد استحدثت بعض المعايير الفقهية لتحقيق هذه الغاية، كضرورة كونها مبتكرة وحديثة، ويستأثر بها صاحبها، أي يمتلكها دون غيره، وبهذه الطريقة ستستبعد بقية البيانات التي قد لا تندرج وفقا للمعايير المذكورة ضمن الفئات المحمية.

حيث أقرت العديد من الحكومات قوانين تحظر الجرائم الإلكترونية، لكنالعديد من هذه القوانين لا تعد محاولات جادة لتعريف الجرائم الإلكترونية، أوتحديد العقوبة على السلوكات الإجرامية الإلكترونية المرتكبة ضمنها، إذ أنخمس بلدان العالم فقط لديها قوانين تعالج الأشكال الجديدة من الجرائم الإلكترونية ،فعند فحص قوانين الأربعة

22 - نائل علي المساعدة، المرجع السابق، ص 60.

أخماسٍ الأخرى، نجد أن الجرائم الإلكترونية المذكورة في قوانينها قد عفا عنها الزمن أو أنها لا تصلح للتطبيق لوقت طويل.

وقد اتضحت شدة التباين بين التشريعات ذات التوجهات الجديدة مع القوانين القائمة، أين قد يكون الفعل غير قانوني في بلد ما ولكنه قانوني في مكان آخر، مما يسمح بذلك للمجرمين بالانتقال من مكان إلى آخر، بلا عقاب على أفعالهم.

ونظرًا لأن العديد من القوانين التي تحكم الجرائم الإلكترونية تستند إلى الولايةالقضائية، فإنها تنطبقفقط في البلد الذي تم فيه تمرير القانون.

وهكذا، عندما ترتكب الجريمة السيبرانية، فمن الممكن أن ينطبق عيها العديد من القوانين، وقد لا ينطبق عليها أي قانون، لأن هذه القوانين غير فعالة أو غير موجودة، مماييسهل على المجرمينالتهرب من تطبيق القانون.

بناء عليه، تتضح صعوبة التحدي الذي يواجه القاعدةالتشريعية الجزائية في تفريد الجرائم الإلكترونية بحسب السلوك الإجرامي المرتكب، وضبط أحكامها وتقرير الجزاءات المناسبة لكل فعل بحسب الخطورة الإجرامية للجريمة والمجرم المعلوماتيين.

وساعد في صعوبة المهمة، غياب الإرادة التشريعية الحقيقية، والقوانين الردعية الدقيقة، ما يجعل المتابعات الجزائية للجناة تقع دون جدوى، وتبقى بيانات الضحايا الرقمية بمختلف فئاتها عرضة للاعتداءات، في وقت يعلم المجرم الإلكتروني أين يقع الخلل التشريعي، وكيف سيفلت من العقاب.

ويوصى لتجنب مثل هذه الحالات، ضرورة استعانة المشرع بالمختصين في مجال التقنية، وذلك لضمان تغطية تشريعية مناسبة لكل الاعتداءات الإلكترونية التي يمكن أن ترتكب.

كما يقترح في سبيل حماية المعطيات الرقمية أن توحد الجهود التشريعية على مستوى دول العالم، خاصة تلك المتقدمة في استحداث منظومات تشريعية متطورة في هذا المجال.

وأخيرا، يمكن التأكيد على أن القاعدة الجزائية في شكلها التقليدي لم تعد تتناسب والتطورات التكنولوجية الحاصلة، وتحتاج –مع الحفاظ على المبادئ العامة– إلى تحيين دائم حتى لا يفلت الجناة بجرائمهم، وتحقق هدفها التشريعي الذي صيغت من أجله.

قائمة المصادر والمراجع:

I -باللغة العربية:

1 -النصوص التشريعية:

– الأمر رقم 66–156، المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديموقراطية الشعبية، العدد 48، المؤرخ في 10 يونيو 1966، ص 622.

- القانون 04/15، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج ر، العدد 71، الصادر بتاريخ 10 نوفمبر 2004، ص 08.
- القانون رقم 09-04، المؤرخ في 5 غشت 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، ج ر العدد 47، المؤرخ في 16 غشت 2006، ص 5.

2 -الكتب:

- أحمد فتحي سرور، **الوسيط في شرح قانون العقوبات ، القسم العام**، دار النهضة العربية، الطبعة السادسة، القاهرة، 1996.

3 -المجلات والدوريات:

- غريبي بشرى، **خصوصية المجرم المعلومات ودوافعه** ، مجلة نوميروس الأكاديمية ، المجلد الثاني، العدد الثاني، 2021، (ص ص 101-115).
- شيخة حسين الزهراني، **الطبيعة القانونية للهجوم السيبراني وخصائصه** ، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد الأول، يونيو 2020، (ص ص 773-799).
- نائل علي المساعدة، **أركان الفعل الضار الإلكتروني في النظام الأردني** ، مجلة دراسات، المجلد 32، العدد الأول، 2005، (ص ص 55-65).
- محمد خليفة، **دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري**، المجلة النقدية للقانون والعلوم السياسية، المجلد 13، العدد الأول، جوان 2018، (ص ص 60-84).

4 -الملتقيات العلمية:

- رفيق يوسفي، حنان دريد، **دور حوكمة البنوك الإلكترونية في حماية العميل الإلكتروني من الاحتيال المصرفي**، الملتقى الوطني الثالث حول المسْتهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، المركز الجامعي عبد الحفيظ بوالصوف ميلة، المنعقد يومي 23 و24 أفريل 2018.

5 -المذكرات:

- حمزة بن عقون، **السلوك الإجرامي للمجرم المعلوماتي** ، بحث مكمل لنيل شهادة الماجيستير في العلوم القانونية تخصص: علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر باتنة، 2012.

6- المواقع الإلكترونية:

- هجوم الزومبي الإلكتروني، مقال بقلم زينب توفيشكي، بتاريخ 18 أوت 2019، متوفر على موقع Scientific American، على الرابط:

https://www.scientificamerican.com/arabic/articles/from-themagazine/attack-of-the-zombie-baby-monitors

– هجمات الحرمان من الخدمات، ويكيبيديا الموسوعة الحرة، متوفر على الرابط:
https://ar.wikipedia.org/wiki/%D9%87%D8%AC%D9%85%D8%A7%D8%AA_%D8%A7%D9%84%D8%AD%D8%B1%D9%85%D8%A7%D9%86_%D9%85%D9%86_%D8%A7%D9%84%D8%AE%D8%AF%D9%85%D8%A7%D8%AA

– آية العضيبات، ما هو هجوم تشويه موقع الإنترنت، مقال منشور على موقع إي عربي E Arabi، متوفر على الرابط:
https://e3arabi.com/technology/%D9%85%D8%A7-%D9%87%D9%88-%D8%AA%D8%B4%D9%88%D9%8A%D9%87-%D9%85%D9%88%D9%82%D8%B9-%D8%A7%D9%84%D9%88%D9%8A%D8%A8-website-defacement-attack/

II - باللغات الأجنبية:

1 – الكتب:

− Janine KremlingAmanda M. Sharp Parker,**Cyberspace, Cyber security, and Cybercrime**,SAGE Publication, United States of America, 2018.

− Diane Rowland, Elizabeth Macdonald, **INFORMATION TECHNOLOGY LAW**, CavendishPublishingLimited, Second Edition,London.

− Joshua B. Hill, Nancy E. Marion, **Introduction to Cybercrime "computer Crimes, Laws, and Policing in the 21st Century**, PRAEGER editions, Santa Barbara, CA, 2016.

بوشارب هانية
boucharebhania@yahoo.com
جامعة غرداية

شبوعات موسى
moussa.chebouat@gmail.com
جامعة غرداية

المجرم المعلوماتي

ملخص:

أثبتت الدراسات أن لا تعد خصوصية الجريمة المعلوماتية هي السمة الوحيدة التي تميزها عن غيرها من الجرائم التقليدية، بل تستمد هذه الجريمة تميزها وخصوصيتها أيضا من شخصية مرتكبيها الذي يطلق عليهم وصف "المجرم المعلوماتي" والذي يتميز عن بقية المجرمين من حيث المواصفات والتصنيف والدوافع وحتى الأساليب والتقنيات التي يلجأ إليها لتنفيذ مخططاته الإجرامية في البيئة الرقمية.

الكلمات المفتاحية: المجرم المعلوماتي؛ الجريمة المعلوماتية؛ دوافع المجرم المعلوماتي.

Abstract:

Studies have proven that the privacy of information crime is not the only feature that distinguishes it from other traditional crimes , Rather this crime also derives its distinction from the personality of its perpetrators, who are called “information criminals” ,Which is distinguished from the rest of the criminals in terms of specifications, classification, motives and even the methods and techniques he uses to implement his criminal plans in the digital environment.

sdrowyeK : *cybercriminal, cybercrime, motives of the cybercriminal*

المقدمة

ظهور شبكة الأنترنت والتطور التكنولوجي الحاصل في عصرنا الحالي أضاف الكثير من الجوانب الإيجابية إلى حياتنا، إلا أنه في المقابل أدى إلى ظهور أشكال جديدة ومستحدثة من الجرائم وأصبح ت الهيئة الالكترونية مسرحا وأرضية خصبة لها وجلبت معها نسلا جديدا من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية، وهذا النوع من الجرائم المستحدثة لا تتطلب من مرتكبها مقدارا من العنف للقيام بها ، فبمجرد كبسة زر على لوحة مفاتيح الكمبيوتر يمكن تجاوز كل الحواجز الالكترونية ومن على مسافات تتعدى عشرات الآلاف من الأميال، وتحقيق الأهداف بهدوء وبدون أي عناء ودون أن يترك أي أثرا ملموسا لملاحقة مرتكبيها ، بناء على ما سبق لنا ذكره نطرح الإشكالية التالية:

فيما تتمثل خصوصية المجرم المعلوماتي؟

تهدف المداخلة في كونها تسعى إلى محاولة التطرق الى:

- محاولة تسليط الضوء على نوع خاص من المجرمين نتاج ظاهرة إجرامية مستحدثة عرفت بإسم الجريمة المعلوماتية؛

- استشهاد ببعض من الوقائع العملية للمجرميين المعلوماتيين لكي حتى أن لا يكون الكلام جازفا وقد يفقد أهميته ان لم يتم التدليل عليه بوقائع عملية.

وإرتأينا أن تكون مداخلتنا وفق المنهج الوصفي بتطرق لخصوصية المجرم المعلوماتي ودوافعه بداية من تحديد المقصود بالمجرم المعلوماتي وذكر أهم تصنيفاته وسماته، ومن ثم إبراز أهم الدوافع التي تؤدي به إلى ارتكاب الفعل الإجرامي.

وللإجابة على الإشكالية المطروحة تم تقسيم المداخلة إلى مبحثين، نتطرق إلى مفهوم المجرم المعلوماتي في (مبحث أول)، أم (مبحث ثان) فقد خصصناه إلى سمات ودوافع المجرم المعلوماتي.

المبحث الأول

مفهوم المجرم المعلوماتي

المجرم المعلوماتي هو المجرم الذي سلك سبيل التقنية لارتكاب جرائمه، وفي هذا المبحث سيتم التعرف عليه من خلال التطرق الى تعريفه في(المطلب الأول)، ومن ثم التطرق الى أهم تصنيفاته في (المطلب الثاني).

المطلب الأول: تعريف المجرم المعلوماتي

ففي الاصطلاح القانوني يطلق فقهاء القانون الجنائي عليه مصطلح " المجرم المعلوماتي" وهو الشخص الذي لديه مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسب الالي الالكتروني والقادر على استخدام هذا التكتيك لاختراق الكود السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه.[1]

أما في الاصطلاح الالكتروني فأطلق عليه خبراء من المعلوماتية الالكترونية اسم "الهاكر" [2]، هو الشخص الذي يخترق الحاسب الآلي ويجد متعة في فحص واستكشاف عن كثب نظام قابل للبرمجة ويسعى إلى توسيع معارفه في هذا المجال إلى أقصى حد، وهو يختلف عن مصطلح" كراكر" الذي يطلق على الفئة التي لديها

---

[1] –مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2008 ، ص143 .

[2]– ويعود الفضل في تسمية الهكترة إلى كاتب الخيال العلمي الامريكي وليم جيسون عام 1984 ويمكن القول أنه استدعى المرور بأربعة أجيال لكي يصل مصطلح مجرم الأنترنت إلى ما هو عليه الآن من حيث الإجرام فقد تشكل الجيل الأول لمصطلح الهاكر في فترة الستينات من القرن العشرين ليتم إطلاقه على المبرمجين المبدعين من طلبة الحاسوب والاتصالات وبصفة خاصة طلاب معهد ماساشوستس للتكنولوجيا و.م.أ.

ثم امتد ليطلق على مطوري علوم الحاسوب وتقنية الاتصالات وقد مثل هؤلاء الجيل الثاني للهكرة، في السبعينيات.

أما الجيل الثالث فقد ظهر في الثمانينيات وأطلق هذا المصطلح على مخترقي الألعاب الإلكترونية وحقوق النسخ عبر الخدمات الشبكة الكمبيوترية ويسمى هذا الجيل بجيل الحاسوب الشخصي (pc).

ثم تطور أخيرا إلى ما هو عليه الآن ليستقر عند المجرمين والتافهين وهم العناصر البشرية للجيل الرابع ، وللمزيد من التفصيل، ينظر: بكوش محمد أمين، هروال نبيلة هبة، خصوصية المجرم الالكتروني –مجرم الأنترنت نموذجا–، مجلة البحوث في الحقوق والعلوم السياسية، المجلد07، العدد01 ،2021 ، ص77.

القدرة على الاختراق وهناك من يعرفهم بمصطلح المحطمون الذي يكون هدفهم الأساسي هو إنشاء أدوات برمجية تسمح بالهجوم على أنظمة معلوماتية أو تحطيم نظم حماية نسخ البرمجيات المدفوعة الثمن[3].

وعلى ذلك فالمجرم الإلكتروني الرقمي هو الذي لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية, وذلك بأداء فعل أو الامتناع عنه مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محليا أو دوليا.[4]

المطلب الثاني: تصنيف المجرم المعلوماتي

هناك العديد من الدراسات التي قامت بوضع تصنيف لمرتكبي الجرائم المعلوماتية، فمن بين أفضل التصنيفات هي التي أورده ا الأستاذ Donn B Parker الذي ذهب الى تصنيف المجرم المعلوماتي الى سبعة طوائف مختلفة، وأيضا تصنيف كل من الأستاذيين David Icovr Karl Seger و William Vonstarch في مؤلفهم جرائم الكومبيوتر الصادر عام 1995 .

الفرع الأول: دراسة الأستاذ (Donn B Parker)

أنقسمت الدراسة الى سبعة أنماط والمتمثلة في مايلي :

أولا: المازحون Prankesters

يقصد بهذه الطائفة الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية[5]، أو كما يسميهم البعض صغار نوابغ المعلوماتية.

تظل الخطورة الاجرامية التي تشكلها هذه الفئة محدودة جدا، وذلك لأنه نادرا ما يترتب على أفعالها أضرار جسيمة ضف إلى ذلك توافر حسن النية في تصرفاتهم التي يعتقدون بأنها غير معاقب عليها قانونا[6].

ولكن في الواقع فإنه يجب عدم التقليل من خطورة هؤلاء الأشخاص، فهذه ال فئة قد تتعدى مرحلة الهواية والعبث لتدخل مرحلة متقدمة أكثر في مجال ارتكاب الجرائم المعلوماتية وهي مرحلة الاحتراف لهذه الجرائم، كما أن هناك مخاوف تتمثل في احتضان منظمات الجريمة المنظمة لهذه الفئة للاستفادة من مهاراتهم وتطويرها من أجل تحقيق مآربهم وغاياتهم الإجرامية من خلال التقنيات الرقمية[7]، وكمثال على ذلك المراهق الكندي الذي

---

[3] –غريبي بشرى، خصوصية المجرم المعلوماتي ودوافعه، مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الثاني ، 2021، ص103.

[4] – خليلي سهام، خصوصية المجرم الالكتروني، مجلة المفكر، العدد 15 ، جوان 2017 ،ص405.

[5] –حنان مسكين، واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر، المجلة الأكاديمية للبحوث القانونية والسياسية ، المجلد الرابع، العدد الاول، 2020 ، ص615.

[6]– لحرش أيوب التومي، النحوي سليمان، طبيعة الخطورة الاجرامية للمجرم المعلوماتي ، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 05 ،العدد01 ،2020، ص988.

[7]– نهلا عبدالقادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008 ،ص 82.

تسبب في احداث حالة من الفوضى الشديدة على شبكة عندما انهال عليها هذا المراهق بالالاف من الرسائل المزعجة وقدرت الخسائر المادية بملايين الدولارات.[8]

وأيضا من أشهر الجرائم التي ارتكبت في الولايات المتحدة الأمريكية جريمة شاب مراهق عمره سبعة عشر عاما يدعى " دينيس موران " وهذه القضية تحولت إلى قضية رأي عام لاختلافها عن الجرائم الاخرى فيما كبدته من خسائر، وقد اختار " دينيس موران " لنفسه اسما حركيا هو " كوليو " وقد قام " كوليو " بشن سلسلة من الهجمات الإلكترونية على مواقع مهمة أنشأتها الحكومة الأمريكية على شبكة الأنترنت، ومنذ نهاية سنة ١٩٩٩ وحتى بداية سنة ٢٠٠٠ استطاع "كوليو" أن يحول حياة المسئولين عن هذه المواقع إلى الجحيم ، حيث دأب على مهاجمة موقع (DARE.ORG) المسئول عن مواجهة مخاطر الإدمان، ونفذ عمليات تخريبية عليه.[9]

ثانيا: المتسلل الى الشبكة Hackers

فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحسابات الآلية غير المصرح لهم وكسر الحواجز الأمنية الموضوعة لهذا الغرض[10]، وهذه الفئة ليس لديها أية دوافع حاقدة أو تخريبية ، وانما تنطلق من دوافع[11] اكتساب الخبرة ، أو بهدف هزم السلطة والتحدي أو بدافع الفضول أو لمجرد اثبات الذات والقدرة على التعامل مع هذه الأنظمة والتغلب عليها أو التسبب بالارباك للأخرين.[12]

ثالثا: المخترق المؤذي (الخبيث) Malicious hackers

غالبا ما يسعى هؤلاء المجرمون إلى إلحاق الضرر بالجهات المجني عليها، ويقومون بأفعالهم بدافع الحقد أو الانتقام[13]، هدفهم إلحاق خسائر بالمجني عليهم أن يكون الحصول على مكتسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرة من مخترقي فيروسات الحاسبات الآلية وموزعيها.[14]

رابعا: حل المشاكل الشخصية Personal Problem Solvers

وهي الطائفة الأكثر شيوعا وهي تضم بين جنباتها أشخاصا يعانون من مشاكل مادية ولا يستطيعون حلها ومواجهتها بالوسائل الأخرى بما فيها اللجوء الى الجريمة التقليدية ، لذا فهم يرتكبون هذا النوع المستحدث من الجرائم بدافع ايجاد حلول لتلك المشاكل.[15]

---

[8]– علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة ، منشورات زين الحقوقية، الطبعة الأولى، 2013 ، ص113.

[9]– خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2009،ص143.

[10]– حنان مسكين، واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر، المجلة الأكاديمية للبحوث القانونية والسياسية ، المجلد الرابع، العدد الاول، 2020 ص615.

[11] –حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها (دراسة مقارنة في التشريع اللبناني والمصري والفرنسي والأمريكي) ، مكتبة بدران الحقوقية ،الطبعة الأولى، 2017 ، ص78

[12]– علي عبود جعفر، المرجع السابق، ص113.

[13]–عادل مشموشي، جرائم المعلوماتية (وتحديات أدواتها الالكترونية أساليبها التقنية مسارحها الافتراضية مقتضياتها التشريعية) ، الطبعة الأولى، المؤسسة الحديثة للكتاب، 2019، ص252.

[14] –حنان مسكين، المرجع السابق، ص616.

[15] –علي عبود جعفر، المرجع السابق، ص113.

كما أنهم يتمتعون بقدر معقول من الخبرة في مجال الحاسبات الآلية وذلك بحكم عملهم، ويبرر المنتمون إلى هذه الطائفة أفعالهم دائما، بحيث لا يجدون غضاضة في ارتكاب الفعل بحجة أن المجني عليه – والذي غالبا ما يكون مؤسسة مالية ينتمي إليها الفاعل – يستطيع أن يتحمل الخسائر الناجمة عن أفعالهم.[16]

خامسا: ممتهنوا الإجرام Career Criminals

وهم فئة من المجرمين الذين اتخذوا من الجريمة المعلوماتية مهنة لهم، وبالتالي يبتغون من خلالها تحقيق الكسب المادي غير المشروع [17]، ويعمل المنتمون إلى هذه الطائفة في أغلب الأحوال بطريقة منظمة بحيث ينطبق على أفعالهم وصف الجريمة المنظمة، أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل[18]، ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.[19]

تتميز هذه الطائفة بسعة الخبرة والادراك الواسع للمهارات التقنية وهم من أخطر مجرمي التقنية، ويصنف هؤلاء المجرمون تبعا لنوع الجريمة المرتكبة والوسيلة المستخدمة كالتجسس الصناعي أو لحساب منافسين أو لحساب المنظمات سواء الارهابية أو السياسية أو لمصالح الدول.[20]

سادسا: أصحاب الآراء المتطرفة extreme Advocates

تتألف هذه المجموعة من أشخاص يدافعون عن قضية أو غاية ليس لها علاقة بمصالحهم الشخصية المباشرة، وهم على استعداد للانخراط في أنشطة إجرامية من شأنها أن تسبب أضرارا جسيمة بالآخرين أو بقطاعات كاملة في المجتمع، وقد يكون وراء ذلك أسباب ذات طابع سياسي أو اقتصادي أو ديني أو تتعلق بحقوق الإنسان[21]، ويسعون من خلال جرائمهم لفرض تلك المعتقدات والنيل ممن يعارضها أو ممن يرونه حجر عثرة في طريق انتشارها وتمددها، ولا يسعون بأفعالهم الجرمية إلى تحقيق أية مكاسب شخصية مادية أو معنوية، إما لمجرد اندفاعهم وتقديرهم لبعض الشخصيات، والتوجهات الفكرية والإيديولوجية [22]، وفي هذا تختلف هذه المنظمات المتطرفة عن المنظمات الإجرامية المنظمة، حيث تهدف الأخيرة إلى تحقيق مصالحها الشخصية المباشرة وتحديدا تحقيق الربح المادي.[23]

كمثال ما قامت به جماعات تنتمي إلى منظمات إرهابية دولية من اليمين المتطرف واليسار مثل جماعة الألوية الحمراء الايطالية ومنظمة (LECLODO) وهي: منظمة فرنسية متخصصة في تدمير نظم المعلومات

---

[16]– طارق ابراهيم الدسوقى عطية ، الامن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر ،الاسكندرية ،2009، ص–ص، 180–181 .

[17]– عادل مشموشي، المرجع السابق، ص253.

[18]– طارق ابراهيم الدسوقى عطية، المرجع السابق، ص181.

[19]– حنان مسكين، المرجع السابق، ص616.

[20] – حسين محمد الغول، المرجع السابق، ص81 .

[21]– بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية ،طبعة 2017، ص41.

[22] –عادل مشموشي، المرجع السابق، ص254.

[23]- نهلا عبدالقادر المومني، مرجع سابق، ص 86.

وغيرها من المنظمات الأخرى بارتكاب أفعال اعتداء على أنظمة المعلومات المنتشرة في أوروبا ابتداء من عام 1978.

وقد تعرضت وزارات وجامعات ومؤسسات مالية لهجمات الألوية الحمراء، ومن هنا أيقنت المنظمات الإرهابية أن في استطاعتها بمجهود بسيط أن تلحق أضرارا ضخمة داخل أي مشروع عن طريق تدمير المركز المعلوماتي له؛ لذا أصدرت الألوية الحمراء في فبراير 1998 منشورا شرحت فيه إسترا تيجيتها وأهدافها من الهجوم على النظم المعلوماتية .[24]

سابعا: مجرمي الأهمال The Criminally Negligent

تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحسابات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية[25]، ولا شك في أن الإهمال في مجال الحاسبات الآلية يمكن أن يترتب عليه في كثير من الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح.[26]

ففي نيوزيلندا على سبيل المثال، قام اثنان من مبرمجي الحاسبات بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائرة بهذ ا التغيير مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل 60 راكبا،كانوا على متنها، ولقد تمت محاكمة المتهمين بتهمة القتل الخطأ.[27]

الفرع الثاني: دراسة الأساتذة (David Icove ، Karl Seger and William Vonstorch)

قسموا مجرمي المعلوماتية إلى ثلاثة طوائف فيما يلي:

أولا: المخترقون (الهاكرز) Hackers

ويطلق على هذه الطائفة مصطلح (الهاكرز) Hacker's ، وهو ذلك الشخص الماهر في التعامل مع الشبكات خصوصا شبكة الانترنت ، وهو خبير في اختراق أجهزة الكمبيوتر وبرامج الحماية بشكل غير قانوني بدافع الفضول[28]، ورغم قدرة الهكرة على الولوج للأنظمة المعلوماتية وتخطي حواجز الأمن المعلوماتي والسباحة في هذا الفضاء الافتراضي بغرض التسلية ، أو بدافع الفضول ، أو لاثبات قدرتهم على الاختراق ، الا انهم غير مؤذين فلا يقومون بالتدمير والاتلاف.[29]

يتميزون بقدر عال من الكفاءة التقنية، ويتفاخرون بإلمامهم بعلوم الحاسوب، وبقدرتهم على اختراق شبكات الحاسب الآلي وبجهدهم الذاتي، ودون الاستعانة بأي تعليمات من أي مصادر، وأغلبهم صغار السن، مراهقون

---

[24]– نفس المرجع، ص 86.

[25]– حنان مسكين، المرجع السابق، ص616.

[26] –طارق ابراهيم الدسوقى عطية، المرجع السابق، ص182.

[27] –علي عبود جعفر، مرجع السابق، ص–ص، 114–115 .

[28]– حسين محمد الغول، المرجع السابق، ص78.

[29]– عبدالاله النوايسة، جرائم تكنولوجيا المعلومات (شرح الأحكام الموضوعية في قانون الجرائم الالكترونية)، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، 2017 ، ص81.

وشباب (طلبة وتلاميذ ثانويات) وشباب عاطل عن العمل [30]، أو أشخاص عاديون يشغلون مناصب محل ثقة ولديهم الكفاءة الخاصة والمعرفة والمهارة المطلوبة في مجال الحواسيب والشبكات الالكترونية.[31]

إلا أن الحقيقة التي يجب أن لا نخفيها هي أن هؤلاء القراصنة الهواة ساهموا في كشف الفجوات الأمنية للأنظمة المعلوماتية في المؤسسات المالية وغيرها الأمر الذي ساهم في تطوير نظم الأمن ضد الاختراقات الأمنية التي قد يقوم بها مجرمو المعلوماتية.[32]

ثانيا: المحترفون

يطلق على هذه الطائفة مصطلح Cracker's ويتميز أفراد هذه الطائفة بالتخصص العالي في مجال الحاسب الآلي[33] وبقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدثون إضرارا كبيرة[34].

يتوصلون إلى أهدافهم باستخدام ما لديهم من مهارات يطورونها باستمرار في لغات البرمجة والتشغيل وتصميم وتحليل البرامج وتشغيلها بسرعة، ويستهدفون المصارف بغرض سحب الأموال من حساباتها، واختراق المواقع المهمة والحساسة بغرض التلاعب ببياناتها أو تدميرها [35]، كما يقومون بفك شفرة برنامج معين بقصد التمكن من استعماله أو نسخه بطريقة غير مشروعة، أو لمعرفة كلمة السر بقصد الحصول على معلومات سرية بدون وجه حق[36].

ويلاحظ أنه جرت العادة على إطلاق لفظ الهاكرز على كلا نوعين الهاكرز والكراكر أو استخدام لفظ القراصنة عموما[37] ف" الهاكرز " يتحدون إجراءات نظم المعلومات، ولكن لا تتوافر لديهم دوافع تخريبية بل لهم دافع التحدي وإثبات قدراتهم وتفوقهم، على عكس "الكراكرز" الذين تعكس اعتداءاتهم الميول الإجرامي الخطير في إحداث التخريب .[38]

ومن بين العمليات التي قامت بها ففي عام 1994 تمكن اثنين من قراصنة الكمبيوتر في بريطانيا الذين يطلق عليهم " Data Stream CowBoy" من اختراق قاعدة سلاح الجو الأميركي في ولاية نيويورك ونسخ الملفات الحساسة وتركيب أجهزة للحصول على كلمة السر إضافة لاقتحام العديد من أنظمة الدفاع الأميركي وتم القاء القبض عليهما وهما من الشباب البالغين 16و20 من العمر.[39]

---

[30] – بن مكي نجاة، المرجع السابق، ص39.

[31]– نهلا عبدالقادر المومني، المرجع السابق، ص 83.

[32]– نفس المرجع، ص 84.

[33]– بن مكي نجاة، المرجع السابق، ص39.

[34]– نهلا عبدالقادر المومني، المرجع السابق، ص 84.

[35] – عميمر عبدالقادر، التحديات القانونية لاثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان–الجزائر، 2021 ، ص47.

[36]– نفس المرجع، ص–ص، 46– 47.

[37] –خالد ممدوح ابراهيم، مرجع سابق، ص145 .

[38]– بن مكي نجاة، المرجع السابق، ص41.

[39]– حسين محمد الغول، مرجع سابق، ص80.

ثالثا: الحاقدون

تكمن خطورة مرتكبي جرائم الحاسب الالي ليس في قدرتهم على اختراق الأنظمة التقنية والفنية التي توضع لحماية المعلومات، انما في كونهم أيضا ممن يعملون داخل المؤسسات وممن يعملون في مجال الادارة وتشغيل الحاسب الالي[40]، وهي فئة من الموظفين الحاقدين على عملهم أو على مؤسساتهم الذين قد يقومون بأفعال إجرامية لا تهدف إلى الكسب المادي بل هدفها الانتقام والثأر من أصحاب عملهم وهذه الفئة يذهب البعض إلى تسميتها " بفئة مجرمي المعلوماتية الحاقدين".[41]

وهم الأخطر لمعرفتهم بنظام المؤسسة وتشغيل النظام والعبث به ومعرفة نقاط الضعف والقوة بذلك النظام [42]، وبيدهم العديد من المعلومات والمعرفة الكافية بنظام الشركة أو المصرف الذي فصلوا منه والعمل على تكبيدها الخسائر المالية الكبيرة وذلك من خلال تدمير النظام المعلوماتي أو اتاحة الفرصة لجهات خارجة عن النظام الدخول عليه وممارسة أنشطة تدميرية ببيئة النظام.[43]

المبحث الثاني

سمات ودوافع المجرم المعلوماتي

بعد التطرق الى تعريف المجرم المعلوماتي وتصنيفاته يمكن استخراج أهم السمات والدوافع التي تؤدي به الى ارتكاب سلوكه الاجرامي، بالرغم ليس بالأمر اليسير حصرها إلا أننا سنعرض لأهمها بما يأتي:

المطلب الأول: السمات المميزة لشخصية المجرم المعلوماتي

أثبتت الدراسات بأن المتورطين في الجرائم ا لمعلوماتية يتميزون بسمات تميزهم عن غيرهم من المتورطين في الجرائم التقليدية.

الفرع الأول: المجرم المعلوماتي يتمتع بالذكاء وبالمهارة والمعرفة

المجرم المعلوماتي يتمتع ب:

أولا: الذكاء

يتميز المجرم المعلوماتي غالبا بالذكاء، حيث أن الجريمة المعلوماتية تتطلب مقدرة عقلية وذهنية عميقة خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبيرة تلحق بالمجني عليه.

فالمجرم المعلوماتي يستخدم مقدرته العقلية ولا يلجأ إلى استخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء[44] دون إحداث أي نوع من الصخب أو اللجوء إلى العنف، فعن طريق استخدام طرق علمية مبتكرة يمكنه تجاوز الحواجز الالكترونية، ولهذا يوصف الإجرام المعلوماتي بإجرام الأذكياء[45].

---

[40] – محمد حماد مرهج الهيتي، جرائم الحاسوب (ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها)، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، 2006، ص140.

[41]– نهلا عبدالقادر المومني، المرجع السابق، ص85.

[42] – مصطفى محمد موسى، مرجع سابق، ص148.

[43]– حسين محمد الغول، مرجع سابق، ص86.

[44] –نهلا عبدالقادر المومني، المرجع السابق، ص 77.

وحسب الدراسة التي أجريت من طرف الباحث عبد الله بن سعود بن محمد السراني سنة 2009 بالمملكة العربية السعودية على عينة مختارة من الأشخاص المختصين في مجال مكافحة الجريمة المعلوماتية خلص فيها إلى أن نسبة 94.2% من أفراد هذه العينة محل الدراسة تم تصنيفهم على رأس قائمة الملامح الاجرامية للشخص المجرم المعلوماتي بأنه شخص يتمتع بالذكاء والمهارة في مجال استخدام تقنيات المعلوماتية، فهو : "

- يتميز بالقدرة على اختراق النظم المعلوماتية والتلاعب بالأنظمة الأمنية
- يبتكر أساليب متطورة لارتكاب أفعاله واخفاء آثاره.
- لديه القدرة الفائقة على المعالجة الالكترونية للنصوص والكليات والتعامل مع البرامج.[46]

ثانيا: المهارة

يتمتع مجرمو المعلوماتية بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والإنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا[47].

فتنفيذ الجريمة المعلوماتية يتطلب قدرا من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات [48]، الا أن هذه المهارة ليست في ذات المستوى لدى كافة مجرمي تكنولوجيا المعلومات وإنما تختلف من مجرم لآخر، لأن جرائم تكنولوجيا المعلومات مختلفة، وكل منها يحتاج لمهارة خاصة وأسلوب مختلف عن غيرها[49].

إلا أن هذا لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال [50]، أو أن تكون لديه خبرة كبيرة فيه، وإنما يكفي أن يكون لديه الإلمام الكاف في علوم تقنية الحاسب الآلي وكيفية اختراق الشبكات المحمية والقدرة على إخفاء جريمته[51]، والواقع العملي قد أثبت أن جانب من أنجح مجرمي المعلوماتية، لم يتلقوا المهارة اللازمة لإرتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال[52]، لأن كثير من فئة الهاكرز اكتسبوا هذه المهارة الفنية كهواية من الآخرين أو من خلال الاطلاع والقراءة في الشبكة العنكبوتية.[53]

---

[45] – عميمر عبدالقادر، مرجع سابق، ص43.

[46]– بكوش محمد أمين، هروال نبيلة هبة، خصوصية المجرم الالكتروني –مجرم الأنترنت نموذجا– ، مجلة البحوث في الحقوق والعلوم السياسية، المجلد07، العدد01 ،2021 ،ص78.

[47] –نهلا عبدالقادر المومني، المرجع السابق، ص 77.

[48] – نهلا عبدالقادر المومني، المرجع السابق، ص 77.

[49]– عبدالاله النوايسة، مرجع سابق، ص85.

[50]– بن عميروش ريمة، عن خصوصية الجريمة المعلوماتية، مجلة الفقه القانوني والسياسي، مجلد2، العدد 2، 2020، ص81.

[51]– زياد بن محمد عادي العتيبي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها خصائصها أركانها والدافع من ارتكابها، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد 03، العدد1، 2020، ص11.

[52]– طارق ابراهيم الدسوقى عطية، مرجع السابق، ص176.

[53] –زياد بن محمد عادي العتيبي، المرجع السابق، ص11.

وفي حال ارتكاب جريمة تكنولوجيا معلومات بالاشتراك ، فلا يلزم توافر هذه المهارة لدى المساهمين فيها بصورة تبعية كالمحرضين والمتدخلين، فقد يتم التحريض أو التدخل في جريمة تكنولوجيا معلومات من أشخاص لا تتوافر لديهم مهارات شخصية في تكنولوجيا المعلومات.[54]

ثالثا: المعرفة

تتم الجريمة المعلوماتية في تحلي المساهمين فيها، وبالتحدي فاعلها وشركائه، بحد أدنى من المعرفة بتقنية المعلومات[55]، وذلك بالتعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها، وإمكانيات نجاحها واحتمالات فشلها [56]، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على المحيط الذي تدور فيه حتى لا يواجهوا باشياء غير متوقعة من شأنها افشال أفعالهم أو الكشف عنهم.[57]

وجل ما تتطلبه هذه الجرائم هو البحث والتحليل والتفكير العلمي والمنطقي، مع توفر خبرة كافية في مجال عمل الحاسب الآلي والبرمجيات المشغلة له.[58]

الفرع الثاني: المجرم المعلوماتي مجرما متخصصا

ثبت أن مجرمي تكنولوجيا المعلومات لا يرتكبون إلا هذا النوع من الجرائم، فهم متخصصون في الإجرام التقني في مجال المعلوماتية [59]، أي يكون خبيرا بالقدر الكافي واللازم بأمور الحوسبة ومحترفا حتى يستطيع أن يقدم على مثل هذا النوع الخطير والمستحدث من الإجرام .[60]

حيث أجريت احصائية على صفات ومواصفات مرتكبي جرائم الحاسب الالي، وقد أثبتت هذه الاحصائية أن من بين أصحاب الخبرة والتخصص في مجال الحاسبات الالية، وتقنية المعلومات يحتل المحللون للنظم في مقدمة مرتكبي هذا النمط من الجرائم، حيث يقترفون مامجموعه 25% من مجمل جرائم المعلوماتية، ومن ثم يليهم بعد ذلك بالتسلسل، أي في المرتبة الثانية، مصمموا النظم حيث يرتكبون الجرائم بنسبة 18% ثم بعد ذلك يأتي مستخدمي النظم المعلوماتية، الذين لديهم خبرة معلوماتية، ونسبتهم في نطاق ذلك 17%، من ثم يأتي الصيارفة، ونسبتهم 16%، ثم الأشخاص غير العاملين بالمنشأة التي تتعرض للاعتداء، ونسبتهم 12% وأخيرا مشغلي الحاسب الالي ونسبتهم11%.[61]

الفرع الثالث: المجرم المعلوماتي يتمتع بالسلطة تجاه النظام المعلوماتي

---

[54]– عبدالاله النوايسة، المرجع السابق، ص85.

[55]– عادل مشموشي، مرجع سابق، ص246.

[56] –طارق ابراهيم الدسوقى عطية، المرجع السابق، ص176.

[57] علي عبود جعفر، مرجع سابق، ص 108.

[58] –عادل مشموشي، مرجع سابق، ص247.

[59] –عبدالاله النوايسة، المرجع السابق، ص85.

[60] –بكوش محمد أمين، هروال نبيلة هبة، مرجع سابق، ص77 .

[61] محمد حماد مرهج الهيتي، مرجع سابق، ص137.

تعني بالسلطة تلك المزايا والحقوق التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته [62]، فكثير من المجرمين في هذا المجال لديهم سلطة مباشرة أو غير مباشرة في مواجهة محل الجريمة [63].

وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، والتي تعطي الفاعل مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو أو تعدل المعلومات التي تحتوي عليها [64]، وقد تتمثل في الحق في استعمال الأنظمة المعلوماتية أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة" [65]، وقد تكون السلطة التي يتمتع بها الجاني غير شرعية، كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.[66]

الفرع الرابع: المجرم المعلوماتي شخص مجرم متكيف إجتماعيا

أن المجرم المعلوماتي بصفته إنسان ذكي فهو إجتماعي، فلا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به[67]، بل على العكس من ذلك هو إنسان قادر على التوافق والتصالح مع الاخرين والتفاعل معهم, الأمر الذي يزيد من درجة خطورته الإجرامية كلما زاد تكيفه الإجتماعي [68]، فشعور المجرم أنه محل ثقة من مجتمعه وشعوره بأنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا تكتشف، وإذا اكتشفت فإنها تواجه صعوبة الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء.[69]

ويلاحظ أنه على النقيض الاخر يكون تكيف هؤلاء الأشخاص مع المجتمع الخارجي محدودا وغالبا ما يكونون منعزلين عن المجتمع .[70]

الفرع الخامس: المجرم المعلوماتي مجرم حذر من كشف جريمته

بالرغم من أن جل الدراسات أكدت بأن للمجرم المعلوماتي شخصية تتسم بالهدوء والمثابرة والصبر والتكيف الإجتماعي والثقة الزائدة بالنفس ونبذ العنف المادي والرغبة في التواجد داخل مجموعات إجرامية لتبادل الخبرات وتطوير الملكة الإجرامية، إلا أن ذلك لا يمنع من وجود حذر شديد وخشية وخوف كبيرين لديهم من إكتشاف أفعالهم وإفتضاح أمرهم[71].

---

[62] – رضا عسال ، عماد عبد الرزاق، الجريمة الالكترونية والمجرم المعلوماتي : مقاربة مفاهمية، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، العدد05،2020، ص155.

[63] –ربيعي حسين ، المجرم المعلوماتي– شخصيته وأصنافه، مجلة العلوم الانسانية ،العدد40 ،جوان 2015 ، ص290.

[64]– طارق ابراهيم الدسوقى عطية، المرجع السابق، ص177.

[65]– رضا عسال، عماد عبد الرزاق، المرجع السابق، ص155.

[66] –طارق ابراهيم الدسوقى عطية، المرجع السابق، ص177.

[67]– رضا عسال، عماد عبد الرزاق، المرجع السابق، ص155.

[68]– لحرش أيوب التومي، النحوي سليمان، مرجع سابق، ص987.

[69]– نهلا عبدالقادر المومني، مرجع سابق، ص 79.

[70] – خالد ممدوح ابراهيم، مرجع سابق، ص137.

[71] – لحرش أيوب التومي، النحوي سليمان، المرجع السابق، ص987.

فخوف المجرم المعلوماتي من انكشاف فعله يعود إلى انتمائه في الغالب الأعم إلى وسط اجتماعي متميز سواء من حيث التعليم أو الثقافة أو المستوى المهني وطبيعة العمل [72]، مما يدفع به إلى إتباع أسلوب تدمير ومحو كل الدلائل الناتجة عن فعله، من خلال محو البيانات وتدمير الحواسيب المستعملة في جريمته [73]، الا أن أكثر ما يعرض المجرم إلى اكتشاف أمره هو أن يستجد أو يطرأ أثناء تنفيذه لجريمته مجموعة من العوامل غير المتوقعة والتي لا يمكن التنبؤ بها، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحواسيب إنما تؤدي عملها غالبا بطريقة آلية، بحيث لا تتغير المراحل المختلفة التي تمر بها[74].

الفرع السادس: عدم شعور المجرم المعلوماتي بالذنب

يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن ما يقوم به لا يدخل في عداد الجرائم [75]، أو بمفهوم أخر أنه لا يمكن لهذا العمل والفعل أن يصنف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله [76] ، بحيث يوجد في هذه الجرائم نوع من الإقرار الذاتي بمشروعية هذا الفعل[77]، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.[78]

غير أن هذا لا يدل أو يعني أن عدم الشعور بعدم أخلاقية هذه الأفعال الإجرامية المعلوماتية لدى فئة كبيرة من مرتكبيها ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على علم وإدراك بعدم مشروعية وأخلاقية هذا الفعل، فهناك فئة تملك اتجاه إجرامي خطير، وسوء نية واضحة وهم على دراية عامة بخطورة أعمالهم وأفعالهم.[79]

الفرع السابع: المجرم المعلوماتي مجرم عائد للإجرام

يتميز مرتكبو الجرائم الإلكترونية بوجود النزعة الإجرامية والميل إلى ارتكاب الجرائم لديهم [80]، وتكون تلك النزعة الاجرامية لدى الشخص نتيجة لتأثره بعوامل عضوية وعوامل نفسية صاحبت نشأة الشخصن ومع اقتران تلك العوامل بعنصر آخر جديد يساعده على استثارة الحالة الإجرامية [81]، الأمر الذي يكسب المجرم مهارة علمية

---

[72] – غريبي بشرى، مرجع سابق، ص105.

[73] – ربيعي حسين، المرجع السابق، ص290

[74] –غريبي بشرى، المرجع السابق، ص105

[75]– نهلا عبدالقادر المومني، المرجع السابق، ص 78.

[76] – حمزة بن عقون، السلوك الاجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، 2012/2011 ، ص–ص، 31–32.

[77]– عبدالاله النوايسة، مرجع سابق، ص86.

[78]– نهلا عبدالقادر المومني، مرجع سابق، ص 78.

[79] –حمزة بن عقون، المرجع السابق، ص32.

[80] –بن عميروش ريمة، مرجع سابق، ص81

[81]– نفس مرجع السابق، ص81.

وتكنولوجية تضاعف من رغبته في سد الثغرات التي سبق التعرف عليها وأدت إلى تقديمه للمحاكمة في المرة الأولى مما يؤدي به إلى العودة للإجرام وقد ينتهي به الأمر بتقديمه للمحاكمة مرة ثانية.[82]

المطلب الثاني: دوافع ارتكاب الجرائم المعلوماتية

اهتم المختصون بجرائم المعلوماتية في بيان دوافع ارتكاب هذه الجرائم، ومع أنه ليس بالأمر اليسير حصر جميع الدوافع لتعدد هذه الجرائم ومبتغى مرتكبها، إلا إننا سنتطرق لأهمها في مايلي:

الفرع الأول: ارتكاب الجرائم المعلوماتية من أجل التسلية

يعتبر دافع المزاح والتسلية من الدوافع التي تجعل الشخص يقوم بتصرفات وإن كان لا يقصد من ورائها إحداث جرائم وإنما بغرض المزاح فقط، ولكن هذه التصرفات قد تنتج عنها نتائج ترقى إلى درجة الجريمة[83]، لأنه من الطبيعي أن الشخص الذي يقوم بمسح مجموعة من الملفات من جهاز شخص آخر، وكانت هذه الملفات تحتوي على معلومات مهمة فلا يمكن القول بأن هذا التصرف مجرد دعابة، بل إن هذا التصرف في حقيقته جريمة إتلاف وتخريب متعمد في حالة ما إذا كان هناك قانون يجرم هذا الفعل[84].

وقد ينطوي تحت الدوافع الترفيهية ارتكاب جرائم تكنولوجيا المعلومات بدافع قهر النظام، وتحدي أنظمة الأمن المعلوماتي من أجل إثبات القدرة على الاختراق، ومن الدوافع الترفيهية التبجح (Bragging) الذي يتم بين الهكرة بسبب الولع والتنافس فيما بينهم على الولوج للأنظمة والمواقع المشهورة[85].

فمن القضايا ماحصل في مدينة العين بدولة الامارات العربية المتحدة عندما توصل المتهم وبغير وجه حق الى الدخول على جهاز الحاسب الالي للمجني عليها ونسخ البيانات والمعلومات الشخصية الخاصة بها وتهديده اياها بأنه سيقوم بنشر صورها عبر فضاء الانترنت اذا لم تضيفه الى قائمة أصدقائها في برنامج المحادثة المرئية والمسموعة " الماسنجر" .[86]

الفرع الثاني: الرغبة في التعلم وفي إثبات الذات

غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الأنترنت هو الرغبة في إثبات الذات وتحقيق إنتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوايا آثمة[87]، إزاء ظهور أي تقنية مستحدثة، لذا فان مرتكب الجريمة لديه شغف في محاولة استكشافها والتغلب عليها مهما بلغت درجة تعقيدها [88] تحول دون الإطلاع عليها، كما أن التغلب على المعوقات، وتجاوز الحواجز ولد شعور بالمتعة والإعتزاز بالنفس، والشعور بالرضى والسعادة لمجرد التغلب على بعض الصعوبات، وتخطي المحظورات، أو التفوق على الآخرين.[89]

---

[82]– لحرش أيوب التومي، النحوي سليمان، المرجع السابق، ص987.

[83]–رضا عسال، عماد عبد الرزاق، مرجع السابق، ص156.

[84] –بن مكي نجاة، مرجع سابق، ص44.

[85]–عبدالاله النوايسة، مرجع سابق، ص89.

[86] –حسين محمد الغول، مرجع سابق، ص85 .

[87] –رضا عسال، عماد عبد الرزاق، المرجع السابق، ص156.

[88] –بن عميروش ريمة، المرجع السابق، ص83.

[89] –عادل مشموشي، مرجع سابق، ص–ص، 242– 243.

الفرع الثالث: تحقيق الكسب المالي

تعتبر الدوافع المادية من أهم البواعث على ارتكاب الجرائم المعلوماتية لما تحققه من ثراء فاحش [90]، فالطمع وحب الثراء السريع يدفع الفرد إلى القرصنة أو السرقة أو الاختلاس عن طريق الحاسوب للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع غير المكلف، بالإضافة إلى تحقيق أغراض معنوية مقصودة وذلك من خلال عمليات الجوسسة واختراق المواقع [91]، مما أخذوا يشكلون خطرا على أنظمة الحاسب بما يشمله من معلومات وكذا على الحياة الخاصة للأفراد وأموالهم.[92]

اذ يقوم مرتكبوا الجريمة عبر الإنترنت ذوي الكفاءة الفنية العالية، بما لديهم من خبرة ومهارة في المجال التكنولوجي بتوجيه هذه الإمكانات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المادية إما بسرقة تلك الأموال أو بتحويلها لحسابه الشخصي داخل البنك [93]، وخصوصا في ظل سهولة نقل الأموال بين الحسابات ولإرتباط المؤسسات المالية جميعها بالشبكة المعلوماتية لإتمام عملياتها ومهامها، مما يسهل على المجرم المعلوماتي الولوج لهذه الشبكات وتحويل الأموال والتحصل عليها.[94]

ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة لاقترافه هذا النوع من الإجرام من خلال ما يرويه أحد هؤلاء المجرمين المحترفين في سجن كاليفورنيا بقوله: (لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية وبإمكاني أن أكرر ذلك في أي وقت لقد كان شيئا سهلا فأنا أعرف أسلوب عمل جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني).[95]

الفرع الرابع: الرغبة في الانتقام

وهي من أخطر الدوافع التي يقوم بها المجرم المعلوماتي، وذلك من خلال الثأر من أشخاص لأسباب شخصية أو انتقام الموظف الذي تم فصله من المنشأة التي كان يعمل بها فيقوم بإختراق نظامها[96].

وغالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها وغالبا ما يكون أحد موظفيها الذي يقوم بارتكاب الجريمة المعلوماتية بدافع الانتقام [97]، نتيجة إما لفصله من العمل [98] أو تخطيه في

---

[90] –بن مكي نجاة، المرجع السابق، ص44.

[91] –نفس المرجع، ص44.

[92] –نفس المرجع، ص44.

[93] –رضا عسال ، عماد عبد الرزاق، المرجع السابق، ص156.

[94] –حنان ريحان مبارك المضحكي ، الجرائم المعلوماتية دراسة مقارنة ، الطبعة الاولى ، منشورات الحلبي الحقوقية، بيروت، 2014، ص 43.

[95]– نهلا عبدالقادر المومني، مرجع سابق، ص91.

[96] –زياد بن محمد عادي العتيبي، مرجع السابق، ص15.

[97]– غريبي بشرى، مرجع سابق، ص 110.

[98] –وأبرز مثال على ذلك :حادثة شركة اوميغا التي ترجع وقائعها في أن مصمم ومبرمج شبكات كمبيوتر و رئيس سابق لشركة OMEGA من مدينة Delaware ويدعى Timothy Allen Lioyd الذي تم اعتقاله في : 17 فيفري 1998 بسبب إطلاقه لقنبلة الكترونية في عام 1996 وذلك بعد 20 يوما من فصله من العمل، كما أنها استطاعت أن تلغي كافة التصاميم وبرامج الإنتاج لإحدى كبرى مصانع التقنية

الحوافز أو الترقية فهذه الأمور تجعله يقدم على ارتكاب جريمته [99]، رغبة منه في الانتقام ليجعل الشركة أو المؤسسة تتكبد الخسائر المالية الكبيرة من جراء ما يسببه لها من ضرر يحتاج إصلاحه إلى وقت لا بأس به.[100]

وتشير التقديرات إلى أن نسبة كبيرة من الجرائم المرتكبة عبر الإنترنت ترتكب من قبل موظفي الجهة نفسها[101]، فحسب تقرير أعده مكتب التحقيقات الفيدرالي FBI عام 1999 تبين أن 55% من جرائم الحاسب الآلي التي ترتكب من الموظفين بحق المؤسسات التي يعملون بها تكون بدافع الحقد [102] ، ومن الوقائع التي حدثت في الولايات المتحدة الأمريكية أنه حكم على أحد الموظفين في إحدى شركات التأمين بالسجن لمدة سبع سنوات وغرامة مقدارها 150 ألف دولار لأنه أدخل فيروسا في أجهزة الشركة التي كان يعمل فيها مما أدى إلى ضياع 160 سجلا من سجلات العملاء، وذلك انتقاما من الشركة لأنها قامت بفصله من العمل.[103]

أو الرغبة بإلحاق الضرر بأحد ما، كسرقة صور شخصية من جهاز حاسب آلي شخصي وإبتزاز صاحب الصورة، أو تشويه سمعته بسرقة هذه الصورة والتلاعب بها أو نشرها كما هي أمام بلايين المستخدمين لهذه الشبكة، أو تحويل أموال من حساب شخص ما بغرض الإضرار به ماديا على سبيل المثال.[104]

الفرع الخامس: دوافع سياسية

تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم، كما أن الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية، كذلك أصبحت شبكة الإنترنت مجالا خصبا لنشر أفكار العديد من الأفراد والمجموعات، ووسيلة للترويج لأخبار وأمور أخرى قد تحمل في طياتها مساسا بأمن الدولة أو بنظام الحكم أو قدحا في رموز دولية أو سياسية والإساءة لها بالذم والتشهير[105] يهدف بعض مخترقي الأنظمة الإلكترونية إلى نشر مبادئهم وأفكارهم السياسية، أو تدمير المواقع الإلكترونية للجهات الحكومية والخاصة لأسباب سياسية، وتلجأ الأجهزة الحكومية في الدول في اختراق مواقع المعارضة وتدميرها ونشر معلومات على هذه المواقع، وقد يتم هذا الصراع المعلوماتي بين الدول المختلفة [106] يتم من خلال المجرمين المعادين للحكومة، وذلك عبر تخريب المواقع الحكومية أو اختراق الحسابات الحكومية عبر منصات التوصيات

العالمية في نيوجرسي و التي تؤثر على نظم تحكم مستخدمة في NASAوالبحرية الأمريكية، ملحقا خسائر بلغت 10 ملايين دولار وتعتبر هذه الحادثة مثالا حيا على مخاطر جرائم التخريب في بيئة الانترنت بل اعتبرت أنها من أكثر و اخطر الجرائم التخريبية للكمبيوتر منذ بروز هذه الظاهرة، وللمزيد من التفصيل، ينظر: غريبي بشرى، مرجع سابق، ص111.

[99]– رضا عسال، عماد عبد الرزاق، المرجع السابق، ص156.

[100] –بن مكي نجاة، المرجع السابق، ، ص–ص، 42 –43.

[101]– رضا عسال ، عماد عبد الرزاق، المرجع السابق، ص156.

[102] – عبدالاله النوايسة، مرجع سابق، ص88.

[103] –رضا عسال ، عماد عبد الرزاق، المرجع السابق، ص157.

[104]– حنان ريحان مبارك المضحكي ، المرجع السابق، ص 43.

[105]–رضا عسال ، عماد عبد الرزاق، المرجع السابق، ص156.

[106]– عبدالاله النوايسة، مرجع سابق، ص89.

الاجتماعي مثل تويتر وفيس بوك لكتابة أخبار ومعلومات غير صحيحة بغرض إثارة الفتنة والرأي العام بين المواطنين[107].

فقد قام بعض القراصنة المتواجدين على الأراضي الروسية باختراق نظم حاسبات حكومية في الولايات المتحدة الأمريكية مدة عام كامل، حيث قاموا بسرقة معلومات غير سرية ولكنها حساسة من أجهزة الحواسيب العسكرية الأمريكية.[108]

الخاتمة:

تسعى دراسات علم الإجرام في الوقت الراهن إلى محاولة التعرف على النوع الجديد من المجرمين الذين أخذو من البيئة الرقمية كأرضية خصبة لممارسة عليها أفعالهم غير المشروعة، وذلك لإختلافهم الجذري عن المجرمين العاديين سواء من خلال تصنيفاتهم أو بأهم السمات التي يتحلون بيها أو سواء بالدوافع التي تدفعهم إلى ارتكاب سلوكهم الاجرامي، وذلك لكي يتسنى للمشرع معرفة أهم الأسباب لهذا الإجرام ومحاولة مكافحته والوقاية منه.

ومن خلال ذلك توصلنا الى جملة من النتائج نذكرها فيما يلي:

- نظرا لحداثة الجريمة المعلوماتية فانه لا يوجد لحد الآن تعريف موحد للمجرم المعلوماتي ولا تصنيف ثابت بسبب التطور السريع والمتجدد في هذا المجال حيث يزداد تعقيدا كلما طفت على السطح تقنيات جديدة؛
- يتميز المجرم المعلوماتي بسمات تميزه عن غيره من المتورطين في الجرائم التقليدية؛
- الجرائم المعلوماتية لا يمكن أن يكون الدافع اليها محددا بدافع معين اذ يختلف باختلاف الجرائم ومن مجرم الى مجرم.

وتجدر بنا الإشارة أنه من خلال هذا البحث توصلنا إلى مجموعة من التوصيات هي:

- ضرورة تدخل المشرع بسن وتعديل بعض النصوص القانونية وتوقيع جزاءات ردعية من أجل الحد من هذه الظاهرة ؛
- من الأنسب تأهيل جهات التحقيق ليكونا قادرين على التعامل مع هذا النوع المستحدث من السلوكيات الإجرامية؛
- من الأن[109]سب نشر الوعي والثقافة القانونية بين المواطنين ومؤسسات المجتمع المختلفة من أجل إدراكهم بخطورة هذه الجرائم.

قائمة المراجع:

أولا: الكتب

1) بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، 2017؛
2) حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها (دراسة مقارنة في التشريع اللبناني والمصري والفرنسي والأمريكي)، الطبعة الأولى، مكتبة بدران الحقوقية ،2017؛

[107]– زياد بن محمد عادي العتيبي، مرجع سابق، ص15.

[108]– نهلا عبدالقادر المومني، مرجع سابق، ص93.

109

3) حنان ريحان مبارك المضحكي ، الجرائم المعلوماتية دراسة مقارنة ، الطبعة الاولى ، منشورات الحلبي الحقوقية، بيروت، 2014؛
4) خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2009؛
5) طارق ابراهيم الدسوقى عطية ، الامن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر ،الاسكندرية، 2009؛
6) عادل مشموشي، جرائم المعلوماتية (وتحديات أدواتها الالكترونية أساليبها التقنية مسارحها الافتراضية مقتضياتها التشريعية)، الطبعة الأولى، المؤسسة الحديثة للكتاب، 2019؛
7) عبدالاله النوايسة، جرائم تكنولوجيا المعلومات (شرح الأحكام الموضوعية في قانون الجرائم الالكترونية)، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، 2017؛
8) علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة، منشورات زين الحقوقية، الطبعة الأولى، 2013؛
9) عميمر عبدالقادر، التحديات القانونية لاثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان–الجزائر، 2021؛
10) محمد حماد مرهج الهيتي، جرائم الحاسوب (ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها)، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، 2006؛
11) مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2008؛
12) نهلا عبدالقادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008.

ثانيا: الرسائل الجامعية

1) حمزة بن عقون، السلوك الاجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، 2012/2011.

ثالثا: المقالات

1) بكوش محمد أمين، هروال نبيلة هبة، خصوصية المجرم الالكتروني –مجرم الأنترنت نموذجا– ،مجلة البحوث في الحقوق والعلوم السياسية، المجلد07، العدد01 ،2021؛
2) بن عميروش ريمة، عن خصوصية الجريمة المعلوماتية، مجلة الفقه القانوني والسياسي، مجلد2 ،العدد 2، 2020؛
3) حنان مسكين، واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر، المجلة الأكاديمية للبحوث القانونية والسياسية ، المجلد الرابع، العدد الاول، 2020؛
4) خليلي سهام، خصوصية المجرم الالكتروني، مجلة المفكر، العدد 15 ، جوان 2017؛

5) ربيعي حسين ، المجرم المعلوماتي– شخصيته وأصنافه، مجلة العلوم الانسانية ،العدد40 ،جوان 2015؛
6) رضا عسال ، عماد عبد الرزاق، الجريمة الالكترونية والمجرم المعلوماتي: مقاربة مفاهمية، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، العدد05 ،2020؛
7) زياد بن محمد عادي العتيبي ، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها خصائصها أركانها والدافع من ارتكابها، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد 03، العدد1؛
8) غريبي بشرى، خصوصية المجرم المعلوماتي ودوافعه، مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الثاني، 2021؛
9) لحرش أيوب التومي، النحوي سليمان، طبيعة الخطورة الاجرامية للمجرم المعلوماتي ، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 05 ،العدد01،2020.

فرنان فاروق
faroukbaraa@gmail.com
جامعة 8ماي1945 قالمة

أدوات المجرم المعلوماتي

مقدمة:

الجرائم الإلكترونية يمكن أن تشتمل على أنشطة إجرامية ذات طبيعة تقليدية كالسرقة و الغش و التزوير، والتي تخضع لعقوبات محددة سلفا في قوانين العقوبات سواء على المستوى المحلي أو الدولي.

كما أوجدت الثورة التقنية التي يعيشها عالمنا و الإنتشار الواسع لتكنولوجيات الإعلام و الاتصال أفعالا يمكن أن تشكل بذاتها تهديدا للمصالح المعتبرة للأفراد والجماعات في مختلف مناحي الحياة الأمنية، الثقافية ، الإجتماعية و الاقتصادية.

على هذا الأساس فإن الجرائم الالكترونية يمكن تقسيمها إلى قسمين رئيسيين: جرائم ترتكب بواسطة تكنولوجيات الإعلام و الاتصال، محددة سلفا في إطار تشريعي وما هذه التكنولوجيات إلا وسيلة لارتكابها فقط، أما القسم الثاني فيشمل الجرائم الواقعة أو الماسة بأنظمة المعالجة الآلية للمعطيات[1].

تتعدد المخاطر الإجرامية التي يكون محلها الكمبيوتر أو شبكة الإنترنتأو أي وسيلة اتصالات إلكترونية [2]، سواء تعلق الأمر بإتلاف تلك الأجهزة و البيانات أو البرامج التي تتضمنها وتستخدمها، او تعلق الأمر بأن تصبح تلك الوسائط بيئة الجريمة المرتكبة عن طريقها كالجرائم المتعلقة بالملكية الفكرية [3] و الصناعية و غيرها.

وتشكل المعلومات حجر الزاوية بالنسبة لهذا النوع الجديد من الإجرام، فالمعلومة أثمن الثروات في هذا العصر، والحصول عليها غاية في حد ذاتها أهم من الوسيلة التي لوصل إليها مشروعة كانت أم غير مشروعة.

---

[1]– المواد 394 مكرر و ما بعدها من الأمر 66–156 المؤرخ في 08يونيو1966 المتضمن قانون العقوبات المعدل و المتمم، القانون09–04 المؤرخ في 05 غشت2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها .

[2]– عرفت المادة 02/فقرة و من القانون 09–04 مصطلح الإتصالات الإلكترونية بأنها: " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة بواسطة أي وسيلة الكترونية "

[3]– د. ممدوح عبد الحميد عبد المطلب: جرائم استخدام شبكة المعلومات العالمية " جرائم الإنترنت"، مؤتمر القانون والكمبيوتر و الإنترنت،1–3 مايو 2000، كلية الشريعة و القانون، جامعة الإمارات العربية المتحدة، المجلد الأول، الطبعة الثالثة 2004، ص216.

– للتفصيل أكثر في أنواع الجرائم المستحدثة أنظر: بلعيد إلهام ، الجرائم المستحدثة، مجلة الباحث للدراسات الأكاديمية، المجلد 09، العدد02 جوان2022، ص521 وما بعدها.

ففي عالم الأعمال الحصول على معلومات حول المنافسين تعني القدرة على الصمود و الهيمنة على السوق، والحصول على المعلومات الخصوصية للأشخاص يعني إمكانية السطو على أموالهم

من المتصور أن يقع ضحية هذه الجرائم جميع الأشخاص سواء الطبيعية منها او المعنوية العامة أو الخاصة، طالما كانت تستخدم وسائل الاتصالات الإلكترونية في أنشطتها سواء الاقتصادية او الإجتماعية أو حتى السياسية و العسكرية، فالكل مستهدف[4].

لكل ما سبق فإن تحقيق الأمن المعلوماتي من أهم الرهانات التي تسعى الدول لكسبها على الصعيدين الداخلي و الخارجي، بل أضحى معيارا يقاس به مدى تقدم الدول، ولن يتأتى لها ذلك إلا بالإحاطة بكافة مظاهر السلوك الإجرامي في هذا المجال والأساليب و الأدوات التي يستخدمها ويستعين بها المجرمون في تنفيذ الجرائم المعلوماتية.

بالنسبة للمشرع الجزائري فقد نظم الأحكام العامة للجرائم الإلكترونية في القسم السابع مكرر تحت عنوان "**المساس بأنظمة المعالجة الآلية للمعطيات**" ضمن الفصل الثالث المتضمن "**الجنايات و الجنح ضد الأموال**" من قانون العقوبات[5]، كما أصدر قانونا خاصا **بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال**[6].

بناء على ما تقدم سنحاول من خلال هذه الورقة البحثية أن نسلط الضوء على أهم صور السلوك الإجرامي في مجال الجرائم المعلوماتية ثم نحاول بيان أهم الوسائل و الأدوات التي يستخدمها المجرم المعلوماتي في تنفيذ جرائمه.

أولا: صور السلوك الإجرامي الماسة بأنظمة المعالجة الآلية للمعطيات

تنص المادة 394مكرر قانون العقوبات:"... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك،

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة،

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة...".

كما تنص المادة 394 مكرر 1 قانون العقوبات:" ...كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

---

[4]– للتفصيل أكثر حول مجالات الجريمة الإلكترونية أنظر: د.نعيمة داودي: الجريمة الإلكترونية(خصائصها و مجالات استخدامها، و أهم سبل مكافحتها)، مجلة مهد اللغات، كلية اللغات الأجنبية، جامعة حسيبة بن بوعلي الشلف، الجزائر،المجلد2 العدد01 2020 ،ص49 وما بعدها.

[5]– المواد 394 مكرر و ما بعدها من الأمر 66–156 المؤرخ في 08يونيو1966 المتضمن قانون العقوبات المعدل و المتمم بموجب القانون04–15 المؤرخ في 10نوفمبر2004.

[6]–القانون09–04 المؤرخ في 05 غشت2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، ج ر عدد47 الصادرة في 16غشت 2009 .

تنص أيضا المادة 394 مكرر 2 قانون العقوبات:"... كل من يقوم عمدا وعن طريق الغش بما يأتي: 1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

من خلال النصوص القانونية السالفة الذكر يمكن أن نصنف السلوك الإجرامي في جرائم المساس بأنظمة المعالجة الآلية للمعطيات أو غيرها من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال [7] إلى أربعة أصناف رئيسية:

1/ الدخول أو البقاء غير المشروع في نظام معالجة آلية للمعطيات: يعني الدخول كافة الأفعال التي تسمح بالولوج إلى منظومة معلوماتية [8]، ويتحقق بالوصول إلى المعلومات و البيانات المخزنة فيها بطريقة غير مشروعة[9]، أي مخالفة لشروط الدخول التي ينص عليها القانون و الإتفاق أو دون إذن أو بمخالفة إرادة صاحب الحق في السيطرة على تلك المنظومة.

أما البقاء فيقصد به البقاء غير الشرعي في المنظومة المعلوماتية، أي التواجد داخل المنظومة ضد إرادة من له الحق في السيطرة عليها، و قد يقترن البقاء غير الشرعي بالدخول غير الشرعي، أو الدخول الشرعي مع تجاوز حدود الحق في البقاء، أو البقاء في حالة الدخول عن طريق الخطأ دون غش [10]، إذ يتعين في هذه الحالة مغادرة المنظومة فور إدراك تحقق الدخول غير المقصود.

2/ الإتلاف غير العمدي للمعطيات: يتمثل السلوك الإجرامي في هذه الحالة فضلا عن الدخول أو البقاء غير المشروع في المنظومة المعلوماتية أن ينتج عن ذلك ودون قصد إحداثها مايلي:

- حذف المعطيات المعلوماتية وإزالتها نهائيا،
- تغيير المعطيات المعلوماتية أي المساس بحالتها الأصلية،
- تخريب نظام اشتغال المنظومة بجعلها غير قادرة على أداء وظيفتها أو تقليل آدائها و كفائتها.

---

[7]- حسب المادة 02/أ من القانون 09-04 يقصد ب:" الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،"

[8]- عرف المشرع الجزائري المنظومة المعلوماتية من خلال المادة 02 /فقرة ب من القانون 09-04 بأنها:" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،"

[9]- بن علية بن جدو: تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن الإنساني، السنة السابعة، المجلد07، العدد02، جويلية 2022، ص304.

[10]- جدي نسيمة: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014، ص 53.

3/ المساس العمدي بالمعطيات:

خلافا للصورة السابقة، فالمساس بالمعطيات المعلوماتية يكون عمديا، إذ يقصد المجرم المعلوماتي من وراء نشاطه الإجرامي تحقيق النتيجة الإجرامية، المتمثلة في تغيير الحالة الأصلية التي كانت عليها المعطيات المعلوماتية محل الإعتداء بشكل يمس بسلامتها وتكاملها وذلك بإتيان أحد الأفعال التالية:

– **إدخال معطيات جديدة للمنظومة المعلوماتية** سواء قام بهذا الفعل شخص غير مرخص له بالدخول لنظام المعالجة الآلية أي دخوله لها غير مشروع، أو كان من الأشخاص المسموح لهم بالدخول ولكنه تجاوز حدود مهامه وقام بإدخال معطيات خاطئة، في ذات السياق اعتبر المشرع الجزائري استخدام الشخص شهادة التصديق الإلكتروني الخاصة به لغير الأغراض التي منحت من أجلها جريمة يعاقب عليها القانون[11].

– **إزالة معطيات موجودة داخل نظام المعالجة الآلية للمعلومات** بأي طريقة كانت، سواء بإخفاء المعلومات وحجبها عن صاحبها الشرعي بحيث لا يتمكن من استعمالها، أو بإزالتها نهائيا من النظام مع احتفاظ الجاني بها أو تبديدها.

– **تعديل المعطيات الموجودة داخل المنظومة المعلوماتية** كليا أو جزئيا أو استبدالها بأخرى، أو إمداد المنظومة بمعطيات مغايرة عن تلك التي صممت لأجلها.

يكفي إدخال معطيات لنظام المعالجة الآلية أو إزالتها أو تعديلها كليا أو جزئيا وبأي شكل كان لتحقق الفعل الإجرامي، غير أن نسخ البيانات ولو بصفة كلية لا يعتبر من قبيل المساس العمدي بالمعطيات حسب المشرع الجزائري[12].

4/ التعامل في المعطيات غير المشروعة:

من خلال نص المادة 394 مكرر2 من قانون العقوبات يتضح لنا أن المشرع حدد على سبيل الحصر المحل الذي ينصب عليه الفعل الإجرامي من جهة، و الأفعال المجرمةمن جهة أخرى.

فمحل الجريمة يتمثل إما في: – معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن تستخدم في ارتكاب أحد جرائم المساس بأنظمة المعالجة الآلية للمعطيات،

– معطيات متحصل عليها من أحد الجرائم المنصوص عليها في المواد 394 مكرر،394 مكرر1.

أما الأفعال المجرمة فتتمثل في: – التعامل في معطيات صالحة لإرتكاب جريمة معلوماتية بكافة أشكال التعامل السابقة على استعمالها و المتمثله حصرا في(التصميم، البحث، التجميع، التوفير، النشر،الإتجار).

– التعامل في معطيات متحصل عليها من أحد جرائم المعالجة الآلية للمعطيات وذلك بإتيان أفعال وردت على سبيل الحصر (الحيازة، الإفشاء، النشر، الإستعمال)، في ذات السياق نص المشرع الجزائري على أن

[11]– أنظر المادة 74 من القانون رقم 15–04، الصادر ب01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، الجريدة الرسميةعدد06، 10فبراير 2015.

[12]– جدي نسيمة: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014، ص 64 وما بعدها.

مجرد حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع الكتروني موصوف خاصة بالغير جريمة يعاقب عليها القانون[13].

ثانيا: الأدوات المستخدمة في الجرائم المعلوماتية

لا يمكن حصر الأساليب و الأدوات التي يلجأ إليها المجرم المعلوماتي فقد يستخدم وسائل مادية تقليدية بسيطة كالسطو والاستيلاء المادي على التجهيزات، وقد يلجأ إلى أدوات تقنية أكثر تعقيدا يصعب أحيانا إكتشافها أو التنبؤ بها، ولا يسعنا في هذا المقام الإلمام بكافة تلك الأساليب والأدوات الإجرامية، لذلك سنركز على أهمها فقط، فنتناول أولا أسلوب الهندسة الإجتماعية ثم نتطرق إلى البرمجيات الخبيثة.

1/الهندسة الإجتماعية: تعتمد هذه الطريقة على خداع واستغلال الآخرين، ولا تحتاج أنيمتلك المجرم خبرات تقنية عالية، ويمكن تعريفها بأنها استخدام المجرم حيلا نفسية لخداع مستخدمي الحاسوب ليمكنوه من الوصول إلى أجهزتهم أو المعلومات المخزنة فيها، أو هي نوع من التقنيات التي يستخدمها المجرمون الإلكترونيون بهدف استدراج المستخدمين غير المرتابين لإرسال بياناتهم السرية، و إصابة حواسيبهم ببرامج ضارة أو فتح روابط إلى مواقع مصابة[14]، ومن ثمة يسهل عليه تنفيذ إعتدائه على معلوماتهم وأموالهم.

تحتل الهندسة الإجتماعية مكانة مرموقة من بين الوسائل و الأدوات التي يستخدمها المجرم المعلوماتي في تنفيذ جرائمه و مرد ذلك إلى أن :

– الهندسة الإجتماعية من أنجع وسائل المجرم المعلوماتي لسهولتها مقارنة بالوسائل التقنية الأخرى .

– المختصين في أمن المعلومات ومستخدمي الحاسوب على اختلافهم لا يعيرون الهندسة الاجتماعية اهتماما كبيرا[15].

أ– وسائل و أساليب الهجوم باستخدام الهندسة الإجتماعية:

تتضمن أغلب الهجمات في الجرائم المعلوماتية صورة أو أكثر من صور الهندسة الإجتماعية، هذه الأخيرة تتنوع و تتزايد باستمرار كلما تم اكتشافها و التصدي لها، وعموما يمكن إيج از أهم الوسائل المستخدمة و الأساليب التي تتخذها الهندسة الإجتماعية في النقاط التالية:

وسائل الهندسة الإجتماعية:

فضلا عن الأجواء النفسية المناسبة التي يسعى المجرم المعلوماتي لخلقها من أجل إيهام الضحية بأن المهاجم شخصية موثوق بها، ولديها صلاحية الإطلاع على المعلومات الحساسة و الخصوصية للشخص أو المنشأة المستهدفة، يستخدم المجرم بعض الوسائل المادية لتنفيذ مخططه الإجرامي يمكن إيجازها في النقاط التالية:

---

[13]– أنظر المادة 68 من القانون رقم 15–04

[14]– الهندسة الإجتماعية مقال منشرو على موقع me.kaspersky.com/resource–center/definition/what –is– social– engineering.

[15] – د.خالد بن سليمان الغثير/ د. مهندس. محمد بن عبد الله القحطاني: أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، جامعة الملك سعود، الطبعة الأولى 2009، ص32.

1-الإنترنت: غالبا ما يلجأ مستخدمي الإنترنت إلى استخدام كلمة مرور يسهل تذكرها للولوج إلى مختلف التطبيقات التي تتطلب كلمة مرور كالبريد الإلكتروني ، مواقع التجارة الإلكترونية، البنوك الإلكترونية و غيرها، ويلجأ عامة المستخدمين إلى استخدام نفس كلمة المرور بالنسبة لكل التطبيقات خشية نسيانها. فإذا ما تمكن المجرم من الحصول على كلمة المرور تلك، أصبح من السهل الولوج إلى تطبيقات الضحية و الإستيلاء على ما يشاء من معلوماته و أمواله.

للحصول على كلمة المرور يلجأ المجرم إلى إنشاء مواقع مزيفة توحي للضحية من خلال التصميم أو المظهر أو الوظيفة أنها جهة موثوق بها كنظام تشغيل أو متصفح انترنت أو كبنك أو هيئة حكومية، أو يتم إرسال رسالة إلى البريد الإلكتروني للضحية ذات محتوى مخادع يحاول من خلاله المجرم حث الضحية على اتخاذ إجراءات لا يجريها عادة إلا مع جهة موثوقة، مثال ذلك مشاركة كلمة المرور أو إعادة تعيينها، الإتصال بفريق الدعم الفني، تنزيل برنامج أو تحديثات، قد تظهر الهندسة الإجتماعية أيضا في مواقع موثوقة بين عموم المستخدمين وذلك شكل إعلانات مرئية أو إعلانات توجيهية لصفحات مزيفة[16].

2-الهاتف: أكثر ما يستخدم المجرم المعلوماتي الهاتف مع صنف خاص من الضحايا كالعاملين في مراكز تقديم الدعم الفني (Help Desk)، يتصل المجرم بالضحية هاتفيا طالبا منه بعض المعلومات الفنية ويستدرجه في الحصول على المعلومات ككلمات المرور وغيرها ومن ثم يسهل عليه إتمام جريمته و شن هجومه على حواسيب المنشأة المستهدفة[17].

3-الولوج إلى أماكن العمل : يتسلل المجرم إلى أماكن العمل منتحلا صفة موظف أو متعاقد أو عامل نظافة أو صيانة، وبتمكنه من ذلك يستطيع جمع ما امكن من كلمات المرور التي عادة ما يقوم الموظفون بإلصاقها على شاشة الحاسوب أو لوحة المفاتيح وغيرها من الأماكن، أو عن طريق التحاور مع الموظفين ومعرفة معلومات كاسم الأم، وعدد أفراد الأسرة ،واسم المدرسة الثانوية، ثم استغلال هذه المعلومات في استرجاع كلمات المرور من المواقع التي توفر خدمة استرجاع كلمات المرور من معرفة الإجابة على هذه الأسئلة[18].

4-جمع النفايات الورقية : لا غرابة في ذلك فقد يتحصل من خلالها على معلومات قيمة، كلمات مرور، ارقام هواتف، مواعيد اجتماعات، نسخ من التقارير النهائية للاجتماعات، مراسلات بين مختلف المصالح وغيرها و التي قد يستخدمها في تنفيذ فعله الإجرامي أو في الحصول على معلومات أخرى تسهل مخططاته.

أساليب الهجوم باستخدام الهندسة الإجتماعية:

---

[16]- developers.google.com/search/docs/advanced/security/social- engineering

[17]- د.خالد بن سليمان الغثير/ د. مهندس. محمد بن عبد الله القحطاني: أمن المعلومات بلغة ميسرة، المرجع السابق، ص35.

[18] - نورة محمد عبد الرحمان الراشد: قضايا أمن المعلومات في التجارة الإلكترونية، مركز التميز لأمن المعلومات، المقالات العلمية، جامعة لملك سعود، ص03.

تتعد أساليب الهندسة الإجتماعية المستخدمة في تنفيذ الجرائم المعلوماتية و تتطور بوتيرة سريعة حتى تبقى الهوة واسعة بين الإجرام المعلوماتي و آليات مكافحته، غير أنه يمكن إيجاز أهم تلك الأساليب في النقاط التالية:

1-أسلوب الإقناع: للوصول إلى النتيجة الإجرامية قد يستعمل المجرم المعلوماتي أسلوب الإقناع المباشر عن طريق محاورة الضحية و مجابهته بحجج منطقية مستغلا ضعف معارفه التقنية و التحايل عليه للوصول إلى مبتغاه.

قد يتخذ كذلك أسلوب الإقناع غير المباشر بالتأثير على نفسية الضحية عن طريق بث مشاعر الخوف و الحماس ليسهل فيما بعد إقناعها بتقديم المعلومات اللازمة، وفي سبيله لذلك ينتهج بعض الأساليب و الأفعال من أهمها:

أ-الظهور بمظهر صاحب السلطة : لأنه في الغالب يسعى الناس لتلبية طلبات ذي السلطة حتى إن لم يكن موجودا.

ب-الإغراء بامتلاك شيء نادر أو ثمين : تجمع الدراسات في مجال علم النفس الإجتماعي أن رغبة الناس في امتلاك شيء ما تزداد كلما شعروا أن قدرتهم على امتلاكه مستقبلا اصبحت محدودة، يستغل المجرم المعلوماتي هذا السلوك فيعرض في موقعه عروضا بتقديم أدوات مساعدة مجانية كالوصول المجاني إلى الإنترنت أو إتصالات الهاتف المحمول، فرصة تنزيل منشئ بطاقات الإئتمان، محتوى إباحي، الحصول على قسيمات شراء من متاجر الكترونية، و غيرها من المحتويات المغرية و التي يصاحبها شرط أن إمكانية الإستفادة من هذه العروض لفترة محدودة و الإشتراك في الموقع بإدراج اسم المستخدم و كلمة المرور، وهنا تقع الضحية في شباك المجرم المعلوماتي[19].

2-أسلوب انتحال الشخصية: في مجال الهندسة الإجتماعية قد ينتحل المجرم شخصية حقيقية أو وهمية تتمتع بالقبول لدى الضحية المستهدفة وعادة ما يتم انتحال شخصية فني صيانة معدات الحواسيب و الشبكات ، عمال النظافة، طرف ثالث مخول من الإدارة العليا في الهيئة أو المؤسسة، و تقمص الشخصية أمر سهل خاصة في الشركات و الهيئات الكبرى التي لا يعرف أفرادها بعضهم بعضا، ما يسهل الوصول إلى المعلومات السرية المطلوبة.

3-أسلوب المداهنة: تؤكدالدراسات في علم النفس الإجتماعي أن الموظف أو العضو في تجمع نعين يسعى بكل السبل لخلق صورة حسنة عن أنفسهم لدى رؤسائهم في العمل، لذلك فإن انتحال المجرم المعلوماتي لشخصية تتمتع بالسلطة داخل ذلك التجمع أو الهيئة سيؤتي بثماره حتما فلن يتردد أغلب الموظفين في تقديم المعلومات التي يطلبها صاحب السلطة او المقرب منه المزيف.

4-أسلوب الهندسة الإجتماعية العكسية : تمثل إحدى أنجع الطرق في كسب صفة المستهدف من الجريمة المعلوماتية، تتلخص هذه الطريقة في خلق المشكلة أو الموقف، ثم ظهور المجرم في صورة صاحب السلطة

---

[19]- الهندسة الإجتماعية مقال منشرو على موقع: me.kaspersky.com/resource-center/threats/malware-social- engineering.

الإدارية أو الفنية وذو المعرفة و الأهلية للتعامل مع الموقف ، فيتوجه إليه الضحايا المستهدفون بطلب المساعدة و يتلقون منه التعليمات، فيكسب ثقتهم و يتمكن من الحصول على المعلومات المطلوبة.

مما سبق يتضح أن الهندسة الإجتماعية تعتبر أسهل الأساليب و أكثرها فعالية ونجاعة في تحقيق المجرم المعلوماتي لنشاطه الإجرامي، ذلك أنها تهاجم العنصر البشري الذي يمثل الحلقة الضعيفة في منظومة حماية المعلومات.

2/البرمجيات الخبيثة[20]

برامج يتم إنشاؤها و تجهيزها لأغراض غير مشروعةكإلحاق الضرر بالحاسوب أو تعطيله، جمع المعلومات و التجسس و عرقلة العمليات، أو استنزاف الموارد (الوقت، المعالج، الذاكرة، وحدة التخزين، سعة النقل الشبكي...الخ)[21].

تستخدم البرمجيات الخبيثة لتحقيق أهداف غير مشروعة تتراوح بين:

– التجسس الصريح و سرقة المعلومات كالأسرار الصناعية و التجارية للشركات بل وحتى الدول المنافسة .

– الإنتقام من المنافسين في سوق البرمجيات كالحرب التي يشنها أفراد و شركات ضد شركة مايكروسوفت لإستحواذها على سوق البرمجيات.

– الإبتزاز فبعد السيطرة على المنظومة المعلوماتية للضحية يبتزها المجرم الإلكتروني و يساومها على تلك المعلومات.

تتعدد طرق إصابة الحواسيب بالبرمجيات الخبيثة يمكن إيجازها فيما يلي:

–وسائط التخزين الخارجية على اختلافها،

–البريد الإلكتروني: يعد أهم نواقل البرمجيات الخبيثة نظرا لسهولة العملية، فقد ينتقل عبر مرفقات الرسالة بمجرد فتحها فيصاب جهاز الضحية و يمكن أن يقوم البرنامج الخبيث بإعادة ارسال تلك الرسالة لجميع جهات الإتصال الخاصة بك على أنها مرسلة من قبلك.

قد ينتقل عن طريق مجرد قراءة الرسالة، عن طريق رابط في الرسالة .

– تحميل برامج من الإنترنت خاصة البرامج المجانية فقد تحوي السم في العسل.

أنواع البرمجيات الخبيثة:

تتعدد البرمجيات الخبيثة و تتزايد أنواعها وخطورتها، كلما تم التصدي للسلف ظهر خلف جديد أشد ضراوة وأكثر فتكا،وعموما يمكن تقسيم أنواع البرمجيات الخبيثة إلى أربعة أنواع رئيسة نتناولها على التوالي:

1/ الفيروسات و أشباهها:

[20] – د. راضية حميدة، الجريمة لإلكترونية عبر مواقع التواصل الإجتماعي...نحو تفعيل دور الأمن السيبراني المعلوماتي، مجلة الإعلام و المجتمع، المجلد 05، العدد02، ديسمبر2021،ص344.

[21]– جميل حسن طويله: البرمجيات الخبيثة، نشر تحت رخصة المشاع الإبداعي، دون سنة نشر، ص 10، كتاب – البمجيات– الخبيثة– noor–book.com/pdf

- **الفيروسات Viruses:** عبارة عن برامج خبيثة يتم إعدادها و تطويرها من أجل إصابة الحواسيب و تدمير الأنظمة المعلوماتية [22]، و تنتقل بالطرق المشار إليه آنفا بالإعتماد على ملفات أخرى و تتميز بقدرتها الهائلة على التدمير بشكل لا يمكن معه إسترجاع البيانات فقد يتم مسحها نهائيا أو تغييرها وتتعدد أنواع الفيروسات بشكل لا يمكن حصره[23].
- **الديدان Worms** : برمجيات خبيثة و مضرة تتميز عن الفيروسات باعتمادها على نفسها للتكاثر و سرعة الإنتقال و صغر الحجم، لا تحدث أضرارا مباشرة في البيانات، بل تتكاثر كالبكتيريا و تنتج نسخا منها لتشغل أكبر مساحة في ذاكرة التخزين بما يؤثر سلبا على كفاءة و فعالية الأجهزة و النظام المعلوماتي المرتبطة به[24].
- **الخداع أو البلاغ الكاذب Hoax:** البلاغ الكاذب عن ظهور فيروسات يبث الرعب في نفوس المستخدمين و يضيع أوقاتهم، في نشره أحد الأشخاص و يساعده كل من صدق الخبر و أعاد نشره بغرض المساعدة على لتصدي للفيروس أو الدودة [25]، فكل من يقوم بفتح الرسالة التحذية الكاذبة و يتبع خطوات فحص مدى إصابة جهازه أو نظامه المعلوماتي سيصاب حتما.

2/ الأحصنة الطروادية TrojanHorses[26]: من أخطر البرمجيات الخبيثة ذلك أنه يتخذ مظهر الصديق النافع كبرنامج عادي يؤدي أعمال مألوفة بينما في الحقيقة يضمر أعمالا خبيثة، حيث ينفذ بصفة خفية أوامر و تعليمات تؤدي عند إعادة التشغيل إلى أضرار غير متوقعة، وهو عكس الفيروسات و الديدان لا يتكاثر، ولكن يكمن في النظام بشكل خفي.

قد يحاول استغلال حاسوب الضحية لشن هجوم على حواسيب و أنظمة معلوماتية أخرى، أو يقوم بالتجسس من خلال الإحتفاظ بجميع ما قام الضحية بإدخاله عن طريق لوحة المفاتيح، و التي قد تحتوي بيانات على قدر من الأهمية كأرقام بطاقة الائتمان أو كلمات المرور الخاصة بحسابات الضحية.

توجد انواع عديدة من الأحصنة الطروادية، تختلف تسمياتها غير أنه يمكن تصنيفها من خلال وظائفها إلى مايلي:

---

[22]– أ.د. هدى حامد قشقوش: الإتلاف غير العمدي لبرامج و بيانات الحاسب الإلكتروني، مؤتمر القانون والكمبيوتر و الإنترنت،1-3 مايو 2000، كلية الشريعة و القانون، جامعة الإمارات العربية المتحدة، المجلد الثالث، الطبعة الثالثة 2004، ص898.

[23]– عدد الفيروسات المعروفة حسب إحصائيات 2004 يقدر بأكثر من 100.000، F-Secure Coropration's Data SecuitySummary for 2005

[24]– جدي نسيمة: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014، ص 34.

[25]– د.خالد بن سليمان الغثير/ د. مهندس. محمد بن عبد الله القحطاني: أمن المعلومات بلغة ميسرة، المرجع السابق، ص66.

[26] – سميت بهذا الإسم نسبة إلى أسطورة قديمة مفادها أن جيش إحدى مدن الإغريق أهدى أعدائهم حصانا خشبيا كبيرا كعربون سلام والذي كان يحمل بداخله غراة دخلوا المدينة واستولوا عليها.

– **معطل البرامج** : يقوم هذا النوع بتعطيل البرامج الحساسة خاصة كبرامج جدران الحماية و مكافحة الفيروسات.

– **مرسل البيانات :** يعمل على إرسال بيانات خاصة بالضحية إلى المجرم المعلوماتي بصفة سرية كأرقام بطاقات الائتمان و كلمات المرور و المحادثات المكتوبة.

– **التحكم عن بعد :** يسمح للمجرم بالتحكم في جهز الضحية عن بعد و سلب ما يريد من معلومات بشكل مخفي.

– **الوسيط:** يسخر حاسوب الضحية وسيطا لمهاجمة حواسيب أخرى عن طريق الوصول المتخفي للإنترنت، ثم يقوم بتنفيذ نشتطه الإجرامي و يتحمل الضحية المسؤولية باعتبار حاسوبه آخر نقطة يمكن تتبع العملية إليها[27].

3/ الإصطياد الإلكتروني phishing:يتمثل هذا النوع من البرامج الخبيثة في رسائل تبدو عادية و مرسلة من جهة حقيقية،تتضمن روابط لمواقع إلكترونية مزيفة تدعي أنها تقدم سلع وخدمات، أو تكون لمواقع إلكترونية مزيفة تدعي أنها بنوك وتقدم خدمات بنكية، ونظرا مواقع مقلدة بصورة دقيقة وتشابه كبير مع المواقع الحقيقية يسها خداع الضحية و إيهامها أن الموقع حقيقي، فيطلب منه ادخال بيانات مهمة كأرقام بطاقة الائتمان أو كلمات مرور، بمجرد إدخالها يقوم المجرم الإلكتروني بتحويل الضحية إلى الموقع الحقيقي[28] بعد أن يكون قد سلب منه ما يريد من معلومات.

4/ البرامج التجسسيةSpyware : [29]

عبارة ن برامج خبيثة يتم تنصيبها في جهاز الضحية دون علمه بهدف التجسس على كل سلوكياته على الحاسوب وعلى الشبكات كالكتابات و كل المواقع التي يزورها، تقلل تلك البرمجيات من فاعلية جهاز الضحية إذ تعمل على استنزاف قدراته التخزينية و سرعته في تبادل البيانات و معالجتها، و من أهم البرامج التجسسيةنذكر ما يلي:

– **برامج تسجيل نقرات لوح المفاتيح:** برامج تثبت في جهاز الضحية أو قطع الكترونية تزرع بين الوصلة التي تربط الوحدة الأساسية للكمبيوتر بلوحة المفاتيح، تسوق على أساس أنها برامج رقابة أبوية، غير أنها تنطوي برامج خبيثة تقوم بتسجيل كل حرف يكتبه الضحية على جهازه بغرض الاستيلاء على بياناته الخصوصية من أرقام الهاتف، بيانات الحسابات البنكية، دردشات نصية، رسائل البريد الإلكتروني، كلمات المرور وغيرها.

---

[27]– د.خالد بن سليمان الغثير/ د. مهندس. محمد بن عبد الله القحطاني: أمن المعلومات بلغة ميسرة، المرجع السابق، ص70،71.

– جميل حسن طويله: البرمجيات الخبيثة، المرجع السابق، ص33.

[28]– د.خالد بن سليمان الغثير/ د. مهندس. محمد بن عبد الله القحطاني، نفس المرجع السابق، ص73،

– نورة محمد عبد الرحمان الراشد: قضايا أمن المعلومات في التجارة الإلكترونية، المرجع السابق، ص03.

[29]– جميل حسن طويله: البرمجيات الخبيثة، المرجع السابق، ص70.

– **برامج الإعلانات:**برمجيات خبيثة تتجسس على السلوك الاستهلاكي للضحية بغرض خلق إعلانات تجارية لحثه على التسوق من مواقع معينة و التأثير في إرادته من أجل اقتناء سلع أو خدمات معينة دون غيرها، فضلا عن كون هذه الإعلانات المزعجة تقلل من أداء الجهاز المصاب وتجعله عرضة للإصابة ببرمجيات خبيثة أخرى.[30]

خاتمة:

ختاما يمكن القول يمكن أن غاية تحقيق الأمن المعلوماتي مسألةصعبة، نظرا لتشعب وتعدد مظاهر وصور السلوك الإجرامي في هذا المجال وتطور الأدوات التقنية المستخدمة في الجرائم المعلوماتية، فالنصوص القانونية يجب أن تواكب سرعة التطور في السلوك الإجرامي بغية مكافحة الجرائم المعلوماتية تحقيقا للغاية المنشودة.

توصلنا من خلال بحثنا المتواضع إلى جملة من النتائجيمكن إيجازها في النقاط التالية:

– اعتبر المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من قبيل الجرائم الواقعة على الأموال وجرم الصور الشائعة من الجرائم المعلوماتية .

– وسع المشرع الجزائري من نطاق تطبيق القانون 09-04 المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها لتطبق أحكامه على كل ما يستجد من جرائم الكترونية ترتكب أو يسهل ارتكابها عن طريق الاتصالات الإلكترونية.

– أكثر الوسائل استخداما من قبل المجرمين في هذا المجال هي وسائل و أدوات تقنية على درجة عالية من التطور و التعقيد يصعب اكتشافها وتطويقها نظرا لتطويرها وتحديثها باستمرار .

كمايمكنتسجيلبعضالملاحظاتوالاقتراحاتنوجزهافيالنقاطالتالية:

–ضرورة إعادة النظر في النصوص القانونية وتحديثها بما يتماشى مع التطور الرهيب في الإجرام الإلكتروني خاصة مع التوجه نحو الرقمنة في مختلف القطاعات والاعتماد على الإتصالات الإلكترونية في مختلف مناحي الحياة.

– ضرورة توعية جمهور المستخدمين لمختلف المنظومات المعلوماتية بالمخاطر التي تتربص مصالحهم خاصة الاقتصادية، للتمكن من الوقاية منها و الحد من آثارها.

– تعزيز الحماية التقنية لمختلف المنظومات المعلوماتية(المنظومة البنكية خصوصا) بأحدث البرمجيات و أكثرها فعالية للتصدي لهجمات البرامج الخبيثة .

[30]– د.خالد بن سليمان الغثير/ د. مهندس. محمد بن عبد الله القحطاني، المرجع السابق، ص78.

قائمة المراجع:

أولا: النصوص القانونية:

1. الأمر 66-156 المؤرخ في 08يونيو1966 المتضمن قانون العقوبات المعدل و المتمم.

2- القانون09-04 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها

3- القانون رقم 15-04، الصادر ب01 فبراير 2015، **يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين**، الجريدة الرسميةعدد06، 10فبراير 2015.

ثانيا: المؤلفات:

1 - د.خالد بن سليمان الغثير/ د. مهندس. محمد بن عبد الله القحطاني: أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، جامعة الملك سعود،المملكة العربية السعودية، الطبعة الأولى 2009

2 - جميل حسن طويله: البرمجيات الخبيثة، نشر تحت رخصة المشاع الإبداعي، دون سنة نشر

ثالثا: الرسائل الجامعية.

1- جدي نسيمة: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014.

رابعا: المقالات.

1- د. ممدوح عبد الحميد عبد المطلب: جرائم استخدام شبكة المعلومات العالمية " جرائم الإنترنت"، مؤتمر القانون والكمبيوتر و الإنترنت،1-3 مايو 2000، كلية الشريعة و القانون، جامعة الإمارات العربية المتحدة، المجلد الأول، الطبعة الثالثة 2004.

2-. نورة محمد عبد الرحمان الراشد: قضايا أمن المعلومات في التجارة الإلكترونية، مركز التميز لأمن المعلومات، المقالات العلمية، جامعة لملك سعود، المملكة العربية السعودية.

3-أ.د. هدى حامد قشقوش : الإتلاف غير العمدي لبرامج وبيانات الحاسب الإلكتروني، مؤتمر القانون والكمبيوتر والإنترنت، 1-3 مايو 2000، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثالث، الطبعة الثالثة 2004.

4- د.نعيمة داودي: الجريمة الإلكترونية(خصائصها و مجالات استخدامها، و أهم سبل مكافحتها)، مجلة مهد اللغات، كلية اللغات الأجنبية، جامعة حسيبة بن بوعلي الشلف، الجزائر،المجلد2 العدد01 2020 .

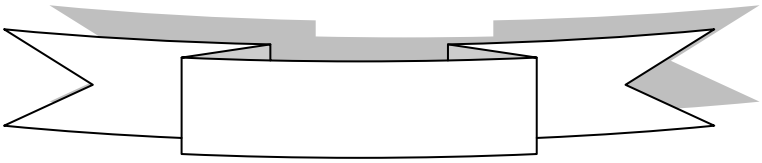
5- بلعيدإلهام،الجرائمالمستحدثة،مجلةالباحثللدراساتالأكاديمية،المجلد 09،العدد02 جوان2022.

6- بنعلية بنجدو: تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن الإنساني، السنة السابعة، المجلد07،العدد02، جويلية 2022،ص304.

7- د. راضية حميدة، الجريمة الإلكترونية عبر مواقع التواصل الإجتماعي...نحو تفعيل دور الأمن السيبراني المعلوماتي، مجلة الإعلام والمجتمع، المجلد 05،العدد02.ديسمبر2021، ص344.

خامسا : المواقع الإلكترونية.

1- الهندسة الإجتماعية مقال منشرو على موقع me.kaspersky.com/resource-
center/definition/what –is- social- engineering.
2developers.google.com/search/docs/advanced/security/social- engi - 3
3- الهندسة الإجتماعية مقال منشرو على موقع:me.kaspersky.com/resource-
center/threats/malware- social- engineering.
4-F-Secure Coropration's Data Secuity Summary for 2005



نورة جحايشية
djehaichianoura@gmail.com
جامعة 8 ماي 1945–قالمة

وفاء عزالدين
Zed.wafa@yahoo.fr
جامعة 8 ماي 1945–قالمة

الحماية الموضوعية للنظام المعلوماتي في التشريع الجزائري

الملخص

يسعى المشرع الجزائري كعادته إلى مواكبة التطورات الحاصلة في شتى المجالات بصفة عامة، وفي مجال المعلوماتية بصفة خاصة، حيث أنه في كل مرة يقوم سواء بتحيين النصوص القانونية القديمة، أو استحداث نصوص جديدة للتصدي لكافة أنواع الجرائم بالأخص تلك التي تحمل الطابع الالكتروني، والتي تفشت بكثرة في المجتمع الجزائري مؤخرا.

من خلال هذه الدراسة حاولنا التدقيق في آليات الحماية الموضوعية للنظام المعلوماتي في التشريع الجزائري، وذلك بالتركيز على كيفية مجابهة الجرائم الالكترونية سواء من خلال قواعد الملكية الفكرية أو عن طريق قواعد قانون العقوبات.

Abstract

As usual, the Algerian legislator seeks to keep abreast of developments in various fields in general, and in the field of informatics in particular, as each time it updates the old legal texts, or the development of new texts to address all types of crimes, especially those of an electronic nature, which are rampant in abundance. in Algerian society recently.

Through this study, we tried to scrutinize the objective protection mechanisms of the information system in the Algerian legislation, by focusing on how to confront electronic crimes, whether through intellectual property rules or through the rules of the Penal Code.

المقدمة

بظهور عصر التكنولوجيا أصبح العالم ككل يعتمد اعتماد كليا على التقنيات الحديثة عبر الانترنت، وأصبح من يجهل استخدامها بشكل سلس يطلق عليه مصطلح الأمي، كما قد أضحت المعلومة أهم شيء يمتلكه الانسان وهي الطفرة العلمية التي تعتبر معيار تقدم المجتمعات فيما بينها.

وبتطور أجهزة الحاسوب بشكل مستمر والتي تعتمد بشكل أساسي على برامج مختلفة، وباتت هذه الأخيرة تشكل ثروة حقيقية في يد مالكيها، حيث يسعى الجميع للحصول عليها، إذ أننا جميعا أصبحنا غير قادرين عن التخلي عن أجهزة الحاسوب ببرامجها في شتى تعاملاتنا اليومية.

إلا أن سوء استخدام مختلف فضاءات الانترنت أدى إلى ظهور العديد من الجرائم، يطلق عليها تسمية الجرائم الالكترونية،وفي البداية كان صعب التعامل معها، خاصة وأنها عابرة للحدود الجغرافية من جهة، وعدم سهولة تحديد فاعليها من جهة أخرى.

هذا ما أدى بكافة الحكومات إلى سن قوانين تنظم مختلف العمليات الالكترونية، وذلك في محاولة منهم إلى التحكم في شتى التعاملات والتصدي لأي مشكلة قد تؤدي إلى عواقب وخيمة.

وعلى ذات السياق سار المشرع الجزائري كونه حاول ضبط كافة التعاملات الالكترونية وتجريم أي فعل من شأنه أن يشكل جريمة الكترونية، لكنه في الغالب اعتمد اعتمادا شبه كلي على قواعد قانون العقوبات، باعتباره تشريعا عاما فيما يخص التجريم والعقاب، لكن هذا القانون أثبت قصوره في مواجهة بعض الجرائم المستحدثة، لكنه يبقى الأساس لتحديد أركان وشروط أي جريمة.

لهذا كان لابد من الاعتماد على مختلف نصوص قانون الملكية الفكرية سواء كانت الملكية الصناعية أو الملكية الأدبية والفنية، باعتبارها الأقرب لتنظيم مثل هذه التعاملات.

وفي هذه الدراسة سنحاول تحديد نقاط القوة ونقاط الضعف في مختلف النصوص القانونية التي تضبط النظام المعلوماتي في الجزائر، خاصة في مختلف جوانبه الموضوعية، انطلاقا من الإجابة على الإشكالية التالية: **ما مدى كفاية نصوص قانون الملكية الفكرية وقانون العقوبات في حماية النظام المعلوماتي في الجزائر؟**

المبحث الأول: الحماية المقررة في نصوص لملكية الفكرية للنظام المعلوماتي في الجزائر

من البديهي أن نصوص الملكية الفكرية تم إقرارها لحماية مختلف الحقوق الذهنية، وبالتالي جاءت لحماية أموالا معنوية غير مادية، وبما أن النظام المعلوماتي يعد معنويا أكثر منه مادي فهذا يعني أن حمايته تكون وفق نصوص قانون الملكية الفكرية.

لكن الاشكال الذي يثار هو أن المشرع الجزائري لم يحسم الأمر فيما يخص برمجيات الحاسوب هل تعتبر ضمن قواعد الملكية الصناعية أو قواعد الملكية الأدبية الفنية، وهذا ما سنحاول توضيحه في هذه الدراسة من خلال تناول مدى خضوع أنظمة الحاسوب الآلي لقواعد الملكية الصناعية في المطلب الأول، ودراسة مدى خضوعها لقواعد الملكية الأدبية والفنية في المطلب الثاني.

المطلب الأول: مدى خضوع برامج الحاسوب الآلي لقواعد الملكية الصناعية

تدخل ضمن قوانين الملكية الصناعية كافة المخترعات والابتكارات العلمية التي يتم اكتشافها حديثا والتي لم تكن معروفة من قبل، ولابد من أن يقدم هذا الاكتشاف إضافة في مجال التقنية، أو كما يقال عنه يجب أن يكون حل تقني لمشكل تقني[1].

وبالتالي فإن أي ابتكار أو اختراع جديد ولم يكن معروفا للجمهور من قبل، فمن البديهي أن يحظى بالحماية المقررة لأحد عناصر الملكية الصناعية، والمتمثلة في براءة الاختراع والعلامة التجارية بالإضافة إلى

الرسوم والنماذج الصناعية وغيرها، إلا أن برامج الحاسوب أقرب ما تكون من براءة الاختراع، باعتبار بعض التشريعات على غرار التشريع الأمريكي ضمنها القانون المتعلق ببراءة الاختراع.

وتحتل براءة الاختراع أهمية كبيرة من بين عناصر الملكية الصناعية والتجارية نظرا لدورها في تشجيع البحث العلمي والإبداع والابتكار الذي ينعكس دائما على التقدم الصناعي والتكنولوجي[2].

وفي هذا السياق يجب علينا التطرق إلى تعريف براءة الاختراع وكذا الاختراع في حد ذاته فقهيا وقانونيا حتى نتمكن من معرفة مدى إمكانية ادراج برامج الحاسوب لنظام براءة الاختراع من عدمه.

الفرع الأول: التعريف الفقهي

يعرف الاختراع بأنه: " **جهد بشري عقلي وعلمي يثمر في النهاية إنجازا جديدا مفيدا للإنسانية ويضيف إلى رصيدها ما يسد حاجة ويحقق أملا**"[3].

وعرّف أيضا بكونه :" **كل اكتشاف أو ابتكار جديد وقابل للاستغلال الصناعي سواء تعلق ذلك الاكتشاف أو الابتكار بالمنتج النهائي أو وسائل الإنتاج وطرقه**"[4].

أما الفقيه Paul mathely فقد عرف الاختراع بما يلي:

"L'invention résout un problème"[5].

كما تناوله أيضا الفقيه Yves Marcelin بالتعريف بأنه: L'invention comme une œuvre de l'esprit qui aboutit à quelque chose de nouveau dans le domaine de l'industrie"[6].

أما عن براءة الاختراع فقد تم تعريفها فقهيا بكونها: " الشهادة أو السند الذي يحدد الاختراع ويرسم أوصافه، ويمنح حائزه الحق القاصر عليه في استغلاله والحماية المقررة قانونا"[7].

كما تم تعريفها أيضا بكونها:

"Le brevet d'invention est un titre délivré par l'institut national de la propriété industrielle qui conforte un monopole d'exploitation de vingt ans [8]."

الفرع الثاني: التعريف القانوني

تناولت العديد من التشريعات تعريف كل من الاختراع وكذا براءة الاختراع، وفي هذه الدراسة حاولنا تناول أكثر التعريفات تداولا.

حيث عرّف التشريع الأردني في مادته الثانية من قانون براءات الاختراع رقم 32 لسنة 1999 على أنه: "أي فكرة إبداعية يتوصل إليها المخترع في أي من مجالات التقنية ويتعلق بمنتج أو بطريقة أو بكليهما تؤدي عمليا إلى حل مشكلة معينة في أي من هذه المجالات"[9].

أما فيما يخص التشريع الجزائري فقد عرّف الاختراع في الأمر 03-07 المتعلق ببراءة الاختراع بكونه:" فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية".

وقد حدد المشرع الجزائري صور الاختراع التي يمكنها أن تحظى بالحماية على سبيل الحصر وهي كالتالي:

- **اختراع منتوج:** وتم تعريفه بأنه إيجاد شيء مادي جديد ذي خصائص معينة يتميز بها عن سائر الأشياء المشابهة له، وتحدد تلك الخصائص إما بهيكلة ميكانيكية أو بتركيبة كيميائية خاصة[10].
- **اختراع طريقة:**ويقصد به إيجاد طريقة صناعية جديدة سواء تم ذلك بوسائل كهربائية أو ميكانيكية أو كيمياوية، مما يسمح بالحصول على شيء مادي يسمى المنتوج، أو أثر غير مادي يسمى النتيجة[11].

أما عن براءة الاختراع فقد قامت العديد من التشريعات بتعريفها، وفيما يلي سنحاول تناول أهمها.

قام المشرع السعودي بتعريف براءة الاختراع في المادة الثانية من نظام براءات الاختراع السعودي الصادر بمقتضى المرسوم الملكي رقم 38 لسنة 1989 على أنها: "الوثيقة التي تمنح للمخترع ليتمتع اختراعه بالحماية المقررة داخل المملكة العربية السعودية"[12].

وعرفها المشرع الفرنسي في المادة 611 من القانون رقم 92-597 الصادر بتاريخ 1 يوليو 1992 المتعلق بالملكية الفكرية المعدل بالقانون رقم 94-102 الصادر بتاريخ 5 فيفري 1994 بنصه على:" كل اختراع يمكن أن يكون محل سند ملكية صناعية مسلم من طرف مدير المعهد الوطني للملكية الصناعية، الذي يمنح لصاحبه أو للخلف حق الاستغلال الاستئثاري".[13]

أما بخصوص التشريع الجزائري فقد عرّف براءة الاختراع بكونها: "البراءة أو براءة الاختراع وثيقة تسلم لحماية اختراع".

وباستقراء كل هذه النصوص نجد أن مجال الملكية الصناعية من بين المجالات الحيوية وليست الجامدة في العالم، حيث أن كافة الدول المتطورة تقوم بتحيين قوانينها في فترات متقاربة وذلك لإضافة كل ما يظهر جديد في الساحة العلمية، وهو ما نفقده في الجزائر، باعتبار جل قوانين الملكية الصناعية لم تعدل منذ سنة 2003.

وحسب نصوص الامر 03-07 المتعلق ببراءة الاختراع نجد أن المشرع الجزائري لم يدرج برامج الحاسوب ضمن الحماية المقررة لبراءات الاختراع.

وبالتالي فإن برامج الحاسوب على الرغم من كونها تحقق كافة الشروط الازمة في الاختراع حتى يضمن بشهادة براءة الاختراع، إلا أن المشرع لم يدرجه ضمنها ويمكن القول أن المشرع الجزائري وكعادته تبع خطوات التشريع الفرنسي الذي أخرج برامج الحاسوب من دائرة الحماية المقررة لبراءة الاختراع.

المطلب الثاني: مدى خضوع برامج الحاسوب لقواعد الملكية الفنية والأدبية

تظهر قواعد الملكية الفنية والأدبية جلّية في حماية المؤلف والحقوق المجاورة، لهذا حاولنا من خلال هذه الدراسة تعريف حقوق المؤلف أولا ومن ثم تحديد مدى كفايتها لتحقيق الحماية المطلوبة لبرمجيات الحاسوب.

الفرع الأول: تعريف حق المؤلف

نظام الملكية الفكرية بشكل عام استقر مكانه بشكل بطيء، حيث أخذ الامر ثلاث قرونمن 1480-1800 على الساحة الوطنية (اوروبا الغربية بالأخص) ، كان يجب ان ننتظر الى غاية نهاية القرن التاسع

عشر حتى يتم عولمة قواعد الملكية الفكرية مع اتفاقية باريس و اتفاقية برن و مدريدمع جولة الارغواي لسنة 1986 تم فرض مسألة الملكية الفكرية على الساحة الدولية ، حيث ان هذه الجولات وصلت الى ابرام اتفاق حول محاور حقوق الملكية الفكرية التي تمس بالتجارة بتاريخ 14/04/1994ملحق باتفاقية مراكش المنشئة للمنظمة العالمية للتجارة و الذي عزز الأهمية الاقتصادية لحقوق الملكية الفكرية.

يعرف حق المؤلف بأنه حق من حقوق الملكية الفكرية المتعلقة بالإبداع ، ومحل حق المؤلف هو الابداعات الادبية والفنية،إذا فهذا الحق هو آلية قانونية لحماية تلك الابداعات بفضل الحقوق المادية والمعنوية التي يضمنها للمؤلف[14].

ولا ينظر لحق المؤلف على انه تعويض مادي مقابل ابداع فكري، بل هو نظام للاحتكار الحصري لفائدة صاحبه لكونه حق ملكية[15].

الفرع الثاني: الضبط التشريعي لبرامج الحاسوب ضمن حقوق المؤلف

اختار المشرع الفرنسي سنة 1985 بمناسبة تعديل قانون مارس 1957 المتعلق بالملكية الأدبية والفنية، أن تكون الحقوق المرتبطة ببرامج الاعلام الآلي حقوقا أدبية فنية محضة.

ولايزال الاجتهاد القضائي الفرنسي لهذا السبب لا يسمح بمنح براءة اختراع ليس في فرنسا فقط بل في كامل أوروبا، ولكن من المؤكد أن الأمر لن يبقى بهذا الشكل، خاصة أمام ضغط العديد من المؤسسات العاملة في هذا المجال.[16]

إلا أن المشرع الجزائري لحد الساعة لم يحدد موقفه ضمن برامج الاعلام الآلي حيث أنه حظر إمكانية حصولها على براءة اختراع، لكنه لم يوضح ما إذا كان صاحب هذه البرامج يحظى بالحماية المقررة في قواعد حقوق المؤلف والحقوق المجاورة.

المبحث الثاني: الحمايةِ المقررة في نصوص قانون العقوبات للنظام المعلوماتي في الجزائر

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتيةِ في أشكال جديدة من الإجرام، مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 [17] تحت عنوان المساس ب أنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانيةِ مواد من المادة 394 مكرر إلى 394 مكرر07

وبغرض تدارك الفراغ القانوني، فقد قام المشرع الجزائري بموجب القانون رقم 15/04 باستحداث جملة من النصوص والتي جرم من خلالها الأفعال المتصلة بالمعالجة الآليةِ للمعطيات، وحدد لكل فعل م نها ما يقابله من الجزاء ؛ إذ قام المشرع الجزائري بسن جمله من القواعد القانونيةِ الموضوعيةِ والتي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات، وما يقابلها من جزاء أو عقوبة وهذا ما سنتناوله ضمن هذا المبحث وفقا مطلبين

المطلب الأول: أنواع الجرائم المقررة في قانون العقوبات لمكافحه الجرائم الالكترونيةِ

ركزت إستراتيجية المشرع الجزائري في التصدي لظاهرة الإجرام المعلوماتي على القسم السابع مكرر من قانون العقوبات رقم 15/04 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وأقرت جمله من

القواعد القانونية الموضوعية حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة وتأخذ هذه الأفعال إما وصف الاعتداء على معطيات نظام المعالجة الآلية كما يمكن لها أن تأخذ وصف الاعتداء على سير نظام المعالجة الآلية .

الفرع الأول: تجريم الاعتداء على نظام المعالجة الآلية للمعطيات

جعل المشرع الجزائري من وجود نظام المعالجة الآلية شرطا أساسيا للبحث عن مدى تحقق الاعتداء أم لا ، فجريمة الاعتداء على نظام المعالجة الآلية للمعطيات تتحقق في صورتين هما : الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات ؛ وتتضمن جريمة الدخول والبقاء غير المرخص بهما في النظام، والصورة المشددة للاعتداء على نظام المعالجة الآلية للمعطيات.

أولا : الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات

1-الدخول غير المرخص : يقصد بفعل الدخول هنا هو الركن المادي لجريمة الاعتداء على نظام المعالجة الآلي للمعطيات، ذلك الدخول المعنوي أو الالكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي ولا يعد فعل الدخول بحد ذاته سلوكا غير مشروع وإنما يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص.[18]

ومن خلال نص المادة 394 مكرر من قانون العقوبات يلاحظ أن هذه المادة تعتبر جريمة الدخول غير المرخص به بمثابة جريمة شكلية، التي لا يشترط لقيام الركن المادي فيها تحقق مجرد الدخول إلى نظام المعالجة الآلي للمعطيات بأكمله أو إلى جزء منه فقط ؛ بشرط أن يكون فعل الدخول بدون ترخيص مقصودا وليس صدفة أو خطأ كما لا تشترط المادة 394 مكرر لتحقيق جريمة الدخول غير المرخص به إلى نظام المعالجة أن يكون هذا النظام محاطا بحماية فنية تمنع الاختراق كالتشفير مثلا بل جاءت عامة ومطلقة أي تحمي كل الأنظمة المعلوماتية من الاعتداء سواء كانت محمية فنيا أم لا [19]

2-البقاء غير المرخص: يقصد بالبقاء غير المرخص به في نظام المعالجة الآلية للمعطيات استمرارية التواجد داخل نظام المعالجة دون إذن من صاحبه أو من له السيطرة عليه، بمعنى آخر هو بقاء شخص داخل نظام المعالجة ملك الغير بعد الدخول إليه خطأ أو صدفة رغم علمه بأن بقائه فيه غير مرخص [20]

مع العلم أن هذا الركن المادي يمكن ان يظهر في صورتين هما:

الصورة الأولى: تتمثل في التحقق من فعل البقاء غير المرخص به داخل نظام المعالجة الآلية للمعطيات منفصلا عن فعل الدخول ؛ ويتجسد هذا عندما يكون فعل الدخول إلى نظام المعالجة مشروعا كأن يدخل الشخص صدفة أو خطأ إلى نظام ما؛ أي دون قصد ففي هذه الحالة يتعين على المتدخل أن ينسحب ويغادر فورا النظام أما إذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المرخص به.

الصورة الثانية : تتمثل في تحقق فعل البقاء غير المرخص به مجتمعا مع فعل الدخول ، ويتجسد هذا الوضع حينما يكون الدخول غير مشروع، كأن يدخل الجاني نظاما دون إذن مسبق من صاحب هذا الأخير ثم يستمر في البقاء داخله وهنا يتحقق الإجماع والتداخل المادي بين الجريمتين.

و يمكن لهذا التداخل المادي بين جريم ة الدخول والبقاء في نظام المعالج ة الآلية للمعطيات بدون ترخيص، أن يثير إشكالا قانونيا حول تحديد الحد الفاصل بين الجريمتين أو النطاق الزمني لكل واحدة منهما؛ بمعنى تحديد الوقت الذي تنتهي فيه جريم ة الدخول وتبدأ فيه جريم ة البقاء، ولقد استقر الفقه الجنائي في ما يخص هذه المسألة على أن بداية سريان جريم ة البقاء داخل النظام يكون منذ اللحظة التي يبدأ الجاني من التجول والتنقل داخل النظام، أما قبل هذه اللحظ ة سنكون أمام جريم ة الدخول غير المرخص به حتى و إن دخل الجاني النظام وبقي ساكنا فيه فترة طويلة من الزمن [21]

ثانيا: الصورة المشددة للاعتداء على نظام المعالجة الآلية للمعطيات

وتتحقق عندما يترتب عن فعل الدخول أو البقاء نتائج غير مشروعه ضد معطيات النظام، وقد نصت المادة 394 مكرر في فقرتها الثانية على أنه تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظوم ة ونلاحظ من خلال نص هذه الماد ة بأن المشرع الجزائري أورد ظرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية، بحيث يتحقق الظرف الأول إذا نتج عن الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام ، ويتحقق الثاني حينما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظوم ة وإعاقته عن أداء وظيفتهم، ولكي تتوفر الظروف المشددة المذكورة في المادة 394 مكرر فقره 02 لابد من إثبات وجود علاقة سببيه بين فعل الدخول أو البقاء غير المرخص به ، والنتيجة الإجرامية التي حددتها الماد ة في محو أو تعديل بيانات النظام أو تخريب تشغيل النظام ذاته و إلا كنا بصدد جريم ة في صورتها البسيط ة المذكورة في نص الماد ة 394 مكرر 01 من قانون العقوبات.

الفرع الثاني: الجرائم المعلوماتية الماسة بالأشخاص

أولا: تجريم الاعتداءات على حرمة الحياة الخاصة

حرصت القوانين في كافه الدول على صيانة الحياة الخاصة لكل المواطنين وذلك بالنص في دساتيرها وتشريعاتها على كفاله هذه الحماية من المساس بها؛ تطبيقا للمبادئ العالمية التي تدرس مبدأ حرية الإنسان في العيش فيه بهدوء وسكينه و أمان والمجسد في حقه بعدم المساس بحرم ة حياته الخاصة، وهذه المبادئ نادت بها الكثير من المواثيق الدولية وقد حذا المشرع الجزائري حذو التشريعات المختلفة فقد عمل على صيانة حرمة الحياة الخاصة في مختلف المجالات تطبيقا لما جاء به الدستور الجزائري ، وقد جسد مشرع الجزائري تطبيق هذه المبادئ وعمل على زجر كل من تخول له نفسه انتهاكها بنصه في الماد ة 394 مكرر 02 من قانون العقوبات بحيث أن عبارة البيانات المخزنة المذكورة في نص الماد ة 394 مكرر 02 من قانون العقوبات ترمي إلى حماية تلك المعطيات أو المعلومات المخزنة في جهاز الحاسب بقصد معالجتها الكترونيا، ويدخل فيها المراسلات عن طريق البريد الالكتروني أو البيانات الموجود ة ببنوك المعلومات والتي تخص أسرار الأفراد؛ كالبيانات الموجود ة بالبطاقات الالكترونية للمؤمن له اجتماعيا إلى غيرها من المعلومات مما جعلها عرضه لانتهاكات عن طريق الجريم ة المعلوماتية، بحيث ظهرت صور جديد ة لانتهاك حرم ة الحياة الخاصة بالتلاعب بهذه البيانات كتغيير فيها أو ارتحال شخصية صاحبها لتحقيق أهداف إجرامية لذلك أيضا

في قانون العقوبات نص على تجريم مجموعة أخرى من الأفعال في المادة 303 مكرر من قانون العقوبات حيث أنه كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية وذلك بالتقاط أو تسجيل أو نقل المكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

ويستخلص من المادة أعلاه أن المشرع أدرك خطر المساس بحرمة الحياة الخاصة عن طريق المعلوماتية بنصه على عبارة بأية تقنية مما يفهم منه أن انتهاك حرمة الحياة الخاصة عن طريق الحاسبات تقع تحت طائلة التجريم في المادة 333 مكرر 01 ، مما يفيد اعتبارها جرائم معلوماتية ماسة بحرمة الحياة الخاصة تجب مكافحتها .

ثانيا : جريمة سرقة المعلومات

حسمت أغلب التشريعات التي سبقت المشرع الجزائري في مكافحة الجريمة المعلوماتية أمرها بعد قيام الجدل الفقهي في التشريع المقارن ؛ حول إمكانية أن تكون المعلومات التي هي شيء غير محسوس وغير مادي محلا للسرقة.

غير أن الوضع غير واضح بالنسبة للمشرع الجزائري الذي لم يجرم سرقة المعلومات صراحة رغم أنه جرم في المادة 394 مكرر 02 فعل الاتجار في المعطيات المعلوماتية والتي تعتبر معلومات كما يطرح التساؤل أيضا حول تحديد مفهوم نص المادة 350 مكرر 01 من قانون العقوبات المعدل بالقانون 01/09 [22] والتي تنص على أنه يعاقب بالحبس من سنتين إلى عشر سنوات وبغرامه من 200،000 إلى 1000,000 دينار جزائري كله من سرق أو حاول سرقه ممتلك ثقافي منقول محمي أو معرف .

فهل ينطبق نص هذه المادة على برامج الحاسب الآلي ككيان منطقي دون دعامتها المادية واعتبار الاستيلاء على المعلومات الموجودة بها جريمة سرقة معلوماتية ؟

للإجابة على هذا السؤال يتعين الرجوع إلى نص المادة الرابعة من الأمر رقم 03/ 05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة والتي تنص على أنه تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي :

1-المصنفات الأدبية المكتوبة مثل المحاولات الأدبية والبحوث العلمية والتقنية والروايات والقصص والقصائد الشعرية وبرامج الحاسب الآلي .

ومنه فقد اعتبرت المادة 04 أعلاه برامج الحاسب الآلي كمصنفات أدبية أو فنية محمية لذلك من الأرجح أن يشمل نص المادة 350 مكرر 01 برامج الحاسب الآلي لأنها تعتبر حسب نص المادة الرابعة من الأمر 05/03 ممتلك ثقافي محمي ومعرف ، وبالتالي نستنتج أن المشرع الجزائري قد عاقب على سرقة المعلومات في المادة 350 مكرر 01 عندما تكون هذه الأخيرة على دعامة مادية بتحديد تجريم سرقة ممتلك ثقافي منقول، لأن الشيء المنقول هو الذي يمكن حيازته وتغيير مكانه إلا أنه لم يحسم الأمر فيما يخص سرقة المعلومات كشيء معنوي أي دون دعمتها المادية وهو ما فصلت فيه التشريعات المقارنة التي سبقته في إمكانية اعتبار المعلومات كشيء معنوي محلا لجريمة السرقة.

المطلب الثاني : العقوبات المقررة للجرائم الالكترونية في قانون العقوبات:

الفرع الأول: العقوبات الأصلية

نص المشرع الجزائري في القانون رقم 15/04 على العقوبات الأصلية لجريمة الدخول والبقاء غير المشروعة للنظام المعلوماتي وهكذا جريمة المساس بالمنظومة المعلوماتية كالتالي:

-عقوبة الدخول أو البقاء غير المشروعان للنظام:

في حالة الدخول غير المشروع من طرف المجرم الالكتروني للنظام كله أو جزء منه، أو متى كان مسموح له بالدخول إلى جزء معين من النظام وتجاوزه ومتى كان الدخول أو التواجد داخل النظام مخالف لإرادة صاحب النظام تكون العقوبة بالحبس من ثلاثة أشهر إلى سنة وغرامة من 50.000 دينار جزائري إلى 100.000 ألف دينار جزائري طبقا للمادة 394 مكرر من قانون العقوبات رقم 15/04 .

أما في حاله الدخول أو البقاء ونتج عنه حذف أو تغيير لمعطيات المنظومة أو انجر عن هذا الدخول أو البقاء تخريب لنظام اشتعال المنظومة فإن العقوبة تضاعف إلى الحبس من ستة أشهر إلى سنتين وغرامه من 50.000 دينار جزائري إلى 150.000 ألف دينار جزائري وذلك وفقا للماد ة 394 مكرر من قانون العقوبات السابق الذكر.

-عقوبة المساس بمنظومة معلوماتية :

نص المشرع الجزائري في الماد ة 394 مكرر 01 من نفس القانون السابق الذكر على عقو بة الاعتداء العمدي على المعطيات الموجود ة داخل النظام وذلك بالحبس من ست ة أشهر إلى ثلاث سنوات وغرامه من 500.000 ألف دينار جزائري إلى 2.000.000 ألف دينار جزائري وذلك في حال ة ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وفي حالة حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، تكون العقوبة بالحبس من شهرين إلى ثلاث سنوات وغرامه من 1.000.000 إلى 5.000.000 دينار جزائري [23]

الفرع الثاني: العقوبات المقررة للشخص المعنوي

نص المشرع الجزائري في الماد ة 51 مكرر من القانون رقم 15/04 على مسائلة الشخص المعنوي وذلك وفق شروط كالتالي:

- أن ترتكب إحدى الجرائم المنصوص عليها قانونا .
-أن تكون بواسطة أعضاء أو ممثلي الشخص المعنوي.
- أن ترتكب الجريمة لحساب الشخص المعنوي.

كما نصت الماد ة 394 مكرر 04 من نفس القانون على العقوبات الواجبة التطبيق على الشخص المعنوي في حاله ارتكابه لأي جريمة اعتداء على نظام المعالجة الآلية للمعطيات؛ بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي. [24]

كما أن الشخص المعنوي يسأل عن هذه الجرائم، سواء بصفته فاعل أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها. [25]

الفرع الثالث : عقوبة الاشتراك والشروع في الجريمة

عقوبة الاشتراك: نصت عليها المادة 394 مقرر 05 من القانون رقم 15/04 "**كل من شارك في مجموعه أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال ماديه يعاقب بالعقوبات المقررة للجريمة ذاتها**"

عقوبة الشروع: نصت عليها الماد ة 394 مكرر 07 من نفس القانون بنصها "**يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها**"

الفرع الرابع : العقوبات التكميلية

نصت المادة 394 مكرر 06 من نفس القانون على مجموع ة من العقوبات التكميلية يحكم بها إلى جانب العقوبات الأصلية وهي كالتالي:

المصادرة: وتعني مصادرة الأجهزة والبرامج والوسائل المستخدم ة لارتكاب الجرائم الماسة بالنظام وذلك ببيعها أو حجزها مع مراعاة حقوق الغير حسن النية .

إغلاق المواقع: إغلاق مواقع الانترنت أو المواقع الالكترونية بصفه عام ة، والتي كانت وسيلة لارتكاب هذه الجرائم أو ساهمت في ارتكابها.

إغلاق المحل أو المقهى الالكتروني: ويكون في الحالة التي يكون صاحب المحل مشاركا في الجريم ة وذلك إذا تمت الجريمة وهو عالم بها ولم يتصدى لها بالإخبار عنها أو يمنع مرتكبها من ارتياد محله لارتكاب مثل هذه الجرائم [26]

ومن الملاحظ أن هذه العقوبات جاءت رادعه حيث تضاعف عند الضرورة كما اشتملت على عقوبات تكميلية وحتى عقوبات الشخص المعنوي.

الخاتمة:

حاول المشرع الجزائري جاهدا التصدي لهذا النوع من الجرائم ومكافحتها بشتى الطرق من خلال سن بعض القوانين وكذا تعديل البعض الآخر منها قانون العقوبات وقانون حماية الملكية الفكرية، والواضح أن المشرع الجزائري تبنى سياسة مزدوجة لظاهره الإجرام والمعلوماتية العام ة بحيث اهتدى من جه ة إلى تعديل الجوانب الموضوعية والإجرائية للتشريعات العقابية العامة وجعلها تواكب التحديات الجديدة الناتجة عن التطور الهائل للتكنولوجيا الحديثة وقام من جه ة ثانية باستحداث قوانين أخرى أكثر تجاوبا مع الطبيع ة الخاصة للجرائم الالكترونية، وهذا التنوع التشريعي من ش أنه أن يساهم بشكل فعال على الأقل في الوقت الراهن في الحد من تفاقم ظاهرة الإجرام الالكتروني في الدولة الجزائرية، مع هذا ينبغي الاعتراف بحقيقة وهي أنه رغم الجهود الجبارة التي يبذلها المشرع الجزائري في سبيل التصدي لظاهرة الإجرام الالكتروني إلا أنها غير كافيه لبلوغ الهدف الذي يتطلع إليه نظرا للتطورات السريع ة والمستمرة التي تعرفها ظاهر ة الإجرام الالكتروني من جهة ونظرا للخاصية العالمية والعابرة للحدود التي تتميز بها هذه الجريمة من جهة أخرى

ومن النتائج المتوصل إليها ما يلي:

-تطرق المشرع الجزائري للجريم ة الواقعة على النظام المعلوماتى وإغفال الجرائم الماسة بمنتجات الحاسب الآلي، حيث لم ينص على جريم ة التزوير المعلوماتي وإنما إخضاعها للنصوص التقليدية الخاصة بتزوير المحرر ولم يوسع من مفهوم المحرر ليشمل المستند المعلومات.

-لم يقم المشرع الجزائري بتحديد الجريم ة المرتكبة باستخدام النظام المعلومات وترك المجال واسع ليدخل في نطاقها كل ما تفرزه التقنية الجديدة وتطوراتها

ومن التوصيات ما يلي :

- مطالبة المشرع الجزائري بتعديل قواعد الملكية الفكرية ككل بشقيها الصناعية وكذا الأدبية والفنية.

-اعتماد طريقة التشفير بشكل أوسع في المعاملات الإلكترونية .

-إيلاء أهمية للعقوبات المسلطة على الجرائم الإلكترونية بجعلها أكثر شدة لأداء وظيفتها الرادعة .

قائمة الهوامش

[1]عصام نجاح، محاضرات في مقياس الملكية الصناعية، ألقيت على طلبة الدكتوراه، جامعة 8ماي 1945- ،2017.

[2]عبد الله حسين الخشروم، الوجيز في الملكية الصناعية والتجارية، الطبعة الأولى، دار وائل للنش ر والتوزيع الأردن، 2005، ص61

[3]صلاح زين الدين، الملكية الصناعية والتجارية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2012، ص 22

[4] محمد حسني عباس، الملكية الصناعية والمحل التجاري، دار النهضة العربية، مصر، 1971، ص 57.

[5] Paul Mathely ,Le droit français des brevets d'invention ,Journal des notaires et des avocats, Paris, 1974, P29.

[6] Yves Marcelin, Droit et pratique des brevets d'invention, 2eme édition –J– Delmas, Paris, 1972, P 2.

[7] صلاح الدين عبد اللطيف الناهي، الوجيز في الملكية الصناعية والتجارية، دار الفرقان، عمان، 1983، ص 61.

[8] Yves Reinhard, Droit commercial, édition Litec, Paris, 1990, P 334

[9]محمد حسن عبد الله علي:<<حماية برامج الحاسب بقانون براءة الاختراع في الولايات المتحدة الأمريكية>>، مجلة الشريعة والقانون، العدد 47، الأردن 2011، ص127.

[10]إلياس ناصيف، الكامل في قانون التجارة "المؤسسة التجارية"، الجزء الأول، الطبعة الثانية، منشورات عويدات، بيروت، 1985، ص 171.

[11] مليكة حمايدية، النظام القانوني لعقد ترخيص براءة الاختراع في مجال نقل التكنولوجيا، رسالة لنيل شهادة الماجستير، كلية الحقوق والعلوم الإدارية، جامعة الجزائر، 2001، ص 13.

[12] أمير فرج يوسف، موسوعة حماية الملكية الفكرية، دار المطبوعات الجامعية، مصر،2009، ص 849

[13]"Toute invention peut faire l'objet d'un titre de propriété industrielle délivré par le directeur de l'institut national de la propriété industrielle qui conféra a son titulaire ou à ses ayant causé un droit exclusif d'exploitation "

[14]عصام نجاح: حق المؤلف في مواجهة الرقمنة–الأزمة والحلول، مداخلة الدكتور عصام نجاح، رئيس المجلس العلمي للكلية، جامعة 8 ماي 1945–قالمة – الجزائر، بالمؤتمر الدولي الحادي عشر مركز جيل البحث العلمي حول التعلم بعصر التكنولوجيا الرقمية والذي نظمه الاتحاد العالمي للمؤسسات العلمية بالتعاون مع جامعة تيبازة في طرابلس لبنان أيام 22 و23 و24 أبريل 2016.

[15] المرجع نفسه.

[16] عصام نجاح، محاضرات مرجع سابق.

[17]– قانون رقم 15/04 المؤرخ في 10/ 11/ 2004 يعدل ويتمم الأمر رقم 156/66 المتضمن قانون العقوبات الجريدة الرسمية عدد 71 الصادرة بتاريخ 2004/11/10 المتمم للأمر رقم 15/22 المتضمن قانون العقوبات

[18]- أمال قارة الحماية الجزائية للمعلوماتية في التشريع الجزائري، طبعه ثانية دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص 106

[19]- راضية عيمور ، الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري ، مقال منشور في المجلة الأكاديمية للبحوث القانونية والسياسة، المجلد السادس العدد الأول، السنة 2022 ، الأغواط، ص 100

[20]- أمال قارة، الجريمة المعلوماتية، المرجع السابق، ص 44

[21]- جميل عبد الباقي الصغير ، جرائم الكمبيوتر والجرائم الأخرى في مجال المعلومات ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة الفترة الممتدة من 25إلى 27 أكتوبر 1993 ص 28

[22]- القانون رقم 01/09 المؤرخ في 25 فيفري 2009 الجريدة الرسمية عدد 15

[23]- خثير مسعود الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى للنشر والتوزيع ، الجزائر، سنه 2010 ، ص 100/99

[24]- خثير مسعود، المرجع السابق، ص 101/100

[25]- فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري ، مداخله ضمن أعمال المؤتمر الدولي الرابع عشر للجرائم الالكترونية، طرابلس 25/24 مارس 2017 ، الصادر عن مركز جيل البحث العلمي ص 13

[26]- خثير مسعود، المرجع السابق، ص 102–103.

حساين عومرية
hassaineomria@yahoo.com
المركز الجامعي بطل المقاومة شريف بوشوشة افلو

الإطار المفاهيمي للجريمة الالكترونية وسبل مكافحتها

مقدمة:

إن تطور المجتمعات مع مرور الوقت، أدى إلى تطور الإجرام ذلك انه وليد بالتبعية لذلك التطور فمع تطور التقنية يتطور الإجرام و يزداد خطورة و تعقيدا، يقف وراء ذلك التقدم العلمي خاصة في مجال الاتصالات شبكة اتصال العالمية او الانترنت، وهي شبكة اتصالات عالمية تسمح بتبادل المعلومات بين شبكات أصغر تتصل من خلالها الحواسيب حول العالم تعمل وفق أنظمة محددة ويعرف بالبروتوكول الموحد وهو بروتوكول إنترنت .

كان استخدام الانترنت في بداية الأمر مقتصرا على المجال العسكري ثم تطور إلى المجال البحث العلمي و مع الوقت أصبح يعتمد عليها في مختلف الحياة و ارتفع عدد مشتركيها و كان من بين هؤلاء من له نوايا إجرامية استخدم تلك الوسائل لتنفيذ ذلك الإجرام ،حيث اصبحت وسيلة حديثة لتنفيذ نوع جديد من الإجرام الخفي،و البعيد عن أعين الرقابة الأمنية

الامر الذي ادى الى ضرورة التفكير في وسائل قانونية و تقنية للحماية و الردع من هذا النوع من الإجرام حيث تصدى له المجتمع في البداية بمختلف القوانين التقليدية التي تعالج الإجرام العادي وذلك حتى لا يفلت الجاني من العقاب ثم بدأ التفكير في إيجاد حلول قانونية تناسب هذا النوع من الإجرام باعتباران الجريمة المرتكبة عبر الانترنت تتميز بالسرعة و التطور و الخفاء و تتطلب أساليب خاصة للتحري و التحقيق ، فكان لابد من مسايرتها عن طريق إجراءات و قوانين خاصة لهذا النوع من الإجرام و هو بالفعل ما تم حيث بدأت عديد من المؤتمرات في انعقاد لإثراء البحوث القانونية بمشاركة فقهاء القانون و علماء الاجتماع في وضع تصورات و خطط لمواجهة هذا النوع من الجريمة.[1]

ومن خلال ما تقد نطرح الاشكال الاتي: **كيف عالج المشرع الجزائري الجريمة الالكترونية انطلاقا من اجراءات واساليب البحث والتحري التي وضعها في سبيل الكشف عنها؟**

---

[1] بذلتجهود الايستهانبها،مؤكدةعلىوجوبتعزيز العملالمشتركبينأعضاءمنظمةالاممالمتحدةمنأجلالتعاونعلىالحدمنانتشار الجريمةالمعلوماتية،وهذا منخلالمؤتمراتهالمنعالجريمةومعاملةالمجرمينبدءابالمؤتمر السابععام 1985إلىغايةالمؤتمر الثانيعشرعام 2010 . إضافةإلىالمؤتمر الخامسعشر للجمعيةالدوليةلقانونالعقوباتوذلكتحتإشرافالأممالمتحدةعام 1994،الذينتجعنهعدةتوصياتوقرار اتذاتصلةبالجر ائمالمعلوماتية،وقدتضمنتشقيناثنينو احدموضو عييتناو لالأفعالالتيتقعتحتطائلةالإجر امالمعلومات ي،وثانيإجر ائييتضمنالإجر اءاتالو اجبإتباعهاالتطبيقالقو اعدالموضو عية . كماكانللمنظمةالعالميةللملكيةالفكريةدوربارز فيهذاالمجال،وذلكمنخلالخلقهالنصوصقانونيةخاصةبحمايةبر امجالحاسبالآليو هذامنخلالالمادة 04 و 05 مناتفاقيةتريبس.

ولمعالجة الإشكالية المطروحة قسمنا الدراسة الى قسمين تناولنا في القسم الاول ماهية الجريمة الالكترونية، اما القسم الثاني فخصصناه لدراسة الاساليب الخاصة بالبحث والتحري في الجريمة الالكترونية.

المبحث الأول:مفهوم الجريمة الالكترونية

خلقت التقنية الحديثة خصوصا نوعا جديدا من الإجرام لم يكن معهودا سابقا مجاله هو عالم الانترنت, لذلك ظهرت مصطلحات جديدة للدلالة على هذا النوع من الإجرام منها جرائم المعلوماتية .و جرائم الحاسوب وتتميز هذه الجرائم بمفاهيم خاصة و مصطلحات محددة .

المطلب الأول :تعريفالجريمة الالكترونية

واكب ظهور الأنترنت بداية الإجرام المعلوماتي بصفة عامة و الإجرام الخاص بعالم الأنترنت بصفة خاصة و الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم[1].

الفرع الأول :التعريف الفقهي

يرى بعض الفقه انه عند تعريف هذه الجرائم يجب الاستناد الى موضوع الجريمة او الى انماط السلوك محل التجريم فيعرفها« Rosenballt » انها نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه او هي أي نمط من انماط الجرائم المعروف في قانون العقوبات طالما كان مرتبط بتقنية المعلومات.

– في حين ترى الدكتورة هدى قشقوش أنها : " كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات"، في الوقت الذي اوجد مكتب المحاسبة العامة للولايات المتحدة الأمريكية « GOA » تعريف لهذه الجرائم بانها » أو إساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم اكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر [2]لكن جرائم الانترنت هي امتداد لما عرف بجرائم الحاسوب والمقصود بجرائم الحاسوب: " كل عمل إجرامي يرتكب باستخدام الحاسوب كأداة أساسية، ودور الحاسوب في تلك الجرائم قد يكون هدفا للجريمة أو أداة لها. "

وهناك تعريفات فقهية انطلقت من وسيلة ارتكاب الجريمة، من بينها تعريف الاستاذ: جون فورستر، والأستاذ(Esliedball)الذي جاء فيه انها: "كل فعل اجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" ويعرفها مكتب تقييم التقنية بالولايات المتحدة الامريكية انها: "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا "،وقد لاقت هذه التعريفات انتقادات كون تعريف الجريمة يجب ان ينصب

---

[1] DEBRAY Stéphane, Internet face aux substances illicites : complice de la cybercriminalité ou outil de prévention ?, DESS média électronique & Internet, Université de Paris 8, 2002-2003, p 08.

[2] بعدتطورأشكالالجريمةمعاستخداماتالحاسبالآليوالانترنتواستهدافهالكافةالمصالحوالحقوق،أصبحتالجرائمالإلكترونيةتقععلىالأشخاصوالأموالوال معلوماتوخلقالبرامجالضارةوإرسالهاوإدخالمعلوماتخاطئةإلىنظاماتالحاسبالآليوالاحتيالوالتلاعبفيالبطاقاتالماليةوسرقةالمعلومات .

على السلوك المكون لها و ليس فقط على الوسيلة التي تم بها فيقول الاستاذ :FandeRson _ R انه "ليس لمجرد ان الحاسب قد استخدم في جريمة ان نعتبرها من الجرائم المعلوماتية[1]".

وامام الانتقادات التي وجهت للتعريفات الفقهية القاصرة على معيار واحد بدأت تظهر تعريفات جمعت بين أكثر من معيار، مثل التعريف الذي جاء به الأستاذ John corrol :وتبناه الأستاذ GION GREEN والذي جاء فيه انها: (أي عمل ليست له في القانون أو أعراف قطاع الأعمال جزاء ، يضر بالأشخاص والأموال أو يوجه ضد أو يستخدم التقنية المتقدمة العالية لنظم المعلومات).

الفرع الثاني:التعريف القانوني

القانون المصري النموذجي في مادته الأولى عرف جرائم المعلوماتية أنها» كل فعل يتم ارتكابه عبر أي وسيط الكتروني ويقصد في تطبيق أحكام هذا القانون بالكلمات والعبارات الآتيةفي حين لم يعرف تعديل قانون العقوبات الجزائري بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 جرائم الانترنت، بل اكتفى بالعقاب على بعض الأفعال، تحت عنوان » الجرائم الماسة بنظام المعالجة الآلية للمعطيات.

اماالمشرع السعودي من خلال نظام مكافحة جرائم المعلوماتية قد وضع تعريفا لها بأنها :" كل فعل يرتكب متضمنا استخدام الحاسب الآلي والشبكة المعلوماتية بالمخالفةلأحكام هذا النظام".[2]

المطلب الثاني: خصائص الجريمة الالكتروني

من بين أهم خصائصها عابرة للحدود، سريعة التنفيذ وصعوبة الإثبات، كما انها جرائم ناعمة.

الفرع الأول: عابرة للدول

فقدت الحدود الجغرافية كل اثر لها في الفضاء الشبكي او الآلي ، فهو لا يعترف بالحدود الجغرافية حيث يتم تبادل البيانات في شكل حزم الكترونية توجه إلى عنوان افتراضي ليس له صلة بالمكان الجغرافي ، فهو فضاء ذو طبيعة لا مركزية و يمكن إجمال أهم خصائصه في عدم التبعية لاي سلطة حاكمة .فالفضاء الآلي: نظام الكتروني معقد لأنه عبارة عن شبكة اتصال لا متناهية غير مجسدة و غير مرئية متاحة لاي شخص حول العالم وغير تابعة لأي سلطة حاكمة فالسلوك المرتكب فيها يتجاوز الأماكن بمعناه التقليدي له وجود حقيقي وواقعي لكنه غير محدد المكان لكنه حقيقة واقعا .

فالشبكة عالمية النشاط والخدمات لا تخضع لأي قوة مهيمنة إلا في بدايتها حيث كان تمويل هذه الشبكة حكوميا يعتمد على المؤسسة العسكرية الأمريكية، أما ألان فقد أصبح التمويل يأتي من القطاع الخاص حيث الشركات الإقليمية ذات الغرض التجاري التي تبحث عن كافة السبل للاستفادة من خدماتها بمقابل مالي[3].

---

[1] الاتفاقيةالدوليةللإجرامالمعلوماتيقدمتتعريفللنظامالمعلوماتيفيمادتهاالثانيةعلىالنحوالتالي:

Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnecté ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement ou tonatisé de données

[2] عبدالفتاحبيوميحجازي/جرائمالكمبيوتروالأنترنتفيالتشريعاتالعربية"دراسةمقارنةمعالتطبيقعلىنظاممكافحةجرائمالمعلوماتيةفيالمملكةالعربيةا لسعودية،ط1 ،دار .النهضةالعربية،الإسكندرية، 2009 ،ص:17 .

[3] خالدممدوحإبراهيم/أمنالجريمةالإلكترونية،دارالجامعية،الإسكندرية،الإسكندرية، 2008 ،ص82.

والجريمة المرتكبة عبر شبكة الانترنت جريمة تعبر الحدود والقارات،وهو ما يدرجها ضمن موضوعات القانون الجنائي الدولي، الذي يقابل القانون الدولي الخاص في القانون المدني، وهو ذلك الفرع من القانون الذي يحدد ضوابط مجالات التعاون الدولي في مجال مكافحة الجريمة بالتزام الدول الموقعة على الاتفاقيات بالعمل بمقتضاها في مكافحة الجريمة .وقد ازدادت أهمية القانون الجنائي الدولي بعدما تطورت الجريمة المنظمة في وقت تقلص فيه المفهوم التقليدي للسيادة، حيث اتسع نظام المعاهدات الدولية لمكافحة الجرائم العابرة للحدود فالجانب الدولي للجريمة المعلوماتية لا يعد عنصرا من عناصرها كما هو الحال في الجريمة الدولية بل يعد هو نطاقها المكاني.

الفرع الثاني :سرعة التنفيذ و صعوبة الإثبات

ضحايا جرائم الانترنت لا يلاحظون أنهم ضحية فعل إجرامي لان هذا النوع من الإجرام يمتاز الخفاء والتستر ,فأثناء وجود مستعمل الانترنت في الشبكة يكون واقع تحت رحمة مجرم في الطرف الأخر من الخط،لان المجرم المعلوماتي يمتاز بالذكاء والحنكة اللتان تجعلان منه مثل الشبح، فمثلا عند إرسال فيروسات مدمرة أو سرقة البيانات الخاصة بالأموال أو إتلافها والتجسس وسرقة المعلومات وغيرها من الجرائم[1] .

فضحية جريمة الانترنت في أكثر صورها خفية لا يلاحظها أو لا يدري حتى بوقوعها. ذلك نظرا لأن المجرمون الإلكترونيون يتبادلون الخبرات و التجارب مع بعضهم البعض في العالم الافتراضي في منتديات خاصة تسمى منتديات القراصنة أو الهاكرز ،لذلك تعتبر جريمة الانترنت أكثر تطورا من التشريعات التي تتصدى لها.[2]

الفرع الثالث: جرائم ناعمة

ترتكب الجرائم التقليدية باستخدام العنف سواء اللفظي أو العضلي مثل جريمة السرقة فهي تمتاز بالعنف العضلي مثل الكسر أو التعدي بالضرب على الضحية.

لكن الجرائم المرتكبة بتقنية الانترنت تمتاز بانها جريمة يمكن ان نطلق عليها الجرائم الصامتة او الناعمة أي تخلو من كل أشكال العنف المادي أو مظاهر العنف مثل الجروح أو الرضوض أو استخدام المعدات الخاصة مثل الأسلحة وهذا ما يجعل منها جريمة خالية من كل اشكال العنف المادي .فسلاح المجرم في جريمة الانترنت لا يعدو ان يكون جهاز معلوماتي متصل بالشبكة الدولية مع وجود مجرم ذو كفاءة عالية في التعامل مع العالم الرقمي ومعرفة معمقة بتقنيات الكمبيوتر ومن امثلة الجرائم الهادئة جريمة التجسس أو سرقة البيانات الخاصة ببطاقات الائتمان.

المبحث الثاني: الاطار الاجرائي للجريمة الالكترونية

وفي هذا الاطار سنحاول تحديد كل من اركان الجريمة الالكترونية، وكذا اساليب البحث والتحري للكشف عنها.

---

[1] محمد عبيد الكعبي/الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت،دار النهضة العربية،لقاهرة،ص 32.

[2] هشام محمد فريد/الجوانب الإجرائية للجرائم المعلوماتية،مكتبة الآلات الحديثة،أسيوط،ط1 ،1994،ص82.

المطلب الاول:اركان الجريمة الالكترونية

حتى تقوم الجريمة يجب ان تتوافر ثلاث الأركان وهي الركن المادي، الركن المعنوي ثم الركن الشرعي.

الفرع الاول: الركن المادي

يتمثل الركن المادي في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات و التي هي:

- الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام.

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتوجات النظام:

الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطياتنصت عليه المادة 394 مكرر قانون العقوبات[1]،وكما نصت على ذلك المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي.

الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.[2]

أ- فعل الدخول: لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، و في نفس الاتجاه إلى جهاز الحاسب الآلي و إنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات.

ب- فعل البقاء Le maintien

قد يتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام، و يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام، وقد يجتمعان. [3]

ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا.ومن أمثلة ذلك: إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورًا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن

---

[1] تنصالمادة 394 مكررمنالقانون04-15 المؤرخفيرمضان 1425الموافق:10نوفمبر 2004 المعدلوالمتمملللأمررقم 66-156 الموافق 8 يونيو 1966 المتضمنقانونالعقوبات "يعاقبالحبسمنثلاثةأشهرإلىسنةوبغرامةمن 50.000 إلى 200.000 دجكلمنيدخلأويبقىعنطرقالغشفيكلأوجزءمنمنظومةللمعالجةالآليةللمعطياتأويحاولذلك" تضاعفالعقوبةإذاترتبعنذلكحذفأوتغييرلمعطياتالمنظومةوإذاترتبعنالأفعالالمذكورةأعلاهتخريبنظاماشتغالالمنظومة "تكونالعقوبةالحبسمنستةأشهرإلىسنتينوالغرامةمن 50000 إلى 300.000 دج".

[2] رشيدخلوفي/قانونالعقوبات،كليكللنشر،المحمدية،الجزائر،2017،ص:142.

[3] عليعبداللهالقهوجي/الحمايةالجنائيةلبرامجالحاسبالآلي،الدارالجامعيةللطباعةوالنشر،بيروت، 1999 ص 17.

المعنوي. ويكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والاطلاع فقط ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، والتي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه.[1]

ويكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع و تلك النتيجة الضارة، و لا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلب مثل هذا الشرط يكون غير معقول ، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة. كما لا يشترط أن تكون تلك النتيجة مقصودة.

وعمومًا التلاعب في المعطيات الموجودة داخل النظام يتخذ إحدى الأشكال التالية:

- **الإدخال L'intrusion**:يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل، ويتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هاته الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، وكذلك الحامل الشرعي لبطاقة الائتمان و التي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب« فيروس...الخ» يضيف معطيات جديدة.[2]

- **المحو L'effacement**: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

- **التعديل Modification**: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة Gomme d'effacement أو برنامج الفيروسات بصفة عامة، وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية.[3].

الفرع الثاني: الركن المعنوي

---

(1) معتوقعبداللطيف/الإطارالقانونيلمكافحةجرائمالمعلوماتيةفيالتشريعالجزائريوالتشريعالمقارن،مذكرة(مكملةلنيل شهادة الماجستيروعلومالجنائية، 2012 2011 ،ص:88 .

(2) معتوقعبداللطيف/الإطارالقانونيلمكافحةجرائمالمعلوماتيةفيالتشريعالجزائريوالتشريعالمقارن،مرجعسابق،2011 /2012،ص:90

(3) سفيانسوير/ جرائممعلوماتية،مذكرةلنيلشهادةالماجستيرفيالعلومالجنائيةوعلمالإجرام،جامعةأبوبكربلقايد،تلمسان،سنة 2010-2011،ص: 86.

الركنالمعنويهوالحالةالنفسيةللجاني،والعلاقةالتيتربطمادياتالجريمة وشخصيةالجاني [1]،كما الركن المعنوي في مختلف الاعتداءات الماسة بالأنظمة المعلوماتية تتخذ صورة القصد الجنائي إضافة إلى نية الغش.

أولا: الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات :يلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء و أن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصريه العلم و الإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى ولو كان الباعث هو الفضول أو إثبات القدرة على المهارة و الانتصار على النظامبالنسبة لنية الغش تبدو من خلال الغش الذي يتم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام، بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام.

ثانيا: الاعتداءات على سير نظام المعالجة الآلية للمعطيات :إن هذه الجريمة جريمة عمدية، إذ أن من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء الغير مشروع داخل النظام وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة.

ثالثا: الاعتداءات العمدية على المعطيات : جريمة الاعتداء العمدي على المعطيات جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بان نشاطه الجرمي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أن ليس له الحق في القيام بذلك وانه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش ، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه.

الفرع الثالث: الركن الشرعي

طبقا لقانون العقوبات وبناءا على المواد 211 و 131 من الإتفاقية الدولية للأجرام المعلوماتي فان العقوبات المقررة للإجرام المعلوماتي يجب ان تكون رادعة و تتضمن عقوبات سالبة للحرية و التي تتمثل في العقوبات الأصلية تكميلية على الشخص الطبيعي و الشخص المعنوي.

اولا:العقوبات المطبقة على الشخص الطبيعي:

[1] خالدممدوحإبراهيم/فنالتحقيقالجنائيفيالجرائمالالكترونية،دارالفكر،الإسكندرية،2009 ،ط1،ص:53.

أ/ العقوبات الأصلية: عقوبة الحبس تتراوح من شهرين إلى ثلاث سنوات،حسب الفعل المرتكب والغرامة تتراوح قيمتها خمسين الف دينار جزائري إل مئة الف دينار جزائري، حسب الفعل المرتكب:الدخول والبقاء بالغش (الجريمة البسيطة)، الدخول والبقاء بالغش(الجريمة المشددة) وتضاعف العقوبة إذا ترتب عن هذه الأفعال حذف او تغيير لمعطيات المنظومة،الإعتداء العمدي للمعطيات.[1]

ب/ العقوبات التكميلية :الصادرة تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية، واغلاق المواقع والأمر يتعلق بالمواقع، التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية،وإغلاق المحل أو مكان الاستغلال اذا كانت الجريمة قد ارتكبت بعلم مالكها.[2]

عقوبة الشروع :جاءت به المادة 11 من الإتفاقية الدولية للإجرام المعلوماتي و اعتمده المشرع الجزائري بالنسبة للجرائم الماسة بالأنظمة المعلوماتية بحيث توسع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، اذ اصبح الشروع معاقب عليه بنفس العقوبة المقررة الجنحة ذاتها.[3]

الظروف المشددة : نص القانون على ظرف تشدد به العقوبة جريمة الدخول و البقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندا ينتج عن الدخول او البقاء اما حذف او تغيير المعطيات التي يحتويها النظام واما تخريب النظام اشتغال النظام،تضاعف العقوبة اذا استهدفت الدفاع الوطني او الهيئات او المؤسسات العامة.[4]

ثانيا: العقوبات المطبقة على الشخص المعنوي:يسأل الشخص المعنوي عن هاته الجرائم سواءا بصفته فاعلا اصليا او شريكا كما يسأل عن الجريمة التامة او الشروع فيها ،كل ذلك بشرط ان تكون الجريمة قد ارتكبت لحساب شخص معنوي بواسطة احد اعضائه او ممثليه وبتالي العقوبة الشخص المعنوي تتمثل في الغرامة في خمس مرات الى لحد الاقصى المقررة للشخص الطبيعي.[5]

---

(1)انظر المواد 394مكرر 1 و 2.

(2) انظر المادة394 مكرر6منالقانون04-15 المؤرخفيرمضان 1425الموافق:10نوفمبر 2004 المعدلو المتمملللأمررقم 66-156 الموافق 8 يونيو 1966 المتضمنقانونالعقوبات "
معالإحتفاظبحقوقالغيرحسنالنيةبحكممصادرةالأجهزةوالبرامجوالوسائلالمتسخدمةمعإغلاقالمواقعالتيتكونمحلاللجريمةمنالجرائمالمعاقبعليهاوفق الهذاالقسمعلىإغلاقالمحلاو المكانالإستغلالاذاكانتالجريمةقدارتكبتبعلممالكها .

(3)انظر المادة 394مكرر7منالقانون04-15 المؤرخفيرمضان 1425الموافق:10نوفمبر 2004 المعدلو المتمملللأمررقم 66-156 الموافق 8 يونيو 1966 المتضمنقانونالعقوبات "يعاقبعلىالشروعفيارتكابالجنحةالمنصوصعليهافيهذاالقسمبالعقوباتالمقررةعلىالجنحةذاتها.

(4) انظر المادة 394 مكرر3 منالقانون04-15 المؤرخفيرمضان 1425الموافق:10نوفمبر 2004 المعدلو المتمملللأمررقم 66-156 الموافق 8 يونيو 1966 المتضمنقانونالعقوبات"تضاعفالعقوبةالمنصوصعليهافيهذاالقسماذاالعقوبةاذااستهدفتالدفاعالوطنياوالهيئاتاوالمؤسسات"

(5)انظر المادة 394 مكررمنالقانون04-15 المؤرخفيرمضان 1425الموافق:10نوفمبر 2004 المعدلو المتمملللأمررقم 66-156 الموافق 8 يونيو 1966 المتضمنقانونالعقوبات 4 "
يعاقبالشخصالمعنويالذييرتكباحدهاتهالجرائمالمنصوصعليهافيهذاالقسمبغرامةتعادلخمسمراتالحدالاقصىالمقررللشخصالطبيعي" .

عقوبات الاتفاق الجنائي: تبنى المشرع الجزائري بغرض تحضير لجرائم الماسة بالأنظمة المعلوماتية وعقوبة الاشتراك بالاتفاق تكون نفس العقوبة التي تم التحضير لها فاذا تعددت الجرائم تكون العقوبة هي العقوبة الجريمة الاشد .[1]

المطلب الثاني: الأساليب الخاصة بالبحث و التحري في الجريمة الالكترونية

للمكافحة هذه الجريمة يحب اعتماد على طرق و أليات تختلف عن تلك المعهودة سابقا و من بين أهم الوسائل والأليات التفتيش، المعاينة و الخبرة .

الفرع الأول التفتيش:هو إجراء من إجراءات التحقيق يقوم به موظف مختص وفق قانون الإجراءات الجزائية يهدف التفتيش إلى جمع الأدلة من مكان وقوع الجريمة .

أما في الجرائم المتعلقة بشبكة الانترنت نجد أن الدخول غير المشروع إلى الأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة عما قد يتصل بجريمة وقعت، إجراء يفيد في كشف الحقيقة عنها وعن مرتكبها، وتقتضيه مصلحة وظروف التحقيق في الجرائم المعلوماتية ،اما طبيعة التكنولوجيا الرقمية قد عقَّدت من التحدي أمام أعمال التفتيش والضبط ، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماماً عن الموقع المادي للتفتيش وإن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية الجاري تفتيشها، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر.

وعند القيام بالتحقيق في الجريمة يتم ذلك بالاعتماد على مجموعة وسائل في هذا المجال هي:

اولا: الوسائل المادية :وهي الأدوات الفنية التي غالباً ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها:

أ. **عناوينIP ، والبريد الإلكتروني، وبرامج المحادثة :** عنوان الإنترنت هو المسئول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يوجد بكل جهاز مرتبط بالإنترنت، وفي حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية، ويمكن لمزود خدمة الإنترنت أن يراقب المشترك، كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضاً إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك.[2]

ب. **البروكسي:PROXY** يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة

---

(1) انظر المادة 394 مكرر 5 منالقانون04-15 المؤرخفيرمضان 1425الموافق:10نوفمبر 2004 المعدلوالمتمملللأمررقم 66-156 الموافق 8 يونيو 1966 المتضمنقانونالعقوبات

"كلمنشاركفيمجموعةأوفياتفاقتألفبغرضالإعدادلجريمةأوأكثرمنالجرائمالمنصوصعليهافيهذاالقسموكانهذاالتحضيرمجسدابفعلأوعدةأفعالمادية،يع اقببالعقوباتالمقررةللجريمةذاتها".

(2) خالدممدوحابراهيم/فنالتحقيقالجنائيفيالجرائمالالكترونية،دارالفكرالجامعي،الإسكندرية،ط1،2009،ص:30.

. Cache Memoryوتقوم فكرة البروكسي على تلقى مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم بإعادة إرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية،أم إنه لم يتم تنزيلها من قبل فيتم إرسال الطلب إلي الشبكة العالمية، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين IP ومن أهم مزايا مزود البروكسي أن ذاكرة Cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوى في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.[1]

ج. **برامج التتبع :** تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم ،وتقدم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوى هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP التي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى.[2]

د. **نظام كشف الاختراق:Intrusion Detection System** ويرمز له اختصاراً بالأحرف IDS وهذه الفئة من البرامج تتولي مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثاً عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب أو الشبكة ، [3] وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عده ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة .

هـ. **نظام جرة العسل :Honey Pot** وهو نظام حاسوبي مصمم خصيصاً لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أية بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعاً خاطئاً بسهولة الاعتداء على هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز آخر في الشبكة، في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء، وتحليلها.

و.**أدوات فحص ومراقبة الشبكات :** هذه الأدوات تستخدم في فحص بروتوكول TCP/IP وذلك لمعرفة ما قد يصيب الشبكة من مشاكل، ومعرفة العمليات التي تتعرض لها، ومن هذه الأدوات:

أداة :ARP ووظيفتها تحديد مكان الحاسب الآلي فيزيائياً على الشبكة.

(1) بلالبنجامع/المشكلاتالأخلاقيةوالقانونيةالمثارةحولشبكةالانترنيت،ماجستيرفيعلمالمكتباتتخصصإعلامعلميوتقني،جامعةمنتوري،قسنطينة، 2006،ص:163.

(2) خالدعياداالحلبي/إجراءاتالتحريوالتحقيقفيجرائمالحاسوبوالانترنيت،دارالثقافة،الأردن،ط2011 ،ص:206.

(3) خالدعياداالحلبي/إجراءاتالتحريوالتحقيقفيجرائمالحاسوبوالانترنيت،المرجعالسابق،ص:208.

برنامج :Visual Route 5.2a وهو عبارة عن برنامج يلتقط أي عملية فحص عملت ضد الشبكة، فيقوم بتقديم أجوبة تبين المعلومات التي حدث فيها مسح، والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان IP أو اسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

أداة :TRACER تقوم هذه الأداة برسم مسار بين جهازين تظهر فيه كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها والوقت والفترات التي قضاها، وهي تسمح برؤية المسار الذي اتخذه IP من مضيف إلى آخر، وتستخدم هذه الأداة الخيار Time To Live TTL التي تكون ضمن IP لكي تستقبل من كل موجه رسالة وبذلك يكون هو العدد الحقيقي للوثبات، ويتم بذلك تحديد وبشكل دقيق المسار التي تسلكه الرزمة، وهذه الأداة تستخدم في الأساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها، إذ أنه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيح ونقاط الضعف، ولكن يمكن أيضاً من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها.

أداة :NET STAT هي أداة لفحص حالة الاتصال الحالي للبرتوكول TCP/IP ، ولها عدد من المهام من أهمها عرض جميع الاتصالات الحالية، ومنافذ التنصت، وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لجدول التوجيه[1].

ثانيا: الوسائل الإجرائية

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

أ / اقتفاء الأثر : من أخطر ما يخشاه مجرم نظم المعلومات تقصي أثره أثناء ارتكابه للجريمة، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح أولاها نصيحة هي قم بمسح آثارك Cover Your Tracks ، فلو لم يقم المخترق بمسح آثاره فمؤكد أنه سوف يتم القبض عليه حتى وإن كانت عملية الاختراق قد تمت بشكل سليم،ويمكن تقصي الأثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.[2]

ب/ الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته : ينبغي على المحقق وهو بصدد التحقيق في إحدى جرائم الانترنت أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء،وعليه الإطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات والإجراءات وتصنيف الموارد العامة، ومدى مزامنة الأجهزة، ومدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور، توزيع الصلاحيات للمستفيدين،إجراءات أمن العاملين،أسلوب النسخ الاحتياطي، والاستعانة ببرامج الحماية.

(1) خالدعيادالحلبي/إجراءاتالتحريوالتحقيقفيجرائمالحاسوبوالانترنيتالمرجعالسابق،ص:211.
(2) نفسالمرجع،ص:213.

ج/ **الاستعانة بالذكاء الصناعي** : أثبتت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها،فيمكن الاستعانة به في حصر الحقائق والاحتمالات والأسباب والفرضيات و استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي، وفق برامج صممت خصيصا لهذا الغرض.[1]

الفرع الثاني:مفهومالمعاينة

المعاينة من المراحل الأولى للإستدلال حول ملابسات الجريمة نظرا لي ما توفره من أدلة جول الإثبات و تزداد أهميتها في النوع من الإجرام لأن م السهولة محو أثار الجريمة،

وهيإجراءبمقتضاهينتقلالمحققإلىمكانوقوعالجريمة

ليشاهدبنفسهويجمعالآثارالمتعلقةبالجريمةوكيفيةوقوعهاكذلكجميعالأشياءالأخرى

،التيتفيدفيكشفالحقيقة،واتخاذمايلزممنإجراءاتكضبطبعضالأشياء.[2]

يجوزالإلتجاءإلىالمعاينةفيكافةالجرائم،وهيإجراءهادفغايتهكشف

وصيانةالعناصرالماديةالتيتتعلقبالجريمة،وتفيدفيالتحقيقالجاريبشأنها،فإذا

انعدمتبالنسبةللتحقيقجدواهاوفائدتهالمتكنثمةمجالأومقتضىلإجرائها،ولا

تجديفيكشفالحقيقةبشأنهالمعاينة،مثلجريمةالتزويرالمعنويوجريمةالقذف والسبالتيتقعبالقولفيغيرالعلانيةوغيرها.

- **مسرحالجريمةالمرتكبةعبرالإنترنت:**

ينبغيعندالشروعفيجمعالأدلةمنمسرحجريمةالحاسوبوالإنترنت،التعامل معهعلىأنهمسرحين.

- **مسرحتقليدي** :ويقعخارجبيئةالحاسوب،ويتكونبشكلرئيسيمنالمكونات المادية المحسوسةللمكانالذيوقعتفيهالجريمة،وهوأقربمايكونإلىالمسرحأية جريمةتقليديةقديتركفيهاالجانيآثارعدة،كالبصماتوغيرها،وربماتركمتعلقات شخصيةأووسائطتخزينرقمية،ويتعاملأعضاءفريقالتحقيقمعالأدلةالموجودةفيه كلبحسباختصاصه.
- **مسرحسيبراني** :ويقعداخلبيئةالحاسوب،ويتكونمنالبياناتالرقميةالتي تتواجدوتنقلداخلبيئةالحاسوبوشبكاته،فيذاكرتهوفيالأقراصالصلبةالموجودة بداخله،والتعاملمعالأدلةالموجودةفيهذاالمسرحيجبأنلايتمإلاعلىيدخبير متخصصفيالتعاملمعالأدلةالرقميةمنهذاالنوع.[3]

أهميةالمعاينةفيالجريمةالمرتكبةعبرالإنترنت:

(1) خالدعياد الحلبي/إجراءاتالتحريوالتحقيقفيجرائمالحاسوبوالانترنيتالمرجعالسابق،صص :213-214.

(2) محمدحمادمرهجالهيتي/جرائمالحاسوب،دارالمناهج،عمان،ط 2006 ، 1،ص:255.

(3) محمدبننصيرمحمدالسرحاني/مهارتالتحقيقالجنائيالفنيفيجرائمالحاسوبوالإنترنت-

دارسةمسحيةعلىضباطالشرطةبالمنطقةالشرقية،رسالةلمتطلباتالحصولعلىدرجةالماجستيرفيالعلومالشرطية،تخصص،القيادةالأمنية،جامعةنايفال عربيةللعلومالأمنية،كليةالدراساتالعليا،قسمالعلومالشرطية،الرياض،2004 ،ص:77.

تكمنأهميةوجدارةالمعاينةعقبوقوعجريمةمنالجرائمالتقليديةفيأنهاتتبوأ
مكانةالصدارةعلىماعداهامنالإجراءاتالاستقصائيةالأخرى،بحكممركزالمحورية
لدورهافيتصوركيفيةوقوعالجريمة،وظروفوملابساتارتكابهاوتوفيرالأدلةالمادية
منالمادةالتيتجمعنطريقهاوتمحيصوتقييمالأدلةالأخروالتنسيقبينهافيضوء
المعلوماتالتيمنها،بمايكفلفيذاتالوقتالتخطيطالسليملعملياتالبحث،والتحقيق الجنائيوتطويرها.[1]
حتىيكونللمعاينةفيالجرائمالمتعلقةبشبكةالإنترنتفائدة
فيكشفالحقيقةعنهاوعنمرتكبيهامراعاةعدةقواعدوإرشاداتفنيةأبرزهاما يلي[2]:
1-تصويرالحاسبوالأجهزةالطرفيةالمتصلةبه،علىأنيتمتسجيلوقتوتاريخ
ومكانالتقاطكلصورة.
2-العنايةبملاحظةالطريقةالتيتمبهاإعدادالنظام.
3-ملاحظةواثباتحالةالتوصيلاتوالكابلاتالمتصلةبكلمكوناتالنظامحتى
يمكنإجراء عملياتالمقارنةوالتحليلحينعرضالأمرفيمابعدعلىالمحكمة.
4-عدمنقلأيمادةمعلوماتيةمنمسرحالجريمةقبلإجراء اختباراتللتأكدمن
خلوالمحيطالخارجيلموقعالحاسبمنأيمجاللقوىمغناطيسيةيمكنأنيتسببفي محوالبياناتالمسجلة.
5-التحفظعلىمعلوماتسلةالمهملاتمنالأوراقالملقاةأوالممزقةوأوراق
الكربونالمستعملةوالشرائطوالأقراصالممغنطةغيرالسليمةوفحصها،ويرفععليها البصماتذاتالصلةبالجريمة.
6-التحفظعلىمستنداتالإدخالوالمخرجاتالورقيةللحاسبذاتالصلة بالجريمة،لرفعومضاهاةماقديوجدعليهامنبصمات.
7-قصرمباشرةالمعاينةعلىالباحثينوالمحققينالذينتتوفرلهمالكفاءةالعلمية والخبرةالفنيةفيمجالالحاسبات.
يتمالتوثيقمسرحالجريمةووصفهبكاملمحتوياتهبشكلجيدمعتوثيقكلدليل
علىحدةبمافيهاالأدلةالرقمية،بحيثيتمتوضيحمكانالضبطوالهيئةالتيكانعليها
ومنقامبرفعهوتحريزهوكيفومتتمذلك،بلإنالبعضيرىأنالتوثيقيجبأن
يشملكافةالمصادرالمتاحةعلىالشبكةالتيترتبطبهاالأجهزةمحلالتحقيقولعل
أبرزالأماكنالتييحتملوجودالأدلةالجنائيةالمتعلقةبجرائمالإنترنتفيهامايلي:
-الورق :علىالرغممنوجودأجهزةالحاسبالآليقللمنحجمالأوراقالملفات
التقليديةالمستخدمةحيثيتمحفظالمعلوماتوالبياناتعلىأجهزةالحاسبالآلي،نجد
الكثيرينممنيقوموابطباعةالمعلوماتلأغراضالمراجعةأوالتأكدمنالشكلالعام
للمستندأوالرسالةأوالرسومات،وبالتاليفهيتعتبرمنالأدلةالتييننبغيالاهتمامبها فيالبحثعنالحقيقة.

(1) عبدالفتاحبيوميحجازي/مبادئالإجراءاتالجنائيةفيجرائمالكمبيوترو الإنترنت،دار الفكر الجامعي،الإسكندرية،الطبعةالأولى،2006 ،ص:101.
(2) محمدابو العلاعقيدة/ "التحقيقو جمعالأدلةفيمجالالجرائمالإلكترونية،.http://arblawinfo.comاطلععليهبتاريخ 2019/04/14 علىالساعة 16:45.

-جهازالحاسبالآليوملحقاته :وجودجهازالحاسبالآليهامجداللقولبأن الجريمةالواقعةهيجريمةمعلوماتيةأوجريمةحاسوبية،وانهامرتبطةبالمكانأو الشخصالحائزعلىالجهاز ،ولأجهزةالحاسبالآليأشكالوأحكاموألوانمختلفةوخبير لحاسبالآليوحدهاالذييستطيعأنيتعرفعلىالحاسبالآليومواصفاتهبسرعة فائقة.[1]

- **البرمجيات** :إذاكانالدليلالرقمييُنشأباستخدامبرنامجخاصأوليسواسع الانتشار ،فإنأخذالأقراصالخاصةبتثبيتوتنصيبهذاالبرنامجأمرفيغايةالأهمية عندفحصالدليل.
- **وسائطالتخزينالمتحركة** :كالأقراصالمدمجة" أقراصالليزر "والأقراص المرنة والأشرطةالمغناطيسيةوغيرها،وتعدهذهالوسائطجزءمنالجريمةالمرتكبةعبرالإنترنتمتىكانتمحتوياتهاعنصرمنعناصرا لجريمة.
- **المراشد:** الخاصةبالمكوناتالماديةوالمنطقيةللحاسبالآليوالتيتفيدفيمعرفة التفاصيلالدقيقةلكيفيةعملها.
- **المودم:**وهوالوسيلةالتيتمكنأجهزةالحاسبالآليمنالاتصالببعضها البعضعبرخطوطالهاتف،وفيالوقتالحاليتطورالمودمليكونجهازإرسال واستقبالفاكسوالردعلىالمكالماتالهاتفيةوتبادلالبياناتوتعديلها.[2]

الفرعالثالث: الخبرة

الخبرةهيالوسيلةلتحديدالتفسيرالفنيللأدلةأوالدلائلبالاستعانةبالمعلومات، فهيفيالحقيقةليستدليلامستقلاعنالقوليأوالدليلالمادي،إنماهيتقييمفنيلهذاالدليلوالعنصرالمميزللخبرةعنغيرهامنإجراءاتالإث باتكالمعاينة،الشهادةوالتفتيش.

ويقصدبها مساعدةفنيةتقدمللقاضيأوالمحققفيمجالالإثبات لمساعدتهفيتكوينعقيدتهنحوالمسائلالتييحتاجتقريرهاإلىمعرفةفنيةأودراية علميةلاتتوافرلديه.

يطلقلفظالخبيرعلىكلشخصتوافرلديهمعرفةعمليةوفنيةلتخصصهفي مادةمعينةوتستعينبهالسلطةالقضائيةوجهاتالتحقيقفيتقديرالمسائلالفنية استكمالالنقصمعلوماتالقاضيفيهذهالنواحي،ومساعدتلهفياكتشافالحقيقة لهذاالغرضيجبأنيتوفرلديهاالقدرةعلىتطبيقتلكالقواعدالنظريةعلىالحالات الواقعيةولايتحققذلكإلابالممارسةالعملية.[3]

أ / مجالاتالخبرةبالنسبةللجرائمالالكترونية:

(1) محمدالأمينالبشري/ مؤتمرالقانونوالكمبيوتروالإنترنت،جامعة،"التحقيقفيجرائمالحاسبالآلي"،جامعةالإماراتالعربيةالمتحدة،كليةالشريعةوالقانون،1-3مايو2000،المجلدالثالث،ص:1058.

(2)حسينبنسعيدالغافري/"التحقيقوجمعالأدلةفيالجرائمالمتعلقةبشبكةالإنترنت" http://www.eastlaws.comاطلععليهبتاريخ 22-04-2019 علىالساعة 13:23.

(3) محمدفاروقعبدالحميدكامل/القواعدالفنيةالشرطيةللتحقيقوالبحثالجنائي،أكاديميةنايفالعربيةللعلومالأمنية،الرياض،الطبعةالأولى، 1999 ،ص:286.

تتنوعالعملياتالإلكترونيةبتنوعالمجالاتالتيتستخدمشبكةالإنترنت،فنجدأمثلة لهافيالأعمالالمصرفية،الإدارةالإلكترونية،والتجارةالإلكترونية،ولذلكفإنهيتصور تنوعالجرائمالتيتقععلىهذهالعملياتوفقالنوعالعملياتالإلكترونيةالمستخدمةفيارتكابها.

تقتضيعملياتالبحثالجنائيوالتحقيقفيجرائمالإنترنتالاستعانةبخبرات عديدةومتنوعة،فإناختيارخبيرفينوعيةالإجرامفيمجالالإنترنتالذيتندرج الواقعةالمرتكبةفياختصاصهيغدوأمرابالغالأهمية،ويمكنالاسترشادفيعملية الاختيارهذهبتصنيفلهذاالإجرام،يرتكزعلىنوعيةالأساليبالمستخدمةفيالارتكاب إلىمايلي[1]:

- تزويرالمستنداتالمدخلةفيأنظمةالحاسباتالآليةأوالناتجةبعدالمعالجة.
- التلاعبفيالبيانات.
- التلاعبفيالبرامجالأساسيةأوبرامجالتطبيقات.
- الغشأثناءنقلوبثالبيانات

ب /الشروطالمتطلبةفيالخبرةفيمجالالجرائمالمرتكبةعبرالإنترنت:

تقتضيفاعليةالخبرةضرورةالجمعبينالتعمقفيكلمنالدراسةالعلمية والنظريةوالممارسةالعمليةللتخصصالعلميوالنظري،وكذامتابعةمستمرةللتطورات التيتلحقبفروعالتخصص،غيرأنذلكليسشرطالازمافيبعضالأحيانفقد يقتصرالخبيرعلىمجردالخبرةالعمليةفيفرعالتخصصدونأنيكونهناكرصيد منالدراسةالعلميةوالنظريةوهوالأمرالذينلاحظهفيمجالاتالخبرةفيالفروع المهنيةالمختلفة،منهامجالالحاسبالآلي،حيثيتعينفيخبراءالحاسبالآلي المنتدبينللتحقيقأنتتوافرلديهمالقدرةالفنيةوالإمكاناتالعلميةفيالمسألةموضوع الخبرة،ولايكفيفيذلكحصولالخبيرعلىشهادةعلمية،بليجبمراعاةالخبرة العمليةلأنهاهيالتيتحققالكفاءةالفنية،ولذلكلاوجودلخبيرلديهمعرفةمتعمقةفي سائرأنواعالحاسباتوبرمجياتهاوشبكاتها،أولديهاالقدرةعلىالتعاملمعكلأنواع الجريمةالمرتكبةعبرالإنترنت.[2]

الخاتمة:

وختاما لما تقدم ذكره ارتأينا ذكر بعض الاقتراحات او التوصيات في شكل فقرات كالاتي:

❖ **على مستوى البحث و التحري:**

➢ ضرورةتخصيص ضباط شرطة قضائيةخاصةلمكافحةالجرائمالمعلوماتية.

---

(1) هشاممحمدفريدرستم/"الجرائمالمعلوماتيةأصولالتحقيقالجنائيالفنيواقتراحإنشاءآليةعربيةموحدةللتدريبالتخصصي " 1-3ماي 2000 ،جامعةالإمارات-بحوثمؤتمرالقانونوالكمبيوترو الإنترنت،العربيةالمتحدة،كليةالشريعةوالقانون،المجلدالثاني،الطبعةالثالثة2004 ،ص:407 .

(2) عبدالفتاحبيوميحجازي/مبادئالإجراءاتالجنائيةفيجرائمالكمبيوترو الإنترنت،دارالفكرالجامعي،الإسكندرية،الطبعةالأولى، 2006،ص:138.

- جعل القواعد الخاصة بالبحث والتحري سلسة ولا تتطلب إجراءات معقدة.

❖ **على مستوى الإجراءات التقاضي:**

- ينبغيمواكبة قواعدالإجراءاتالجزائيةلتتلاءممعهذهالجرائم.
- استحداث اقسام خاصة بالجرائم المعلوماتية في المحاكم و المجالس.
- ضرورة تخصص قضاة في هذا النوع من الإجرام.

❖ **على مستوى التعاون الدولي:**

- ضرورةالتنسيقوالتعاونالدوليقضائياوإجرائيافيمجالمكافحةالجرائمالمعلوماتية.
- تعزيزالتعاونوالتنسيقمعالمؤسساتالدوليةالمعنيةبمكافحةالجرائمالمعلوماتية،وخصوصا الإنتربول.

قائمة المراجع:

اولا : باللغة العربية

أ/ الكتب:

1 _كري يوسف بكري/التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية 2011.

2-خالدعيادالحلبي/إجراءاتالتحريوالتحقيقفيجرائمالحاسوبوالانترنيت،دارالثقافة،الأردن،ط1 2011 .

3 _ خالدممدوحإبراهيم/أمنالجريمةالإلكترونية،دارالجامعية،الإسكندرية،الإسكندرية، 2008 .

4 _خالدممدوحإبراهيم/فنالتحقيقالجنائيفيالجرائمالالكترونية،دارالفكر،الإسكندرية،2009 .

5-رشيد خلوفي/قانون العقوبات،كليك للنشر،المحمدية،الجزائر،2017.

6-عبدالفتاحبيوميحجازي/الدليلالجنائيوالتزويرفيجرائمالكمبيوتروالإنترنتدراسةمتعمقةفيجرائم الحاسبالآليوالإنترنت،بهجاتللطباعةوالتجليد،مصر، 2009

7-عبدالفتاحبيوميحجازي/جرائمالكمبيوتروالأنترنتفي التشريعاتالعربية"دراسةمقارنةمعالتطبيقعلىنظاممكافحةجرائمالمعلوماتيةفيالمملكةالعربيةالسعودية،ط1 ، دار . النهضةالعربية،الإسكندرية، 2009.

8-علي عبد الله القهوجي/الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999.

10-محمد عبيد الكعبي/الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت،دار النهضة العربية،القاهرة،2006

ب _الرسائل والمذكرات :

-

1معتوقعبداللطيف/الإطارالقانونيلمكافحةجرائمالمعلوماتيةفيالتشريعالجزائريوالتشريعالمقارن،مذكرةمكملةلنيلشهادةالم اجستيرفي علومالجنائية،2011 -2012 .

2-سفيان سوير، جرائم معلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، سنة 2010-2011.

4-بلالبنجامع/المشكلاتالأخلاقيةوالقانونيةالمثارةحولشبكةالانترنيت،ماجستيرفيعلمالمكتباتتخصص إعلامعلميوتقني،جامعةمنتوري،قسنطينة،

5-محمد بن نصير محمد السرحاني/مهارت التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت- دارسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، تخصص، القيادةالأمنية،جامعةنايفالعربيةللعلومالأمنية،كليةالدراساتالعليا،قسمالعلومالشرطية،الرياض،2004 .

ج_ القوانين

1-الأمر رقم 04-15 المؤرخ في رمضان 1425الموافق ل:10نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات.

2-اتفاقية برن سنة 1971.

3-الاتفاقية الدولية للإجرام المعلوماتي.

4-معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية 1990 .

5-اتفاقية تتعلق بالتعاون القضائي المتبادل في الشؤون المدنية والتجارية ج.ر رقم 92، سنة 1970.

6-معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999.

7-اتفاقية بودابست،في23نوفمبر/تشرينالثاني2001.

ثانيا: المراجع بالغة االفرنسية

2-DEBRAY Stéphane, Internet face aux substances illicites : complice de laUne cooperation international estindespensable, carles paysqui ne se pas dotes de lois contrela cybercri minalite sont des paradisnumerique voir chernaouti heli slange

مواقع الأنترنت

https://ar.wikipedia.org/wiki

http://arblawinfo.com

http://www.eastlaws.com

بخوش هشام
h.bekhouche@univ-soukahras.dz
جامعة محمد الشريف مساعدية سوق أهراس

حندل رشيد
r.handel@univ-soukahras.dz
جامعة محمد الشريف مساعدية سوق أهراس

فعالية التشريعات العقابية في مكافحة الجريمة الإلكترونية

ملخص

لقد تطورت الظاهرة الإجرامية في العصر الحديث تطورا ملحوظا سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها وذلك باستخدام أخر ما توصلت إليه العلوم التقنية والتكنولوجية وتطويعها في خدمة الجريمة ولما كانت جرائم الحاسبات الالكترونية ظاهرة إجرامية حديثة النشأة لتعلقها بتكنولوجيا المعالجة الآلية للمعلومات فقد اكتنفها الغموض، وأن تطبيق النصوص التقليدية على هذه الأنماط المستحدثة من الجرائم قد أسفر عن الكثير من المشكلات القانونية حيث اختلفت أراء الفقهاء بشأن تطبيق النصوص التقليدية عليها، سنحاول من خلال هذه المداخلة استعراض وتحليل القوانين الوطنية الخاصة بالجرائم المعلوماتية لبعض الدول وكيفية معالجة كل منها لهذه الجريمة داخل حدودها، وعليه تتبلور مشكلة الدراسة حول ما مدى فعالية القوانين الوطنية للجرائم المعلوماتية في نطاقها المحلي في التصدي للجريمة المعلوماتية.

Abstract:

The criminal phenomenon has grown in modern development with noticeable development, whether by people who have been delivered or developed, using the latest findings and adapting them to the traditional service. Through this intervention, we will try to review and analyze the national laws on information crimes for some countries and how each of them deals with this crime within its borders, and accordingly the problem of the study crystallizes about the effectiveness of national laws for information crimes in their local scope in addressing information crime.

مقدمة

لقد رافق التطور الكبير الذي شهده العالم منذ منتصف القرن الماضي تطورات في مختلف جوانب الحياة في المجتمع مما أدى إلى ظهور صعوبة في تسيير الأمور العادية الشيء الذي أدى إلى التفكير بوسيلة يتم من خلالها تجاوز هذه الصعوبات إلى أن ظهر الكمبيوتر أين يتم من خلاله المعالجة الآلية للمعلومات، ولم يقتصر استخدامه على الشركات والمؤسسات بل امتد إلى الأفراد لما فيه من مزايا أين يتم تجميع و تركيب وترتيب واسترجاع المعلومات في وقت قصير وبدقة متناهية، إلا أن استخدامه بطريقة غير مشروعة أدى إلى ظهور ما يسمى بالجرائم المعلوماتية أي استخدامه عادة في إرتكاب الجرائم التقليدية كسرقة الأموال عن طريق اختراق نظام الكمبيوتر أو سرقة المعلومات عن طريق اختراق شبكة اتصالات معلوماتية، أو العدوان على

البرامج عن طريق قرصنتها وهو اعتداء على الملكية الفكرية والذي ينتج عنه خسائر كبيرة مباشرة أو غير مباشرة، بالإضافة إلى نشر فيروسات تساهم في تدمير النظم المعلوماتية وإتلاف البرامج وتزوير المستندات، ومهاجمة المراكز المالية والبنوك،والإرهاب الإلكتروني،ونشر الشائعات والنيل من هيبة الدول، إضافة إلى نشر الرذيلة والإباحية وغيرها من الجرائم الإلكترونية.

إن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة، أو ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية ومدى ملائمة النصوص القانونية في مواجهة مثل هذه الأفعال، ولما كان القاضي الجزائي مقيدا عند نظره في الدعوى الجنائية بمبدأ شرعية الجرائم والعقوبة، فإنه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا على مستوى عال من الخطورة الإجرامية، وهذا وفقا لمبدأ لا جريمة ولا عقوبة ولا تدبير أمن إلا بنص.

تكمن **أهمية** هذه الدراسة في أن الجرائم المعلوماتية هي ظاهرة إجرامية حديثة النشأة اكتنفها الكثير من الغموض أدى إلى القول أنها جرائم عادية يمكن تطبيق النصوص الجزائية التقليدية بشأنها، غير أن تطبيق هذه النصوص على هذا النوع من الأنماط المستحدثة من الجرائم أسفر عن الكثير من المشكلات القانونية، منها من أيد تطبيق النصوص التقليدية عليها، ومنها من اعتبر هذه الأفعال سلوكا مباحا لم يرد بشأنه نص يجرمه التزاما بمبدأ الشرعية الجزائية والذي يقضي بأن (لا جريمة ولا عقوبة إلا بنص).

تهدف هذه الدراسة إلى التأكيد على أن مبدأ الإقليمية المطبق في مكافحة الجريمة الإلكترونية مبدأ يفقد صلاحيته للتطبيق بالنسبة لمثل هذا النوع من الجرائم على اعتبار أنها جرائم عالمية تحتاج إلى تعاون دولي لمواجهتها، واستصدار المشرع الجزائري لنصوص المواد من 394 مكرر إلى 394 مكرر 7 لمعاقبة مرتكبي الجرائم الإلكترونية غير كاف، مع عدم تهيئة الأسس التقنية الكفيلة بتصنيف درجات هذه الجرائم وتحديد أضرارها قبل إصدار العقوبة، هذا فضلا عن غياب التواصل الدائم بين القضاء والمختصين في الاتصالات، ما أفرز غموض في شأن العقوبات الدقيقة في مثل هذه الجرائم، والملاحظ من خلال هذه النصوص أن القانون الجزائري يعاقب في الغالب مرتكبي هذه الجرائم بالسجن القصير المدى الذي لا يزيد عن ثلاث سنوات أو بالغرامة المالية، بحكم أن جل الجرائم الإلكترونية المرتكبة في الجزائر تصب أو تصنف قانونيا كسرقة.

أما بالنسبة **للمنهج** المتبع في هذا البحث، هو المنهج الوصفي الذي يقوم على تحليل المضمون والمقارنة مع بعض القوانين الأخرى، حيث سيتم وصف نصوص المواد المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات وتحليل مضمونها ومقارنتها وإبراز الفوارق بينها لمعرفة مدى قصورها في التصدي للجريمة المعلوماتية والوصول للنموذج المقترح.

تتمحور إشكالية البحث في **ما مدى إمكانية استعانة القاضي بقانون العقوبات التقليدي لتوفير الحماية من هذا النوع من الجرائم ؟** خاصة أن المشرع لم يكن في ذهنه وقت وضع النصوص التقليدية هذا النوع من الجرائم، على اعتبار أن القانون الجنائي له مبادئه وأصوله وعلى رأسها مبدأ الشرعية والذي يتفرع عنه مبدأي التفسير الضيق وخطر القياس في مجال التجريم، **فهل يستطيع القاضي الجزائي من خلال النصوص الحالية تحقيق حماية جزائية معلوماتية دون المساس بالمبادئ الراسخة التي يرتكز عليها القانون الجنائي ؟** ومن

أجل الإحاطة بهذا الموضوع قسم هذا البحث إلى مبحثين، نتناول في المبحث الأول الجرائم المعلوماتية في التشريع الجزائري، آليات مكافحة الجرائم المعلوماتية .

المبحث الأول: الجرائم المعلوماتية في التشريع الجزائري.

حققت تكنولوجيا المعلومات والإتصالات فوائد عديدة تزايد الإعتماد عليها في مجالات الحياة كافة، وبقدر ما أفرزته الوسائل التقنية الحديثة في مجال الرقي والتقدم الإنساني، بقدر ما مهدت إلى بروز أنماط جديدة من الجرائم بالغة الخطورة (الشهري، 2011، صفحة 06) ألا وهي (جرائم المعلوماتية) لارتباطها بنظم المعالجة الالية للمعلومات وهي ظاهرة اجرامية حديثة النشأة لتعلقها بتكنولوجيا الحاسبات الالية وقد اكتنفها الغموض إلى حد القول أنها جرائم عادية يمكن تطبيق النصوص الجزائية التقليدية بشأنها.

غير ان تطبيق النصوص التقليدية على هذه الأنماط المستحدثة من الجرائم أدى إلى حدوث الكثير من الإشكالات القانونية اختلفت بشأنها اراء الفقهاء وتضاربت فيها أحكام القضاء أين طبقت النصوص التقليدية على مثل هذه الجرائم واعتبرته أحكام اخرى سلوكا مباحا لم يرد بشأنه نص يجرمه التزاما بمبدأ الشرعية الجزائية والذي يقضي بأن (لا جريمة ولا عقوبة إلا بنص) (الشكري، 2008، صفحة 111).

أما بالنسبة لمسألة وضع تعريف للجريمة المعلوماتية فقد كانت محلا لاجتهادات الفقهاء، أين تناولوا تعريفها من عدة زوايا منها القانونية ومنها تقنية (فنية) والتي تعني بأن الجريمة المعلوماتية هي (**نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود)** (البشري، 2005، صفحة 06)، وهناك جانب من الفقه من يعتبر هذه الجريمة جريمة مستترة، تتسم بالسرعة والتطور في وسائل ارتكابها، وهي أقل عنف في التنفيذ من الجرائم التقليدية، وعابرة للحدود، ويصعب إثباتها، وهناك اتجاه في الفقه يذهب إلى تعريف الجريمة المعلوماتية اعتماداً على وسيلة ارتكاب الجريمة وغيرها من التعريفات الأخرى (الشكري، 2008، صفحة 112).

المطلب الأول: الجرائم الإلكترونية في ظل قانون العقوبات الجزائري.

استحدث المشرع الجزائري مؤخرا ولو نسبيا نصوص عقابية لقمع المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون 15/04 المؤرخ في 2004.11.10 المتضمن تعديل قانون العقوبات ولكنه أغفل الاعتداءات الماسة بمنتجات الإعلام الآلي، وقد تطرق في المادة 394 مكرر إلى الدخول غير المشروع أو حذف أو تغيير المعطيات أو تخريب نظام المعالجة الآلية للمعطيات، وسواء كانت الجريمة تامة أو شرع في ارتكابها ويتضح ذلك من خلال كلمة "**أو يحاول ذلك**" (04/15، 2004) ويقصد بمحاولة الدخول أو البقاء في النظام المعلوماتي، الشروع في إرتكاب الجريمة دون تحقيق النتيجة، وفي هذه الحالة يعاقب الجاني بنفس عقوبة الذي تمكن من إرتكاب الفعل، ويتمثل الشروع في جملة من التصرفات أولها مادية من خلال إرتكاب الجاني السلوك الإجرامي (اللبيدي، دون سنة طبع، صفحة 02) وثانيها توافر النية الجرمية، وبسبب غموض التكييف القانوني لفعل الدخول أو البقاء سواء في القانون الفرنسي من خلال نص المادة 323–1 من قانون العقوبات الفرنسي أو القانون الجزائري في المادة 394 مكرر (نسيم، 2013، صفحة 28) وبسبب غياب

اجتهادات قضائية جامعة وفاصلة ظهرت بعض الاجتهادات الفقهية حول هذا الموضوع.
(LEMARTELEUR، Le scan de port : une intrusion dans un STAD ?، 2008)

الملاحظ بالنسبة للمادة 394 مكرر ان موضوع **حيازة** أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات لا تقوم إلا إذا كانت على شيء مادي أي على جهاز أو أوراق أو أي شيء أخر مادي، وعدا ذلك لا يمكن أن تقوم الجريمة الإلكترونية لأن حيازة المعلومات الإلكترونية يمكن أن تتم عن طريق الالتقاط الذهني بالبصر أو بالسمع.

أما في نص المادة 394 مكرر 1 فقد تطرق المشرع إلى جريمة **التزوير** في نظام المعالجة الآلية للمعطيات من خلال إدخال أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها النظام، ويقصد بذلك إتلاف وتدمير المعطيات بأي طريقة كانت، (04/15، 2004) فالدخول في الأنظمة المعلوماتية يعتبر جريمة إذا تم بطريقة عمديه أو احتيالية وبالتالي الدخول الخطأ لا يعاقب عليه القانون، (04/15، 2004) وعلى ذلك فإن عملية الدخول في النظام المعلوماتي باعتبارها مسألة تقنية بحتة تتم بالاتصال المادي المباشر بالنظام المعلوماتي أو بالاتصال المعنوي عن بعد وهذا ما نصت عليه المادة 323–1 فقرة 1 من القانون الفرنسي، (الصغير، 1992، صفحة 150)

وفي نص المادة 394 مكرر 2 تطرق المشرع إلى جريمة الاستيلاء على المعطيات عندما يقوم أي شخص **عمدا** وبطريق الغش تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية أو **حيازة** أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم السابق ذكرها. (04/15، 2004)

يقصد هنا المشرع الجزائري جريمة الاحتيال المعلوماتي يستخدم فيها الجاني كافة الوسائل التقنية للتوصل إلى البيانات المالية أو التي تتصل بحقوق مالية أو قيامه بأعمال احتيالية موجهة لنظام الكمبيوتر فيجني المنافع المادية عن طريق العبث بالبيانات أو البرامج أو حتى عمليات النظام ذاته، أو الاحتيال باستغلال مواقع الإنترنت لجني مبالغ ماليه عبر مشاريع وهمية لمنتجات أو خدمات أو من خلال الوصول إلى أرقام بطاقات ائتمان .

وبسبب عدم وجود نشاط مادي مجسم يتحقق به فعل الاستلام في جرائم خيانة الأمانة لا يمكن خضوع البرامج والمعلومات للنشاط الإجرامي في هذه الجريمة، وهذا ما نصت عليه المادة 376 من قانون العقوبات الجزائري باعتبار أن الاختلاس يقع على مال منقول سلم إلى الجاني بمقتضى عقد من عقود الأمانة، وعليه لا تقع جريمة خيانة الأمانة على غير المنقولات المادية، كما لا يوجد نشاط مادي يتحقق به التسليم والاستلام في جريمة النصب، وحتى لو تم ذلك فانه لن ينتج عنه حرمان المجني عليه من المعلومات التي نقلها بالقول بل تظل تحت سيطرة من نقلها وفي حوزته وهو أمر وان كان يتفق وطبيعة البرامج والمعلومات إلا انه لا يتفق وطبيعة النشاط الإجرامي في جريمة النصب وهذا يعني عدم صلاحية البرامج للخضوع للنشاط الإجرامي في جريمة النصب، وهذا ما نصت عليه المادة 372 ق ع بأنه ليس كل شيء مادي ومنقول يصلح أن يكون

محلا لجريمة النصب بل يجب أن يكون ضمن الأشياء التي عددتها هذه المادة على سبيل الحصر. (فشار، 2009)

أما بالنسبة للفقرة الثانية من المادة 394 مكرر2 فقد حدد المشرع النتيجة المتوصل إليها من خلال إرتكاب الغش في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، (04/15، 2004، الصفحات 11–12) وأولها الحيازة، والتي يقصد بها نقل الشيء أو نزعه من حيازة المجني عليه وإدخاله في حيازة الجاني بشرط أن يكون على جهاز أو أوراق أو أي شيء أخر مادي، أما إذا احتفظ الشخص بالمعلومة في ذهنه دون تسجيل أو تدوين فانه لا يقع تحت طائلة قانون العقوبات.

لو تم الرجوع إلى نص المادة **350** من قانون العقوبات الجزائري "كل من اختلس شيئا غير مملوك له يعد سارقا " نجد أن الجاني في جريمة السرقة وان كان يدخل في ذمته ما استولى عليه من برامج إلا انه في نفس الوقت لم يخرج هذه البرامج من ذمة صاحبها الشرعي إذ تظل رغم مباشرة أفعال الاختلاس عليها تحت سيطرة هذا الأخير دون انتقاص من محتواها، بالإضافة إلى أن هذه المعلومات قد انتقلت من ذهن إلى ذهن أو من ذاكرة إلى ذاكرة وأنها من طبيعة غير مادية أي أنها شيء معنوي فكيف يتصور أن يرد فعل الاختلاس الذي هو من طبيعة مادية لذلك ليس من السهل بسط أحكام السرقة على برامج الحاسب الآلي وخاصة في حالة سرقة المعلومات عن طريق النسخ غير المشروع للبيانات المخزنة الكترونيا. (فشار، 2009)

أما الجزاءات المقررة بموجب القسم السابع مكرر فتتمثل في العقوبات الأصلية و هي عقوبة الحبس و الغرامة، فقد نصت المادة 394 مكرر 4 على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في القسم السابع مكرر بغرامة تعادل 05 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي غير أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة، (04/15، 2004) و الشروع في الجريمة المعلوماتية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها و هو ما نصت عليه المادة 394 مكرر 7 من قانون العقوبات. (04/15، 2004).

أما العقوبات التكميلية نصت عليها المادة **394 مكرر 6** وتتمثل في مصادرة الأجهزة والبرامج و الوسائل المستخدمة والمحل أو أماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، و قد أورد المشرع ظروفا تشدد في حالة الدخول و البقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب للنظام أو إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام، (04/15، 2004) وبموجب المادة **394 مكرر 5** جرم الاشتراك (سواء شخص طبيعي أو معنوي) في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية – بعقوبة الجريمة– و كان التحضير لهذه الجرائم مجسدا بفعل أو بعدة أفعال مادية. (04/15، 2004).

المطلب الثاني: الجرائم الإلكترونية في ظل النصوص القانونية الأخرى.

1 – القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

أغفل المشرع الجزائري تعريف مصطلح "**معالجة آلية**" عند تناوله للمواد المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، واكتفى بتقرير عقوبات للشخص الطبيعي والمعنوي حال المساس بهذه الأنظمة أو حتى الشروع في ارتكابها في المواد 394 مكرر إلى غاية 394 مكرر 7 ، لكنه تدارك ذلك بالقانون 09-04 حيث نصت المادة 2 على أن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال هي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

أما بالنسبة للمنظومة المعلوماتية فهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، وبخصوص المعطيات المعلوماتية فهي عملية عرض للوقائع المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها. (مريم، 2013، صفحة 08).

يتضح من خلال هذا التعريف أن المشرع الجزائري عرف المنظومة المعلوماتية بأنها أي نظام أو مجموعة من الأنظمة منفصلة كانت أم متصلة ببعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، وبذلك يكون المشرع الجزائري قد أخذ بالتعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي (على، 2016) (إتفاقية بودابست) (بودابست، 2001) .

وبخصوص مجال تطبيق القانون فقد تمت الإشارة إلى انه وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائرية وفي هذا القانون ومع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية، (القانون 09-04، 2009، صفحة 06) وينص القانون في شقه المتعلق بمراقبة الاتصالات الالكترونية على الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية. (القانون 09-04، 2009).

حدد القانون من جهة أخرى قوانين الإجراءات المتعلقة بتفتيش المنظومات المعلوماتية حيث يتعين على مانحي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها، (القانون 09-04، 2009) وتطرق النص أيضا إلى التزامات مانحي خدمات الانترنت، وبخصوص التعاون والمساعدة القضائية الدولية أشار القانون إلى أن المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المرتكبة خارج الاقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني. (القانون 09-04، 2009).

2- الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة. (05-03، 2003، صفحة 04) .

نظم المشرع الجزائري قانون الملكية الأدبية والفنية بمقتضى الأمر **14/73** المؤرخ في 1973/04/03 المعدل والمتمم بمقتضى الأمر **10/97** المؤرخ في 1997/03/06 المعدل والمتمم بموجب الأمر **05/03** المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة، وقد عرف المشرع " **المصنف الأدبي والفني**" في المادة الأولى من الأمر **14/73** ونصت المادة **2** منه على المصنفات التي تشملها حماية حق المؤلف دون ذكر حماية البرامج المعلوماتية.

وفي تعديل قانون حق المؤلف بمقتضى الأمرين 10/97 – 05/03 ادمج المشرع الجزائري برامج الإعلام الآلي ضمن المصنفات الأصلية، حيث نصت المادة 4 من الأمر 05/03 تعتبر على الخصوص كمصنف أدبية أو فنية، المصنف الأدبية المكتوبة، مثل المحاولات الأدبية، والبحوث العلمية والتقنية، والروايات والقصص، والقصائد الشعرية، وبرامج الحاسوب .... (فشار، 2009).

بالإضافة إلى القوانين سالفة الذكر هناك بعض النصوص التشريعية المتصلة بمكافحة الجريمة المعلوماتية منها القانون 03/2000 المؤرخ في 05 أوت 2000 المحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، (03-2000، 2000، صفحة 03) بالإضافة إلى نص المادة 323 مكرر 1 من القانون المدني التي تنص على أن الإثبات بالكتابة في الشكل الإلكتروني يعتبر كالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها. (05-10، 2005، صفحة 24) .

المبحث الثاني: مدى فاعلية التشريع العقابي الجزائري في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

بعد التقدم العلمي والتكنولوجي في مجال المعلوماتية، وانتشار المعالجة الالية للمعلومات واتساع نطاق التجريم المعلوماتي، وتدخله في كافة نواحي الحياة الإدارية والاقتصادية والسياسية والاجتماعية والحياة الشخصية والحريات الفردية وأمن المواطنين وإسرارهم ونظرا لحداثة الجرائم المعلوماتية وتطورها السريع وسهولة ارتكابها وإدراكا لخطورتها وأثارها السلبية على الأشخاص والأموال، تدخل المشرع الجزائري لحماية المجتمع من هذه الظاهرة الاجرامية المستحدثة بوضع قواعد قانونية جديدة لمكافحة الإجرام المعلوماتي وسنتناول ذلك في مطلبين، نتناول في المطلب الأول، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، وفي المطلب الثاني، الجرائم الإلكترونية في ظل قانون الإجراءات الجزائية.

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

أصدر رئيس الجمهورية مرسوم رئاسي رقم 15-261 مؤرّخ في 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نص في

مادته الاولى على انه تطبيقا لأحكام المادة 13 من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها يهدف هذا المرسوم تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تدعى في صلب النص "**الهيئة**، (15-261، 2015، صفحة 16) وحسب نص المادة الثانية تعتبر هذه الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل، (15-261، 2015) وهو نفس الأمر لما هو في فرنسا إذ أُنشِأت الوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال Office central de lutte contre la criminalité liée aux technologie de l'information et de la communication (Décret no 2000-405 du 15 mai.2000, 2000)وهي هيئة تابعة للمديرية العامة للشرطة الوطنية الفرنسية وخاضعة للمديرية المركزية للشرطة القضائية. (Judiciaire، 2013) .

الفرع الأول: مهام الهيئة.

تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون رقم 04/09 المؤرخ في 5 أوت سنة 2009 تحت رقابة السلطة القضائية طبقا لأحكام التشريع الساري المفعول لا سيما منها قانون الإجراءات الجزائية والقانون والمذكور أعلاه تكلف الهيئة في ظل احترام الأحكام التشريعية المبينة أعلاه على الخصوص بما يأتي:

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (15-261، 2015، صفحة 17) وتكون إجراءات الوقاية بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم، التجسس على الاتصالات والرسائل الالكترونية، التلاعب بحسابات العملاء أو ببطاقات ائتمانهم، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية..الخ. (مريم، 2013)

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وهو ما نصت عليه المادة 14 فقرة ب من القانون 04/09، وبالنسبة للوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال بفرنسا فإن لها مهام أدرجها المرسوم رقم 2000 -405 المؤرخ في 15 ماي 2000 المتضمن إنشاء هذه الهيئة فهي تتمثل في تنشيط وتنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين والمشتركين في ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

بالإضافة إلى ذلك تقوم الهيئة بإذن من السلطات القضائية بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة لمصالح الشرطة القضائية المختصة بتحقيقات لجرائم خاصة ارتكبت أو سهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال، ولكن دون المساس باختصاص باقي الهيئات الوطنية المختصة

بمكافحة جرائم معينة نص عليها القانون، وكذا تقديم المساعدة لمصالح الأمن والدرك الوطنيين، ولجميع إدارات ومصالح الدولة المركزية فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك. (مريم، 2013، صفحة 46).

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

– تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، (15–261، 2015، صفحة المادة 04) وفي هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثمّ مشاركة المنظمات المماثلة لها على المستوى الدولي، دون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم. (مريم، 2013، صفحة 46).

الفرع الثاني: تشكيل الهيئة وتنظيمها.

تضم الهيئة لجنة مديرة ومديرية عامة ومديرية للمراقبة الوقائية واليقظة الإلكترونية ومديرية للتنسيق التقني ومركز للعمليات التقنية وملحقات جهوية، (15–261، 2015، صفحة 17) حيث يرأس اللجنة المديرة الوزير المكلف بالعدل وتتشكل من الوزير المكلف بالداخلية والوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال وقائد الدرك الوطني والمدير العام للأمن الوطني وممثل عن رئاسة الجمهورية وممثل عن وزارة الدفاع الوطني وقاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء. (15–261، 2015، صفحة 17).

تكلف اللجنة المديرة على الخصوص بتوجيه عمل الهيئة والإشراف عليه ومراقبته ودراسة كل مسألة تخضع لمجال اختصاص الهيئة لاسيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 04–09 المؤرخ في 5 أوت سنة 2009، بالإضافة إلى ذلك تختص الهيئة بضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه والقيام دوريا بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة، واقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ودراسة مشروع النظام الداخلي للهيئة والموافقة عليه، بالإضافة إلى دراسة مشروع ميزانية الهيئة والموافقة عليه ودراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه وإبداء رأيها في كل مسألة تتصل بم هام الهيئة وتقديم كل اقتراح مفيد يتصل بم جال اختصاص الهيئة. (15–261، 2015، صفحة 17).

أما المادة 11 فتنص على أن مديرية المراقبة الوقائية واليقظة الإلكترونية تكلف على الخصوص على تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول، وإرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة، بالإضافة إلى تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم وكذا جمع واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذا تنظيم و /أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال وحول المخاطر المتصلة بها وتنفيذ توجيهات اللجنة المديرة وتزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال. (15-261، 2015، صفحة 17).

تكلف مديرية التنسيق التقني على الخصوص بإنجاز الخبرات القضائية في مجال اختصاص الهيئة وتكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها وإعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال والقيام بمبادرة منها أو بناء على طلب اللجنة المديرة بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها. (15-261، 2015، صفحة 17).

المطلب الثاني: الجرائم الإلكترونية في ظل قانون الإجراءات الجزائية.

تناول قانون الإجراءات الجزائية المعدل بموجب القانون 14/04 المؤرخ في 2004/11/10، استحداث المحاكم الجزائية ذات التخصص الموسع، التي أجيز لها تمديد اختصاصها للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهذا في المواد **37** (تمديد الاختصاص المحلي لوكيل الجمهورية) والمادة **40** (تمديد الاختصاص المحلي لقاضي التحقيق) والمادة **329** (تمديد الاختصاص المحلي للمحكمة). (الإجراءات، 2004).

كما نص المشرع الجزائري في المادة **45** من قانون الإجراءات الجزائية على إمكانية تفتيش المساكن دون حضور المشتبه فيه الذي ساهم في ارتكاب جناية، أو الذي يحوز على أوراق أو أشياء لها علاقة بالأفعال الإجرامية، ونص في المادة **47** من ق إ ج على إمكانية التفتيش دون حضور صاحب المسكن ودون حضور الشهود، وأكد على إمكانية تفتيش المحلات السكنية وغير السكنية في كل ساعة من ساعات الليل والنهار بإذن من وكيل الجمهورية، ونص في المادة **16** من ق إ ج على تمديد الاختصاص الإقليمي لضباط الشرطة القضائية في كامل التراب الوطني، ونص في المادة **51** على إمكانية تمديد فترة التوقيف مرة واحد في حالة التلبس. (06-22، 2006).

أما المادة 65 مكرر 5 فقد أكدت أنه إذا اقتضت ضرورات التحري في الجرائم المتلبس بها أو التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو الإرهاب أو الجريمة المنظمة أو جرائم تبيض الأموال يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل

الاتصال السلكية واللاسلكية، ووضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة او سرية، وبالتالي لا يمكن اعتراض مراسلات في إطار تحريات الشرطة القضائية أو تحقيقات قضائية في جرائم غير تلك المذكورة في هذه المادة، ولكن بصدور القانون 09-04 تبنى المشرع الجزائري مراقبة الاتصالات الالكترونية كإجراء خاص لعمليات الوقاية من الجرائم السالفة الذكر، أو كإجراء تقتضيه التحريات والتحقيقات القضائية.

أكدت المادة 4 من القانون 09-04 على انه يمكن اللُّجوء إلى المراقبة الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وفي حالة في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللّجوء إلى مراقبة الاتصالات الالكترونية، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة كما هو منصوص عليه في المواد 16-17-18 من القانون 09-04. (القانون 09-04، 2009).

أما المادة 65 مكرر 11 فأكدت أنه عندما تقتضي ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية او قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته بمباشرة عملية التسرب. (06-22، 2006).

أما بالنسبة لأحكام المرسوم التنفيذي 06-348 المؤرخ في 5 أكتوبر 2006 فقد نصت على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دائرة اختصاص محاكم أخري ويتعلق الأمر بكل من محكمة سيدي محمد بالجزائر العاصمة ومحكمة قسنطينة ومحكمة ورقلة ومحكمة وهران، وفي نطاق الجرائم المعلوماتية قد يقع السلوك في مكان وتحدث انتيجة في مكان اخر، وفي هذا المجال ينعقد الإختصاص لمكان إرتكاب السلوك أو مكان حدوث النتيجة، وتعد الجريمة المعلوماتية إذا تمت على شبكة الانترنت جريمة مستمرة. (اللطيف، 2012، صفحة 105).

خاتمة

بعد ان اصبح المجتمع المعلوماتي ومنذ اواخر القرن الماضي ومطلع هذا القرن حقيقة واقعة لا تجريد بات واضحا أن هناك قصور في التشريع الجزائي في مجال مكافحة الجرائم المعلوماتية، واذا سلمنا بأن قانون العقوبات بوضعه الحالي لا يكفي لمواجهة هذا النوع الجديد والخطير من الجرائم، فالقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، وكذا ما جاء به قانون الإجراءات الجزائية قد سد بعض من جوانب القصور، ومن النتائج المتوصل إليها ما يلي:

1- تم التوسع في الاختصاص الإقليمي للسلطة القضائية في متابعة جرائم تمس مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

2- عالمية استغلال تكنولوجيات الإعلام والاتصال وخاصة الانترنت أدت إلى حذف الحدود الإقليمية وتدخل المشرع عن طريق تمديد الاختصاص، وكذا متابعة أي شخص حتى لو كان أجنبي إرتكب سلوك إجرامي أو حدثت نتيجة فوق التراب الجزائري.

3- كذلك الأمر بالنسبة لتنسيق القوانين الجزائية العالمية سيؤدي بالتأكيد لإحكام قبضة العدالة على المجرمين في أي دولة يكونون فيها.

4- تبنى المشرع في القانون 09-04 طرق التحري في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال فالمراقبة الالكترونية للاتصالات وتفتيش نظم المعلوماتية أعطى لها القانون صفة الشرعية القانونية بتقنينها وإدخالها ضمن الترسانة الإجرائية الجزائية في القانون الجزائري.

5- تنصيب الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنصوص علاها في القانون 09-04 أمر مهم للوقاية من هذا النوع من الإجرام ومكافحته، وكذلك تقديم المساعدة للسلطات القضائية في التحقيقات الجارية حول هذه الجرائم.

أما بالنسبة للتوصيات فتتمثل في ما يلي

1- تعد مراقبة الاتصالات الالكترونية وتفتيش النظم المعلوماتية من أهم وأخطر الإجراءات التي جاء بها قانون 09-04 لأن هذين الإجراءين يمسان بشكل مباشر الحياة الخاصة للأفراد، فكان من الأحسن بالمشرع وضع قيود قانونية لتبرير اللجوء إلى هذين الإجراءين كما هو الحال بالنسبة للحالة أ من المادة 04 من القانون 09-04.

2- وجب إصدار نصوص جديدة او تعديل النصوص الجزائية القائمة لمواجهة الجرائم المعلوماتية وذلك بتقرير الجرائم وتحديد العقوبات المناسبة لها بغية حماية النظام المعلوماتي.

3- إيجاد أدلة إثبات جديدة تتلائم مع طبيعة هذه الجرائم وذلك لعدم ملائمة ادلة الاثبات التقليدية في القانون الجنائي لإثباتها.

4- اعتماد الدقة القانونية والوضوح عند تحديد انماط السلوك الاجرامي والابتعاد عن التعبيرات الغامضة التي تحمل اكثر من معنى او دلالة.

5- عدم الاقتصار عند التجريم والعقاب على انماط السلوك المحظور المرتكبة حالياً بل يجب مراعاة الابعاد المستقبلية لان تكنولوجيا المعلومات في تطور سريع.

المراجع:

1 – اتفاقية بودباست تم اعتماد الاتفاقية وتقريرها التفسيري من لدن لجنة وزراءمجلس أوروبا في دورتها التاسعة بعد المائة (8 نوفمبر/تشرين الثاني 2001) وفتح باب التوقيع على الإتفاقية في بودابست، في 23 نوفمبر/تشرين الثاني 2001، بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية.
tension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Frm.coe.int%2Fbudapest-convention-in-arabic%2F1680739173&clen=209436

2 – الدكتور إبراهيم محمود اللبيدي، السلوك الإجرامي في جرائم الانترنت، مركز الإعلام الأمني، دون سنة.

3– أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09–04، مذكرة مقدمة لنيل شهادة الماجستير، جامعة ورقلة، 2013.

4– جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، دار النهضة العربية، 1992، مصر (القاهرة).

5– الدكتور حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 27 العدد 53، جامعة نايف العربية للعلوم الأمنية.

6– فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009.

7– عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة الكوفة للعلوم القانونية والسياسية، العدد السابع، 2008.

8– الدكتور محمد الأمين البشري التحقيق في جرائم الحاسب الالي بحث مقدم الى مؤتمر القانون والكومبيوتر والانترنيت كلية القانون والشريعة جامعة الإمارات مايو 2005.

9– معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة ماجستير في العلوم القانونية، جامعة باتنة، 2012.

10– رشدي محمد على، الجرائم المعلوماتية دوليا خطر دولى مواجهة جرائم الإنترنت بين اتفاقية « بودابست» والتشريعات الوطنية، الأهرام، 08 يوليو 2016، العدد 47331، السنة 140.
https://gate.ahram.org.eg/daily/News/536569.aspx

11– دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق، جامعة قسنطينة، 2013.

12– القانون 03/2000 المؤرخ في 05 أوت 2000 المحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الصادر بتاريخ 6 أوت 2000، جريدة رسمية رقم 48.

13– الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة، الصادر بتاريخ 2003/07/23، الجريدة الرسمية رقم 44.

14– القانون رقم 04–14 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66–155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 2004/71.

15– القانون رقم 05–10 المؤرخ في 20 جويلية 2005، جريدة رسمية رقم 44.

16– القانون 22/06 المؤرخ في 20 ديسمبر 2006، جريدة رسمية رقم 84.

17– القانون 09–04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

18– المرسوم الرئاسي رقم 15–261 المؤرّخ في 8 أكتوبر سنة 2015، ج الرسمية عدد 53.

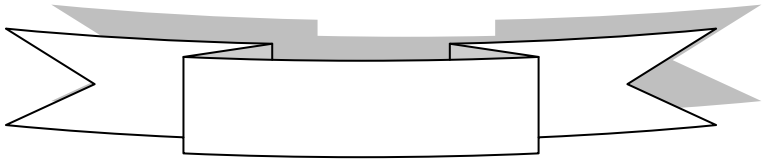
19- Xavier LEMARTELEUR, ***« Le scan de port : une intrusion dans un STAD ? »***, Article de recherche édité sur le site Web : www.juriscom.net le 13/06/2008 à l'adresse : http://www.juriscom.net/pro/visu.php?ID=1074 ***(voir la page de présentation du sujet de recherche)***

18- Bensoussan Alain (sous la direction de), **Internet : aspect juridique**, édition Hermès, juin 1996, (France.

19- http://www.pointdecontact.net/partenaires/oclctic#sthash.furyewvy.dpuf

20- Direction Centrale de la Police Judiciaire . https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire

21- Décret no 2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, JORF no 113 du 16 mai 2000, p. 7338–7339, texte no 19, NOR INTX0004111D.



الزهرة رزايقية
zohrarezaiguia@gmail.com
جامعة 8 ماي 1945 قالمة

أحكام مكافحة الجريمة الإلكترونية في قانون العقوبات الجزائري

Anti-cybercrime provisions in Algerian Penal Code

ملخص

إن تطور الحياة في جانبها التكنولوجي، جعل الجرائم هي الأخرى تأخذ أبعادا جديدة تماشيا وهذه التطورات، فظهر ما يسمى بالجريمة الإلكترونية، وقد أسس لتطور هذه الجريمة وسرعة انتشارها إلى كافة دول العالم الوسائل التكنولوجية الحديثة المستخدمة في إتيانها في مقدمتها 'الانترنت'. الجزائر لم تكن في منأى عن هذه الجريمة، الأمر الذي دفع بمشرعها إلى وضع مجموعة من القواعد القانونية خاصة ضمن قانون العقوبات وهذا لمكافحة هذا النوع من الجرائم الذي مس جميع مناحي الحياة حتى الشخصية منها.

الكلمات المفتاحية: الجريمة الإلكترونية، المجرم الإلكتروني، أنظمة المعالجة الآلية للمعطيات ، قانون العقوبات.

Abstract:

The evolution of life in its technological aspect, has made crimes also take on new dimensions according to these developments, thus the so-called electronic crime has appeared, and it has established the development of this crime and the speed of its spread to all the countries of the world, the modern technological means used for its introduction, in the forefront of which "Internet". Algeria was not immune to this crime, which prompted its legislator to put in place a set of legal rules, particularly within the penal code, in order to combat this type of crime, which affects all aspects of life, even personal ones.

Keywords: *Cybercrime, cybercriminal, automated data processing systems, criminal law.*

مقدمة

إذا كانت الوسائل المستحدثة في مجال التكنولوجيات الحديثة(خاصة مجال الإعلام والاتصال) كالحاسوب ، الهاتف النقال، الأنترنت وغيرها قد ساهمت بشكل كبير في تطوير مجالات متعددة من حياة الأشخاص. فهذه الوسائل والآليات كان لها الأثر الكبير في بروز واستفحال نوع جديد من الجرائم المستعصية والتي قد نشبهها بالمرض المزمن الذي يصعب تشخيصه ومن ثمة يصعب توفير علاج فعال له،إنها الجريمة الإلكترونية التي

أصبحت تهدد استقرار حياة الأشخاص؛الشخصية، الاجتماعية، المالية والاقتصادية. كما لم تسلم اقتصاديات الدول من آثارها الوخيمة.

تصديا لهذه الجريمة الإلكترونية سعى المشرع الجزائري وكغيره من مشرعي مختلف الدول واستئناسا بما أتت به عديد الاتفاقيات الإقليمية[1] منها والدولية[2] في مجال مكافحتها، إلى سن مجموعة من القواعد القانونية منها تلك التي ضمنها في قانون العقوبات [3]، تتلخص في مجموعة من الأحكام الموضوعية تتمثل في إقراره لمجموعة من الجرائم تمثل أصنافا من هذه الجريمة وملحقا بكل صنف العقوبة التي رآها مناسبة لها، بينما تُرك الجانب الإجرائي لمتابعة هذه الجريمة بمختلف أصنافها إلى القانون رقم 09-04[4] وكذا قانون الإجراءات الجزائية[5].

إن البحث في مختلف هذه الأحكام وتبيُن مدى نجاعتها لمكافحة الجريمة الإلكترونية يدفعنا لطرح الإشكالية التالية:

كيف عالج المشرع الجزائري الجريمة الإلكترونية ضمن قانون العقوبات؟ وما مدى نجاعة هذه المعالجة؟

الإجابة على الإشكالية المطروحة تكون من خلال البحث في ماهية هذه الجريمة (أولا) ثم تقصي جملة الأحكام التي كرسها المشرع الجزائري ضمن قانون العقوبات في إطار السياسة الجنائية المتبعة لمعالجة أو بالأصح لمكافحة هذا الصنف من الجرائم، الذي يعرف تطورات سريعة تتماشى والتطورات التي تعرفها التكنولوجيات والمعارف(ثانيا).

أولا: ماهية الجريمة الالكترونية

تحديدالماهية الجريمة الإلكترونية نوضح مفهومها(1) ثم نعرف بفاعلها(2) فدوافعه لإتيانها(3).

1. مفهوم الجريمة الإلكترونية

يمكن أن نُوضح مفهوم الجريمة الإلكترونية بالتعريف بها(أ) وكذا بتقديم جملة من خصائصها(ب).

أ. تعريف الجريمة الإلكترونية

[1] على سبيل المثال: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[2] اتفاقية بودابست المتعلقة بالجرائم الإلكترونية لسنة 2001، يمكن تفحص مضمونها بالرجوع إلى الملف التالي الذي تم الولوج إليه بتاريخ: 2022/05/21، 09:07،
https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf

[3] أمر رقم 66-156، مؤرخ في 18 صفر عام 1386ه الموافق 8 يونيو سنة 1966م، يتضمن قانون العقوبات، جريدة رسمية عدد 49، مؤرخة في 21 صفر عام 1386ه الموافق 11 يونيو سنة 1966م، معدل ومتمم.

[4] قانون رقم 09-04، مؤرخ في 14 شعبان عام 1430ه الموافق 5 غشت سنة 2009م، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47، مؤرخة في25 شعبان عام 1430ه الموافق 16 غشت سنة 2009م.

[5] أمر رقم 66-155، مؤرخ في 18 صفر عام 1386ه الموافق 08 نوفمبر سنة 1966م، يتضمن قانون الإجراءات الجزائية، جريدة رسمية عدد 48، مؤرخة في 20 صفر عام 1386ه الموافق 10 يونيو سنة 1966م، معدل ومتمم.

تتباين التعريفات التي أعطيت للجريمة الإلكترونية، حيث عرفها جانب من الفقهاء بأنها: "فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية"[1]. وعرفها فقه آخر بأنها: " واقعة تتضمن تقنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب" [2]. وحسب منظمة التعاون الاقتصادي والتنمية (OCDE)، فالجريمة الإلكترونية تشمل 'كل سلوك غير قانوني أو غير أخلاقي أو غير مرخص له يتعلق بالمعالجة الآلية للبيانات و/ أو نقل البيانات' [3]. أما عن التعريف القانوني أو التشريعي للجريمة الإلكترونية فالمشرع الجزائري لميقدم تعريفا لهذه الجريمة ضمن قانون العقوبات بل ذكر بعضا من صورها مثالها ما نصت عليه المادة 394 مكرر 1: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج ،**كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها** ". أما في القانون رقم 09-04 فوصفها في نص المادة 2 بـ 'الجرائم المتصلة بتكنولوجيات الإعلام والاتصال' معرفا إياها بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

من كل ما تقدم من تعريفات للجريمة الإلكترونية يمكننا القول بأنها كل سلوك غير مشروع يستهدف المساس بالمعطيات أو البيانات المعالجة آليا.

ب. خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية عن الجريمة التقليدية بمجموعة من الخصائص نسرد البعض منها في النقاط التالية:

- هي جريمة لا تترك آثارا مادية بعد ارتكابها، حيث لا وجود لأي وثائق أو مستندات ورقية لكونها تتم في بيئة إلكترونية تُنقل فيها المعلومات بصورة غير مرئية من خلال النبضات الإلكترونية[4].
- توصف الجريمة المعلوماتية بأنها جريمة ناعمة، لا يتطلب إتيانها العنف أو استعمال الشدة أو أداة حادة خطرة أو حتى سلاح، هي فقط تحتاج الضغط على بعض الأزرار بعد استخدام غير مشروع لبيانات الغير[5]؛

---

[1] نقلا عن: أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها-دراسة تحليلية تأصيلية مقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص 27.

[2] نقلا عن: محمود أحمد محمد القرعان، الجرائم الإلكترونية، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، الأردن، 2017، ص 24.

[3] Brigitte PEREIRA, 'La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité', Revue internationale de droit économique, 2016, p. 389, in https://www.cairn.info/revue-internationale-de-droit-economique-2016-3-page-387.htm, 21/05/2022, 06:29.

[4] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية للطباعة والنشر، الإسكندرية، 2008، ص 45.

[5] شول بن شهرة، مراد مشوش، "السمات الخاصة للجريمة المعلوماتية"، مجلة المستقبل للدراسات القانونية والسياسية، معهد الحقوق والعلوم والعلوم السياسية، المركز الجامعي أفلو، الأغواط، المجلد 04، العدد 01، جوان 2020، ص 3، https://www.asjp.cerist.dz/en/article/129107، 2022/05/18، 23:23.

– هي من الجرائم التي ترتكب عن بعد ومرتكبها لا أثر لوجوده في مسرح الجريمة...[1]

إن الجرائم الإلكترونية لا تقف عند صنف واحد بل هي عديدة بتعدد غايات إتيانها وكذا سبل ارتكابها، من هذه الجرائم مثلا "جريمة إفشاء الأسرار الخاصة"[2] و"جرائم الاعتداء على البريد الإلكتروني"[3].

وقد وضعت اتفاقية بودابست لسنة 2001 عديد التصنيفات للجرائم الإلكترونية، وتتلخص في الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية، الجرائم المعلوماتية، الجرائم المتصلة بالمحتوى ثم الجرائم المتصلة بالاعتداءات على الملكية الفكرية[4].

2. التعريف بالمجرم الإلكتروني

يطلق على مرتكب الجريمة الإلكترونية إسم 'المجرم الإلكتروني' أو 'المجرم المعلوماتي' أو Cybercriminel باللغة الأجنبية أو غيرها من التسميات المبتدعة في هذا المجال، ويتميز هذا المجرم ببعض السمات الخاصة:

– المجرم الإلكتروني في الغالب شخص ذي ذكاء حاد ويمتلك مهارات تقنية عالية ودقيقة، وله دراية واسعة باستخدام أنظمة الحواسيب ومن ثم كيفيات الحصول على المعلومات وتخزينها، بينما يتميز غالبا مرتكب الجريمة التقليدية بكونه شخصا أميا بسيطا يملك مستوى تعليميا متوسطا[5].

– المجرم المعلوماتي هو مجرم محترف لأن هذا النوع من الجرائم يتطلب منتهى الدقة والتخصص للتغلب على أنظمة الحماية التي وضعها المتخصصون لحماية المنظومة المعلوماتية، ونادرا ما يستطيع الأشخاص العاديون خرق مثل هذه المنظومات[6].

– المجرم المعلوماتي يكتسب شخصية اجتماعية، فهو يحيا وسط المجتمع ممارسا عمله سواء في المجال المعلوماتي أو أي مجال آخر، وتمثل هذه الميزة التي يتمتع بها المجرم الإلكتروني إحدى الفوارق بين الإجرام الإلكتروني والإجرام التقليدي[7].

---

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 44.

[2] عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي - دراسة متعمقة في التعريف بجرائم التقنية الحديثة والمجرم المعلوماتي، إنحراف الأحداث بسبب الإنترنت- مكافحة إدمان الإنترنت لدى بعض الفئات، الطبعة الأولى، بهجات للطباعة والتجليد، مصر، 2009، ص 163.

[3] خالد ممدوح إبراهيم، مرجع سابق، ص 90.

[4] لأكثر توضيح ينظر إلى: جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص93-94.

[5] إبراهيم رمضان إبراهيم عطايا، "الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية(دراسة تحليلية تطبيقية)"، مجلة كلية الشريعة والقانون بطنطا، العدد الثلاثون، الجزء الثاني، 2015، ص 373، https://mksq.journals.ekb.eg/article_7802.html، 2022/05/21، 05:58.

[6] بثينة حبيباتني، "الطبيعة الخاصة للجريمة المعلوماتية"، مجلة دراسات وأبحاث، المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والإجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 12، العدد 03، جويلية 2020، ص 610، https://www.asjp.cerist.dz/en/article/121414in، 2022/05/21، 06:48.

[7] حسين ربيعي، "المجرم المعلوماتي – شخصيته وأصنافه"، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، العدد 40، جوان 2015، ص ص 289، https://www.asjp.cerist.dz/en/article/88190، 2022/05/21، 09:43.

- يمتاز المجرم الإلكتروني بسعة التحمل والصبر، ذلك أن إتيان الجريمة الإلكترونية يتطلب الوقت، حيث قد لا تنجح المحاولات الأولى ومن ثم فتكرارها يتطلب صبرا كبيرا لتحقيق المبتغى [1]. وعن السمة الاجتماعية للمجرم الالكتروني أسماه بعض الفقه[2] بأنه مجرم متكيف اجتماعيا.
- لا يستعمل المجرم الإلكتروني العنف عند قيامه بجريمته، بل يستخدم بدل ذلك الحيل وهذا يعود إلى أن هذا الصنف من الجرائم لا يحتاج إتيانه إلى العنف[3].

3. دوافع المجرم الإلكتروني لإتيان الجريمة الإلكترونية

المجرم الإلكتروني بسعيه لإتيان هذه الجريمة تدفعه مجموعة من الدوافعأو البواعث نلخص بعضا منها في النقاط التالية:

- قد يكون الدافع لارتكاب عديد الجرائم الإلكترونية الحصول على الأموال، ويكون ذلك مثلا بابتزاز الغير ومساومته حول ما تم اختلاسه من برامج حاسوبه أو استخدام بطاقة سحب آلي انتهت صلاحيتها [4]. فالسعي للحصول على الربح ومن ثمة تحقيق الثراء الشخصي يعتبر دافعا مشتركا بين مختلف جرائم الاعتداء على الأموال بما فيها الجريمة الإلكترونية[5].
- يمثل الانتقام أحد الدوافع لارتكاب الجريمة الإلكترونية، فهو غريزة متأصلة في الإنسان، ومثال عنه تعرض موظف ما لفصل تعسفي من مؤسسته فيرد لها الصاع صاعين بأن يُكبدها خسائر مالية كبيرة خاصة إن كان يحوز معلومات تتعلق بسير نظامها المعلوماتي من جهة ومُلم كفاية بهذا المجال من جهة ثانية، حيث ما قد يسببه للمؤسسة من ضرر يتطلب من الجهد الكثير ومن الوقت الزمن الطويل ليتم إصلاحه[6].
- قد تكون أيضا الرغبة الجامحة في التفوق على الآلة أي الحاسوب ومن ثمة إثبات القدرات الذاتية في مجال التكنولوجيات الحديثة بتخطي عقبات الحماية المكرسة لحفظ الأنظمة المعلوماتية هي الدافع إلى ارتكاب الجريمة الالكترونية، وما يميز هذا الدافع أن سن المجرم ليس لها أهمية، ففي الغالب نجد هؤلاء المجرمين من فئة صغار السن نوابغ المعلوماتية الذين يسعون لإبراز تفوقهم علميا كان أو عمليا[7].
- من الدوافع الخطيرة للجريمة الالكترونية نجد الإرهاب، فقد تتخذ مجموعات إرهابية مجال التكنولوجيات الحديثة في مقدمتها الأنترنت كآلية لبث سمومها الإجرامية من تحريض على القتل والعصيان المدني،

---

[1] المرجع نفسه، ص 290.
[2] عبد الفتاح بيومي حجازي، مرجع سابق، ص 100.
[3] المرجع نفسه، ص 97.
[4] يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات –قانون الإجراءات الجزائية – قوانين خاصة، دار الجامعة الجديدة ، الإسكندرية، 2019، ص 37.
[5] أحمد عبد اللاه المراغي، مرجع سابق، ص 41.
[6] حسين ربيعي، مرجع سابق، ص 292.
[7] يزيد بوحليط، مرجع سابق، ص 37-38.

وهي تبتغي من وراء ذلك نشر الفزع والرعب في أوساط المواطنين وإن كانت في الغالب تستهدف النظم المعلوماتية الحكومية لتدميرها[1].

ثانيا: أحكام مكافحة الجريمة الإلكترونية

لتبيُن مضمون الأحكام المقررة ضمن قانون العقوبات لمكافحة الجريمة الإلكترونية نتطرق لمختلف صور هذه الجريمة التي أقرها المشرع الجزائري(1) ثم نفصل في مُجمل العقوبات التي سنها في جانب من يأتيها(2).

1. صور الجريمة الإلكترونية

عدد المشرع الجزائري من خلال القسم السابع مكرر [2] والذي تم استحداثه بموجب القانون رقم 04-15[3] المعدل لقانون العقوبات مجموعة من الجرائم وهذا تحت مسمى 'المساس بأنظمة المعالجة الآلية للمعطيات'، موزعة على مجموعة نصوص هذا القسم.

وقد أدرج المشرع الجزائري جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضمن ما يسمى بـ 'الجرائم المتصلة بتكنولوجيات الإعلام والاتصال' عند تعريفه إياها ضمن نص المادة 2 من القانون رقم 09-04.

يمكن أن نلخص مجموع هذه الجرائم وحسب ما استخلصه عديد الباحثين فيما يخص هذا الصنف من الجرائم المستحدثة في قانون العقوبات الجزائري في الصور التالية:

أ. الإعتداء على منظومة للمعالجة الآلية للمعطيات

كُرست هذه الصورة من صور الجريمة الالكترونية ضمن نص المادة 394 مكرر من قانون العقوبات المعدل والمتمم. وقد ألحقت المادة لهذا الدخول والبقاء صفة الغش أي أن آتيه لم يتبع السبل القانونية للولوج إلى هذه المنظومة ومن ثمة البقاء فيها.وهذه الصورة للجريمة تأخذ أبعادا تتفاوت خطورتها بحسب ما يترتب عنها من نتائج، وتتمثل هذه الصور أو الأبعاد في:

– الدخول والبقاء دون إذن أو محاولة ذلك وهذا دون أن يترتب عنها مساس معين بالمنظومة المعنية وهو ما أقرته الفقرة الأولى من المادة المذكورة **(...كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.)** .إذن يتحقق الفعل الإجرامي في هذه الصورة من جريمة الإعتداء على منظومة للمعالجة الآلية للمعطيات من خلال الدخول العمدي للمنظومة المعنية دون ترخيص من صاحبها، أو الدخول والبقاء في المنظومة دون إذن من صاحبها، ثم أخيرا مجرد محاولة الدخول العمدي دون إذن أيضا لمثل هذه المنظومة تحقق هي الأخرى الفعل الإجرامي ومن ثم يقع مرتكبها تحت طائلة العقوبة المكرسة في ذات المادة لهذا السلوك.

---

[1] حسين ربيعي، مرجع سابق، ص 294.

[2] من الفصل الثالث من الباب الثاني(الجنايات والجنح ضد الأفراد) من الكتاب الثالث(الجنايات والجنح وعقوباتها) من الجزء الثاني(التجريم) من قانون العقوبات.

[3] قانون رقم 04-15، مؤرخ في 27 رمضان عام 1425ه الموافق 10 نوفمبر سنة 2004م، ج ر عدد 71، صادرة بتاريخ 27 رمضان 1425ه الموافق 10 نوفمبر سنة 2004م، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386ه الموافق 8 جوان سنة 1966م والمتضمن قانون العقوبات.

– الدخول مع البقاء والتسبب في حذف أو تغيير في معطيات المنظومة المعنية وهو ما جاء في الفقرة الثانية من نفس المادة **(...إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.)** . في هذه الحالة لا يكفي الدخول والبقاء في المنظومة لتحقق هذه الصورة للجريمة الإلكترونية بل لا بد من ترتيب نتيجة عن هذا الدخول أو البقاء تتمثل في حذف(إتلاف) أو تغيير في معطيات المنظومة. وهي صورة أشد خطورة من سابقتها كما أن عقوبتها أيضا كما سنرى لاحقا مشددة مقارنة بالصورة الأولى لهذا الصنف من الجريمة الإلكترونية.

– الدخول مع البقاء ثم ينتج عن ذلك تخريب نظام اشتغال المنظومة وهو ما كرسته الفقرة الثالثة والأخيرة من ذات المادة **(وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة...)** . في هذه الحالة أيضا يتحقق الفعل الإجرامي لهذه الصورة بتحقق نتيجة عن عملية الدخول والبقاء في منظومة المعالجة الآلية للمعطيات والتي تتمثل في تخريب نظام اشتغال المنظومة وهي الأخرى شدد لها المشرع العقوبة كما سنرى.

ب. المساسبمعطيات نظام[1]للمعالجة الآلية للمعطيات

أقرت هذه الصورة من الجريمة الإلكترونية المادة 394 مكرر 1 من قانون العقوبات، ويتشكل الفعل المكون لهذه الجريمة حسب ما جاء في نص المادة في إدخال معطيات عن طريق الغش [2] إلى نظام للمعالجة الآلية أو إزالة المعطيات الموجودة أصلا في نظام المعالجة الآلية أي حذفها وإتلافها أو تعديلها كصورة ثالثة للمساس بهذه المعطيات.

ت. الاستغلال غير المشروع لمعطيات منظومة للمعالجة الآلية للمعطيات

تتحقق هذه الصورة للجريمة الإلكترونية من خلال إتيان عمدا أو عن طريق الغش إحدى التصرفات التي سردتها المادة 394 مكرر 2:

" – تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

---

[1] تم استعمال مصطلح نظام تبعا لما جاء في نص المادة 394 مكرر 1 المتضمنة هذه الصورة من صور الجريمة الإلكترونية. وهي المادة الوحيدة ضمن هذا الفصل المخصص للجريمة الإلكترونية التي استخدم فيها المشرع مصطلح 'نظام' بدل مصطلح 'منظومة' الذي استخدمه في باقي نصوص الفصل. وإن كان المشرع عرف مصطلح منظومة معلوماتية ضمن الفقرة ب من المادة 2 من القانون رقم 09-04 بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

[2] وإن كان البعض عقب على استعمال المشرع لهذا المصطلح حيث يحبذ لفظ الاحتيال بدل الغش الذي يراه أقرب للارتباط بالمواد والسلع. لأكثر توضيح ينظر إلى: ياسين بن عمر، 'المعالجة القانونية للجرائم الالكترونية في القانون الجزائري والتشريعات المقارنة (التشريع المغربي والإماراتي نموذجا)'، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر، الوادي، الجزائر، المجلد 10، العدد 03، ديسمبر 2019، ص 715، https://www.asjp.cerist.dz/en/article/108511in، 2022/09/10، 17:51.
ونراه صائبا في هذا التعقيب.

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

إذن تتلخص الأفعال المكونة للفعل الإجرامي لهذه الصورة من الجريمة الإلكترونية تبعا لنص المادة المذكورة في إستغلال المعطيات المتضمنة أصلا في نظام للمعالجة الآلية بطرق متعددة ويكون ذلك عمدا أوعن طريق الغش. من هذه الطرق نشر هذه المعطيات، تجميعها لإخراجها في تصميم جديد يخدم مصالح المجرم، الاتجار بها مثلا في صورتها الأصلية كمعطيات أولية لم يلحقها أي تعديل وغيرها أو بعد إدخال تعديلات معينة عليها أو غيرها من التصرفات التي يسعى آتيها من ورائها إلى استغلال هذه المعطيات لتحقيق مآرب أو منافع معينة ولو بطرق غير قانونية.

2. العقوبات المقررة للجريمة الإلكترونية

أقر المشرع الجزائري لمختلف أصناف الجريمة الإلكترونية المذكورة آنفا مجموعة من العقوبات. تتلخص هذه العقوبات في العقوبات الأصلية والمتمثلة في الغرامات المالية أو الحبس والعقوبات التكميلية والتي تتنوع بين غلق محل الجريمة، مصادرة الوسائل المستعملة لإتمام الجريمة...

أولى هذه العقوبات هي تلك المخصصة لجريمة الدخول والبقاء دون إذن في منظومة للمعالجة الآلية للمعطيات، وهذا في صورتها العادية أو البسيطة أي دون أن يخلف هذا الولوج أو البقاء أي نتائج وتتمثل هذه العقوبة في الحبس من 3 أشهر إلى سنة مع غرامة مالية تتراوح بين 50000 دج و100000 دج(الفقرة الأولى المادة 394 مكرر). أما إن ترتب عن هذا الدخول والبقاء حذف أو تغيير في معطيات المنظومة فالعقوبة المذكورة تضاعف(الفقرة 2 من نفس المادة).

أما في حال تحقق الصورة الأخيرة من هذه الجريمة أي دخول وبقاء ثم تخريب لنظام اشتغال المنظومة فتتمثل العقوبة في الحبس من 6 أشهر إلى سنتين(2) وغرامة مالية تتراوح بين 50000 دج إلى 150000 دج(الفقرة 3 من نفس المادة).

وتزداد العقوبات شدة فيما يخص الصنف الثاني من الجريمة الالكترونية المقرر ضمن نص المادة 394 مكرر 1وهذا تبعا لدرجة المساس بأنظمة المعالجة الآلية التي تعرف هي الأخرى حدة أكبر من تلك الناتجة عن الجريمة المذكورة في نص المادة 394 مكرر. فالعقوبة إذن هي الحبس من 6 أشهر إلى 3 سنوات وغرامة مالية من 500000 دج إلى 2000000 دج.

أما بالنسبة للجرائم المكرسة في المادة 394 مكرر 2، فعقوبة الحبس المقررة لآتيها فتتراوح بين شهرين(2) و3 سنوات، بينما تقدر الغرامة بين 1000000 دج كحد أدنى و5000000 دج كحد أقصى. وقد تُضاعف جميع هذه العقوبات وهذا في حال استهدفت الجريمة المرتكبة الدفاع الوطني أو الهيئات والمؤسسات التي تخضع للقانون العام وهذا أقرت المادة 394 مكرر 3. أي أن كل جريمة من الجرائم

المذكورة آنفا تكون غايتها المساس بالأمن والدفاع الوطني وكذا هيئات ومؤسسات الدولة فالعقوبة الموجهة لآتيها تكون أكثر صرامة وشدة.

الملاحظ أيضا أن المشرع ميز ضمن هذه العقوبات بين الشخص الطبيعي والشخص المعنوي، فهذا الأخير وفيما يخص الغرامات المالية يعاقب بما يعادل 5 مرات ما يعاقب به الشخص الطبيعي من غرامة في حدها الأقصى وهذا طبعا يعود للقوة الاقتصادية التي يملكها عادة الشخص المعنوي مقارنة بالشخص الطبيعي(وهو ما تقرره المادة 394 مكرر 4).

كذلك تقرر المادة 394 مكرر 5 في حق الشريك في الجريمة نفس عقوبات الفاعل الأصلي حيث تنص على أن: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

كما لم يستثن المشرع الشروع من العقوبة وهذا ما كرسته المادة 394 مكرر 7 من قانون العقوبات حيث تنص على أنه: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

وتُكمل هذه العقوبات الأصلية بعقوبات تكميلية تتمثل حسب نص المادة 394 مكرر 6 في: "...مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها". إذن وحرصا من المشرع على استئصال كل ما يتعلق بالجريمة الإلكترونية أقر مجموعة من العقوبات التكميلية في حق سواء الفاعل الأصلي للجريمة أو شريكه في هذا الجرم، تأتي في مقدمتها مصادرة كل الوسائل التي استعملت لإتمام الجريمة وهي عادة مجموعة أجهزة كالحواسيب وما تتضمنه من برامج، وأيضا إغلاق المواقع التي قد تكون محلا لإحدى الجرائم المذكورة في الفصل السابع مكرر المذكور آنفا. كما تؤكد المادة أيضا أن عملية غلق محل الإجرام تكون حتى لو لم يكن المجرم صاحبه ولكن شريطة أن يكون مالكه عالما بقيام هذه الجريمة في محله.

الخاتمة

كرس المشرع الجزائري ضمن قانون العقوبات بعد تعديله بموجب القانون رقم 04-15 جملة من الأحكام الموضوعية لمكافحة الجريمة الإلكترونية. تتضمن هذه الأحكام مجموعة من الجرائم تمثل صورا أو أصنافا للجريمة الإلكترونية ومجموعة من العقوبات كُرست لتكون ردعا لمن يأتي إحدى هذه الجرائم.

لم يتضمن هذا الفصل المخصص للجريمة الإلكترونية أي تعريفات لأي مصطلح مستخدم ضمنه بالرغم من أن المصطلحات المستخدمة تتعلق بمجال تقني يتميز بدقة مصطلحاته والتي قد يُصعب على القانونيين كالقضاة مثلا إن لم يكونوا على دراية بمجال التكنولوجيات الحديثة الإلمام بأدق تفاصيلها للفصل بدقة في

القضايا المتعلقة بهذا الصنف من الجرائم. وإن كان المشرع ضمَّن القانون رقم 09-04في المادة 2 منه بعض التعريفات لبعض المصطلحات ولكنها حسبنا قليلة وغير مفصلة وغير واضحة كفاية.

يمكن القول أن المشرع الجزائري سعى واجتهد بوضعه مجوعة من الأحكام الموضوعية ضمن قانون العقوبات لمعالجة الجريمة الإلكترونية وهذا بالتكامل مع القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها وقانون الإجراءات الجزائية المعدل والمتمم. لكن تبقى هذه المعالجة كتجربة أولى له تحتاج لمجموعة من التعديلات الدورية تتماشى وما يطرأ من جديد فيما يخص هذه الجريمة المرتبطة بمجال تقني دقيق وسريع التطور ومن ثمة فوسائل إتيان هذه الجريمة تتطور هي الأخرى بسرعة وبالتالي تحتاج لقواعد لضبطها تتماشى وهذه التطورات السريعة خاصة وأن هذا النوع من الجرائم يمس باستقرار المجتمع من كافة مناحي الحياة(أخلاقيا، اجتماعيا، سياسيا واقتصاديا)، الأمر الذي يستدعي الفطنة المستمرة من المشرع للتصدي له بأحكام صارمة تدعمها إجراءات لتطبيقها في واقع الأمر حتى يرتدع من يفكر في إتيان مثل هذه الأعمال غير المشروعة.

قائمة المصادر والمراجع

أولا: باللغة العربية

1. المصادر

النصوص القانونية

- أمر رقم 66-155، مؤرخ في 18 صفر عام 1386هـ الموافق 08يونيو سنة 1966م، يتضمن قانون الإجراءات الجزائية، جريدة رسمية عدد 48، مؤرخة في 20 صفر عام 1386هـ الموافق 10 يونيو سنة 1966م، معدل ومتمم.
- أمر رقم 66-156، مؤرخ في 18 صفر عام 1386هـ الموافق 8 يونيو سنة 1966م، يتضمن قانون العقوبات، جريدة رسمية عدد 49، مؤرخة في 21 صفر عام 1386هـ الموافق 11 يونيو سنة 1966م، معدل ومتمم.
- قانون رقم 04-15، مؤرخ في 27 رمضان عام 1425هـ الموافق 10 نوفمبر سنة 2004م، جريدة رسمية عدد 71، مؤرخة في 27 رمضان 1425هـ الموافق 10 نوفمبر سنة 2004م، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386هـ الموافق 8 يونيو سنة 1966م والمتضمن قانون العقوبات.
- قانون رقم 09-04، مؤرخ في 14 شعبان عام 1430هـ الموافق 5 غشت سنة 2009م، يتضمن القواعد الخاصة للقواعد من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47، مؤرخة في25 شعبان عام 1430هـ الموافق 16 غشت سنة 2009م.

2. المراجع

أ. الكتب

- أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها–دراسة تحليلية تأصيلية مقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2017.
- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.
- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2008.
- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي– دراسة متعمقة في التعريف بجرائم التقنية الحديثة والمجرم المعلوماتي– إنحراف الأحداث بسبب الإنترنت– مكافحة إدمان الإنترنت لدى بعض الفئات، الطبعة الأولى، بهجات للطباعة والتجليد، مصر، 2009.
- محمود أحمد محمد القرعان، الجرائم الإلكترونية، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، الأردن، 2017.
- يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات – قانون العقوبات –قانون الإجراءات الجزائية – قوانين خاصة، دار الجامعة الجديدة ، الإسكندرية، 2019.

ب. المقالات

- إبراهيم رمضان إبراهيم عطايا، 'الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية(دراسة تحليلية تطبيقية)'، مجلة كلية الشريعة والقانون بطنطا، العدد الثلاثون، الجزء الثاني، 2015.
- بثينة حبيباتني، 'الطبيعة الخاصة للجريمة المعلوماتية'، مجلة دراسات وأبحاث، المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 12، العدد 03، جويلية 2020.
- حسين ربيعي، 'المجرم المعلوماتي – شخصيته وأصنافه'، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، العدد 40، جوان 2015.
- شول بن شهرة، مراد مشوش، "السمات الخاصة للجريمة الالكترونية"، مجلة المستقبل للدراسات القانونية والسياسية، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، الأغواط، المجلد 04، العدد 01، جوان 2020.

- ياسين بن عمر، 'المعالجة القانونية للجرائم الالكترونية في القانون الجزائري والتشريعات المقارنة (التشريع المغربي والإماراتي نموذجا)'، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر، الوادي، الجزائر، المجلد 10، العدد 03، ديسمبر 2019.

ثانيا: باللغة الفرنسية

Articles

- Brigitte PEREIRA, 'La lute contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité', Revue internationale de droit économique, 2016.

بن بو عبد الله نورة
norabenbouabdallah@gmail.com
جامعة باتنة 1 الحاج لخضر

تسليم المجرمين كآلية دولية لمكافحة الجرائم الالكترونية الاقتصادية

ملخص:

تعتبر الجرائم الالكترونية الاقتصادية ظاهرة اجرامية مستحدثة بحيث تعاني منها معظم المجتمعات في الآونة الأخيرة ، فهي تشكل انتهاك للحقوق والخصوصيات الإلكترونية ، لذا تعتبر من أبرز تحديات العصر، لما لها من تأثير على جوانب متعددة لا سيما على الاقتصاد، خاصة وأن المعاملات الالكترونية أصبحت على نطاق واسع من الاستعمال من جميع الناس ، فهي غالبا لا ترتكب من طرف شخص طبيعي فقط بل تعدت إلى الشخص المعنوي، و تكون عابرة للحدود ، فهي لا تتم من داخل دولة ويكون تأثيرها منحصر في تلك الدولة ، وإنما تلك الجرائم ترتكب عبر عدد من الدول لتتم في دولة أخرى ، وتكون آثارها ممتدة لتصل إلى عدد غير محدود من الدول، وعليه فإن الأساس الذي يرتكز عليه مجال مكافحة الجرائم الالكترونية هو التعاون الدولي بتقديم المساعدة القانونية والتقنية و البيانات المتوافرة وتقديم المعلومات والأدلة وصولا لتسليم المجرمين، من أجل تنسيق الجهود المبذولة بين كافة دول العالم لتكون هناك نتائج عملية يمكن الارتكاز عليها وتقويتها للحد من تلك الجرائم ذات النتائج الخطيرة على اقتصاديات الدول والكيانات الاقتصادية.

كلمات مفتاحية: الجرائم الالكترونية الاقتصادية ، مكافحة ، التعاون الدولي ، تسليم المجرمين.

Summary:

Economic electronic crimes are considered a new criminal phenomenon that most societies suffer from in recent times. All people, they are often not committed by a natural person only, but transcend the legal person, and are transboundary, as they are not carried out from within a state and their impact is limited to that state, but those crimes are committed across a number of states to take place in another state and their effects extend to reach An unlimited number of countries, and accordingly, the basis for combating cybercrime is international cooperation by providing legal and technical assistance and available data and providing information and evidence to the extradition of criminals, in order to coordinate efforts made among all countries of the world so that there are practical results that can be based and strengthened to limit Among those crimes that have serious consequences for the economies of countries and economic entities.

***Keywords**: economic cybercrime, combating, international cooperation, extradition.*

مقدمة:

تشهد البشرية في العصر الحديث تقدم علمي وتكنولوجي هائل يلقي بظلاله ونتائجه على كافة جوانب الحياة والعلاقات بين الأفراد والدول، ويبدو ذلك بوضوح بصدد الثورة المعلوماتية التي أخذت قدم السبق بفضل الوسائل التكنولوجيا المعلوماتية الحديثة التي أثرت على تطور أنشطتنا اليومية من حيث الإنجاز والسرعة والشكل والمضمون والزمان والمكان، فـغيرت بشكل كبير العديد من المفاهيم القانونية نظرا لظهور مراكز قانونية ذات طبيعة خاصة، وأدى الاستخدام المضطرب للمعلومات سواء في شكل أموال معلوماتية أو أساليب مستحدثة إلى ظهور ما يعرف بالإجرام الالكتروني، كنتيجة حتمية لكل تقدم تقني مستحدث، فلم تعد وسائل الاتصال الحديثة مجرد أداة إيجابية، بل أصبحت تشكل خطورة كبيرة لكل المستخدمين عند استخدامها لأغراض غير شريفة، وتتسبب في المساس بأمن الأشخاص ، كاختراق المواقع الشخصية عبر الإنترنت، وسرقة حسابات مصرفية و الغش في التسويق ونقل الأموال بالوسائل الالكترونية وغسيل الأموال والتهرب الضريبي حيث تساعد التحويلات الالكترونية في إخفاء عائدات الجريمة ونقلها وإخفاء الأرباح المشبوهة عبر الإيداع ببطاقات الائتمان مباشرة.

كما تتيح التجارة الالكترونية فرصاً للغش في البيع من سندات واسهم مزورة واستثمارات كاذبة، وكذلك الاعتراض واختراق سرية البنوك وسرقة الأرصدة وتحويلها إلي حسابات أخري ودعم هذه الأموال في تحويل أنشطة إجرامية أخرى، بل الأسوأ من ذلك في تدمير الاقتصاد الوطني بكامله.

لذا بات التصدي لها والقضاء عليها من أولويات تحقيق العدالة الجنائية على الصعيد الوطني والدولي، من خلال إيجاد وسائل فعالة لقمع هذا النوع من الجرائم ومن بين هذه الوسائل نظام تسليم المجرمين الذي يعد من أهم مجالات التعاون الدولي، وتبرز أهميته في أنه يحرم المجرمين من العثور على مأوى آمن لهم ، وكذلك يحرمهم من الاستفادة من تفاوت الأنظمة القانونية والقضائية ، فقد أصبح في وقتنا الحالي نظام تسليم المجرمين ضرورة ملحة وحتمية دولية تستدعيها الخطورة الاجرامية والتطور الذي وصلت اليه الجريمة اليوم بعبورها حدود الدولة الواحدة، يضاف إلى ذلك التزايد الملحوظ في هذا النوع من الجرائم المستحدثة وتنوع أشكالها خاصة الاقتصادية منها التي تؤثر بالسلب على الاقتصاد الوطني وتفشل محاولات التنمية.

والتساؤل الذي يطرح نفسه في هذا المقام : مدى فاعلية التنسيق الدولي عن طريق نظام تسليم المجرمين في التصدي للإجرام الالكتروني الاقتصادي؟، آخذين بعين الاعتبار أن هذه الجريمة تكتسب ثلاث خصوصيات هي إمكانية التنقل عبر المناطق والسرعة والتقنية وهذا يؤدي إلى صعوبة تشخيص المجرمين ولا يسهل التحري مما يفرض ضرورة التعاون بين الدول وحماية قانونية دولية.

-لمعالجة الإشكالية المطروحة في هذه الورقة البحثية، قسمت إلى:

المحور الأول: مفهوم نظام تسليم المجرمين

المحور الثاني: عن فاعلية نظام تسليم المجرمين في مكافحة الجرائم الالكترونية الاقتصادية

المحور الأول: مفهوم نظام تسليم المجرمين

معلوم أن تعاون الدول يتمثل في تطبيق الاتفاقيات الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية والاجراءات المتفق عليها بمقتضى القانون الخاص بالتماثل أو المعاملة بالمثل القوانين الوطنية والمحلية، ولأقصى درجة ممكنة للأغراض الخاصة بالعمليات المتعلقة بالتحقيق والبحث أو الاجراءات المتعلقة بالجرائم أو الخاصة بنظم وبيانات الكمبيوتر أو لتجميع الأدلة الخاصة بالجريمة في صورة الكترونية، وهي مسألة تتعلق بعمليات تسليم المجرمين، ومن المكان هنا أن نتعرف على تعريف نظام تسليم المجرمين وشروطه ، لأن ذلك يستتبعه تحديد أساسه القانوني الذي يستقي منها هذا النظام أحكامه كنظام إجرائي دولي، يقوم بالأساس على التعاون والتكافل والتضامن بين الدول.

أولا: تعريف تسليم المجرمين

يعتبر اصطلاح تسليم المجرمين ذا أصل لاتيني ، حيث كان يعبر عنه إعادة الشخص المطلوب إلى الدولة ذات السيادة و السلطة في محاكمته و كان يطلق عليه آنذاك باللاتينية extrudere إن المتتبع للدراسات الفقهية و التشريعات المعاصرة للتسليم يجد أن استخدامها لا يخرج عن اصطلاح extradition باللغة الإنجليزية و L'extradition باللغة الفرنسية اللذان يعنيان الترحيل ، أما في الأنظمة العربية فقد درجت على واستخدام أحد الاصطلاحين إما اصطلاح " تسليم المجرمين " كما هو متعارف عليه في مصر أو اصطلاح " الاسترداد "[1].

وقد تعددت التعاريف التي قيلت بشأن مصطلح " تسليم المجرمين " ، إلا أنها تشترك في مضمونها رغم اختلاف صياغتها ، فعرف تسليم المجرمين بأنه" العملية التي تقوم بتنفيذها الدولة المطلوبة في حق شخص أوقف على أراضيها بموجب نشرة بحث دولية تكون الدولة الطالبة قد أصدرتها في حقه ،وهذا حتى يتسنى للسلطات القضائية المختصة متابعة الفاعل على إثر جرم ارتكبه ، أو بغرض تنفيذ حكم قضائي تم النطق به في حقه مسبقًا"[2].

وعرف تسليم المجرمين بأنه الإجراء القانوني المؤسس على معاهدة أو معاملة بالمثل أو قانون وطني ، حيث تتسلم دولة ما مـن دولة أخرى شخصا متهما أو مرتكبا لمخالفة ضد القوانين الخاصة بالدولة الطالبة أو مخالفة للقانون الجنائي الدولي ، حيـث يعاقب على ذلك في الدولة الطالبة [3].

ويوجد من عرفه بأنه

" L'extradition est le mécanisme juridique par lequel un état (l'état requis) sur le territoire du quelle ce trouve un individu, remet ce dernier à un autre état (l'état

---

[1] – معمر محمد زكريا و بوشريحة حسين :نظام تسليم المجرمين ، رسالة الماجستير ، جامعة قسنطينة ،2013/2012 ، ص 9

* - يستعمل قانون العقوبات السوري و اللبناني اصطلاح استرداد المجرمين عوضا عن تعبير تسليم المجرمين الشائع في مصر و بعض البلدان العربية الأخرى ثم عاد المشرع لاصطلاح تسليم المجرمين .

[1] - عبود السراج : مقال بعنوان استرداد المجرمين، على الموقع الإلكتروني: http://www.arab-ency.com/index.php?module=pnEncyclopedia&func=display_term&id=295&m=1 ،

[2]- عباد بن يمينة ، إجراءات تسليم المجرمين المطلوبين دوليا ، مجلة الشرطة ، عدد خاص ، المديرية العامة للامن الوطني ،الجزائر ، 2008، ص32 .

[3] - Voir dans ce sens:ANNE-Marie la Rosa: le dictionnaire de droit international pénal- publication de l'institut universitaire de hautes étude international GENEV PUF 98.

requérant à fin qu'il le juge (extradition à fin de jugement) on lui fasse exécuté sa peine (extradition à fin d'exécution)[1].

وعليه **فتسليم المجرمين أو استردادهم هو أن تتخلى دولة عن شخص موجود إقليميا إلى دولة أخرى بناء على طلبها لتحاكمه على جريمة يعاقب عليها قانونها أو لتنفيذ فيه حكما صادرا عليه من محاكمها .**

و ينجم عن هذا التعريف أن التسليم يتناول فئتين من الأشخاص من الأشخاص : فهو إما أن يتناول المتهمين و إما أن يتناول المحكومين .

في الحالة الأولى : كأن يقترف شخص جناية في العراق و قبل أن يلقي عليه القبض يهرع هاربا إلى سوريا فتطلب الحكومة العراقية من سوريا استرداد هذا المتهم لملاحقته ومحاكمته أمام محاكمتها من أجل التهمة المعزوة إليه .

في الحالة الثانية : كأن يقترف شخص جرما في القطر المصري مثلا فيلاحق و تصدر المحاكم المصرية قرارها بالحكم عليه ، و لكن قبل أن ينفذ الحكم القطعي يفر لاجئا إلى سوريا فتطلب حكومة الجمهورية العربية المتحدة إلى الحكومة السورية استرداد هذا المحكوم عليه لا لمحاكمته كما هي الحال في الفرضية الأولى و إنما لتنفذ فيه العقوبة المحكوم عليه بها قبل هربه[2]. و التسليم يراعي مصالح الدولتين فهو من صالح الدولة طالبة التسليم لأنه يضمن معاقبة المجرم الذي أخل بقانونها و عبث بنظامها ، وهو من صالح الدولة المطلوب إليها التسليم لأنه يساعدها على إنقاذ بلادها من عنصر سيء غير مرغوب فيه .

ثانيا: شروطه:

هناك تباين في تحديد شروط نظام تسليم المجرمين، لذا نميز بين نوعين من الشروط:

1- الشروط المتعلقة بثبوت الاختصاص التشريعي للدولة طالبة التسليم : إذ يجب أن يتقرر ابتداء للدولة طالبة التسليم الاختصاص التشريعي بملاحقة الشخص المطلوب تسليمه ،وذلك وفقا لأحد المعايير الثلاثة الآتية:

* **معيار الإقليمية** : ذلك بأن تكون الجريمة المطلوب التسليم بشأنها قد ارتكبت في إقليم هذه الدولة[3]، ولا يقبل التسليم إذا ارتكبت الجريمة في الإقليم الجزائري.[4]

* **معيار الشخصية** : ذلك بأن يكون الشخص المطلوب تسليمه أحد رعايا تلك الدولة.

* **معيار العينية** : وذلك بأن تمثل الجريمة سبب التسليم إخلالا بأحد المصالح الأساسية للدولة الطالبة[5]

2- الشروط المتعلقة بالجريمة المطلوب التسليم من اجلها : يمكن إجمالها فيما يلي:

[1] - Voir : les professeur ANDRE Heut et RENEE Koering-joulin : droit pénal international.(P.U.F).

[2] - محمد الفاضل : محاضرات في تسليم المجرمين ، جامعة الدول العربية معهد الدراسات العربية العالية ،1966 ، ص 22 ، ص 23 .

[3] - المادة 696 من قانون الإجراءات الجزائية المعدل والمتمم.

[4] - المادة 698 من قانون الإجراءات الجزائية المعدل والمتمم.

[5] - المادة 696 من قانون الإجراءات الجزائية المعدل والمتمم.

* ينبغي أن تكون الجريمة مما يجوز فيه التسليم ، فتستثنى الجرائم ذات الصبغة السياسية ، أو إذا تبين من الظروف أن التسليم مطلوب لغرض سياسي[1] ، كما تستثنى أيضا الجرائم العسكرية.[2]

ومما سبق فيمكن تسليم المجرمين في الجرائم الالكترونية بصفة عامة بشرط أن تكون هذه الجرائم معاقب عليها في قوانين الدول الاطراف ومن بينها [3] الدخول غير المشروع أو الاعتراض غير المشروع أو الاعتداء على سلامة البيانات أو اساءة استخدام أجهزة الحاسب الآلي أو الاستخدام غرير المشروع لأدوات الدفع الالكتروني، كذلك في جرائم التزوير و الاحتيال المرتبطة بالحاسب الآلي أو جرائم الارهاب الالكتروني أو في الجرائم المنظمة المرتكبة بواسطة تقنية المعلومات كتبييض الأموال ...

والجريمة الالكترونية من الجرائم التي يطبق عليها إجراءات تسليم المجرمين طبقا لنص المادة 697 الفقرة 1و2من قانون الإجراءات الجزائية، ذلك أن هذه الجريمة وصفها جنحة في قانون العقولات الجزائري، [4] ومعاقب عليها في الحالة العادية الحبس من ثلاث أشهر إلى سنة طبقا لنص الفقرة 1من نص المادة 394مكرر 4منه.

* يجب أن تكون الجريمة على درجة معينة من الجسامة ، أي أن تكون جناية أو جنحة يعاقب عليها قانون الدولة الطالبة بسنتين أو أقل ، وإذا تعلق الأمر بمتهم قضي عليه بالعقوبة فيجب أن تساوي العقوبة أو تجاوز الحبس لمدة شهرين.[5]

- * يجب أن يكون الفعل المنسوب إلى الشخص المطلوب تسليمه مجرما في قانون كلا الدولتين ، وهو ما يعرف بشرط ازدواج التجريم*، وهو يمثل شرط أساسي في التسليم، إذ أنه يصعب التفكير في دولة تقبل تسليم فرد بسبب تصرف صدر عنه ولا يعاقبه قانون هذه الدولة. [6] ونلاحظ أن المشرع الجزائري قد أخذ بضرورة توفر شرط إزدواج التجريم، إلا أنه لم يشدد في هذا الشرط، كأن يشترط تطابق الوصف والتسمية، بل اكتفى بأن تكون الأفعال المطلوبة بشأنها التسليم تشكل جناية أو جنحة في قانون الدولة طالبة التسليم وبالمقابل يعاقب عنها التشريع الوطني.

---

[1]- المادة 698 من قانون الإجراءات الجزائية المعدل والمتمم.

2- المادة 687 الفقرة الأخيرة قانون الإجراءات الجزائية المعدل والمتمم.

[3]- أنظر الفقرة الأولى من 31 ، المرسوم الرئاسي رقم 252/14، المؤرخ في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ21 ديسمبر 2010، الجريدة الرسمية، العدد57، المؤرخ في 28 سبتمبر 2014.

[4]- قانون رقم02/16المؤرخ في19جوان 2016المعدل والمتمم للأمر156/66والمتضمن قانون العقوبات الجزائري.

[5]- المادة 697 من قانون الإجراءات الجزائية المعدل والمتمم.

* - إن الشرط الحديث الذي ينص على أنه يجب أن تكون المخالفة المزعومة مخالفة يعاقب عليها القانون في البلدين المعنيين اتضح وبصورة جلية في قضية" جيرهارت ايسلر " ، فقد فر هذا الرجل وهو أجنبي شيوعي في الولايات المتحدة بصورة غير مشروعة حين كان طليق السراح بموجب كفالة في انتظار البت في استئنافه حكما صدر عليه بتهمة اليمين الكاذبة وتحقير الكونجرس ، ووصل الي بريطانيا بعد أن اختبأ بين ركاب السفينة البولندية باتوري ، وطلبت حكومة الولايات المتحدة من الحكومة البريطانية اعتقال ايسلر واحتجازه وتسليمه لأنه مجرم بتهمة حلف اليمين الكاذبة فيما يتعلق بطلبه مغادرة الولايات المتحدة ، غير أن المحكمة البريطانية" محكمة الصلح في بوستريت بلندن " قررت بتاريخ 27 ماي 1949 أن التهمة الموجهة إلى آيسلر لا تشكل حلف يمين كاذبة بموجب القانون الانجليزي وبناء عليه رفض التسليم وأفرج عن آيسلر وغادر إنجلترا والتجأ إلى بلدان ما وراء الستار الحديدي ..... للمزيد انظر جيرهارد فان غلان : القانون بين الامم ، مدخل الي القانون الدولي العام – تعريب عباس العمر– الجزء الاول ، منشورات دار الافاق الجديدة – بيروت _ ص 22.

[6]- سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين-دراسة مقارنة-دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص 130.

هذا ويتحقق شرط إزدواج التجريم وفقا لأحد المعيارين: إما القائمة الحصرية التي تعتمد على تعداد الجرائم التي يجوز فيها التسليم واستعباد ما عداها وهذا الأسلوب أخذت به إتفاقية الأمم المتحدة لمكافحة الفساد، وكذا إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية. وإما أسلوب الحد الأدنى للعقوبة المقررة والذي يسمح بالتسليم بشأن الجرائم التي تتجاوز عقوبتها حدا أدنى معينا، فإذا كانت الجريمة سبب التسليم يعاقب عليها بأقل من الحد الأدنى المطلوب كان التسليم محظورا.

وبالنسبة للمشرع الجزائري فقد أخذ بمعيار الحد الأدنى للعقوبة المقررة وهذا ما يؤكده البند الأول من الفقرة الثانية من المادة 697 ق. إ. ج ج، والتي تنص " **الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جنحة إذا كان الحد الأقصى للعقوبة المطبقة طبقا لنصوص ذلك القانون سنتين أو أقل أو إذا تعلق الأمر بمتهم قضي عليه بالعقوبة إذا كانت العقوبة التي قضي بها من الجهة القضائية للدولة الطالبة تساوي أو تتجاوز الحبس لمدة شهرين**".

ومتى توافر شرط إزدواج التجريم وجب القيام بإجراءات التسليم مهما كانت طبيعة الجريمة والعقوبة المقررة لها كأصل عام، غير أن الاتفاقيات الدولية والتشريعات الوطنية درجت على استبعاد بعض الجرائم والعقوبات من مجال التسليم، ومن بين الجرائم المستثناة الجرائم السياسية والعسكرية، هذا بالإضافة إلى الجرائم المالية. أما من حيث العقوبات فنجد أنه قد درج على استبعاد التسليم متى كانت الجرائم محل هذا التسليم معاقبا عليها بالإعدام أو بعقوبة بدنية مشوهة.

والملاحظ أن استبعاد بعض الجرائم من التسليم نظرا لعقوبتها القاسية أو الوحشية في بعض الحالات أمر ممكن ومقبول، أما استبعاد الجرائم السياسية فهو أمر يثير بعض الإشكالات خاصة ما تعلق منه بمفهوم الجريمة السياسية الذي ما يزال يشوبه الغموض والإلتباس ويفتقر إلى التحديد والوضوح. ورغم ما يعتري صعوبة تحديد وتعريف الجريمة السياسية إلا أن هناك إجماع قانوني على استبعاد الجرائم السياسية من نطاق التسليم، وهذا ما كرسته إتفاقية الأمم المتحدة لمكافحة الفساد في مادتها 4/44، كما نجد المشرع الجزائري قد أخذ بهذا المبدأ عندما نص في المادة 698 ق إ ج ج، أنه" **لا يقبل التسليم في الحلات الآتية:**

1. **إذا كان الشخص المطلوب تسليمه جزائري الجنسية والعبرة في تقدير هذه الصفة بوقت وقوع الجريمة المطلوب التسليم من أجلها،**
2. **-إذا كانت للجناية أو الجنحة صبغة سياسية أو إذا تبين من الظروف أن التسليم مطلوب لغرض سياسي ...**"

- يشترط أيضا لقبول التسليم أن تكون الجريمة التي إتهم بارتكابها الشخص المطلوب تسليمه وكذا العقوبة الصادرة بحقه لا تزال قائمة ولم تسقط أو تنقضي لأي سبب من أسباب الإنقضاء، كالتقادم أو صدور عفو أو لسبق الفصل فيها.

وبهذا فإن سقوط الدعوى العمومية أو تقادم العقوبة يعتبر سببا أو مانعا لعدم التسليم، وذلك لانتفاء إجراء التسليم للسند القانوني الذي يجيز ملاحقة الأشخاص المطالب بتسليمهم.[1] وهذا ما أكدته المادة 5/698 ق إ ج ج، بنصها على أنه " **لا يقبل التسليم إذا كانت الدعوى العمومية قد سقطت بالتقادم قبل تقديم الطلب أو كانت العقوبة قد انقضت بالتقادم قبل القبض على الشخص المطلوب تسليمه وعلى العموم كلما انقضت الدعوى العمومية في الدولة الطالبة وذلك طبقا لقوانين الدولة الطالبة أو الدولة المطلوب إليها التسليم**". وكذا المادة 6/698 من ق إ ج ج، بصها على أنه " **لا يقبل التسليم إذا صدر عفوا في الدولة الطالبة أو الدولة المطلوب إليها التسليم ويشترط في الحالة الأخيرة أن تكون الجريمة من عداد تلك التي كان من الجائز أن تكون موضوع متابعة في هذه الدولة إذا ارتكبت خارج إقليمها من شخص أجنبي عنها**".

*- أما بالنسبة إجراءات تسليم المجرمين في مجال مكافحة الجرائم الالكترونية ، فتتمثل في وجوب تقديم طلب التسليم من طرف الحكومة الطالبة إلى الحكومة المطلوب منها وبالطريق الدبلوماسي، بواسطة وزير الخارجية الذي يحيله بعد فحصه للمستندات والملف إلى وزير العدل للنظر فيه وتقرير مدى أحقيته، كما يجب أن يرفق مع طلب التسليم بيان الأفعال المطلوب التسليم من أجلها وزمان ومكان ارتكابها، وتكييفها القانوني والنصوص الواجبة التطبيق.[2]

أما إذا كان غرض التسليم هو تنفيذ عقوبة على الشخص المطلوب تسليمه ، فيجب أن يرفق بطلب التسليم حكم قضائي بات صادر بالإدانة، ذلك حتى يتم التحقق من توافر شروط التسليم طبقا للاتفاقيات في هذا الصدد.[3]

ثالثا: الأساس القانوني لتسليم المجرمين:

أساس التسليم و مصدره الرئيسي يرجع للعلاقات الأساسية بين الدول الأطراف في هذا الإجراء و هناك اختلاف بين إعادة الشخص ، و تسليم المجرمين ، إذ أن الأولى كانت تعبر عن مرحلة تاريخية نشأ منها التسليم تلبية لحاجات الحكام و الملوك إذ أن الاعتبارات السياسية في العلاقات الدولية كانت من أساسيات التسليم و ذلك على عكس ما شهده نظام التسليم من مراحل متطورة في العلاقات الدولية تأسس فيها على المعاهدات الدولية و القوانين الوطنية و شرط المعاملة بالمثل ، مما ترتب عليه وجود التزام دولي لإتمام إجراءات التسليم ، كما أن إعادة الشخص المطلوب تقوم عليه علاقة بين دولتين فقط ألا و هي الدولة الطالبة والثاني هي الدولة المطالبة ، أما التسليم في صورته المعاصرة تتداخل فيه علاقات الدول بعضها ببعض ومنها على سبيل المثال جواز التسليم إلى دولة ثالثة و السماح بالمرور في دولة العبور حسب القواعد الثابتة و المعمول بها في هذا الشأن. [4]

ا- الاتفاقيات الدولية:

---

[1]- سليمان عبد المنعم، المرجع السابق، ص 274.

[2]- المادتين702و703من قانون الإجراءات الجزائية المعدل والمتمم.

[3]- طارق إلراهيم اليسوقي عطيه، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة للنشر، مصر،2009، ص715.

[4]- فريدة شبري : تحديد نظام تسليم المجرمين ،مذكرة الماجستير في القانون فرع القانون الدولي الإنساني ،كلية القانون بودواو جامعة بومرداس ، تاريخ المناقشة 2007 ،ص9،ص10 .

تعتبر الاتفاقيات الدولية أهم المصادر التي يستمد منها تسليم المجرمين شروطه وإجراءاته وقوته الإلزامية ، فكلما كانت هناك معاهدة للتسليم فإن ذلك يعتبر الأساس الأول الذي يجب أن تلتزم به الدول عند إجراء التسليم ، بل إن هناك من الدول من لا تقبل التسليم إلا إذا كانت ثمة اتفاقية تلزمها بذلك كالدول الأنجلو أمريكية ، وتظهر أهمية الاعتماد على الاتفاقيات في المادة 694 من قانون الإجراءات الجزائية[1] ، ومن بين أهم الاتفاقيات الثنائية التي أبرمتها الجزائر اذكر على سبيل المثال ما يلي:

-اتفاقية التعاون القضائي بين الجزائر و بريطانيا الموقعة في جويلية 2006 والتي دخلت حيز التنفيذ في 25فيفري2007 .

-اتفاقية التعاون القانوني والقضائي في مجال مكافحة أشكال الجريمة المنظمة التي .وقعتها الجزائر مؤخرا مع الولايات المتحدة الأمريكية بتاريخ 07 أفريل2010 .

ب- مبدأ المعاملة بالمثل:

يعد مبدأ المعاملة بالمثل مبدأ دوليا أساسه السابقة في التعامل في حالة عدم وجود اتفاقية دولية ، بحيث إذا تقدمت إحدى الدول طالبة التسليم من دولة أخرى فإن موقف الدولة المطلوب منها سواء أكان بالموافقة أو بالرفض يمثل سابقة تعتمد عليها الدولتين في حالات طلب التسليم الأخرى.

ج- القوانين الداخلية:

تلجأ معظم الدول إلى تنظيم إجراءات وشروط التسليم في قوانينها الداخلية ، وهذا لتصور عدم وجود اتفاقية دولية ، بالإضافة إلى قلة العمل بمبدأ المعاملة بالمثل ، والجزائر على غرار باقي الدول ونظرا لأهمية نظام التسليم فقد نصت عليه في الدستور،[2] ونظمت أحكامه بدقة في قانون الإجراءات الجزائية في المواد من 694الى 720 في الكتاب السابع المتعلق بالعلاقات بين السلطات القضائية الاجنبية، ووضح شروط تسليم المجرمين بموجب المواد من 694 الى 701 ، وآثار التسليم من المواد 702 الى 713، وآثار التسليم في المواد من 714 الى 718 من قانون اجراءات ، ويفهم من المادة 718 من هذا القانون أنه لا يجوز للدولة ان تقوم باعادة تسليم شخص تم تسليمه اليها الى دولة أخرى وهو ما يعرف في الاتفاقيات الدولية بمبدأ عدم جواز اعادة التسليم.

المحور الثاني: عن فاعلية نظام تسليم المجرمين في مكافحة الجرائم الالكترونية الاقتصادية

تتعرض الجهود الدولية في مجال تسليم المجرمين في الجرائم بصفة عامة و الالكترونية إلى عوائق تؤثر في الجانب القانوني والتطبيقي عند تنفيذ إجراءات التسليم، فتصطدم سياسة التعاون القضائي في ظل صعود ثقافة حقوق الإنسان بالاعتبارات السياسية والاتجاهات الدولية ذات المصلحة الخاصة المختلفة، وهو في نفس الوقت يحظى بمجموعة من الايجابيات تميزه عن غيره من الإجراءات التي تتخذها الدول من أجل

[1]- تنص المادة 694 من قانون الاجراءات الجزائية المعدل والمتمم على: "تحدد الأحكام الواردة في هذا الكتاب شروط تسليم المجرمين وإجراءاته وآثاره وذلك ما لم تنص المعاهدات والاتفاقيات السياسية على خلاف ذلك".

[2] - تنص المادة 50 من التعديل الدستوري لسنة 2020 **الجريدة الرسميّة للجمهوريّة الجزائريّة ، العدد82، الصادرة في 30 ديسمبر 2020 على أنه:** "..... لا يمكن تسليم أحد إلاّ بمقتضى اتفاقية دولية مصادق عليها، أو بموجب قانون. لا يمكن، في أي حال، تسليم أو إبعاد أي لاجئ سياسي استفاد قانونا من حق اللجوء"

مواجهة الجرائم ذات الخطورة على أمنها السياسي الذي يتأثر بالوضع الاقتصادي، لكن رغم هذه الإيجابيات فإن هذا النظام تعترضه صعوبات ومعيقات تحد من التنفيذ الفعال له في مكافحة الجريمة لاسيما محل دراستنا الجرائم الالكترونية الاقتصادية.

أولا: أهمية نظام تسليم المجرمين في مكافحة الجرائم الالكترونية الاقتصادية

يعد نظام تسليم المجرمين أمرا محتما خاصة في مجال مكافحة الجرائم الالكترونية الاقتصادية وتنفيذ الأحكام الجنائية بصفة خاصة، لذالك فان لنظام تسليم المجرمين عدة ايجابيات تبرز فاعليته وذلك من خلال مكافحته للجريمة وتعاون الدول في هذا التسليم ، والتي نذكر منها مايلي:

-تأكيد حجية الأحكام الصادرة على الأشخاص أيا كانت جنسياتهم، لأن هروب الشخص بعد صدور الحكم عليه لا ينبغي أن يكون مبررا لإهدار هذه القيمة والحجية للحكم.

- تأكيد احترام الأحكام القضائية الصادرة من السلطات القضائية للدول الأخرى.

- احترام الضحايا المضرورين من الجريمة المرتكبة لان إعادة الشخص لا تطلب لذاتها ولكنها مرتبطة بحقوق مدنية أخرى.

- منع التفكير لدى الضحايا في اقتضاء حقوقهم بطرق غير قانونية، ولاشك أن هذه الأفكار الإجرامية مرفوضة تماما ولكنها للأسف تحصل فور فشل أجهزة الانتربول في استعادة الحقوق. [1]

- يعتبر نظام تسليم المجرمين من أقدم صور التعاون القضائي الدولي في المواد الجنائية، وهو مشهود له بكونه واحدا من أنجع وسائل هذا التعاون في مكافحة الجريمة بصفة عامة والالكترونية بصفة خاصة، وأكثرها فعالية لتحقيق العدالة الجنائية، وردع الجناة الذين لا تقف الحدود عائقا أمام ارتكابهم لعملياتهم الإجرامية حيث يحرم المجرمون من العثور على مأوى آمن لهم.[2]

ثانيا: الصعوبات العملية التي تعترض نظام تسليم المجرمين في مكافحة الجرائم الالكترونية الاقتصادية

هناك عدت صعوبات يتعرض لها نظام تسليم المجرمين تحد من فاعليته في مكافحة الجرائم الالكترونية الاقتصادية، وبالتالي تؤدي إلى كثرة الجرائم وانتشارها مما ينتج عنها إفلات الجناة من العقاب والمحاسبة الجنائية، وبالتالي استفحال الجريمة في المجتمعات، لذا سوف نتعرض لبعض هذه الصعوبات لتسليط الضوء عليها ودراستها.

-عدم اتفاق كافة الدول على بعض مواد الاتفاقيات والمعاهدات

المقصود منها أن العديد من الدول ترفض التعاون في حال توافرت لديها أسباب حقيقية تدعو إلى الاعتقاد بأنه سيكون في خطر التعرض للتعذيب، أو في حالة وجود نمط ثابت من الانتهاكات الفادحة أو

[1]- سراج الدين محمد الروبي: المرجع السابق ، ص 203-202.

[2]- حمد عبد الله حسين العاقل، النظام القانوني الدولي للجريمة المنظمة عبر الدول، دراسة نظرية - تطبيقية، دار النهضة العربية، القاهرة 2010، ص639.

الصارخة أو الجماعية لحقوق الإنسان في الدولة المعنية، أو في حالة كان لدى الشخص المراد إعادته خوفا مسببا بأنه لن يتمتع بمحاكمة عادلة في الدولة المتلقية. [1]

- تنوع واختلاف النظم القانونية الإجرائية

بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا تسمح بإجرائها، فإذا اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق انها قانونية في دولة معينة، فقد تكون ذات الطريقة غير مشروعة في دولة أخرى، بالإضافة إلى السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة انها طرق غير مشروعة حتى وان تم الحصول عليه في اختصاص قضائي وبشكل مشروع. [2]

إضافة إلى الاختلاف في الأنظمة السياسية الطبقة في كل دولة، فالنظم السياسية المتبعة في الدول الاشتراكية تنعكس بصورة تلقائية ومؤثرة في النظام القانوني والاقتصادي والاجتماعي والأمني في مجال تسليم المجرمين، وفي هذا النظام تعطى الأولوية للسيادة الوطنية مما يؤدي إلى صعوبة التعامل وتحقيق صور التعاون القضائي وعدم الاعتراف بالإجراءات والأحكام الأجنبية.

كما ينعكس الجانب السياسي في الأنظمة الرأسمالية على عدم الثقة بالأنظمة القانونية للدول السارية في طريق النمو *، مما يؤدي إلى عدم التعامل في مجال التعاون القضائي إذ أصبح عدم كفاية الضمانات المتعلقة بحقوق الإنسان حجة لرفض التسليم أو من موانعه.[3]

- صدور تشريع جنائي في الدولة المطلوب منها التسليم ينفي الصفة التجريمية عن الفعل المطلوب التسليم من اجله:

بعد تقديم طلب التسليم قد تصدر الدولة المطلوب منها اتخاذ قرار التسليم ، تشريع جنائي ينفي الصفة التجريمية عن الفعل مما يؤدي إلى عدم استمرار طلب التسليم إلا بالرجوع إلى النصوص الأخرى في قانونها العقابي إذ يمكن أن يطبق على هذا الفعل نموذج تشريعي آخر، وفي حالة عدم التوصل إلى هذا الوصف التجريمي فان طلب التسليم سيرفض تماما ولا عبرة بما قد يقرره البعض من أن طلب التسليم قد قدم في وقت كان الفعل معاقبا عليه. [4]

- عدم وجود قنوات اتصال فعالة

---

[1]- متعب بن عبد الله السند: التعاون الدولي في تنفيذ الأحكام الجنائية وأثره في تحقيق العدالة الجنائية-رسالة الماجستير في العدالة الجنائية- جامعة نايف العربية للعلوم الأمنية، الرياض ، 2011، ص 155.

[2]- حسين بن سعيد الغافري: المرجع السابق ، ص 25 .

[3]- محند ارزقي عبلاوي: تسليم المجرمين في نطاق المعاهدات الدولية والتشريع الجزائري- أطروحة دكتوراه الدولة في القانون القسم العام – السنة الجامعية 2009- 2010. ، ص 340- 341 .

* لمواجهة هذا المشكل نجد أن الصكوك الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعال، نقلا عن متعب بن عبد الله السند, المرجع السابق.

[4]- سراج الدين محمد الروبي: المرجع السابق ، ص 181 .

لقد كان الحصول على المعلومات والبيانات المتعلقة بالمجرمين وتنفيذ الأحكام الجنائية ذو أهمية بالغة، وللحصول على هذه المعلومات كان لزاما أن يكون هناك نظام اتصال فعال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة فعدم وجود مثل هذا النظام أو عدم فاعليته يعني عدم القدرة على جمع الأدلة التي غالبا ما تكون مفيدة للتصدي لجرائم معينه من حيث عقابهم وتنفيذ الأحكام الجنائية عليهم وبالتالي تنعدم الفائدة من هذا التعاون. [1]

- التجريم المزدوج

التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين, فهو منصوص عليه في اغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين، وبالرغم من أهميته تلك نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم الالكترونية، إذ أن هناك من الدول من ترضى بالتسليم، وهناك دول أخرى لا تجيز ذلك نظرا لعدم تجريمها لذلك الفعل، بالإضافة إلى انه من الصعوبة أن تحدد فيما إذا كانت النصوص التقليدية لدى الدول المطلوب منها التسليم يمكن أن تنطبق على هذا النوع من الجرائم، خاصة وأنها من الجرائم المستحدثة ، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم الالكترونية. [2]

ولأجل القضاء على مشكلة ازدواجية التجريم، ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الاجراء، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين من خلال سرد الأفعال التي تتطلب أن تجرم كجرائم أو افعال مخلة بمقتضى قوانين الدولتين معا، أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة.[3]

- تدهور الحالة السياسية داخل الدولة المطلوب منها التسليم

إن تأثير تدهور الحالة السياسية داخل أي دولة من الدول إنما ينصرف إلى النظر في طلبات التسليم التي تقدم إلى الدول التي تتدهور حالتها السياسية ، فمن غير المعقول مطالبة دولة ما بالقبض على شخص ما في الوقت الذي لا يستطيع النظام السياسي في هذه الدولة أن يحمي نفسه أو أن يتحرك داخل دولته لوجود اضطرابات شمولية داخل تلك الدولة.

كما أن توقيت طلب الاسترداد هام جدا لان تقديم طلب التسليم في وقت غير ملائم من الوجهة السياسية يعني التسليم مقدما برفض طلب التسليم، وفي هذه الحالة وحتى مع تحسن الظروف السياسية مستقبلا فان احتمال الاستجابة لطلب التسليم لا تجاوز نسبة الصفر. [4]

- الاختصاص في الجرائم

---

[1]- متعب بن عبد الله السند: المرجع السابق، ص 158 .

[2]- حسين بن سعيد الغافري: الجهود الدولية في مواجهة جرائم الانترنت، ص 26 على الموقع الالكتروني :hssnrg@yahoo.com

[3]- أومدور رجاء: خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه الطور الثالث ل.م.د، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة البشير الابراهيمي، برج بوعريريج الجزائر، 2020-2021، ص 235.

[4]- سراج الدين محمد الروبي: المرجع السابق ، ص 179 – 180 .

يقصد بها عدم وجود مختصين مدربين ومؤهلين للنظر الجرائم الالكترونية خاصة وأنها من الجرائم المستحدثة ذات طبيعة خاصة حيث يعتمد مرتكبوها على مهاراتهم الفائقة في تنفيذها، إذ لا توجد أي مشكلة بالنسبة للاختصاص الوطني حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك، منها: مكان القبض على المتهم, مكان وقوع الجريمة أو محل إقامة المتهم... وغيرها.

لكن المشكلة تثار بالنسبة للاختصاص الدولي * وذلك راجع إلى اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول. [1]

اضافة الى ذلك ينبغي التنويه أن اتفاقية بودابيست أوجدت حلولا فعالة لتجاوز العقبات المصادفة لإجراء التحقيق في الجرائم الالكترونية عبر الوطنية، خاصة ما تعلق منها باختلاف النظم الاجرائية أمام التعاون الدولي، و مشكلة الاختصاص و الولايات القضائية، ومشكلة التجريم المزدوج، وعدم وجود قنوات اتصال دولية مباشرة بين سلطات انفاذ القانون، والصعوبات المرتبطة بإجراءات المساعدة القضائية، لذا على الدول الاسراع خاصة المتخلفة منها في تبني الحلول المنصوص عليها، وذلك اما بإدراجها ضمن قوانينها الداخلية و الالتزام بالعمل بها، أو من خلال الانضمام الى الاتفاقية الأوروبية مادام أنها متاحة للتوقيع من جميع الدول، و من ثم يسري عليها من هذه الأحكام ما يسري على الأطراف الأخرى.[2]

خاتمة

توصلنا من خلال ورقتنا البحثية أن نظام تسليم المجرمين باعتباره شكل من أشكال التعاون الدولي هو نتيجة حتمية للتطورات الحاصلة في كافة المجالات، ومنها مجال الاتصالات وتقنية المعلومات، وبالتالي لا مناص من التسليم بأن هذه التكنولوجيا هي نتاج حتمي للعولمة التي نعيشها ونتعايشها، وتعتبر من أهم تحديات العصر بالنظر إلى المعادلة الصعبة التي تطرحها خاصة على الأنظمة القانونية، فمن جهة عليها واجب الاعتراف بها في إطار قانوني حتى تواكب التطور، ومن جهة أخرى أهمية حمايتها والتصدي لما تثيره من جرائم خطيرة ومتطورة.

وعليه توصلنا الى مجموعة من النتائج تتمثل في:

- تسليم المجرمين هو عمل بمقتضاه تقوم الدولة التي لجا إلى أرضها شخص متهم أو محكوم عليه في جريمة بتسليمه إلى الدولة المختصة لمحاكمته أو تنفيذ العقوبة بحقه.

- نظام تسليم المجرمين مطابق للعدالة ولمصلحة الدول بما انه يهدف إلى منع وقوع الجرائم والمعاقبة عليها، وتوقيع العقاب على الجاني يكون من طرف الدولة بنفسها إذا أمكنها ذلك وإما بتسليمه إلى سلطات الدولة التي اضر بمصلحتها أو خرق قوانينها، غير أن التسليم لا يكون إجباريا إلا إذا تعهدت حكومة البلد الذي لجا

[1]- حسين بن سعيد الغافري: المرجع السابق ، ص 26 .

*- لمواجهة مشكلة الاختصاص في الجرائم خاصة المستحدثة منها، ثمة حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية او جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب مع سرعة انتشار هذا النوع من الجرائم نقلا عن متعب بن عبد الله السند المرجع السابق.

[2]- أومدور رجاء: المرجع السابق ، ص238.

إليه الجاني بمقتضى معاهدة بإجابة طلب التسليم، فهذا الأسلوب هو وسيلة فعالة للتعاون الدولي سواء تمثل هذا التعاون في صور اتفاقيات ثنائية أو متعددة الأطراف، وهذه الفعالية ناتجة عن تنظيم أحكام تسليم المجرمين من خلال أو من طرف التشريعات الوطنية إذ أن هدف التسليم يتسم بالطبيعة الدولية وهو حماية الإنسان أينما وجد من الانتهاكات التي قد تصيبه أو تصيب الحقوق المتمتع بها.

– غير أن التسليم بهذا المعنى لا ينفذ إلا في حالة تلقي الدولة المطلوب منها التسليم، طلبا بتسليم مجرم هارب إليها من طرف الدولة طالبة التسليم وذلك بسبب ارتكابه جريمة على أراضيها وهرب دون توقيع العقاب عليه، والغرض من طلب التسليم هو محاكمة المتهم في حال عدم مثوله أمام المحكمة أو توقيع العقاب عليه إذا تم تحديد العقوبة التي وجب توقيعها عليه.

– رغم كل ايجابيات نظام تسليم المجرمين لتي أسلفنا ذكرها لم يصل إلى المرحلة التي يمكن معها تحقق كل الفائدة المرجوة والغرض الذي أنشئ بسببه ،إذ أن هذا النظام تتضمنه بعض السلبيات التي تحول دون تحقق الهدف منه والتي من أبرزها: عدم تعاون الدول في القبض على المتهم المطلوب تسليمه مما يعطل تنفيذ الاتفاقيات وبالتالي إفلات المجرم من العقاب فهناك من الدول التي لا يوجد في قانونها نظام تسليم المجرمين أو عدم وجود اتفاقية بينها وبين الدول طالبة التسليم تلزمها بذلك، إضافة إلى المردود السلبي من عملية رفض التسليم فمجرد رفض طلب التسليم من جانب الدولة المطلوب منها التسليم تصيب جميع المسؤولين عن تنفيذ القانون بصدمة، خاصة إذا كان هناك تأكيد من جانب السلطات العامة في هذه الدولة على التسليم من الوجهة المبدئية ولكن يأتي القرار بعد ذلك مخيبا لكل التوقعات والمستندات السابق تقديمها من جانب تلك الدولة بالرفض، وسبب هذا الرفض غالبا ما يكون لمصلحة اقتصادية أو سياسية مثل ضياع الاستثمارات الاقتصادية لذلك الشخص والتي كان يزاولها في إقليم الدولة المطلوب منها التسليم، أو ضياع العلاقات السياسية بين الدولتين الدولة المطلوب منها التسليم والدولة الموطن الأصلي للمتهم هذا من جهة.

– ومن جهة أخرى نجد موانع التسليم التي تقف عائق أمام تنفيذه والتي هي عديدة أيضا والتي من بينها عدم التوصل إلى الشخص المطلوب تسليمه أو منح الشخص المطلوب صفة اللاجئ السياسي أو رفع الصفة التجريمية للفعل المسند للشخص ارتكابه او صدور الحكم من قضاء غير طبيعي أو تمتع الشخص المطلوب بجنسية الدولة المطلوب منها التسليم.... وغيرها من الموانع، كما أن عدم التزام الدول بتسليم المطلوبين يعد كذلك احد عوائق تحقيق العدالة الجنائية على الصعيد الوطني والدولي على السواء.

تأسيسا على ما سبق دراسته، خلصنا في الأخير إلى مجموعة من التوصيات:

1 – الإسراع بالانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة الجرائم المعلوماتية، خاصة المعاهدات الدولية لمكافحة الإجرام الالكتروني الاقتصادي و هذا ما يجب أن يحدث بالنسبة للجزائر، مع ضرورة تحديث القوانين الجنائية– الموضوعية والاجرائية–بما يواكب التطورات التكنولوجية المستمرة.

2– ضرورة تعزيز التعاون و التنسيق الدولي بين الدول مع بعضها البعض، و بين الدول و المؤسسات المعنية بهذه المشكلة و خاصة الإنتربول، خاصة في مجال تسليم المجرمين .

3 – العمل على وضع تشريعات داخلية متقاربة ومسايرة لمختلف الاتفاقيات في مجال مكافحة الجرائم الالكترونية بين مختلف الدول خاصة دول العالم الثالث.

4 – صياغة شكل جديد لآلية تسليم المجرمين خاصة في مجال التحقيق يتماشى والطبيعة الخاصة للجريمة الالكترونية، مع ايجاد آليات تعاون تقني دولي في مجال تدريب أجهزة مواجهة الجرائم المعلوماتية.

5 –على الجزائر الاستفادة من القواعد التي جاءت بها الاتفاقية الأوروبية بودابيست 2001 لما لها من دور فعال في تنظيم تسليم المجرمين في مجال مكافحة الجرائم الالكترونية.

قائمة المصادر والمراجع

أولا: المصادر

- التعديل الدستوري لسنة 2020 الجريدة الرسميّة للجمهوريّة الجزائريّة ، العدد82، الصادرة في 30 ديسمبر 2020.
- قانون رقم02/16المؤرخ في19جوان 2016المعدل والمتمم للأمر156/66والمتضمن قانون العقوبات الجزائري.
- الأمر رقم 66–155، المؤرخ في 8 جوان 1966، المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية العدد 48، الصادرة في 10 جوان 1966، المعدل والمتمم
- – المرسوم الرئاسي رقم 252/14، المؤرخ في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ21 ديسمبر 2010، الجريدة الرسمية، العدد57، المؤرخ في 28 سبتمبر 2014
- **ثانيا: المراجع**
- **1/ باللغة العربية**
- **الكتب**
- – طارق إلراهيم اليسوقي عطيه، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة للنشر، مصر،2009.
- – جيرهارد فان غلان : القانون بين الامم ، مدخل الي القانون الدولي العام – تعريب عباس العمر– الجزء الاول ، منشورات دار الافاق الجديدة – بيروت _ صفحة 22.
- – سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين–دراسة مقارنة–دار الجامعة الجديدة للنشر، الإسكندرية، 2007.
- –حمد عبد الله حسين العاقل، النظام القانوني الدولي للجريمة المنظمة عبر الدول، دراسة نظرية – تطبيقية، دار النهضة العربية، القاهرة 2010.
- **المقالات والمحاضرات**
- – عباد بن يمينة ، إجراءات تسليم المجرمين المطلوبين دوليا ، مجلة الشرطة ، عدد خاص ، المديرية العامة للامن الوطني ،الجزائر ، 2008 .
- حسين بن سعيد الغافري: الجهود الدولية في مواجهة جرائم الانترنت، ص 26 على الموقع الالكتروني hssnrg@yahoo.com:
- –عبود السراج : مقال بعنوان استرداد المجرمين، على الموقع الإلكتروني: http://www.arab–ency.com/index.php?module=pnEncyclopedia&func=display_term&id=295&m=1 ،
- محمد الفاضل : محاضرات في تسليم المجرمين ، جامعة الدول العربية معهد الدراسات العربية العالية ،1966

- مليكة درياد، احكام تسليم المجرمين في قانون الإجراءات الجزائية. ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد01، 2019.

- -**الرسائل العلمية**

– أومدور رجاء: خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه الطور الثالث ل.م.د، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة البشير الابراهيمي، برج بوعريريج الجزائر، 2020-2021.

– فريدة شبري : تحديد نظام تسليم المجرمين ،مذكرة الماجستير في القانون فرع القانون الدولي الإنساني ،كلية القانون بودواو جامعة بومرداس ، تاريخ المناقشة 2007 .

-- متعب بن عبد الله السند: التعاون الدولي في تنفيذ الأحكام الجنائية وأثره في تحقيق العدالة الجنائية-رسالة الماجستير في العدالة الجنائية- جامعة نايف العربية للعلوم الأمنية، الرياض ، 2011.

– محند ارزقي عبلاوي: تسليم المجرمين في نطاق المعاهدات الدولية والتشريع الجزائري- أطروحة دكتوراه الدولة في القانون القسم العام – السنة الجامعية 2009- 2010.

– معمر محمد زكريا و بوشريحة حسين :نظام تسليم المجرمين ، رسالة الماجستير ، جامعة قسنطينة ،2013/2012 ،

2/ باللغة الأجنبية

-ANNE-Marie la Rosa: le dictionnaire de droit international pénal- publication de l'institut universitaire de hautes étude international GENEV PUF 98.

- ANDRE Heut et RENEE Koering-joulin : droit pénal international.(P.U.F).

مجدوب لامية
lamia.meha@yahoo.fr
جامعة 8 ماي 1945 قالمة

الصعوبات التي تواجه التعاون الدولي في مواجهة الجرائم الالكترونية الاقتصادية

ملخص.
تعد الجرائم الالكترونية الاقتصادية من أهم المعوقات التي تحول دون تحقيق فكرة الإقلاع الاقتصادي وصولا إلى التنمية الاقتصادية الحقيقية، سواء على المستوى الوطني لكل دولة أو حتي على الصعيد الدولي، لذلك تسعى جميع الدول جاهدة إلى تعزيز وتكثيف آليات التعاون الدولي لمجابهة ومحاربة هذا النوع المستحدث من الإجرام الالكتروني بكل صوره في المجال الاقتصادي والمالي وقطاع الأعمال ، ذلك أن الأمن ألمعلوماتي الاقتصادي يتطلب تضافر الجهود الدولية للقضاء على الصعوبات التي تواجه المجتمع الدولي في مكافحة الجريمة الالكترونية الاقتصادية وإيجاد آليات وحلول فعالة للحد والقضاء على هذه العراقيل، هذا ما تهدف إليه هذه الورقة البحثية.

Abstract:
Economic cybercrime is one of the most important obstacles that prevent the realization of the idea of economic take-off and real economic development, whether at the national level of each country or even at the international level. Therefore all countries strive to strengthen and intensify international cooperation mechanisms to confront and combat this new type of crime. Electronic security in all its forms in the economic, financial and business sectors, because economic information security requires concerted international efforts to eliminate the difficulties facing the international community in combating economic electronic crime and finding effective mechanisms and solutions to reduce and eliminate these obstacles, and this is what this research paper aims at.

مقدمة.

في ظل عالم افتراضي أو بيئة إلكترونية مزدحمة بشبكات اتصال عالمية وحواسيب مزودة بأحدث التكنولوجيا والمعلومات، تشغل وتنقل من خلالها البيانات والمعلومات أو المعطيات بين مناطق متباعدة باستخدام تقنيات لا تكفل لها أمنا كاملا،برز ما يعرف بالإجرام الالكتروني الاقتصادي هذا الخير يعد خرقا أو مساسا أو إخلالا بقواعد التشريع الاقتصادي أو السياسة الاقتصادية للدول حيث يتاح في ظلها التلاعب والاعتداء على تلك المعطيات الاقتصادية المعالجة الكترونيا سواء المدخلة أو المنقولة أو المخزنة أو المخرجة في جهاز الحاسوب المزود بشبكة الانترنت أو الاتصالات العالمية، مما قد يسبب لبعض الدول أو الأشخاص

القانونية أضرار فادحة على جميع الأصعدة خاصة المجال الاقتصادي، وبعد أن اكتسحت التجارة والعقود الالكترونية كل جوانب المجال الاقتصادي تكريسا لسياسة الانفتاح والتحرر الاقتصادي، اتضح جليا فعالية التعاون الدولي في مكافحة الجريمة الإلكترونية الاقتصادية بمختلف صورها ، أمرا محتما ومع ضرورة هذا التعاون والمناداة به، إلا أنه ثمة صعوبات ومعوقات تقف دون تحققه، وتجعله صعب المنال وفي سبيل تحقيق فكرة الإقلاع الاقتصادي وصولا إلى التنمية الاقتصادية الحقيقية لابد من تعزيز فكرة التعاون الدولي في مكافحة هذا النوع المستحدث من الجرائم الالكترونية ذات الطابع الاقتصادي وعليه يمكن طرح الإشكالية التالية: ما هي الاستراتجيات المتبعة في مجال التعاون الدولي لمحاربة الجرائم الالكترونية الاقتصادية والتصدي لها؟

في سبيل الإجابة على هذه الإشكالية اتبعنا المنهج الوصفي لتحديد ووصف أهم العراقيل التي تواجه التعاون الدولي في مجال الإجرام الالكتروني الاقتصادي والية التصدي لها،ناهيك عن المنهج التحليلي أين اقتضت الدراسة إسقاطات و استنتاجات بين الجرائم الالكترونية عموما والجرائم الالكترونية الاقتصادية تحديدا،وقد قسمنا هذه المداخلة إلى قسمين أو مطلبين على النحو التالي:

المطلب الأول: المعوقات التي تواجه التعاون الدولي في مجال الجرائم الالكترونية الاقتصادية.

إن التعاون الدولي بكافة صوره في مجال مكافحة أو مواجهة أو التصدي للجرائم الإلكترونية عموما الجرائم الإلكترونيةِ الاقتصادية تحديدا، وإن كان يعد مطلبا تسعى إلى تحقيقه أغلب الدول إن لم نقل كلها بما فيها الجزائر، غير أنه ثمة صعوبات أو عراقيل تقف دون تحقيقه أهمها ما يلي:

الفرع الأول: عدم وجود نموذج موحد للنشاط الإجرامي للجريمة الالكترونية الاقتصادية.

بالرجوع إلى مختلف الأنظمة القانونية الجزائية القائمة في جل الدول لمواجهة الإجرام الإلكتروني الاقتصادي يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت والتلاعب فيها، الواجب تجريمها في المجال الاقتصادي ، فما هو مباح في أحد الأنظمة قد يكون مجرما وغير مباح في نظام قانوني آخر ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئة الاجتماعية والعادات والتقاليد والديانات والثقافات من مجتمع إلى آخر وبالتالي اختلاف السياسات التشريعية في نطاق القانون الجنائي سواء في مفهومه التقليدي أو الحديث من دولة إلى أخرى.[1] ،ذلك أن تشعب وتنوع صور الجرائم الالكترونية الاقتصادية عبر مختلف مراحل العملية الاقتصادية داخل الدولة الواحدة يخلق صعوبات ومعوقات للحد من هذا النوع المستجد من الإجرام فما بالك بتشعب وتنوع هذه الجرائم ضمن وحدات المجتمع الدولي ككل.

الفرع الثاني: تنوع واختلاف النظم القانونية الإجرائية.

كنتيجة طبيعية لاختلاف السياسات التشريعية العقابية في مجابهة الجرائم الالكترونية ككل والالكترونية الاقتصادية تحديدا ، اختلفت وتنوعت كذلك النظم القانونية الإجرائية أو الشكلية، حيث نجد أن

[1] عبد الفتاح بيومي مجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت،طبعة مزيدة، دار الكتب القانونية، مصر،2009، ص 102.

أساليب البحث والتحري والتحقيق والمحاكمة التي تثبت فاعليتها في دولة معينة، قد تكون عديمة النفع في دولة أخرى أو قد لا يسمح بإجرائها نهائيا كما هو الحال بالنسبة للمراقبة الإلكترونية والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات المستحدثة، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق القضائي أنها قانونية وشرعية في دولة معينة، قد تكون تلك الطريقة نفسها غير مشروعة في دولة أخرى، مما قد يترتب عليها من عدم مشروعية الأدلة وقوتها الثبوتية وبطلان الإجراءات[2].

الفرع الثالث: عدم وجود قنوات اتصال.

إن الغاية الأساسية أو المرجوة من تعميق التعاون الدولي في مجال الإجرام الإلكتروني الاقتصادي، هي الحصول على المعلومات والبيانات اللازمة والكافية لمحاربة الجريمة ومعاقبة مقترفيها ولتحقيق هذه الغاية كان لزاما وجود نظام اتصال واسع النطاق يسمح للجهات القائمة على التحقيق القضائي بالاتصال بجهات أجنبية لجمع الأدلة وكل ما يتعلق بالجريمة الالكترونية ، لذلك فإن غياب قنوات الاتصال هذه يقف عائقا دون جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي للجرائم الإلكترونية الاقتصادية والمجرم المعلوماتي في المجال الاقتصادي عبر مختلف مراحل العملية الاقتصادية وبالتالي تزول الفائدة من وراء هذا التعاون الدولي.[1]

الفرع الرابع: إشكالية الاختصاص القضائي في الجرائم الإلكترونية الاقتصادية.

إن الجرائم الإلكترونية بما فيه الاقتصادية تعد من أكثر الجرائم التي تثير مسألة الاختصاص القضائي على المستوى العالمي أو الدولي، وإن كانت لا توجد أي مشكلة بالنسبة للاختصاص القضائي على المستوى الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك.[2]

غير أن الإشكال يثار بالنسبة للاختصاص على المستوى الدولي أو العالمي حيث اختلفت التشريعات والنظم القانونية التي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم الإلكترونية الاقتصادية التي تتميز بكونها عابرة للحدود، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي وتحدث آثارها في دولة أخرى وتكون ماسة بأمن وسلامة هذه الدولة الأخيرة، ففي هذا الفرض تكون الجريمة خاضعة للاختصاص القضائي الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص دولة الأجنبي على أساس مبدأ الاختصاص الشخصي في إحدى شقيه، وقد تكون هذه الجريمة من اختصاص الدولة الثالثة التي مست بأمنها وسلامتها استنادا إلى مبدأ العينية، كما قد تثار مسألة الاختصاص القضائي تبعا لمبدأ الإقليمية، كما لو قام الجاني بالتلاعب أو تزييف المعطيات المعلوماتية ذات الصلة بالعملية التسويقية في إقليم دولة معنية وتم تحقيقها في دولة أخرى في هذا الفرض يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها جريمة التلاعب بالمعطيات في البيئة الإلكترونية.[1]

الفرع الخامس: التجريم المزدوج "ثنائية التجريم".

---

[1] يوسف مصري، الجرائم المعلوماتية والرقمية للحاسوب والانترنت،ط1،دار العدالة، القاهرة،2011 ،ص130.

[2] تتمثل هذه المعايير في :مكان القبض على المتهم،مكان وقوع الجريمة،أو محل إقامة المتهم.

إن التجريم المزدوج أو ثنائية التجريم يعد من أهم الشروط الخاصة بنظام تسليم المجرمين فهو منصوص عليه في أغلب التشريعات الوطنية والاتفاقيات الدولية المعنية بتسليم المجرمين ولكن رغم أهميته تلك، نجده عقبة كبيرة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم الإلكترونية الاقتصادية على غرار التلاعب، سيما وأن أغلب الدول لا تعاقب على هذه الجرائم، إضافة إلى صعوبة تحديد ما إذا كانت النصوص التقليدية لدى الدول المطلوب منها التسليم يمكن تطويعها لتنطبق على الجرائم الإلكترونية الاقتصادية أولا، الأمر الذي يحول دون تطبيق المعاهدات الدولية في مجال تسليم المجرمين ويعوق بالتالي عملية جمع الأدلة ومتابعة مرتكبي الإجرام الإلكتروني الاقتصادي بمختلف صوره.)

الفرع السادس: الصعوبات الخاصة بالمساعدات القضائية الدولية.

معلوم أن الأصل بالنسبة لطلبات الإنابة القضائية الدولية التي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم وتتم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتصف بالبطء والتراخي والتعقيد، الذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة وتطور، وهو الأمر الذي انعكس على الجرائم الإلكترونية عموما والجرائم الالكترونية الاقتصادية تحديدا.

كذلك من بين الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة البطء في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في القواعد الإجرائية التي تعقد الاستجابة وغيرها من الأسباب.[2]

الفرع السابع: الصعوبات الخاصة بالتعاون الدولي في مجال التدريب.

تتمثل هذه الصعوبات في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما أخذه أو تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من معلومات وخبرات في هذا المجال، ومن المعوقات أيضا التي قد تهدد التعاون في مجال التدريب، ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات والقدرات الفنية والشخصية المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين، سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال، حيث يوجد بعض الأفراد ممن لا يعرف شيئا في هذا المجال والعكس من ذلك يوجد من هم متفوقون في هذا المجال، إضافة إلى نظرة المتدرب في حد ذاته حول الدورة التدريبية على أنها عبئ لا مفر منه تهدد العملية التدريبية برمتها وبالطبع تنسف التعاون الدولي في هذا المجال، كذلك من الصعوبات التي قد تؤثر على العملية التدريبية وعلى التعاون الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلا متقننا وكاملا من حيث ما يجري بها من

---

(1) شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية ، دار الجامعة الجديدة، الإسكندرية،2007،ص367

2.(2)Yann Padova :"un aperçu de la lutte contre la cybercriminalité en France",Revue de science criminelle et de Droit pénal comparé, N=4, Octobre-Décembre 2002,p774.

(2)يوسف مصري، مرجع سابق ، ص 131.

وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تصل إلى حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية أو الحقيقية التي يعملون فيها.[3]

المطلب الثاني: آلية القضاء على المعوقات التي تواجه التعاون الدولي في مجال الجرائم الالكترونية الاقتصادية.

هناك عدة محاولات سواء على الصعيد الوطني أو الدولي للقضاء على مجمل الصعوبات التي قد تواجه التعاون الدولي في مكافحة الإجرام الإلكتروني الاقتصادي، فيما يخص العقبة الأولى المتمثلة في عدم وجود نموذج موحد للنشاط الإجرامي، فإن الأمر يقتضي توحيد هذه النظم القانونية، ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد في إيجاد وتفعيل التعاون الدولي، بحيث يتفق ذلك مع هذا النوع المستحدث من الإجرام ويخفف من عمق الفوارق بين الأنظمة العقابية الداخلية وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم الالكترونية ذات الطابع الاقتصادي [4] وإبرام معاهدات خاصة يراعي فيها هذا النوع من الإجرام.

أما فيما يخص العائق الثاني والخاص بتنوع واختلاف النظم القانونية الإجرائية أو الشكلية نجد أن الاتفاقيات الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة المستحدثة، الشيء الذي يخفف من غلو واختلاف النظم القانونية الإجرائية ويفتح المجال أمام تعاون دولي حقيقي وفعال في هذا النطاق، فمثلا المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الصدد إلى التسليم المراقب [5] والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة والتي تعد من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستعمالها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة.

هذا ما أكدت عليه الاتفاقية الأوروبية للإجرام ألمعلوماتي حيث نصت المادة 29 على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر والتي ينوي الطرف طالب المساعدة أن يقدم طلبا للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار إليها، كما أكدت المادة 30 من ذات الاتفاقية على المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، فأجازت لأي طرف الطلب من الطرف الآخر أن يقوم بالتفتيش أو أن يدخل بأية طريقة مشابهة، وأن يضبط ويكشف عن البيانات المحفوظة بواسطة شبكة

---

[3] المرجع نفسه، ص ص131،132.

[4] ميساء مصطفى بركات، جرائم التعدي على المعلوماتية الإتلاف والتزوير ،رسالة أعدت لنيل درجة الماجستير ،كلية الحقوق والعلوم السياسية،قسم الدراسات العليا،جامعة بيروت العربية،2009، ص 138.

[5] يوسف المصري، مرجع سابق، ص 133.

المعلومات داخل النطاق المكاني لذلك الطرف والتي تكون فيها أيضا البيانات المحفوظة وفقا للمادة 19 من نفس المعاهدة ولابد من الاستجابة لمثل هذا الطلب بأسرع ما يمكن في الحالات التالية:

– إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية عرضة على وجه الخصوص لمخاطر الفقد أو التعديل.

– إذا كانت الرسائل والاتفاقيات والتشريعات تستلزم تعاونا سريعا.[6]

وباستقراء نصوص المواد 31، 32، 33 و 34 من ذات الاتفاقية، الاتفاقية الأوروبية للإجرام المعلوماتي، يمكن القول بأن هذه الاتفاقية أوجدت بعض الحلول التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم الإلكترونية.

للحد من ظاهرة عدم وجود قنوات اتصال بين جهات انفاذ القانون نلاحظ أنه غالبا ما تشجع الاتفاقيات الدولية الدول الأعضاء على التعاون فيما بينها، وتدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير في الحصول على هذه المعلومات وتبادلها، ومن أمثلة هذه المعاهدات اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في المادة 27 منها والمادة 09 من اتفاقية 1988 والمادة 48 من اتفاقية الأمم المتحدة لمكافحة الفساد، والبند الثاني من المادة 27 من الاتفاقية الأوروبية بشأن الإجرام المعلوماتي والمادة 35 من ذات الاتفاقية الأوروبية والتي فرضت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يوميا طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو استقبال الأدلة ذات الشكل الإلكتروني في المجال الاقتصادي.

لأجل القضاء على مشكلة التجريم المزدوج والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الشديد أو الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين وذلك إما بسرد الأفعال التي تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضى قوانين الدولتين معا أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة.[7]

أما بالنسبة لمشكلة الاختصاص في الجرائم الإلكترونية عموما والاقتصادية تحديدا على غرار التزوير منها، فثمة حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرامية بما يتناسب والتقدم الكبير الذي تشهده تكنولوجيا المعلومات والاتصالات يوما بعد يوم.

فيما يخص الصعوبات الخاصة بالمساعدات القضائية الدولية والتباطؤ في الرد فإننا نجد الحاجة ملحة لضرورة إيجاد وسيلة تتسم بالسرعة تسلم من خلالها طلبات الإنابة كتعيين سلطة مركزية مثلا أو

---

[6] ميساء مصطفى بركات، مرجع سابق، ص 138.

[7] يوسف المصري، مرجع سابق، ص 135.

السماح بالاتصال المباشر بين الجهات المختصة في نظر مثل هذه الطلبات للقضاء على مشكلة التعقيد والبطء في تسليم طلبات الإنابة، وهذا ما أكد عليه وأوصى به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية الذي انعقد في بانكوك في الفترة من 18 إلى 2005/04/25 حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية ضمان تنفيذ الطلبات في الوقت المناسب.[8]

أما فيما يتعلق بالصعوبات أو العراقيل التي تواجه التعاون الدولي في مجال التدريب فإنه يمكن التغلب عليها بإجراء المزيد والعديد من حملات التوعية للتنبيه من مخاطر الجرائم الإلكترونية والأضرار الناجمة عنها وبأهمية تدريب رجال العدالة الجنائية على مواجهتها، كما أنه وبمزيد من التنسيق بين الأجهزة المعنية بتدريب رجال القضاء وأعوانه وضرورة إيجاد برامج تدريبية مشتركة تناسب جميع الفئات، إضافة إلى القيام ببعض العمليات المشتركة والتي من شأنها صقل مهارات القائمين على مكافحة الجرائم الاقتصادية في البيئة الإلكترونية وتقريب وجهات النظر بشأنها[9].

خاتمة.

في خاتمة هذه المداخلة التي تمحورت حول أهم المعوقات أو الصعوبات التي واجهت التعاون الدولي في مجال مكافحة الجرائم الالكترونية الاقتصادية وكيفية التصدي لها، لتحقيق فكرة الإقلاع الاقتصادي وصولا إلى تجسيد التنمية الاقتصادية الحقيقية، هذه الأخيرة تعد البوابة الفعلية لتطور وتقدم الشعوب والدول وازدهارها على جميع الأصعدة نقترح جملة من التوصيات في سبيل مجابهة الجرائم الالكترونية في المجال الاقتصادي والتي تحول دون تحقيق فكرة التعاون الدولي في هذا المجال كما يلي:

-العمل على وضع مواقع الكترونية متخصصة للتبليغ عن هذا النوع من الجرائم الالكترونية الاقتصادية بمختلف صورها عن طريق ما يعرف بالبلاغات الالكترونية.

-إيجاد آلية كفيلة بحل مشكل تنازع القوانين بين كل التشريعات القانونية في ما يخص محاكمة مرتكبي هذا الفئة من الجرائم المستحدثة وذلك بإيجاد حل نهائي لمشكلة الاختصاص القضائي الدولي الذي تثيره هذه الجرائم العابرة للحدود الوطنية.

-ضرورة وضع آليات تنسيق بين مختلف الهيئات الدولية المعنية بمكافحة هذه الجرائم بما يضمن تفعيل مسالة تبادل المعلومات والخبرات حول الشبكات العالية للاتصالات بما فيها الشبكة العنكبوتية.

-الحث على إيجاد استراتجيات دولية عن طريق المعاهدات الدولية لإرساء قواعد التعاون الدولي تماشيا وطبيعة هذه الجرائم سواء كانت ذات طابع فني أو قانوني أو قضائي.

قائمة المراجع.

1 -عبد الفتاح بيومي مجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت،طبعة مزيدة، دار الكتب القانونية، مصر ،2009.

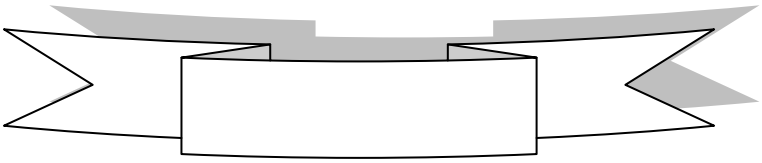
[8] المرجع نفسه، ص ص135، 136.

[9] نفس المرجع ، ص 136.

2 - يوسف مصري، الجرائم المعلوماتية والرقمية للحاسوب والانترنت،ط1،دار العدالة، القاهرة،2011.

3 -ميساء مصطفى بركات، جرائم التعدي على المعلوماتية الإتلاف والتزوير،رسالة أعدت لنيل درجة الماجستير،كلية الحقوق والعلوم السياسية،قسم الدراسات العليا،جامعة بيروت العربية،2009.

4- Yann Padova :"un aperçu de la lutte contre la cybercriminalité en France",Revue de science criminelle et de Droit pénal comparé, N=4, Octobre-Décembre 2002,p774.



حاتم مولود
hatemmy@hotmail.fr
جامعة مولود معمري تيزي وزو

الأدلة الرقمية، آلية لمكافحة الجريمة الالكترونية

الملخص:

إنّ تطور شبكات الاتصال وانتشار الإنترنت ، وكذلك الوصول السهل والمستمر إلى البيانات الحساسة داخل الشركات والكيانات الاقتصادية ، أدى إلى زيادة الجرائم الإلكترونية. إذا كانت الجريمة متأصلة في المجتمعات، فهي مرتبطة بالتنمية الاقتصادية.

إن تحديد المسؤوليات يشمل صعوبات عديدة، أمام تعدد مقدمي خدمات الاستضافة أو أصحاب منصات الوصول إلى الإنترنت أو الناشرين. علاوة على ذلك، فإن هذه الجريمة تأخذ بُعدًا عالميًا، فإن توطين الأفعال يثير مناقشات حول تطبيق مبدأ الإقليمية في تطبيق القوانين على الجريمة الإلكترونية. في ضوء هذه الصعوبات في التحكم في هذا النوع من الجرائم التي تؤثر بشدة على القطاع الاقتصادي، مما يقتضي مواكبة التطور من خلال التكوين التقني للمحققين والقضاة وأسلاك الشرطة القضائية والجمارك للتحكم في الجوانب الشكلية والموضوعية للأدلة الرقمية، والذي يتم في إطار تعاون دولي فعال ترتبط به بعض العراقيل التي قد ترهن نجاح المساعي الدولية في محاصرة هذه الحرب الالكترونية ضد اقتصاديات الدول.

الكلمات المفتاحية: *الأدلة العلمية ؛ الجريمة الإلكترونية، الأمن الرقمي.*

Abstract:

The development of networks and the spread of the Internet, as well as easy and continuous access to sensitive data within companies and economic entities, have led to an increase in cybercrime. If crime is inherent in societies, it is linked to economic development, as crimes committed in cyberspace continue to increase, Defining responsibilities involves many difficulties, with multiple hosting service providers, internet access platform owners or publishers. Moreover, this crime takes on a global dimension, and the localization of acts provokes discussions about the application of the principle of regionalism in the application of laws to cybercrime.

In the light of these difficulties in controlling this type of crime, which severely affects the economic sector, which requires keeping pace with the development through the technical composition of investigators, judges and judicial police and customs to control the formal and objective aspects of digital evidence, which is carried out within the framework of effective international cooperation linked to some obstacles that may depend on the success of international efforts to contain this electronic war against the economies of States.

Keywords*: Scientific evidence; cybercrime, digital security*

مقدمة

التكنولوجيات الجديدة، ولا سيما المعلومات والاتصالات السلكية واللاسلكية، لها مكانة مهمة في الحياة الاقتصادية، ومقدار المعاملات والتبادلات التي تجريها، والتي تسهم بشكل إيجابي في تطوير الحياة الاقتصادية، لكنها توفر وسائل جديدة لارتكاب الجرائم الاقتصادية، مما يكشف عن مخاطر كبيرة.

في ضوء هذه الصعوبات في التحكم في هذا النوع من الجرائم التي تؤثر بشدة على القطاع الاقتصادي، مما يقتضي مواكبة التطور من خلال التكوين التقني للمحققين والقضاة وأسلاك الشرطة القضائية والجمارك للتحكم في الجوانب الشكلية والموضوعية للأدلة الرقمية، والذي يتم في إطار تعاون دولي فعال ترتبط به بعض العراقيل التي قد ترهن نجاح المساعي الدولية في محاصرة هذه الحرب الالكترونية.

حيث أن الجرائم المرتكبة في الفضاء الإلكتروني في تزايد مستمر، كما أن الفضاء السيبراني لا حدود له، مما يشكل تحديا لسلطات تنفيذ القانون والسلطات القضائية في التحقيق الجنائي والمقاضاة، مع وجود خطر كبير للإفلات من العقاب؛ لذلك توجهت الدول الأوروبية نحو التصدي للجرائم السيبرانية في إطار التعاون القضائي في المسائل الجنائية، بدعم من الشبكة القضائية الأوروبية المعنية بجرائم الفضاء الحاسوبي.

يكتسي مكان ارتكاب الجرائم أهمية قصوى من حيث التطبيق الإقليمي للمعيار وتحديد هوية مجرمي الفضاء الحاسوبي. ومع ذلك، فإن التعامل مع مواقع الجرائم السيبرانية يعني التوفيق بين الطبيعة المحددة للقانون الجنائي على المستوى المكاني والطبيعة العالمية للشبكات. ويتيح هذا الأخير انتشار تبادل المعلومات وفوريته في كل مكان. ومع ذلك، فإن فعالية القانون القمعي في الفضاء السيبراني العالمي تعاني من نسبية معينة نظرا لطابعها السيادي أساسا، مما يستدعي التطرق للتجارب الرائدة في المجال، للبحث حول آليات وأطر الوصول للأدلة الالكترونية واستغلالها؟.

المحور الأول: النظام القانوني لاستغلال الأدلة الرقمية في فرنسا

تتمثل العقبة الرئيسية التي يواجهها القضاة في صعوبة الوصول إلى الأدلة الرقمية، واستغلالها بما يكرس نجاعتها، وهو الأمر الذي يتوقف على مدى تخصص وتمديد اختصاص المتدخلين في الوصول واستغلال هذه الأدلة.

أولا- دور المضيفين في الوصول إلى الأدلة الرقمية ومبدأ حرية التعبير:

يعتمد جمع الأدلة الرقمية على فترة الاحتفاظ بالبيانات من قبل كل مضيف، والذي لا يعتمد أي معيار مشترك ثابت، ولكن أيضًا على الضمان الذي يمكن للمحققين تقديمه بأن الأدلة لم يتم تزويرها. حيث أن أية مسألة جزائية تعزز متطلبات المحققين الذين سيتعين عليهم إثبات أصلها وأصالتها[1].

يعد الامتثال لإجراءات الوصول إلى الأدلة الرقمية ذا أهمية أساسية لأنه يجعل من الممكن إثبات سلامة البيانات الإلكترونية وشرح كيفية الحصول عليها وفقًا لحقوق الأطراف في مواجهتهم بالأدلة. حيث أن

المفاوضات جارية حاليًا على مستوى الاتحاد الأوروبي، كجزء من حزمة "الأدلة الإلكترونية"، من أجل تنسيق القواعد المطبقة على المستوى الأوروبي[2].

تتجاوز مسألة الوصول إلى الأدلة الرقمية إطار مكافحة الجرائم الإلكترونية في حالات التعقيد المعين، مهما كانت طبيعتها، غالبًا ما يكون المحققين بحاجة لاستغلال بيانات الهاتف المحمول أو المراقبة بالفيديو أو طلب خبرة في تكنولوجيا المعلومات، والتي تتطلب تأمين هذه البيانات.

خضع في فرنسا مشروع قانون يتعلق باستغلال الأدلة الرقمية (الذي قدمه النائب ليتيسيا أفيا) لرقابة المجلس الدستوري ، والذي ضاعف مجلس الشيوخ التحذيرات بشأنه. حيث كان هذا النص يهدف إلى فرض السحب في فترة زمنية قصيرة لبعض المحتويات غير القانونية. إذ كان سيُلزم بعض مشغلي المنصات عبر الإنترنت ، تحت طائلة العقوبة الجنائية[3]، بإزالة /أو منع الوصول في غضون أربع وعشرين ساعة للمحتوى غير القانوني، على أساس تقرير بسيط من قبل المستخدم. كان سيتطلب أيضًا من مضيفي أو ناشري خدمة الاتصال عبر الإنترنت إزالة في غضون ساعة واحدة ، محتوى إرهابي أو محتوى إباحي للأطفال يتم إخطاره من قبل السلطة الإدارية. ويعاقب على عدم الامتثال لهذه الالتزامات بعقوبة جنائية شديدة. اعتبر المجلس الدستوري ، بقراره رقم 801-2020 دي سي المؤرخ في 18 جوان 2020 [4]، أن هذه الأحكام تشكل اعتداء على حرية التعبير والتواصل، لذلك تم اعتباره بأنه غير دستوري.

كان من الممكن أن يمنحوا الإدارة سلطة كبيرة لاتخاذ قرار بشأن المحتوى المراد إزالته ووضع قيود قوية على المشغلين الذين قد يميلون إلى إزالة كل المحتوى المبلغ عنه لحماية أنفسهم من الملاحقة الجنائية ، نظرًا لصعوبة تنفيذ الفحص الحقيقي للمحتوى المتنازع عليه في الوقت القصير المسموح به لهم.

ثانيا: دور أجهزة السلطة القضائية في استغلال الأدلة الالكترونية.

إن مسألة تخصص الموارد البشرية تعتبر أهم العوامل من أجل تقديم خدمات متخصصة. حيث أن البعد التقني القوي للجرائم الإلكترونية يستلزم تخصص بعض خدمات التحقيق والقضاة، على مستوى تقني جيد، يمكن لهذه الخدمات أن تستفيد من التوسع، لا سيما على الجانب القضائي الذي يبدو أنه يعاني من نقص الموارد بشكل خاص.

أ/- **بالنسبة لدوائر التحقيق** : لكل من الإدارات المكلفة بقمع الجرائم الجنائية أو الضريبية أو الجمركية خدماتها المتخصصة.

1- **الشرطة القضائية:** اكتسبت الإدارة المركزية للشرطة القضائية التابعة لوزارة الداخلية مديرية فرعية مسؤولة عن مكافحة الجرائم الإلكترونية .(SDLC) ، توظف المديرية الفرعية حوالي 130 شخصًا ، من بينهم حوالي عشرة مهندسين وفنيين. ويشمل على وجه الخصوص مكتب تنسيق استراتيجي ، ومكتب إنترنت، ومكتب للتدريب على مكافحة الجرائم الإلكترونية ، وقسمًا للتنبؤ والتحليل ، بالإضافة إلى المكتب المركزي لمكافحة الجريمة المرتبطة بتكنولوجيا المعلومات والاتصالات. تعمل بالاشتراك مع الإدارات الأخرى بوزارة الداخلية ومع الإدارات المركزية الأخرى.

تعتبر مديرية مكافحة الجرائم الالكترونية كيان يسهل التعرف عليه من قبل شركائه المؤسسيين في الاقتصاد الرقمي والأفراد. حيث تظهر أهميته في:

– يلعب دورًا مهمًا في التدريب المتخصص للمحققين على مكافحة الجرائم الإلكترونية و التهديد السيبراني.

– يوفر معلومات للخدمات التي تبحث في هذا المجال ويساعدهم على إقامة اتصالات مع مشغلات الإنترنت بفضل دليل جهات الاتصال المحجوزة.

– يعد مصدرًا للخبرة بفضل قسم المساعدة الفنية والبحث والتطوير.

– استغلال الوسائط الرقمية وتصميم أدوات تحقيق رقمية جديدة.

– يمكن لقسم الأدلة الرقمية إرسال مجموعة دعم للعمل على الآثار الرقمية.

– يساهم في تطوير الأدوات التي تستهدف عامة الناس. والتي تجمع التقارير من مستخدمي الإنترنت الذين يكتشفون السلوك أو المحتوى العام على الويب الذي يعتبرونه غير قانوني.

– قمع الهجمات على أنظمة معالجة البيانات الآلية.[5]

2– الجمارك: تمتلك إدارة التحقيقات الجمركية، هيكلها الخاص لمحاربة الجرائم الإلكترونية ، والذي يُطلق عليه خدمة الجمارك الإلكترونية أو وحدة الجمارك الإلكترونية. تقوم الخدمة بجمع واستخدام جميع المعلومات المفيدة في مكافحة الاحتيال على الإنترنت فيما يتعلق بالاتجار بالسلع المحظورة أو الخاضعة للتنظيم أو الخاضعة لضرائب. يقوم وكلاؤه بمراقبة الإنترنت من أجل إنشاء روابط بين المواقع أو المنتديات أو الكلمات الرئيسية المختلفة ورسم خرائط لعمليات الاحتيال المعقدة[6].

تسعى التحقيقات من خلاله إلى تحديد الأشخاص الطبيعيين أو الاعتباريين الذين يختبئون وراء موقع مبيعات عبر الإنترنت أو عنوان بريد إلكتروني أو اسم مستعار على موقع إعلانات مبوبة أو منتدى أو مدونة أو شبكة اجتماعية[7] .

ب – بالنسبة للنيابة العامة: فرضت الحاجة إلى التخصص نفسها أيضًا منذ دخول القانون رقم 2016–731 المؤرخ 3 جوان 2016 حيز النفاذ، المتعلق بتعزيز مكافحة الجريمة المنظمة والإرهاب وتمويلهما. وتحسين كفاءة وضمانات الإجراءات الجنائية[8].

في إطار الادعاء، فإن المادة 706–72–1 من قانون الإجراءات الجنائية تكلف المدعي العام، بمحكمة الجنايات ومحكمة جنايات باريس بالاختصاص الوطني المتزامن في مسائل الاعتداءات على الآليين. أنظمة معالجة والهجمات على المصالح الأساسية للأمة (والتي قد تغطي فرضيات التخريب السيبراني) [9].

يُعهد بهذا الاختصاص إلى قسم الجرائم الإلكترونية. هذا التغيير هو نتيجة لإعادة التنظيم التي قررها المدعي العام لباريس ، في بداية عام 2020. حيث تم دمج القسم المسؤول عن الإجراءات العامة المتخصصة الذي كان ملحقًا بالنيابة العامة. ، وتخصيص قسم ثان الذي يتعامل مع القضايا التي تقع تحت الولاية القضائية الوطنية لمكافحة الجريمة المنظمة، القضايا التي تتميز بضخامة أو تعقيدها الشديد في مجال التنظيم أو الجريمة الاقتصادية والمالية[10].

يدخل في اختصاص قسم الجرائم الالكترونية ذات الاختصاص الوطني التعامل مع قضايا الجرائم الإلكترونية المعقدة، أينما حدثت في الدولة، حيث تمارس ولايتها القضائية الوطنية في أربع قضايا:

-1- في حالة تعدد الجناة أو الضحايا في الإقليم ، وذلك لتجنب إجراء تحقيقات موازية من قبل العديد من المحاكم

-2- عندما يكون للقضية بعد دولي قوي ، يكون القسم على دراية بإجراءات التعاون القضائي الدولي.

-3- بسبب الطبيعة التقنية أو تعقيد طريقة التشغيل

-4- فيما يتعلق بوضع الضحية، إذا كان مشغلًا ذا أهمية حيوية، أو وزارة[11]

تم تقديم العديد من الأمثلة في هذا التقرير على القضايا التي تم حلها عن طريق خدمات العدالة والتحقيق. لذلك لا يوجد إفلات من العقاب فيما يتعلق بالجرائم الإلكترونية، حتى لو كانت العدالة لا تزال تواجه في كثير من الأحيان صعوبة القبض على مرتكبي الجرائم عندما يكونون في الخارج، على أراضي الدول غير المتعاونة. إذ هناك زيادة في الوسائل المخصصة لمكافحة الجريمة السيبرانية ، وهو ما يتوافق مع المكانة المتنامية للتكنولوجيا الرقمية في الحياة اليومية وفي النشاط الاقتصادي[12].

المحور الثاني: توحيد الجهود الدولية المشتركة في استغلال الأدلة الالكترونية.

اعتمد الاتحاد الأوروبي في 9 جوان 2016 استنتاجات في سبيل قمع الجرائم الإلكترونية وتحسين العدالة الجنائية في الفضاء الإلكتروني ، والتي بموجبها دُعيت الدول الأعضاء إلى تقديم مبادرة تشريعية تهدف إلى تسريع وتبسيط وصول القضاة إلى عناصر الأدلة الإلكترونية، وهو ما تم من خلال مشروع اللوائح والتوجيهات بشأن الوصول عبر الحدود إلى الأدلة الإلكترونية.

أولا/- الإطار الهيكلي والتنظيمي:

يعتبر هذا النهج العابر للحدود ذا أهمية نظرًا لأهمية الوصول إلى الأدلة الإلكترونية في سياق التحقيقات العابرة للحدود الوطنية التي تقتضيها عدد كبير من قضايا الجرائم الإلكترونية. كما أشارت إدارة الشؤون الجنائية والعفو بوزارة العدل الفرنسية أن ثلاثة أرباع هذا النوع من القضايا، لم يتم العثور على الأدلة في الدولة التي وقعت فيها الجريمة[13].

يهدف العمل الدولي المشترك إلى الاحتفاظ بالبيانات بشكل موحد ، حيث يمثل تحديًا كبيرًا في مكافحة الجرائم الإلكترونية ، فإن الأحكام الصادرة عن محكمة العدل التابعة للاتحاد الأوروبي في عدة مناسبات قضت بإبطال الأنظمة الوطنية والأوروبية مما جعل الدول الأعضاء في حالة من عدم اليقين بشأن إمكانيات الحصول على البيانات. فمثلا في حكمها الخاص بالحقوق الرقمية في أيرلندا ، الصادر في 8 أبريل 2014 ، ألغت أحكام توجيه عام 2006 الذي يسمح لمشغلي الاتصالات بتخزين بيانات هواتف عملائهم لمدة أقصاها 6 إلى 24 شهرًا ، بحيث يمكن للشرطة استخدامها للتحقيق في أعمال الإرهاب والجرائم الخطيرة، على أساس أنها تنتهك الحقوق الأساسية بشكل خطير [14]. إلا أنه في بعض الدول الأعضاء، لا يزال العمل بالتوجيهات

المشتركة لضمان احتفاظ مزودي خدمة الإنترنت بالبيانات بغرض استغلالها، بينما تم إلغاء التشريعات الوطنية في دول أخرى تطبيقا لحكم المحكمة الأوروبية[15].

إن مثل هذه التناقضات تعرقل عمل السلطات المختصة وقد تؤدي إلى فقدان خيوط التحقيق وتضعف في النهاية القدرة على مقاضاة النشاط الإجرامي بشكل فعال عبر الإنترنت، فإن غالبية سلطات التحقيق والسلطات القضائية في الدول الأعضاء ستؤيد وضع إطار تشريعي على المستوى الأوروبي.

اعتمد المجلس الأوروبي استنتاجات تتطلب إعداد دراسة متعمقة حول الحلول الممكنة للاحتفاظ ببيانات الاتصالات السلكية واللاسلكية لأغراض تنفيذ القانون، بما في ذلك دراسة مبادرة تشريعية مستقبلية [16]. استجابت الهيئة لهذا الطلب وأكدت أن الدراسة ستكون متاحة قبل نهاية عام 2019. ومع ذلك، فإن هذه الدراسة لم يتم نشرها. ليقوم المجلس بعد ذلك بتعيين لجنة "فون دير لاين" للعمل على عدة مشاريع تتعلق بمكافحة الجريمة السيبرانية في برنامج عملها لعام 2020 والذي يندرج تحت المحور "الرقمي" و محور "طريقة الحياة الأوروبية". من خلال:

- استكشاف عدة طرق الفرص التي يوفرها الذكاء الاصطناعي ، بما في ذلك وضع هذه التكنولوجيا في خدمة أمن الاتحاد ومكافحة التهديدات الإلكترونية.
- المبادرات التي تهدف إلى جعل التمويل الرقمي أكثر مقاومة للهجمات الإلكترونية ، على سبيل المثال اقتراح بشأن أصول التشفير.
- تطوير استراتيجية لمكافحة الاعتداء الجنسي على القاصرين ، والتي يجب أن تشمل بالضرورة بعدًا رقميًا
- تقييم مدى نجاعة مبادرة تشريعية في مكافحة سرقة الهوية ، وهي ظاهرة إجرامية إلكترونية اتخذت أبعادًا مقلقة في السنوات الأخيرة .
- تطوير استراتيجية أمنية جديدة للاتحاد الأوروبي، بتجهيز الدول بالأدوات اللازمة لمكافحة الجريمة السيبرانية بشكل أفضل. باعتماد مجموعة أدوات الجيل الخامس(5G) التي تهدف إلى ضمان أمن الشبكات من خلال تعزيز المتطلبات الأمنية، وتقييم ملفات تعريف المخاطر للموردين ، وتطبيق قيود مفيدة على الموردين الذين يعتبرون عاليي المخاطر وتنفيذ استراتيجيات تنويع الموردين.

تم التخطيط لتقرير عن متابعة تنفيذ "صندوق الأدوات" هذا في صيف عام 2020. وفيما يتعلق بالأمن السيبراني المناسب[17] .

جعلت المفوضية الأوروبية الدفاع عن السيادة التكنولوجية للاتحاد الأوروبي من المجالات الرئيسية في برنامج عملها. تهدف الإستراتيجية الرقمية التي قدمتها في 19 فبراير 2020 إلى نشر إستراتيجية أوروبية للأمن السيبراني، مع إنشاء وحدة مشتركة للأمن السيبراني ، ومراجعة التوجيهات ودفع السوق الموحدة للأمن السيبراني من أجل إحراز تقدم في التفاوض بشأن اقتراح تنظيم إنشاء المركز الأوروبي للكفاءة الصناعية والتكنولوجية والبحثية في مجال الأمن السيبراني وشبكة مراكز التنسيق الوطنية.

تهدف المفوضية إلى المساهمة في هيكلة قطاع الأمن السيبراني الأوروبي إلى إنشاء مثل هذا المركز الأوروبي لمدة سبع سنوات وتكليفه بتخصيص الإعانات ومنح عقود البحث والتطوير، نشر التقنيات الأوروبية

ودعم الصناعة وخلق أوجه تآزر مع قطاع الدفاع السيبراني ، حيث سيأخذ المركز الأوروبي شكل شراكة تضم الاتحاد الأوروبي. وستستند إلى شبكة من مراكز التنسيق الوطنية المسؤولة عن تحديد ودعم المشاريع الأكثر صلة في الدول الأعضاء وتشجيع المشاركة في المشاريع العابرة للحدود[18].

سيتم إنشاء مجتمع من المهارات يجمع مختبرات البحث والصناعيين لتعزيز نشر الخبرات والقدرات وتحسين التعاون والتآزر. بعد انقطاع المفاوضات في آذار / مارس 2019 ، عقب رفض التفويض الثلاثي ، استؤنفت المناقشات ، لكن لا تزال هناك أسئلة كثيرة حول الطبيعة القانونية للمركز وحوكمته وقدرته على تنفيذ برامج المفوضية[19].

تم إنشاء الوكالة الوطنية لأمن أنظمة المعلومات (ANSSI) في عام 2009، وهي ملحقة بالأمانة العامة للدفاع والأمن القومي. هي السلطة المختصة بأمن نظم المعلومات. مع ما يقرب من 600 وكيل وميزانية تقارب 100 مليون يورو ، فهي تساهم بشكل أساسي في:

– تصميم وتنسيق السياسة المشتركة لأمن الكمبيوتر. الذي يلعب دورًا مهمًا في منع هجمات الكمبيوتر من خلال مساعدة الوزارات والمصنعين والمشغلين ذوي الأهمية الحيوية لبناء شبكات كمبيوتر صلبة.

– تقوم بإجراء عمليات التدقيق وتحديد المعايير الفنية والترويج لعرض وطني فيما يتعلق بمنتجات وخدمات أمن تكنولوجيا المعلومات من خلال اعتماد مقدمي الخدمات الخاصين.

– تقوم بمهمات تدريبية للموظفين المؤهلين في مجال أمن أنظمة الكمبيوتر ، في المقام الأول لإدارات الدولة والمشغلين ذوي الأهمية الحيوية.

– يلعب دور الكشف والتنبيه عند حدوث هجوم إلكتروني. ضمنه ، يعمل المركز التشغيلي لأمن أنظمة المعلومات (COSSI) على تحليل التهديد ، وتحديد نقاط الضعف في الأنظمة والأدوات الحالية ، والبحث في الهجمات الجارية وتحديد الردود عليها[20].

– القيام بمهمة الإصلاح من خلال التدخل في الكيانات العامة أو الخاصة الكبيرة التي تقع ضحية للهجوم من أجل مساعدتهم على تطبيق تدابير تصحيحية عاجلة واستعادة أنظمة تكنولوجيا المعلومات الخاصة بهم . وبالنتيجة فهي ليست خدمة تحقيق [21].، ولكن يمكنها التبادل مع السلطات القضائية عندما يتم ضبط نظام العدالة لهجوم إلكتروني عملت فيه الوكالة. كما أنها ليست خدمة استخبارات ولا تنفذ هجمات على الكمبيوتر أو هجمات مضادة. وقد مكنها هذا الموقع من خلق مناخ من الثقة مع جميع الأطراف، مما أدى إلى ممارسة مهمتها الأمنية في مجال تكنولوجيا المعلومات. يبدو أن الوكالة لديها الوسائل المناسبة لتنفيذ مهامها[22].

ثانيا/–الإطار القانوني للتعاون الدولي في مجال الأدلة الالكترونية:

أ/– على الصعيد الدولي: يستمد الالتزام بالتعاون الأمني والقضائي من عدة نصوص قانونية منها:

1– اتفاقية الأمم المتحدة في مكافحة الجريمة المنظمة العابرة للحدود: تطبيقا للمادة 21 منها[23].

2– اتفاقية بودابست لمكافحة الإجرام الالكتروني: تطبيقا للمواد 2 و 1/25 منها[24].

3– اتفاقية الأمم المتحدة لسنة 2000 المتعلقة بالتعاون الدولي في مجال التدريب: المادة 29 منها[25].

إن أحد العوامل الرئيسية لتفاقم الجريمة التي يسهل الإنترنت ارتكابها في أفريقيا يتمثل في افتقار العديد من البلدان إلى سياسات واستراتيجيات شاملة لمكافحة الجريمة السيبرانية. رغم أن الاتحاد الأفريقي قد اعتمد في عام 2014 اتفاقية بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، التي لم توقع عليها سوى 07 دول من أصل البلدان الـ 55 الأعضاء في الاتحاد الأفريقي. مما يبيّن أن العديد من البلدان الإفريقية تعتبر الأمن السيبرالي مسألة غير ضرورية.

ب/- **على الصعيد الأوروبي:** تتولى المفوضية الأوروبية إصدار تقارير المراقبة والتقييم من أجل تقييم مدى تنفيذ هذه اللوائح في الدول الأعضاء. تتضمن هذه اللوائح الأوروبية حاليًا عدة نصوص أهمها:

1 – التوجيه EU 93/2011 / بتاريخ 13 ديسمبر 2011 بشأن مكافحة الاعتداء الجنسي والاستغلال الجنسي للأطفال ، وكذلك استغلال الأطفال في المواد الإباحية واستبدال القرار الإطاري JHA: 68/2004 / هذا النص يجعل معاقبة هذه الجرائم أكثر فعالية من خلال استغلال الأدلة الرقمية،

2- التوجيه EU 40/2013 / بتاريخ 12 أوت 2013 بشأن الهجمات على أنظمة المعلومات واستبدال القرار الإطاري JHA: 222/2005 / يهدف هذا النص إلى مكافحة الهجمات الإلكترونية واسعة النطاق من خلال دعوة الدول الأعضاء إلى تعزيز ترسانتها التشريعية فيما يتعلق بالأمن السيبراني و فرض عقوبات جنائية أكثر صرامة .

3 – التوجيه (الاتحاد الأوروبي) 1148/2016 المؤرخ 6 يوليو 2016 بشأن التدابير التي تهدف إلى ضمان مستوى مشترك عالٍ من أمن الشبكات وأنظمة المعلومات في الاتحاد ، والمعروف باسم "توجيه NIS": هذا النص ، وهو جزء من الخطة الرقمية الذي أطلقه الاتحاد الأوروبي في عام 2010 ، ويهدف إلى تعزيز مستوى أمن الشبكات والمعلومات في سياق يشكل فيه التداخل بين الشبكات وأنظمة الكمبيوتر خطرًا جماعيًا على الدول الأعضاء. تم الإبقاء على مراجعته ، التي أُعلن عنها لعام 2020 ، في برنامج العمل المتمم الذي قدمته اللجنة في سياق جائحة كوفيد 19 .

4 – التوجيه (الاتحاد الأوروبي) 713/2019 الصادر في 17 أفريل 2019 بشأن مكافحة الاحتيال وتزوير وسائل الدفع بخلاف النقد واستبدال القرار الإطاري JHA: 413/2001 / يقوم هذا النص بتحديث الإطار القانوني ، ويزيل العقبات أمام التعاون ويعزز الوقاية ومساعدة الضحايا ، لجعل التدابير القمعية ضد الغش وتزوير وسائل الدفع الافتراضية أكثر فعالية.

5- اللائحة (الاتحاد الأوروبي) رقم 2013/526 (اللائحة المتعلقة بالأمن السيبراني) ، والمعروفة باسم قانون الأمن السيبراني، تحدد هذه اللائحة الإجراءات اللازمة لحماية الشبكات وأنظمة المعلومات ، ومستخدمي هذه الأنظمة والأشخاص الآخرين المعرضين لتهديدات إلكترونية[26].

6 – القرار 2019/797 (CFSP) المؤرخ 17 مايو 2019 بشأن التدابير التحفظية ضد الهجمات الإلكترونية التي تهدد الاتحاد أو الدول الأعضاء فيه[27].

الخاتمة:

من خلال ما سبق يمكن التوصل لمجموعة من النتائج والتوصيات:

– تعتمد فعالية التحقيقات الجنائية والمتابعات القضائية في الجرائم السيبرانية بشكل خاص على الحصول على البيانات والاحتفاظ بها كأدلة رقمية، مع تسجيل غياب نظام للاحتفاظ بالبيانات على مستوى الدولي. بما فيها دول الاتحاد الأوروبي. مما يستدعي اعتماد نظام موحد للاحتفاظ بالبيانات لاستغلالها من طرف سلطات تنفيذ القانون والسلطات القضائية، مع مراعاة متطلبات محكمة العدل الأوروبية واحترام الحقوق الخصوصية وحماية البيانات الشخصية وقرينة البراءة.

– تحسين آليات مكافحة الجريمة السيبرانية وضمان الأمن السيبراني، لا يتأتى إلا بتخصيص موارد مالية وبشرية كافية لمواجهة التحديات الجديدة التي يفرضها التقدم التكنولوجي والتهديدات المتطورة، بما في ذلك تعزيز الشراكة مع القطاع الخاص. لما لها من أهمية التدريب على الأمن الرقمي.

– مكافحة الجريمة السيبرانية تتطلب تعاونا دوليا فعالا لتعزيز أمن واستقرار الفضاء الحاسوبي؛ إذ أن تحسين هذا التعاون يتطلب تصديق جميع الدول الأعضاء على اتفاقية بودابست واختتام المفاوضات بشأن البروتوكول الإضافي الثاني لها.

– تنظيم المجتمع الدولي نفسه لمقاضاة مجرمي الإنترنت بشكل أكثر فعالية؛ حيث أن إقليمية القانون الجنائي لا تزال تشكل في كثير من الأحيان عقبة أمام القضاء، ولا سيما عندما تشمل جرائم الفضاء الحاسوبي عدة دول. مما يقتضي توسيع نطاق اختصاص لمكتب المدعي العام الأوروبي في مجال اختصاصه، حيث أن مركزية معالجة قضايا الجرائم السيبرانية عبر الحدود في مكتب المدعي العام الأوروبي من شأنها أن تسمح بمزيد من التكامل بين أداء الاتحاد الأوروبي في مواجهة التهديدات المتزايدة.

الهوامش والإحالات:

1- M- CHAWKI ;Essai sur la notion de cybercriminalité, IEHEI , juillet 2006. P 06.

2- Brigitte PEREIRA, La lutte contre la cybercriminalité : de l'abondance de la norme a sa perfectibilité, laboratoire métis, Normandie – France, 2008 , pp 8-10

3 -Selon l'article 32 du code des postes et communications électroniques (CPCE), les communications électroniques correspondent à « toute transmission, émission ou réception de signes, signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil, optique, radioélectricité ou autres systèmes électromagnétiques ».

4 -Décision n° 2019-778 DC du 21 mars 2019.

5- Typhaine BONNET, La crise de la sanction face a la cybercriminalité ; l'exemple de droit dauteur, mémoire maitrise en droit , université de paris-sud, France, 2017, p40

6- Brigitte PEREIRA, op-cite, p 32.

7- Typhaine BONNET , op- cite, p 91

8 - La DCPJ concourt à l'exercice des missions de police judiciaire sur l'ensemble du territoire, ainsi qu'à la prévention et à la répression des formes spécialisées, organisées ou transnationales de la délinquance et de la criminalité.

9 - Voir le rapport d'information n° 93 (2013-2014) « Les douanes face au commerce en ligne : une fraude fiscale importante et ignorée », d'Albéric de Montgolfier et Philippe Dallier au nom de la commission des finances.

10 - La section J1 traite de la criminalité organisée et la section J2 de la criminalité financière.

11 -Lors de l'audition organisée par les rapporteurs le 5 juin 2020, ce poste était vacant, le capitaine de police qui l'occupait ayant quitté ses fonctions sans être immédiatement remplacé..

12- L'Union européenne s'est par ailleurs dotée en 2013 d'une stratégie de cybersécurité (texte JOIN (2013) 1 final du 7 février 2013), actualisée en 2017 (texte JOIN (2017) 450 final du 13 septembre 2017).

13- Le cycle politique est une méthodologie adoptée en 2010 par l'Union européenne : chaque cycle, qui dure quatre ans, prévoit les modalités d'organisation de la coopération opérationnelle dans plusieurs domaines de criminalité.

14- Texte COM (2018) 640 final.

15- Cette proposition de règlement avait fait l'objet d'une communication de Jacques Bigot et André Reichardt devant la commission des affaires européennes, le 21 février 2019.

16- C'est également lors de cette réunion du Conseil que mandat a été donné à la Commission pour négocier avec le Conseil de l'Europe le deuxième protocole additionnel à la convention de Budapest (cf. supra).

17-Texte COM (2018) 225 final.

18- Texte COM (2018) 226 final.

19- Qui permettent des transactions avec des tiers virtuels de confiance.

20-Texte COM (2018) 630 final du 12 septembre 2018.

21- Computer Emergency Response Team.

22- Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité.

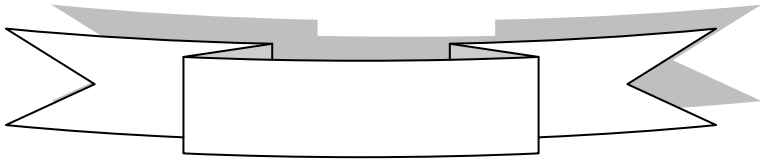
23- Décision 2009/426/JAI du Conseil du 16 décembre 2008 sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité.

24- Règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil.

25- Trafic illicite de stupéfiants, filières d'immigration clandestine, trafic de véhicules volés, traite des êtres humains, faux-monnayage et falsification, trafic de matières radioactives et nucléaires, cybercriminalité, terrorisme et criminalité organisée transnationale.

26- Plus connues sous l'acronyme anglais de CSIRT (Computer Security Incident Response Team).

27- Texte COM (2018) 641 final.



العايب ريمة
laib.rima@gmail.com
جامعة 8 ماي 1945 قالمة

الحماية الجنائية للمستهلك الالكتروني
من الإعلانات المضللة في عقود التجارة الالكترونية

الملخص:

يكفل القانون حرية الإشهار التجاري من حيث المبدأ، إلا أن بعض أنواع الإشهار ممنوعة قانونا، فالإشهار المضلل أو الكاذب عبارة عن تقديم معلومات أو مؤشرات أو طبيعة مغايرة لما هو عليه المنتج حقيقة، بحيث تغالط المستهلك، ويعتبر مثل هذا الفعل مجرم ويُكيف على أنه جنحة، [1]فيكون الإعلان كاذبا منذ اللحظة التي لا تتطابق فيها الرسالة الإعلانية التي يتضمنها مع واقع المنتج [2] المعلن عنه، وهناك من يفرق بين التضليل والكذب، كون الكذب تزييف للحقيقة، والأصل أنه عمل عمدي، بينما التضليل يعتبر خداع للمستهلك دون ذكر معلومات كاذبة، فالإعلان في هذا الفرض صادق، لكنه يُصَاغُ بطريقة تخدع المستهلك،[3]فلا يوجد اختلاف في مفهوم الكذب والتضليل في الإعلانات التي تتم عبر وسائل إلكترونية عن التي تتم بوسائل تقليدية، وهذا ما أكده مجلس المنافسة الفرنسي[4]، ونفس الرأي تبنته اللجنة الفيدرالية الأمريكية للتجارة ، ولهذا حاولنا توضيح وضع حدود فاصلة لجريمة الإشهار المضلل عن ما تلتبس به من جرائم ومصطلحات مثل: الإشهار والإعلام ، جريمة الخداع و جريمة الإشهار المضلل و جريمة النصب والإشهار المضلل، و تسليط الضوء على آليات الحماية الجنائية للمستهلك الالكترونـي من الإعلانات المضللة في عقد البيع الالكتروني أو ما اصطلح عيه قانونا بعقود التجارة الالكترونية.

مقدمة:

يعتبر الإعلان التجاري مظهرا من مظاهر المنافسة المشروعة، وعامل من عوامل التسويق، وأداة من أدوات إعلام الجمهور بالمنتجات [5]، يمكن القول أن الإشهار التجاري تقنية ترمي في جوهرها إلى الرفع من سمعة المؤسسة وتنمية البيوع عبر طرق فنية، مهما كانت وسائل الاتصال المعتمدة لتصل للمستهلك، و تؤثر عليه وتوجه أذواقه، وهذا التأثير خاصة المعنوي، يمكن أن يكون سلبيا إذا كانت الغاية منه مخادعة المستهلك لا غير، بقصد الربح غير المشروع . [6]وقد عُرِّف الإعلان المضلل بأنه الإعلان الذي يكون من شأنه خداع

---

[1]Brigitte Hess Fallon ; Anne-Marie Simon ; droit des affaires ;Collection : Aide-mémoire 12e edition ,1999 ; SIREY Editons , 1999 , Pris , p 207.

[2]- منى أبو بكر الصديق، الالتزام بإعلام المستهلك عن المنتجات، د ذ ط، دار الجامعة الجديدة، الإسكندرية، مصر،2013، ص 148.

[3]-ناصر حمد ناصر البريكي، حماية المستهلك وفقا لقانون حماية المستهلك العماني ، دار النهضة العربية، مصر ، 2016، ص 151.

[4]- روسو عطية موسى نو، الحماية الجنائية من الغش في مجال المعاملات التجارية، دراسة مقارنة، دار المطبوعات الجامعية، الإسكندرية،مصر، 2014، ص 127.

[5]-فتيحة محمد قوراري، "الحماية الجنائية للمستهلك من الإعلانات المضللة"، دراسة في القانون الإماراتي والمقارن، مجلة الحقوق، العدد الثالث سبتمبر 2009، جامعة الكويت، الكويت، 2009، ص 255.

[6]-سمير العكروت، الاشهار التجاري وحماية المستهلك، مجلة القضاء والتشريع، تصدرها وزارة العدل وحقوق الإنسانالتونسية، العدد 8، السنة47، أكتوبر2005، تونس، 2005، ص152.

المستهلك، أو يمكن أن يؤدي إلى ذلك،[1] لكن مساوئ الإعلان تكمن في إمكانية اتسام زاوية الرسالة الإعلانية بعدم الموضوعية أو المبالغة أو عدم الوضوح، وإما من زاوية الآثار المترتبة عنها، من إرباكٍ للشؤون المالية للأفراد نتيجة زيادة النفقات، وخلقَ أنماطٍ استهلاكية سيئة التأثير على اختيار المستهلك بين المنتوجات المطروحة في السوق [2]، بحيث تكمن الخطورة المحدقة بالمستهلك، في كون الإعلان يركز على الجوانب الإيجابية للمنتج، وتظل الأضرار التي تحيط باستخدامه بمنأى عن الإعلان، وتظهر أيضا في الحدود الفاصلة بين المبالغة الإعلانية، والكذب والتضليل المفضيان إلى الخداع الإعلاني، وإذا امتدت هذه المبالغة وأثّرت على التعاقد إضافة إلى البيانات المتعلقة بحقيقة السلع، فهنا أصبحت الإعلانات التجارية مجالا خصبا لمحاولات الكذب والتضليل، وهو ما ألزم المشرع في جلّ الدول، التدخل بتجريم الممارسات المخالفة لقواعد النزاهة المطلوبة في المعاملات التجارية عن طريق تجريم الإعلانات الخادعة[3].

ونظرا للأهمية البالغة التي تكتسيها الإعلانات أو الإشهارات ، تتبلور إشكالية الدراسة فيما يلي:

ماهي آليات الحماية الجنائية للمستهلك الالكتروني من الإعلانات المضللة في عقود التجارة الالكترونية؟

وللإجابة عن هذه الإشكالية اتبعنا المنهج الوصفي والتحليلي ذلك أن طبيعة موضوع الدراسة تستلزم الاستناد إلى تحليل مختلف النصوص القانونية التي تنظم هذه المسألة ، لاكتشاف مدى توفرها على نظام حمائيجنائي للمستهلك من الإعلانات المضللة في عقود التجارة الالكترونية ، مما يجعلنا نجمع بين المنهج الوصــفي لتحديد الظاهرة المدروسة كما هي منظمة قانونيا والتحليلي.

و لكي نتمكن من الإحاطة بموضوع الدراسة تم تقسيم الورقة البحثية إلى قسمين: تشدهما مقدمة وخاتمة

المبحث الاول: ضبط الإطار المفاهيمي لجريمة الإعلانات المضللة.

المبحث الثاني : آليات الحماية الجنائية للمستهلك الالكتروني من الإعلانات التجارية المضللة.

المبحث الأول: ضبط الإطار المفاهيمي لجريمة الإعلانات المضللة.

يجب أن يكون الإشهار قانونيا، ولا يتأتى ذلك إلا إذا كان الإعلان عن مواصفات حقيقية للمنتوج، ولا تكون قائمة على أساس الخداع والغش، بل منطوية على مبررات موضوعية مقنعة، واحترام أساليب الإشهار[4]،

[1]-أيوب يوسف سالم محمد العبيدي، الالتزام بالإعلام في عقود التجارة الالكترونية، مذكرة ماجستير، جامعة المنصورة، مصر، ص 139.بن سالم المختار، المرجع السابق، ص246.

[2]- منى أبو بكر الصديق، مرجع سابق، ص 193، 144، 147.

[3]- روسو عطية موسى نو، الحماية الجنائية من الغش في مجال المعاملات التجارية، دراسة مقارنة، دار المطبوعات الجامعية، الإسكندرية،مصر، 2014، ص 122.

الإشهار[1]، ولهذا سنتناول في هذا المبحث التعريف القانوني للاشهار كمطلب أول، و الفرق بين الاشهار المضلل و الخداع كمطلب ثان، والفرق بين الاشهار والاعلام كمطلب ثالث.

المطلب الاول: التعريف القانوني للإشهار

تمت الإشارة إلى الأساس القانوني للإشهار في التشريع الجزائري في أنظمة قانونية سابقة، بصورة بسيطة من خلال المادة 26من القانون82-01[2]المتعلق بالإعلام المعدل سنة 1990، 2012، ،2015حيث ألغى القانون05/12القانون 07/90 المتعلق بالإعلام ولم يرد فيه مايعرف الإشهار، وقد نص في المادة 26 السالفة الذكر،أنه يقصد بالإشهار، كل إعلام ينشر بواسطة الوسائل المنصوص عليها في المادة 4 أعلاه ويكون ذات طابع أو أهداف تجارية، وحصرت نفس المادة من نفس القانون ممارسة الإشهار من قبل المؤسسات العمومية :تتولى الدولة احتكار الإشهار المنصوص عليه في المادة 26 أعلاه ويمكن إسناد ممارسة هذا الاحتكار لمؤسسة أو مؤسسات عمومية.[3]

عرّفت كذلك المادة 2 فقرة 9 من المرسوم التنفيذي 90-39 [4]المتعلق برقابة الجودة الإشهار [5]بأنه: «جميع الاقتراحات أو الدعايات أو العروض أو الإعلانات أو المنشورات أو التعليمات المعدة لترويج سلعة أو خدمة بواسطة أسناد بصرية أو سمعية بصرية».

- وردت ضوابط الاشهار بموجب المرسوم التنفيذي 91-101 المؤرخ في 20 أفريل 1991[6]يتضمن منح إمتياز عن الأملاك الوطنية والصلاحيات والأعمال المرتبطة بالخدمة العمومية للتلفزيون إلى المؤسسة العمومية للتلفزيون،خاصة المادة 41 منه: «يجب أن يوضع تصور للإشهار في إطار احترام مصالح المستهلكين،ولا يجب أن تضلل البلاغات الإشهارية المستهلكة بصفة مباشرة أو غير مباشرة عن طريق المبالغة أو الحذف أو بحكم طابعها الغامض».
- وتؤكد المادة 38 على ضرورة مطابقة الإشهار لمقتضيات الصدق واللياقة واحتراماالأشخاص.
- المرسوم التنفيذي 91-103[7] المتضمن منح امتياز عن الأملاك الوطنية العقارية والمنقولة للإذاعة المسموعة، المادة 37منه تنص على إلزامية مطابقة الإشهار لمقتضيات الصدق.
- القانون 04-02 [8]الممارسات التجارية المادة 28: «يعتبر إشهارا غير شرعي وممنوع كل إشهار تضليلي تضليلي لاسيما إذا كان:

---

[1]- بركات كريمة، حماية أمن المستهلك في ظل اقتصاد السوق، أطروحة دكتوراه، جامعة مولود معمري، تيزي وزو، الجزائر، 2003 ، ص 115.

[22]-القانون82-01المتعلق بالإعلاممعدل ومتمم،المؤرخ في 6 فيفري 1982المتعلق بالإعلام عدد الجريدة الرسمية5.

[3]-معيزي خالدية، النظام القانوني للإشهار الكاذب أو المضلل،أطروحة دكتوراه علوم، جامعة ابي بكر بلقايد، تلمسان، الجزائر، 2019/2018، ص 31.

[4]- المرسوم التنفيذي 90-39 المتعلق برقابة الجودة الإشهار، المؤرخ في 30 يناير1990، عدد الجريدة الرسمية 5.

[5]-بركات كريمة، مرجع سابق ، ص 113.

[6]- المرسوم التنفيذي 91-101 المؤرخ في 20 أفريل 1991، يتضمن منح امتياز عن الأملاك الوطنية والصلاحيات والأعمال المرتبطة بالخدمة العمومية للتلفزيون إلى المؤسسة العمومية للتلفزيون، عدد الجريدة الرسمية 19.

[7]- المرسوم التنفيذي 91-103 المتضمن منح امتياز عن الأملاك الوطنية العقارية والمنقولة للإذاعة المسموعة، المؤرخ في 20 أفريل1991، جريدة رسمية19.

[8]- القانون 04-02 يحدد القواعد المطبقة على الممارسات التجارية، المؤرخ في 23 يونيو 2004جريدة رسمية عدد 41.

- يتضمن تصريحات أو بيانات أو تشكيلات يمكن أن تؤدي إلى التضليل بتعريف منتوج،أو خدمة أو بكميته أو بوفرته أو مميزاته.
- عناصر يمكن أن تؤدي إلى الالتباس مع بائع آخر،أو مع منتوجاته أو خدماته أو نشاطه.
- يتعلق بعرض معين لسلع أو خدمات، في حين أن العون الاقتصادي لايتوفر على مخزون كاف من تلك السلع،أو لايمكنه ضمان الخدمات التي يجب تقديمها عادة بالمقارنة مع ضخامة الإشهار»

عرّف توجيه المجلس الأوروبي الصادر في 10 سبتمبر 1984 في المادة 2 منه الإعلان التضليلي أوالمضل أوالخادع بأنه: «أي إعلان بأي طريقة كانت يحتوي في طبيعة تقديمه على أي تضليل، وقد يؤدي إلى تضليل لهؤلاء الذين يوجه أويصل إليهم ».[1] وقد عدّل التوجيه الأوروبـي بتوجيه آخر CE /2005/29 مؤرخ في 11/ 05/ 2005، واعتبر الإشهار مهما كان شكله في إطار نشاط تجاري،أو صناعي أو حرفي أو مهنة حرة، يهدف إلى ترويج السلع أو الخدمات بما في ذلك الأموال العقارية، وكذا الحقوق والالتزامات[2]،وأضافت المادة 3 من التوجيه السابق على أن الإعلان المضلل يقع عن طريق إغفال إحدى الخصائص الجوهرية للسلعة المعلن عنها.

أورد التعريف عنصري الإعلان وهما: العنصر المادي، المتمثل في أدوات التعبير المستخدمة في الإعلان التي تدرك بالحواس[3]للسعي وراء الربح ومن بين هذه الوسائل، الملصقات، اللوحات الثابتة، المتنقلة، المضيئة، المعارض، اللافتات الموجهة، والعنصرالمعنوي التأثير النفسي على الجمهور ، حيث أشار إلى الهدف من استخدامها، وهو ترويج وتسيير تسويق السلع والخدمات لدى الجمهور، فالإشهار هو الفعل أو التأثير على الجمهور[4] لأغراض تجارية حسب معجم Robert، ووسائل الإشهار الأكثر شيوعا في الجزائر الراديو، التلفزيون[5]، مواقع التواصل الاجتماعي.

المطلب الثاني: الفرق بين جريمة الخداع والإعلان المضلل

بالوقوف عند المعنى الحرفي لنص المادة 69 من قانون حماية المستهلك وقمع الغش الجزائري في فقرتها الأخيرة، يتبادر إلى أذهاننا بأن جنحة الإعلان الخادع هي وليدة الخداع المشدد، إذن لا يوجد داعي لتنظيم جنحة الإعلان الخداع في قانون خاص به، وإذا كان الفيصل بين جريمة الخداع وباقي الجرائم هو وجود عقد في جنحة الخداع، وغيابه في الجرائم الأخرى[6]، فهذا يستحق أن تنظم كل جريمة على حدى، فلا يكفي الإشارة الإشارة إلى جنحة الإعلان أو الإشهار التضليلي كظرف مشدد للخداع، فالإعلان الخادع أو المضلل سلوك مُجرّم حتى ولو لم يدفع متلقيه إلى التعاقد، هذا من جهة ، ومن جهة أخرى ما دام أهم ما يميز جريمة الخداع

[1]- روسو عطية موسى، مرجع سابق، ص 125.
[2]-حمزة قتال، المرجع السابق، ص 62.
[3]- محمد بودالي، حماية المستهلك في القانون المقارن، دراسة مقارنة مع القانون الفرنسي، دون ذكر طبعة، الكتاب الحديث، الجزائر، 2006، ص 188.
[4]-سمية الكيلاني، الاشهار التجاري وحماية المستهلك، مذكرة ماجستير في القانون الخاص، جامعةسوسة، تونس ،2015/2014ص 5.
-هدى الطالب علي، "حماية المستهلك من خلال أثر الأحكام الخاصة بالاستهلاك على الأحكام العامة لعقد البيع"، مجلة القانون والسياسة المجلة التونسية للدراسات القانونية والسياسية، مجلة كلية الحقوق والعلوم السياسية بسوسة، العدد02، سنة2014، ص 187.
[5]- بركات كريمة، مرجع سابق، ص 113.
[6]- نتكلم في هذه النقطة عن قانون العقوبات لأنه صرح بمصطلح المتعاقد المشمول بالحماية في جريمة الخداع.

عن باقي الجرائم وأولها الغش هو العقد، فإن لهذه الذاتية ما يكفي من أهمية حتى تنظم كل جريمة على حدى[1]، ويلتقي الخداع والإشهار في توجههما إلى المتعاقد أو إلى المستهلك.

يتحدد نطاق السلوك الخادع من حيث الأشخاص،أو من حيث محل الجريمة[2] أوموضوع الخداع ،وأخيرا من حيث الإطار العقدي.

الفرع الأول: من حيث الأشخاص:

لقد استعمل المشرع الجزائري مصطلح «كل من» يعاقب كل من يخدع أويحاول أن يخدع، وسعت من دائرة الأشخاص الذين يمكن أن يحملوا صفة الجاني سواء متدخل أوغير متدخل[3].

يكون السلوك خادعا متى كان صادرا من المتدخل، وانصب على عنصر من عناصر المنتج المذكورة في النص[4]، وكان من شأنه خلق انطباع غير حقيقي للمستهلك ،إذن اتجاه الحماية منصب على المستهلك، وقد عرف ق ح م المصري 2018/181السلوك الخادع في المادة 1 فقرة 10السلوك الخادع ب: «كل فعل أو امتناع عن فعل من جانب **المنتج أو المعلن** يؤدي خلق انطباع غير حقيقي أو مضلل لدى المستهلك يؤدي إلى وقوعه في خلط أو غلط »،إلا أن قانون حماية المستهلك الجزائري أحالنا إلى أحكام قانون العقوبات، وبالتالي تشمل دائرة الحماية كل شخص سواء كان مستهلك حسب قانون حماية المستهلك وقمع الغش، ويمكن أن يقع المتدخل أيضا ضحية الخداع[5] حسب قانون العقوبات،وتأثير السلوك الخادع سواء كان ايجابي أوسلبي أوسلبي على ذهن "المستهلك" –الطرف المحمي في عقود الاستهلاك– فيدفعه إلى الاعتقاد بأمور تناقض الفطرة السليمة بشأن المنتج وعناصره[6].

الفرع الثاني: من حيث محل الجريمة[7]أوموضوع الخداع:

يجب أن ينصب الخداع على السلع[8]les biens وهو يدل على البضائع والمنتجات، ولقيام المسؤولية عن عن جريمة الخداع يجب أن تكون الوسائل المستعلمة فيه واقعة على خصائص المنتوج التي ع ددتها المادة 429 عقوبات جزائري ، والمادة 9قانون حماية المستهلك المصري، والمادة 1 قانون عقوبات تكميلي مصري الخاص بقمع الغش والتدليس لسنة 1994 : «كل من خدعأو شرع في أن يخدع المتعاقد معه في عدد البضاعة» والمادة 63قانون حماية المستهلك المصري 2018/181،أما المشرع الفرنسي لم يقصر محل جنحة الخداع على البضائع فقط، بل يشمل أيضا الخدمات، فيمكن تطبيق جنحة الخداع في مجال الخدمات[9]. الخدمات[9].

---

[1]- مجدوب نوال، مرجع سابق، ص 269.
[2]- علي حساني، مرجع سابق، ص 415.
[3]- مجدوب نوال، مرجع سابق، ص 268.
[4]- الصغير محمد مهدي، مرجع سابق، ص 169.
[5]- فاطمة بحري، المرجع السابق، ص 75.
- محمد بودالي، حماية المستهلك في القانون المقارن، مرجع سابق، ص 309.
-ولد عمر طيب، مرجع سابق، ص 247.
[6]- محمد الصغير مهدي، مرجع سابق، ص 170.
[7]- علي حساني، مرجع سابق، ص 415.
[8]- فاطمة بحري، مرجع سابق، ص 76، محمد بودالي، حمايةالمستهلك في القانون المقارن، مرجع سابق، ص 309.
[9]- حامق ذهبية، مرجع سابق، ص 348.

الفرع الثالث :من حيث الإطار العقدي

إن الأصل ألا تقوم جريمة الخداع ما لم يوجد متعاقد في قانون العقوبات ، إلاأن أمن وسلامة المستهلك يحتم افتراض وجود متعاقد عند عرض منتجات غير مطابقة من حيث مصدرها أوتركيبها أومن حيث صلاحيتها، وهو ما يتوافق مع مبدأ الاحتياط الذي تبناه المشرع الجزائري بموجب الفصل الأول من الباب الرابع من القانون 03/09 المتعلق بحماية المستهلك وقمع الغش المعدل بالقانون 09/18، المعنون بـ «التدابير التحفظية» ، ومبدأ الاحتياط ناجم عن ا عتبار جرائم الاستهلاك من جرائم ا لخطر لا من جرائم الضرر.[1]

نصت المادة 429قانون عقوبات جزائري «يعاقب كل من يخدع أويحاول أن يخدع المتعاقد "ويتبين من النص القانوني سريانه على كل من يشمله العقد ، إذن هذا يعني اشتراط وجود علاقة عقدية بين الضحية «المتعاقد» والجاني[2] سواء كان متعاقدا أومن الغير[3]، إذا سلمنا بذلك فهذا يتنافى مع قصد المشرع الذي يجرم الخداع ولو لم يقع فعلا بل مجرد محاولة[4]، وسواء تم عقد البيع أم لا، فلم يشترط المشرع الجزائري إبرام العقد.

وعليه نستنتج قيام جنحة الخداع بمجرد عرض السلعة فهذا يعتبر ركن مادي، ومهما كانت صيغ عقود الاستهلاك[5]، فالمشرع الجزائري لم يحدد اسم أوطبيعة أونوع العقود التي تتم به جريمة الخداع ، فالغالب المألوف أن يكون عقد بيع ويمكن أن يكون عقد تبرع كالهبة،[6]وبما أن المادة 68 قانون حماية المستهلك وقمع الغش الجزائري 03/09 المعدل بالقانون 09/18 لم تشترط أن يكون الجاني طرفا في العقد على عكس المادة 429 قانون عقوبات وسواء كان العقد باطلا من الناحية المدنية أوك ان العقد صحيحا، فالهدف من تجريم الخداع هو حماية المستهلك في التعامل التجاري والصناعي ، بغض النظر عن صحة العقد أوبطلانه[7]،على عكس قانون العقوبات ، مما يدل على إمكانية متابعة كل من كان مسؤول عن الخداع سواء ارتبط مع الضحية الضعيف بعقد أوبدون عقد، سواء المنتج أوالموضب رغم غياب العلاقة العقدية بينهما[8].

نلاحظ من خلال استقراء أحكام جنحة الخداع الواردة في قانون العقوبات إلزامية توافر الركن المعنوي المتمثل في سوء نية الخادع، الذي يهدف إلى إخفاء الحقيقة باستعمال وسائل معينة،ولا يوجد نص يقضي بذلك في ق ح م ج وهذا باستقراء المادة 68 قانون حماية المستهلك 03/09 المعدل والمتمم بالقانون09/18، وهذا

-ولد عمر طيب، المرجع السابق ، ص 249.

[1]- مجدوب نوال، مرجع سابق، ص 271.

[2]- حساني علي، المرجع السابق، ص 416.

- فاطمة بحري، مرجع سابق، ص 81.

[3]- بركات كريمة، مرجع سابق، ص 250.

[4]-محمد بودالي، حماية المستهلك في القانون المقارن، مرجع سابق، ص 311

[5]-بركات كريمة، نفس المرجع، ص 251

[6]- فاطمة بحري، المرجع السابق، ص 79.

- تنص المادة 2 من قانون 03/09 المتعلقة بحماية المستهلك وقمع الغشعلى أنه: «تطبق أحكام هذا القانون على كل سلعة أوخدمة معروضة للاستهلاك بمقابل أومجانا...».

[7]- ولد عمر طيب، مرجع سابق، ص 248.

[8]- حامق ذهبية، مرجع سابق، ص 347.

ما يدل على أن الجريمة يعاقب عليها متى توافر ركنها المادي [1] وسواء ألحق ضرر بالمستهلك وسواء أيضا تحققت الجريمة فعلا أوكانت مجرد محاولة، إذ يفترض سوء النية والقصد الجنائي.

سنشير هنا إلى النقاط التي يلتقي فيها الخداع والاشهار في توجههما إلى المتعاقد المستهلك.

فكلاهما جريمة تستهدف تضليل المتعاقد، عكس جريمة الغش التي تقع على السلع.

يهدف المشرع إلى حماية كيفيات التعامل والثقة في جريمة الخداع، فلم يتطلب وسائل معينة، عكس جريمة النصب فالخداع يقع بطرق مختلفة، ومتعددة ومنها الكذب أي باستعمال الإعلانات الكاذبة.إلا أن القضاء نفى ذلك فالإعلان الكاذب لا يعد جريمة خداع، فالإعلان سابق للعقد، وجريمة الخداع أو الشروع فيه يلزم أن يكون هناك عقد أو الشروع في التعاقد [2]، مما جعلنا نستنتج أن جريمة الخداع لا توفر الحماية من الإعلان الكاذب،خاصة في حالة تحقق جريمة الإعلان الخادع ولم يتبعها عقد.

المطلب الثالث: تمييز الإشهار عن الالتزام بالإعلام:

نص المشرع الجزائري على الالتزام بالإعلام في المادة 17 من قانون 09-03 المتعلق بحماية المستهلك وقمع الغش المعدل والمتمم بالقانون09/18: «يجب على كل متدخل أن يعلم المستهلك بكل المعلومات المتعلقة بالمنتوج الذي يضعه للاستهلاك بواسطة الوسم ووضع العلامات أو أية وسيلة أخرى مناسبة».

إذن يمكن اعتبار الإشهار وسيلة لإعلام المستهلك، كونه أداة المؤسسات لإثبات وجودها وتدعيم قوتها على المنافسة، ومصدرا للإعلام بالمنتجات والخدمات في علاقة المؤسسات مع المستهلكين، ويساهم في تدعيم الهدف من الوسم هو: إعلام المستهلك بالخصائص الجوهرية للسلعة، وطريقة استعمالها، وصولا إلى تاريخ إنتاجها وانتهاء صلاحياتها، من خلال بيانات تُميِّز السلعة عن غيرها من السلع المطروحة في السوق، فإذا تعدت هذه البيانات وصف السلعة، إلى إبراز محاسنها والترغيب بشرائها يصبح الغلاف وسيلة إعلانية[3].

<u>المبحث الثاني : آليات حماية المستهلك الالكتروني من الإعلانات الكاذبة أو</u> تجريم الإعلانات المضللة في القانون الجزائري

لا ننكر ما للإعلان من إيجابيات بتعريف المستهلك إلى كل ما هو جديد في عالم السلع والخدمات، فضلا عن دوره في شرح خصائص المبيع ومميزاته، ولكي يحقق إعلانا ما غايته، يجب بالضرورة أن يبين الجانب الإيجابي للسلعة محل الإعلان، وهو ما يعرف بالغش المباح، كل هذا من قبيل حث المستهلك على اقتناء السلعة أو الخدمة التي يروج لها، لكن هذا الغش البسيط الذي يتضمنه كل إعلان يمكن أن يؤدي إلى غش حقيقي، إذ أن الإعلان فن وصناعة الإغراء[4].

سندرس بالتفصيل تجريم الإعلانات الخادعة أوالمضللة في القانون الجزائري فيما يلي.

1_حسب قواعد قانون العقوبات:

[1]-المرجع نفسه، ص 350.

[2]- محمد بودالي ،حماية المستهلك في القانون المقارن ، ص196 .

[3]- روسو عطية موسى نو، مرجع سابق، ص 126.

[4]- المرجع نفسه، ص 123.

_الاعتماد على أحكام جريمة النصب.

_الاعتماد على أحكام جريمة الخداع.

2_حسب قواعد قانون حماية المستهلك: التي لم تعالج جريمة الإعلان الخادع بصورة مستقلة عن جريمة الخداع، وهذا ماورد في الفقرة الأخيرة من المادة 69 ق ح م ج حيث اعتبرا الخداع الذي يتم عن طريق الإعلان المضلل ظرف من ظروف التشديد.

3_الاعتماد على قانون التجارة الالكترونية الجزائري 05/18[1].

المطلب الأول: الاعتماد على قانون التجارة الالكترونية الجزائري

تنص المادة 30 من القانون **05/18:**«دون المساس بالأحكام التشريعية والتنظيمية المعمول بها في هذا المجال كل إشهار أو ترويج أو رسالة ذات طبيعة أو هدف تجاري تتم عن طريق الاتصالات الإلكترونية يجب أن يلبي المقتضيات الآتية:

- أن تكون محددة بوضوح كرسالة تجارية أو إشهارية،
- أن تسمح بتحديد الشخص الذي تم تصميم الرسالة لحسابه،
- ألا تمس بالآداب العامة والنظام العام،
- أن تحدد بوضوح ما إذا كان هذا العرض التجاري يشمل تخفيضا أو مكافئات أو هدايا، في حالة ماإذا كان هذا العرض تجاريا أو تنافسيا أو ترويجيا،
- التأكد من أن جميع الشروط الواجب استيفاؤها للاستفادة من العرض التجاري ليست مضللة ولا غامضة.»

أشارت المادة 40 من قانون التجارة الالكترونية الجزائري إلى عقوبة الإعلان المضلل: «دون المساس بحقوق الضحايا في التعويض، يعاقب بغرامة من 50000دج إلى 500000دج كل من يخالف أحكام المواد 30.... » وتنص المادة 45 من نفس القانون على إمكانية فرض غرامة صلح من الإدارة المكلفة بحماية المستهلك، ومبلغ غرامة الصلح هو الحد الأدنى من الغرامة المنصوص عليها في هذا القانون،وفي حالة قبوله تخفض إلى 10 بالمئة من قبل الإدارة المؤهلة،[2]

في حالة عدم امتثال المخالف لدفع غرامة الصلح بعد آجال الإخطار المنقضية، وبعد انقضاء أجل 45 يوما، يرسل المحضر إلى الجهة القضائية المختصة.[3]

ويضاعف مبلغ الغرامة في حالة العود خلال 12 شهرا من تاريخ العقوبة السابقة.[4]

المطلب الثاني: الحماية الجنائية للمستهلك من الإعلانات الخادعة وفق أحكام جريمة النصب:

[1]-قانون التجارة الالكترونية الجزائري 05/18 المؤرخ في 10 ماي 2018، عدد الجريدة الرسمية28.

[2]-المادة 46 من قانون التجارة الالكترونية 05/18

[3]- المادة 47 من قانون التجارة الالكترونية 05/18.

[4]-المادة 48 من قانون التجارة الالكترونية 05/18.

النصب هو الاستيلاء على مال الغير، ولاعتبار الإشهار نصبا لابد من توافر أركان النصب التي يتطلبها قانون العقوبات، وهي الركن المادي والركن المعنوي[1]، وعلى الرغم من أن جريمة النصب المنصوص عليها في هذا القانون، ليست خاصة بحسب الأصل بحماية المستهلك، إلا أن القضاء يعتبر هذه الجريمة متوافرة في حق المتدخل الذي يستعمل دعاية كاذبة، وكأنه يعتبر هذه الدعاية بمثابة طرق احتيالية.[2]

الفرع الأول: الركن المادي:

يستلزم لقيام الركن المادي للنصب استخدام طرق احتيالية، فلا يكفي الكذب والكتمان فقط، وإنما إضافة إلى تعلق الأمر بعملية وهمية، يجب توافر الوسائل الاحتيالية أو أحد طرق التدليس الجنائي، التي وردت في المادة 372 ق ع ج على سبيل الحصر، لكن أغفل المشرع الجزائري تعريف الطرق الاحتيالية، واكتفى بتحديد نوعها والغرض منها، وذلك باستعمال الجاني لطرق وأساليب ذات مظهر خارجي احتيالي يغطي كذبه ، مثل: الاستعانة بشخص آخر لتأييد الادعاءات الكاذبة، وقد يكون بتوزيعه إعلانا في الصحف يعزز به أقواله، فأكثر حالات النصب التي تتصل بالنشاط المالي بطريق الإعلان أو النشر في الصحف، فالإشهار يولد الثقة بين القارئ والصحيفة أو المحطة الإذاعية أو التلفزيونية، ويجب أن يكون الغرض من الطرق الاحتيالية إحدى البنود الواردة في المادة 372 ق عج«الإيهام بوجود مؤسسة أو مشروع كاذب.

- الإيهام بسلطة كاذبة.
- الإيهام بائتمان خيالي.
- إحداث الأمل أو الخوف بحصول ربح وهمي، أو حادثة أو أية واقعة وهمية أخرى»، وهذه الأغراض وردت على سبيل الحصر، ليتحقق معنى جريمة النصب ولو باتخاذ اسم كاذب أو صفة غير صحيحة حتى ولو لم يستعن بطرق احتيالية أخرى.

الفرع الثاني : الركن المعنوي:

يشترط في جريمة النصب القصد الجنائي العام أي أن الجاني عالم باحتياله، والقصد الجنائي الخاص المتمثل في الغاية من وراء طرق الاحتيالية هي سلب جزء من مال الغير أو كله، لهذا يجب العقاب على الإعلان الكاذب أو الخادع بجريمة النصب متى توافرت الأركان السالفة الذكر.

لقد أيد القضاء الفرنسي ذلك، حيث اعتبر الإعلان يشمل أركان جريمة النصب، بالنسبة للإعلانات التي يزعم فيها المعلنون بقدرتهم على شفاء الناس بالتنجيم وأعمال السحر[3].

تجدر الإشارة إلى أنه وبالرغم من أهمية استعمال نص المادة 372 قانون عقوبات جزائري كسبيل لمكافحة الإعلان الخادع، إلا أن هذا النص يرتكز على العديد من الشروط الدقيقة لتفعيله، فلا يكفي الكذب إذا لم يقترن بأعمال مادية، إضافة إلى الأهداف المنصوص عليها على سبيل الحصر في المادة، ليصبح

[1]- محمد بودالي، مرجع سابق، ص 192-193-194.

[2]-عبد العظيم مرسي وزير، حماية المستهلك في ظل قانون العقوبات الاقتصادي في مصر، تقرير مقدم إلى الحلقة التمهيدية للمؤتمر المنعقدة في مدينة فريبورج بألمانيا الاتحادية، من 20 الى 23 سبتمبر 1982 منشور في مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، السنة 53، مصر، سنة 1983، ص 164.

[3]- محمد بودالي، حماية المستهلك في القانون المقارن، مرجع سابق، ص 195.

بذلك النص قاصرا عن توفير الحماية للمستهلك المتضرر من الإعلانات الكاذبة، ولهذا حاول الفقه الاستناد على أحكام جريمة الخداع.

المطلب الثالث: الاعتماد على أحكام جريمة الخداع:

إن الأساليب الترويجية في الواقع ليست كلها نظيفة، فقد يقع المستهلك ضحية لتجاوزات المتدخلكالخداع والإعلان المضلل[1]بحيث تؤثر عليهم، وتحثهم على التعاقد دون تبصر بالعواقب خاصة بالنسبة للمستهلك الالكتروني،[2]ويُعرّف الخداع في اللغة العربية يعني التغيير في الحال، يقال خدع فلا ن تغير بغير خلقه ، وخديعة: أظهر له خلاف ما يخفيه، أراد به المكروه من حيث لا يعلم.[3]

لم يعرف المشرع الجزائري على غرار المشرع ا لفرنسي جريمة الخداع[4]، ولم يتطلب أن يترتب على هذا الخداع إلحاق ضرر بالمستهلك، فبمجرد إتيان الفعل المادي أو محاولة اتيانه يعتبر جريمة تامة، فهي من جرائم الخطر وليس من جرائم الضرر.[5]

تنص المادة 68 قانون حماية المستهلك وقمع الغش الجزائري رقم 03/09 المعدل بالقانون 09/18 على: «يعاقب بالعقوبات المنصوص عليها في المادة 429 من قانون العقوبات، كل من يخدع أويحاول أن يخدع المستهلك بأية وسيلة أوطريقة كانت حول:

- كمية المنتوجات المسلمة.
- تسليم المنتوجات غير تلك المعينة مسبقا.
- تاريخ أومدة صلاحية المنتوج.
- طرق الاستعمال أو الاحتياطات اللازمة لاستعمال المنتوج».

يعاقب المشرع الجزائري حسب المادة 429 ق ع ج [6]على جريمة الخداع [7]بالحبس من شهرين إلى 3 سنوات، وبغرامة من 2000 دج إلى20.000دج أوبإحدى هاتين العقوبتين، ويعاقب على الشروع في هذه الجريمة، بذات العقوبة المقررة للجريمة في صورتها التامة ، أيأن العقوبة المنصوص عليهافي قانون حماية

---

[1]-عابد فضلية، "حماية المستهلك في الجمهورية العربية السورية"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مجلة علمية محكمة دورية، المجلد 17-العدد الأول -2001،ص 125.

[2]-هيثم حامد المصاورة، احمد عبد الرحمان المجالي، المرجع السابق، ص 27.

[3] -https://www.almaany.com/ar/dict

-الصغير محمد مهدي، مرجع سابق، ص 165.

[4]- مجدوب نوال «حماية المستهلك جنائيا من عملية تسويق المواد الغذائية»، مجلة جامعة قاصدي مرباح، ورقلة، دفاتر السياسة والقانون، عدد 15،سنة 2016، ص 276.

[5]-علي فتاك، المرجعالسابق، ص446.

[6]-«يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 2.000 إلى 20.000 دج أوبإحدى هاتين العقوبتين فقط كل من يخدع أو يحاول أن يخدع**المتعاقد**:

- سواء في الطبيعة أو في الصفات الجوهرية أو في التركيب، أو في نسبة المقومات اللازمة لكل هذه السلع،
- سواء في نوعها أو مصدرها،
- سواء في كمية الأشياء المسلمة أو في هويتها،

في جميع الحالات فإن على مرتكب المخالفة إعادة الأرباح التي حصل عليها بدون حق».

[7]- حامق ذهبية، مرجع سابق، ص 346.

المستهلك وقمع الغش 03/09 المادة 68 منه ،تحيلنا فيما يخص نفس الجريمة إلى المادة 429 قانون عقوبات.

وتشدد المادة 430 قانون عقوبات في العقوبة فترفع مدة الحبس إلى 5 سنوات، والغرامة إلى 500.000 دج إذا ارتكبت الجريمة أوشرع فيها بالوسائل الآتية:

- سواء بواسطة الوزن أوالكيل أوبأدوات أخرى خاطئة أوغير مطابقة.
- سواء بواسطة طرق احتياليةأووسائل ترمي إلى تغليط عمليات التحليل ،أوالمقدار أوالوزن أوالكيل ،أوالتغيير عن طريق الغش في تركيب أووزن أوحجم السلع، أوالمنتجات، ولو قبل البدء في هذه العمليات.
- سواء بواسطة بيانات كاذبة ترمي إلى الاعتقاد بوجود عمليات سابقة وصحيحة ،أوإلى مراقبة رسمية لم توجد[1].

بينما شدد القانون 03/09 المتعلق بحماية المستهلك وقمع الغش المعدل بالقانون 18 /09 من عقوبة هذه الجريمة بمقتضى المادة 69التي تنص: «ترفع العقوبات إلى خمس سنوات حبسا وغرامة قدرها خمسمائة ألف دينار 500.000 دج إذا كان الخداع أومحاولة الخداع قد ارتكبت بواسطة:

- الوزن أوالكيل بأدوات اخرى مزورة أوغير مطابقة.
- طرق ترمي إلى التغليط في عمليات التحليل أوالمقدار أو الوزن أوالكيل أوالتغيير عن طريق الغش في تركيب أووزن أوحجم المنتوج.
- إشارات أوادعاءات تدليسية.
- كتيبات أومنشورات أونشرات أوإعلانات أوبطاقات أوأي تعليمات أخرى»[2].

نستنتج أنه لتتحقق جريمة الخداع لا بد من توافر الركنينالمادي والمعنوي.

الفرع الأول: الركن المادي:

يتحقق بتوفر إحدى الوسائل [3]التي عددتها المادة 68 قانون حماية المستهلك وقمع الغش الجزائري 03/09 المعدل والمتمم بالقانون 09/18 المذكورة سابقا والمادة 429 قانون عقوبات جزائري.

يستوجب لقيام هذه الجريمة أن تقع وسائل الخداع على إحدى خصائص المنتوج والتي عددتها المادة 429 قانون عقوبات جزائري، ويكاد يغطي هذا التعداد جميع فرضيات الخداع المعروفة علميا وهي:

- الخداع في طبيعة السلعة [4]: هو إعطاء صورة مغايرة عن خصائص المنتوج،بحيث يتحول الى شيء ذي طبيعة أخرى[5]، كبيع شمعدان من نحاس فإذا به من حديد مطلي بالنحاس[6].

---

[1]- بن داود ابرهيم، قانون حماية المستهلك وفق أحكام القانون 03/09، دون ذكر طبعة، دار الكتاب الحديث، د ذ الس، الجزائر، ص 29.

[2]- فاطمة بحري، مرجع سابق، ص 259.
- بركات كريمة، مرجع سابق، ص 246.
- حساني علي، مرجع سابق، ص 416.

[3]-شعباني نوال، مرجع سابق، ص 268.

[4]-عمرو درويش سيد العربي، المرجع السابق، ص 220.

[5]-حساني علي، المرجعالسابق، ص417.

[6]-بودالي محمد، شرح جرائم الغش في بيع السلع والتدليس في المواد الغذائية والطبية دراسة مقارنة،د ذ ط، دار الفجر للنشر والتوزيع،القاهرة، مصر،ص18.

- الخداع في الصفات الجوهرية : وهي الصفات التي تم التعاقد من أجلها ثم اتضح انعدامها، ومن أجل تقدير الخداع فيها يتم الاستناد الى المراسيم التي تحدد خصائص العديد من المنتجات، والتي من شأنها أن تسهل مهمة المحاكم، وتجنب أيضا وقوع المستهلك في الخداع ، غير أن القضاء الفرنسي يذهب إلى القول بقيام جريمة الخداع حتى في حالة غياب أو انعدام النص اللائحي للمنتوج[1]على أساس أن المنتجات تحكم استنادا الى العادات التجارية المشروعة و الثابتة، وانتقد هذا التوجه على أساس أن المنتج موجه للمستهلك، وبالتالي فإن معيار الرغبة المشروعة للمستهلك المتوسط هي الواجبة التطبيق، وقد نصت المادة 429 قانون عقوبات جزائري على مصطلح الصفات الجوهرية،إلا أننا لم نجد هذا المصطلح في المادة 68 قانون حماية المستهلك وقمع الغش، وإنما نص على تاريخ ومدد صلاحية المنتوج، وطرق استعمال المنتوج وقابليته لذلك[2].
- الخداع في التركيب أو في نسبة المقومات اللازمة للمنتوج: كإعطاء بيانات غير صحيحة تتعلق بتركيب منتوج، وتتحددهذه العناصر إما بالتركيب الذي تحدده اللوائح للخاصة بالمنتوج إن وجدت،وإما وفقا للعادات التجارية، وإما بالرجوع الى بيانات العقد،وإما بالرجوع إلى عناصر متفرقة كالفاتورات،أو الاشهار والذي يتضمن أحيانا المقومات اللازمة للمنتوج.[3]
- الخداع في الكمية: سواء في الوزن أو الكيل أو العدد، [4] ومهما كانت وسيلة الخداع المستعملة في تعديل هذه العناصر، كوجود اختلاف بين الوزن الحقيقي للمنتوج والوزن المبين على الغلاف، وفي هذه الحالة يمكن تصور وقوع الخداع، إما بفعل من يقوم بتسليم السلعة، وبكل وسيلة ترمي خداعا منه إلى رفع الوزن أوالكيل[5]، ويتحقق الشروع في الجريمة بمجرد قيام البائع بعرض سلعة تحتوي على بي انات للوزن أوالكيل غير صحيحة،[6]أي عبارة عن تأكيد لمعلومات خاطئة.
- الخداع في هوية الأشياء: أي تسليم منتجات غير تلك المعينة والمتفق عليها، فيجب أن يقوم المتدخل بتسليم مبيع مطابق لما تم الاتفاق عليه، كمثال عن نوع السلعة بيع زيت ذرة عباد الشمس على أنه زيت زيتون أما عن مصدر السلعة مثال بيع حصان انجليزي على أنه حصان عربي أصيل، وغالبا ما تقترن هذه الأعمال باستعمال بيانات تجارية كاذبة أوعلامات تجارية غير صحيحة، [7] غير أن المشرع الفرنسي أضاف فقرة أخرى بموجب قانون 10 جانفي 1978 للمادة 1 من قانون 1905، المقابلة للمادة 429 قانون عقوبات جزائري هي : الخداع في صلاحية الاستعمال، وفي المخاطر اللازمة لاستعمال منتوج، والمراقبة المنجزة، وطريقة الاستعمالوالاحتياطات الواجبة الاتخاذ، والتي أشار إليها المشرع الجزائري.

---

[1]. -المرجع نفسه، ص19.
[2]. -حساني علي،المرجع السابق،ص419.
[3]. -بودالي محمد ،شرح جرائم الغش في بيع السلع والتدليس في المواد الغذائية والطبية ،المرجع السابق ،ص 20 .
[4]. حساني علي ،المرجع السابق ،ص 417 .
[5]. - محمد بودالي، حماية المستهلك في القانون المقارن، المرجع السابق، ص 313.
[6]. - المرجع نفسه، ص 315.
[7]. -حساني علي،المرجع السابق، ص 418.

أشار قانون العقوبات إلى الخداع الواقع على النوع والمصدر، بينما لم ينص قانون حماية المستهلك وقمع الغش على ذلك.

نصت المادة 430 ق ع ج على عدة ظروف مشددة لهذه الجريمة تؤدي إلى رفع العقوبة إلى خمس سنوات، وهي استعمال وسائل احتيالية من أجل خداع المستهلك، أو بيانات كاذبة، أو أدوات قياس غير صحيحة، حيث اعتبر المشرع الجزائرياً ن جنحة الخداع قائمة بغض النظر عن الوسائل المستعملة في الخداع،إذ لم يشمل الوسائل بالتنظيم، وأحسن المشرع الجزائري لأن جرائم الاستهلاك في تطور دائم كل يوم [1]، واستعمل مصطلح «بأ ية وسيلة أوطريقة ك انت»، ليدخل بذلك الخداع بطريقته التقليدية أو الالكترونية في نطاق التجريم.

الفرع الثاني: الركن المعنوي

رأى بعض الفقهاء أنه إذا كانت محكمة النقض تتطلب من قضاة الموضوع البحث عن العناصر المكونة لسوء النية، فإنه يجوز أن يستخلصوا سوء نية الجاني من عدم قيامه بمراقبة السلعة المبيعة قبل عرضها للبيع، وأن هذا تسليم ضمني من القضاة بأن جنحة الخداع يجوز ارتكابها بإهمال أو عدم احتياط،وهذا التوجه يتماشى وغرض قانون حماية المستهلك الذي أصبح غرضه أسمى، فانعدام مراقبة السلعة المبيعة أصبح يماثل في خطورته الخداع عن قصد وتعمد، الأمر الذي يؤدي إلى القول بجواز قيام جريمة الخداع بإهمال، على غرار ما تم التسليم في جريمة الإعلان أو الإشهار الخادع [2]، حيث نظمها المشرع الفرنسي بالتفصيل، وهذا ما ستتم الإشارة إليه لاحقا في تمييز جريمة الخداع عن الإعلان الخادع.

اعتبربعض الفقهاء أن هذا التوسع مستوحى من الأفكار الحديثة التي ابتدعها القضاء المدني في مجال العيوب الخفية، بما يذهب إليه من تشبيه المحترف بالبائع سيء النية، وبالتالي فإن المحاكم ترى أن المتدخل يقع عليه التزام بفحص ومراقبة المبيع قبل البيع، إلا أن هذا الإسقاط أُنتقد لأنه يصعب القبول به في المسؤولية الجنائية[3].

إذن لا يعاقب القانون على الخداع الذي يقع بناء على جهل أو غلط يقع فيه البائع أو التاجر إزاء المتعاقد الآخر، لأن الخداع جريمة عمدية يضاف إلى ذلك أن الإهمال لا يعادل الخداع، إلا أنه يلاحظ أن الغلط الذي ينفي القصد الجنائي لدى الجاني هو الغلط في الواقع وليس في القانون، فالقانون ينص صراحة على التزام المتدخل بفحص ومراقبة السلعة قبل بيعها وبالتالي فمخالفة ذلك يقيم المسؤولية [4]، لأن الغلط يستبعد التدليس الجنائي[5].

---

[1]- مجدوب نوال، مرجع سابق، ص 268.
[2]- بودالي محمد، شرح جرائمالغش في بيع السلع والتدليس في مواد الغذائية، المرجع السابق، ص 22.
[3]- المرجع نفسه، ص 25.
[4]- نفس المرجع، ص 26.
[5]- بركات كريمة، المرجع السابق، ص 253.

من المتصور في جريمة الخداع حدوث إهمال من التاجر أو المنتج على حسب الأحوال في تنفيذ التزامه بالرقابة أو فحص المنتجات، مع إمكانية توافر العلم لديه بطبيعة أو أوصاف البضاعة التي يفحصها، والإهمال غير عمدي والخداع جريمة عمدية[1].

إذن الخداع جريمة متعمدة ، تنطوي بالضرورة على سوء نية ، يجب لتوافر أركانها تبوث القصد الجنائي لدى المتهم، وهو علمه بالغش الحاصل في البضاعة، وإرادته إدخال هذا الغش على المتعاقد معه، ويتطلب لقيام القصد الجنائي توافر شرطان أساسيان، وهما توجيه إرادة الجاني نحو إتيان الفعل المادي وهو الخداع أو الشروع فيه، والعلم بخداع المتعاقد [2]، ويتطلب القانون الجزائري أو الفرنسي أو المصري ثبوت القصد الجنائي لدى المتهم [3]بعنصريه العلم والإرادة[4]،أو إهمال الجاني؛ يُقيّم القاضي كل حالة على حدى وفقًا للظروف، يمكن استنتاجه من أي عمل أو ادعاء أو عرض تقديمي قد يحجب الواقع، أو حتى السكوت عن بعض العيوب أو خصائص المنتج.

خاتمة:

كحوصلة لما سبق نستنتج أن التشريعات حاولت التطرق إلى إشكاليات الإشهار وضبط مسؤولية أطراف العلاقة، حمايةً للمستهلك الحلقة الأضعف فيها، إلا أنها تعتبر قاصرة وهذا ماجعلها تلجأ إلى تقنين سلوكيات البيع عن بعد، وتكريس آليات وقائية تعمل على توعية أطراف التجارة الالكترونية حول المخاطر المحتملة، وقد أشرنا إلى ذلك من خلال موقف المشرع الجزائري من خلال قانون التجارة الالكترونية 05/18، كون التجارة من أكثر وجوه النشاط البشري إغراءً لما فيها من أرباح، لكنها تعتبر أيضا من أوسع المجالات غشًا وتحايلا عندما يقوم المتدخل بإخفاء العيوب بهدف ترويج السلعة، لذلك انتشر الخداع والتدليس انتشارا واسعا حتى أصبح ظاهرة، بسبب التقدم العلمي والتكنولوجي خاصة في المجال الصناعي الذي جعل اكتشافه أمرا في غاية الصعوبة، ولأنه لا يمكن فصل القانون عن الاقتصاد، نجد لكل تنظيم قانوني أهداف اقتصادية، إذ ترمي الأهداف الاقتصادية للقواعد المنظمة للعقود إلى تخفيض التكاليف، والإفصاح عن المعلومات من خلال أحكام ضمان العيوب الخفية، مما يتيح إمكانية تحديد قيمة المبيع، ناهيك عن تحليل العقود غير المكتملة أو المنقوصة.

ولهذا نلخص آليات حماية المستهلك من الإعلانات المضللة في النقاط التالية:

1حسب قواعد قانون العقوبات:

[1]- عمرو درويش سيد العربي، المرجع السابق، ص 239.

–عساني عبير، معامير سفيان، "آليات حماية المستهلك من مخاطر انتشار ظاهرة الخداع والغش التسويقي (حالة الجزائر)"، مجلة معارف، جامعة البويرة، قسم علوم اقتصادية، العدد 19، ديسمبر 2015، ص 19.

[2]- عمرو درويش سيد العربي، المرجع السابق، ص 233-234.

[3]-بودالي محمد، شرح جرائم الغش في بيع السلع والتدليس في المواد الغذائية والطبية، المرجعالسابق، ص21.

[4]-بركات كريمة، المرجع السابق، ص252

_الاعتماد على أحكام جريمة النصب.

_الاعتماد على أحكام جريمة الخداع.

2_حسب قواعد قانون حماية المستهلك: التي لم تعالج جريمة الإعلان الخادع بصورة مستقلة عن جريمة الخداع، وهذا ماورد في الفقرة الأخيرة من المادة 69 ق ح م ج حيث اعتبرا الخداع الذي يتم عن طريق الإعلان المضلل ظرف من ظروف التشديد.

3_الاعتماد على قانون التجارة الالكترونية الجزائري 05/18[1] .

قائمة المراجع:

أولا: النصوص القانونية:

القوانين العادية:

- القانون82-01المتعلق بالإعلام معدل ومتمم،المؤرخ في 6 فيفري 1982المتعلق بالإعلام عدد الجريدة الرسمية5.
- القانون 04-02 يحدد القواعد المطبقة على الممارسات التجارية، المؤرخ في 23 يونيو 2004جريدة رسمية عدد 41 معدل ومتمم.
- القانون رقم 09-03، المؤرخ في 25فيفري 2009، المتعلق بحماية المستهلك وقمع الغش الجزائري ، الجريدة الرسمية عدد 15.
- القانون رقم 09/18، المؤرخ في 10يونيو2018، المعدل والمتمم للقانون 03/09، المتعلق بحماية المستهلك وقمع الغش، الجريدة الرسمية عدد 35.
- القانون المتعلق بالتجارة الإلكترونية الجزائري رقم 05/18، المؤرخ في 10ماي 2018، عدد الجريدة الرسمية 28.

المراسيم التنفيذية:

- المرسوم التنفيذي 90-39 المتعلق برقابة الجودة الإشهار، المؤرخ في 30 يناير 1990، عدد الجريدة الرسمية 5

_ المرسوم التنفيذي 91-101 المؤرخ في 20 أفريل 1991، يتضمن منح امتياز عن الأملاك الوطنية والصلاحيات والأعمال المرتبطة بالخدمة العمومية للتلفزيون إلى المؤسسة العمومية للتلفزيون، عدد الجريدة الرسمية 19.

- المرسوم التنفيذي 91-103 المتضمن منح امتياز عن الأملاك الوطنية العقارية والمنقولة للإذاعة المسموعة، المؤرخ في 20 أفريل1991، جريدة رسمية19.

[1]-قانون التجارة الالكترونية الجزائري 05/18 المؤرخ في 10 ماي 2018، عدد الجريدة الرسمية28.

ثانيا: المؤلفات:

- الصغير محمد مهدي، قانون حماية المستهلك، دراسة تحليلية مقارنة، د ذ ط، دار الجامعة الجديدة، مصر، 2015.

_ أمينة أحمد محمد أحمد، حماية المستهلك في عقود التجارة الالكترونية، دراسة مقارنة، د ذ ط، دار النهضة العربية، القاهرة، مصر، 2016.

- حساني علي، ضمان حماية نحو نظرية عامة في التشريع الجزائري، الطبعة الأولى، دار الفكر الجامعي، مصر، 2016.

_ حمزة قتال، مصادر الالتزام العقد، د ذ ط، دار هومة للطباعة والنشر والتوزيع، الجزائر،2018.

_ بن داود ابرهيم، قانون حماية المستهلك وفق أحكام القانون 03/09، دون ذكر طبعة، دار الكتاب الحديث، د ذ الس، الجزائر.

_ بودالي محمد، شرح جرائم الغش في بيع السلع والتدليس في المواد الغذائية والطبية دراسة مقارنة،د ذ ط، دار الفجر للنشر والتوزيع،القاهرة، مصر

_ حامق ذهبية، الإلتزام بالإعلام في عقود الاستهلاك، رسالة دكتوراه، قانون خاص، جامعة الجزائر، بن يوسف بن خدة، الجزائر، 2005.

_ روسو عطية موسى نو، الحماية الجنائية من الغش في مجال المعاملات التجارية، دراسة مقارنة، دار المطبوعات الجامعية، الإسكندرية،مصر، 2014.

_ علي فتاك، المستهلك وتأثير المنافسة على ضمان علامة المنتج، الطبعة الأولى، دار الفكر الجامعي، مصر، 2014.

_ فاطمة بحري، "التطور التاريخي لجريمة الغش"، مجلة الحضارة الإسلامية، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، الجزائر، العدد 25، 2014.

_ مجدوب نوال «حماية المستهلك جنائيا من عملية تسويق المواد الغذائية»، مجلة جامعة قاصدي مرباح، ورقلة، دفاتر السياسة والقانون، عدد 15، الجزائر، 2016.

_ محمد بودالي، حماية المستهلك في الفانون المقارن، دراسة مقارنة مع الق انون الفرنسي، دون ذكر طبعة، الكتاب الحديث، الجزائر، 2006.

_ منى أبو بكر الصديق، الالتزام بإعلام المستهلك عن المنتجات، د ذ ط، دار الجامعة الجديدة، الإسكندرية، مصر،2013.

_ ناصر حمد ناصر البريكي، حماية المستهلك وفقا لقانون حماية المستهلك العماني رقم66/ 2014 شرحا وتعليقا، د ذ ط، دار النهضة العربية، مصر، 2017.

_ هيثم حامد المصاروة، أحمد عبر الرحمان المجالي، حماية المستهلك في العقود الالكترونية، دراسة تحليلية في الفقه الإسلامي والقانون السعودي، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2015.

ثالثا: المقالات:

– سمير العكروت، الاشهار التجاري وحماية المستهلك، مجلة القضاء والتشريع، تصدرها وزارة العدل وحقوق الإنسان التونسية، العدد8، السنة47، أكتوبر2005، تونس، 2005.

– فتيحة محمد قوراري، "الحماية الجنائية للمستهلك من الإعلانات المضللة "، دراسة في القانون الإماراتي والمقارن، مجلة الحقوق، العدد الثالث سبتمبر 2009، جامعة الكويت، الكويت، 2009.

_ عبد العظيم مرسي وزير، حماية المستهلك في ظل قانون العقوبات الاقتصادي في مصر، تقرير مقدم إلى الحلقة التمهيدية للمؤتمر المنعقدة في مدينة فريبورج بألمانيا الاتحادية، من 20 الى 23 سبتمبر 1982 منشور في مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، السنة 53، مصر، سنة 1983.

_ عابد فضلية، "حماية المستهلك في الجمهورية العربية السورية "، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مجلة علمية محكمة دورية، المجلد 17–العدد الأول –2001.

_ عساني عبير، معامير سفيان، "آليات حماية المستهلك من مخاطر انتشار ظاهرة الخداع والغش التسويقي (حالة الجزائر)"، مجلة معارف، جامعة البويرة، قسم علوم اقتصادية، العدد 19، ديسمبر 2015

_ هدى الطالب علي، "حماية المستهلك من خلال أثر الأحكام الخاصة بالاستهلاك على الأحكام العامة لعقد البيع"، مجلة القانون والسياسة المجلة التونسية للدراسات القانونية والسياسية، مجل ة كلية الحقوق والعلوم السياسية بسوسة، العدد02، سنة2014.

– مجدوب نوال «حماية المستهلك جنائيا من عملية تسويق المواد الغذائية»، مجلة جامعة قاصدي مرباح، ورقلة، دفاتر السياسة والقانون، عدد 15،سنة 2016.

رابعا: الرسائل الجامعية

مذكرات ماجستير

_أيوب يوسف سالم محمد العبيدي، الالتزام بالإعلام في عقود التجارة الالكترونية، مذكرة ماجستير، جامعة المنصورة، مصر.

_ سمية الكيلاني، الاشهار التجاري وحماية المستهلك، مذكرة ماجستير في القانون الخاص، جامعةسوسة، تونس ،2015/2014.

_ شعباني حنين نوال، التزام المتدخل بضمان سلامة المستهلك في ضوء قانون حماية المستهلك وقمع الغش، مذكرة ماجستير، فرع مسؤولية مهنية، جامعة مولود معمري تيزي وزو، الجزائر، 2012.

رسائل دكتوراه

– بن سالم المختار، الالتزام بالإعلام كآلية لحماية المستهلك، رسالة دكتوراه تخصص قانون المنافسة والاستهلاك، جامعة ابي بكر بلقايد، جامعة تلمسان ، الجزائر2018/2017

- بركات كريمة، حماية أمن المستهلك في ظل اقتصاد السوق، دراسة مقارنة، أطروحة دكتوراه، تخصص قانون، جامعة مولود معمري، تيزي وزو، الجزائر، ماي 2014

_ معيزي خالدية، النظام القانوني للإشهار الكاذب أو المضلل،أطروحة دكتوراه علوم، جامعة ابي بكر بلقايد، تلمسان، الجزائر، 2019/2018.

_ عمرو درويش سيد العربي، الحماية الجنائية للمستهلك من الغش، رسالة دكتوراه في الحقوق، جامعة عين شمس، مصر، 2004.

المراجع باللغة الأجنبية:

- Brigitte Hess Fallon ; Anne-Marie Simon ; droit des affaires ;Collection : Aide-mémoire 12e ,1999 ; SIREY Editons , 1999 , Paris edition.

- https://www.almaany.com/ar/dict **المواقع الالكترونية** :

حنان حمدي
d.hanane.hamdi@gmail.com
جامعة العربي بن مهيدي أم البواقي – الجزائر -

عبد العزيز شملال
chemlalapc@yahoo.fr
جامعة العربي بن مهيدي أم البواقي – الجزائر -

الآليات المستحدثة لمكافحة الجرائم الالكترونية الاقتصادية في مرحلة البحث والتحري

ملخص:

لقد حاولنا من خلال هذه الورقة البحثية التطرق الى الاليات المستحدثة لمكافحة الجرائم الالكترونية الاقتصادية مقتصرين على مرحلة البحث والتحري التي تتولاها أجهزة الضبطية القضائية، وهي المرحلة السابقة للإجراءات القضائية التي تتخذ من طرف الجهات القضائية كقضاة النيابة وقضاة التحقيق والحكم.

نظرا لطبيعة الجرائم الالكترونية الاقتصادية فقد خصها المشرع بمجموعة من الاجراءات والاليات التي تساعد على البحث فيها والكشف عن مرتكبيها، فوسع من اختصاصات الضبطية القضائية لتسهيل مهامهم .

الكلمات المفتاحية :الاليات المستحدثة، الجرائم الالكترونية الاقتصادية، مرحلة البحث والتحري

Summary:

We have tried, through this research paper, to address the mechanisms developed to combat economic cybercrime, limited to the stage of research and investigation carried out by the judicial police, which is the previous stage of the judicial procedures that are taken by the judicial authorities, such as prosecutors, investigative judges and judges.

Due to the nature of economic electronic crimes, the legislator has singled out a set of procedures and mechanisms that help in researching them and detecting their perpetrators. He expanded the powers of the judicial police to facilitate their tasks.

Keywords: *new mechanisms, economic cybercrime, research and investigation stage.*

مقدمة:

نظرا للانتشار الكبير للإجرام الالكتروني الذي صاحب التطور الحاصل في مجال تكنولوجيات الاعلام والاتصال وخاصة ارتباطه بالاقتصاد ، سارع المشرع الى استحداث اليات من خلالها يتم تعزيز المنظومة الاجرائية والعقابية وجعلها تواكب هذ التطور الحاصل ، وأول ما تم تعزيزه في المنظومة الاجرائية سلطات الضبطية القضائية في مجال البحث والتحري عن الجرائم، خاصة تعديل قانون الاجراءات الجزائية بموجب القانون 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية، اصدار القانون رقم 01/06 المؤرخ في 20 فبراير 2006 يتعلق بالوقاية من الفساد ومكافحته .

اضافة الى استصدار قانون 04/09 المتضمن القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها .

ومن هذا المنطلق يتعين طرح اشكالية الدراسة كما يلي : ما هي الاليات الاجرائية التي مكنها المشرع للضبطية القضائية لمكافحة الاجرام الالكتروني الاقتصادي؟

للإجابة عن الإشكالية اخترنا اتباع الخطة التالية:

المبحث الاول :الضبطية القضائية المكلفة بالاستدلال فيالجرائم الماسة لنظم المعالجة الالية للمعطيات

المطلب الاول: تنظيم الضبطية القضائية المكلفة بالاستدلال

المطلبالثاني: نطاق اختصاص الضبطية القضائي المكلفة بالاستدلال

المبحث الثاني : اجراءات الاستدلال في الجرائم الماسة بأنظمة المعالجة الالية للمعطيات

المطلب الاول : الترتيبات التقنية على الاتصالات الالكترونية

المطلب الثاني : اجراءات التفتيش والحجز داخل المنظومة المعلوماتية

المبحث الاول :الضبطية القضائية المكلفة بالاستدلال فيالجرائم الماسة لنظم المعالجة الالية للمعطيات

أوكل المشرع الجزائري لفئة من الموظفين أطلق عليهم مصطلح الضبطية القضائية مهمة جمع الاستدلالات حول الجرائم ومرتكبيها وذلك تحت ادارة [1]واشراف[2] النيابة العامة ، وحدد لهم نطاقا يمارسون فيه مهامهم وصلاحياتهم المخولة لهم قانونا .

سنتناول من خلال هذا الم بحث تنظيم الجهات الأمنية المكلفة بالاستدلال التي تتمثل في الضبطية القضائية، ونطاق اختصاص هذه الجهات .

المطلب الاول: تنظيم الضبطية القضائية المكلفة بالاستدلال

نص المشرع الجزائري على تحديد الفئات التي تتمتع بصفة الضبطية القضائية من خلال نص المادة 14 من قانون الاجراءات الجزائية وهم ، ضباط الشرطة القضائية وأعوان الضبط القضائي اضافة الى الموظفين المنوط بهم قانونا بعض مهام الضبط القضائي .

[1] نصت المادة 17 من قانون الاجراءات الجزائية على أنه " عند مباشرة التحقيقات وتنفيذ الانابات القضائية لا يجوز لضباط الشرطة القضائية طلب أو تلقي أوامر أو تعليمات الا من الجهة القضائية التي يتبعونها وذلك مع مراعاة أحكام المادة 28 " .كما نصت المادة 36 من نفس القانون في فقرتها 1 و 2 على أنه : " يقوم وكيل الجمهورية بما يأتي : ادارة نشاط ضباط وأعوان الشرطة القضائية في دائرة اختصاص المحكمة وله جميع السلطات والصلاحيات المرتبطة بصفة ضابط الشرطة القضائية . – مراقبة تدابير التوقيف للنظر . وعليه فهم مساعدون مباشرون لوكيل الجمهورية ينفذون اوامره ، وموافاته بالمحاضر التي يعدونها ، والجرائم التي تصل الى علمهم، وبالتوقيف للنظر ولا يمددونه الا باذن مكتوب منه الى غير ذلك من الاجراءات التي يقومون بها تحت ادارته. للتفصيل أكثر أنظر : محمد حزيط، أصول الإجراءاتالجزائية فيالقانون الجزائري ، دون طبعة ، دار هومه للطباعة والنشر والتوزيع، بوزريعة، الجزائرالعاصمة،، 2018، ص 171.172 .

[2] اذ يعتبرون تابين للنائب العام باعتباره رئيس النيابة العامة على مستوى المجلس القضائي ، ومنه فهم خاضعين لإشرافه فيها يتعلق بأعمال وظائفهم القضائية،، فبموجب المادة 18 مكرر أصبح النائب العام يمسك ملفا فرديا لكل ضابط شرطة قضائية اين يتم تنقيطه، كما يمكنه احالة الضابط على غرفة الاتهام في حال تقصيره في عمله لتحريك الدعوى التأديبية ضده. أنظر محمد حزيط،مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة العاشرة، دار هومه للطباعة والنشر والتوزيع، بوزريعة، الجزائرالعاصمة، 2015، ص120 .

الفرع الاول : ضباط الشرطة القضائية

تم تحديدهم قانونا وفقا لنصوص المواد 15 و15 مكرر و 15 مكرر 1 من قانون الاجراءات الجزائية ، حيث يتكونون من 6 فئات تصنف الى صنفين :

1 -الصنف الاول يكتسبون صفة ضباط الشرطة القضائية بقوة القانون : وهم الفئات الثلاث الاولى وهم

- رؤساء المجالس الشعبية البلدية [3]
- ضباط الدرك الوطني [4]
- والموظفون التابعون للأسلاك الخاصة للمراقبين
- ومحافظي وضباط الشرطة للأمن الوطني[5] .

2 -الصنف الثاني : يكتسبون صفة ضباط الشرطة القضائية بقرار مشترك : وهم

- الذين تم تعيينهم بقرار مشترك بين وزير العدل ووزير الدفاع ويتعلق الامر، بذوي الرتب في الدرك ورجال الدرك الذين أمضوا في سلك الدرك الوطني 3 سنوات على الاقل، والضباط وضباط الصف التابعين للمصالح العسكرية للأمن .
- الذين تم تعيينهم بموجب قرار مشترك بين وزير العدل ووزير الداخلية والجمعات المحلية وهم الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ واعوان الشرطة للأمن الوطني الذين أمض 3 سنوات على الاقل بهذه الصفة .

الفرعالثاني : اعوان الضبط القضائي

تم تصنيف هؤلاء بدورهم الى فئتين هما

1 -الاعوان المعينون بقوة القانون وهم صنفين :

- الصنف الاول تم النص عليهم بالمادة 19 من قانون الاجراءات الجزائية وهم موظفو مصالح الشرطة وذوي الرتب في الدرك الوطني ورجال الدرك الوطني ومستخدمو مصالح الأمن العسكري الذين ليست لهم صفة ضباط الشرطة القضائية [6].

---

[3] يتم تعيين رئيس المجلس الشعبي البلدي (لمدة انتخابية تقدر ب 5 سنوات) من قبل أعضاء القائمة الانتخابية التي نالت أغلبية المقاعد بتعيين عضو منهم رئيسا للمجلس الشعبي البلدي ويتم تنصيبه في مدة أقصاها 8 أيام من تاريخ اعلان نتائج الاقتراع على أن يعلن للعموم ويبلغ للوالي بذلك فورا . ويتمتع رئيس المجلس الشعبي البلدي باختصاص مزدوج فهو تارة يمثل البلدية من خلال تمثيلها ورئاسة المجلس وادارة أموال البلدية والمحافظة على حقوقها ، ويمثل تارة أخرى الدلة من خلال تمتعه بصفة ضابط الحالة المدنية التي يمكنه أن يفوضها لغيره، أو ضابط للشرطة الادارية للحفاظ على النظام العام والصحة العامة والسكينة العامة ، أو تنفيذا للقوانين والتنظيمات ، اضافة الى تمتعه بصفة ضابط الشرطة القضائية وذلك بموجب المواد 92، 93، 94، 95، من القانون رقم 10/11 المؤرخ في 20 رجب عام 1432 الموافق 22 يونيو سنة 2011 ، يتعلق بالبلدية (الجريدة الرسمية عدد 37) .للتفصيل أكثر أنظر محمد الصغير بعلي ، قانون الادارة المحلية الجزائرية، دار العلوم للنشر والتوزيع، دون طبعة، دون سنة نشر، ص 86 – 92 .

[4] مرسوم رئاسي رقم 143/09 المؤرخ في 2 جمادى الأولى عام 1430 الموافق ل 27افريل 2009 يتضمن مهام الدرك الوطني و تنظيمه، (الجريدة عدد 26).

[5] تم اضافة هذا الصنف من قبل المشرع الجزائري من خلال تعديل المادة 15 من قانون الاجراءات الجزائية بموجبالأمر رقم 15 / 02 المؤرخ في 23 جويلية 2015 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية (الجريدة الرسمية عدد 40).

- الصنف الثاني تم النص عليهم بالمادة 26 من قانون اجراءات جزائية وهم ذوي الرتب في شرطة البلدية [7]

2 -الاعوان المعينون بموجب مرسوم تنفيذي ويقصد بهم الحرس البلدي اذ خول لهم المرسوم التنفيذي رقم 265/96 المتضمن انشاء سلك الحرس البلدي [8] بموجب المادة 6 منه صفة أعوان الضبط القضائي [9]، الا أنه بتحويل وصايتهم لوزارة الدفاع بموجب المادة 1 من المرسوم الرئاسي 89/11 لم يبقى للحرس البلدي صفة أعوان الضبط القضائي[10] .

الفرعالثالث :الموظفين المنوط بهم قانونا بعض مهام الضبط القضائي .

ايضا يقسم هؤلاء الى فئتين هما :

1 -الموظفون المنصوص عليهم بموجب المواد 21 و28 من قانون الاجراءات الجزائية وهم

- رؤساء الاقسام المختصون في الغابات وحماية الاراضي،
- المهندسون المختصون في الغابات وحماية الاراضي واستصلاحها،
- الاعوان الفنيون المختصون في الغابات وحماية الاراضي واستصلاحها[11]،
- الولاة سلطته جوازية يمارسها وفق ما تقتضيه ظروف البلاد [12]،

2 -المحددون بموجب نصوص خاصة تم الاشارة اليهم في المادة 17 من قانون اجراءات جزائية [13]وهم:

- أعوان الدرك نصت عليهم المادة 241 من قانون الجمارك
- مفتشي العمل نصت عليهم المادة 4 من قانون المتضمن اختصاصات مفتشي العمل .
- اعوان الصحة النباتية حسب المادة 52 من القانون المتعلق باختصاص أعوان الصحة النباتية
- أعوان شرطة المياه المادة 160 من القانون رقم 12/05 المعلق بشرطة المياه
- أعوان الشرطة العمرانية المواد 76 و 77 من القانون رقم 29/90 المتعلق بالتهيئة والتعمير

المطلبالثاني: نطاق اختصاص الضبطية القضائي المكلفة بالاستدلال

---

[6] تنص المادة 19 من قانون الاجراءات الجزائية " يعد من أعوان الضبط القضائي، موظفو مصالح الشرطة وضباط الصف في الدرك الوطني ومستخدمو المصالح العسكرية للأمن الذين ليست لهم صفة ضباط الشرطة القضائية " وقد تم تعديلها بموجب القانون رقم 10/19 المؤرخ في 14 ربي الثاني عام 1441 الموافق ل 11 ديسمبر 2019 يعدل ويتمم الامر رقم 155/66 السابق الذكر (الجريدة الرسمية رقم 78)

[7] جاءت نص المادة 26 من قانون الاجراءات الجزائية تحت عنوان الموظفين والأعوان المكلفين ببعض مهام الضبط القضائي، رغم أن نص المادة 19 من قانون الاجراءات الجزائية المعدلة بموجب القانون رقم 10/19 لم تتضمن شرطة البلدية وبالتالي لم تضفي عليهم صفة عون للضبط القضائي ، كما أن المراسيم التي تتضمن انشاء شرطة البلدية وتحديد مهامها وكيفيات عملها قد تم الغاؤها وبالتالي تبقى المادة 26 من قانون الاجراءات الجزائية غير دستورية، للتفصل أكثر أنظر عبد الله أوهايبية ، شرح قانون الاجراءات الجزائية ، التحري والتحقيق ، دار هومة ، الطبعة الخامسة ، 2013-2014 ، ص 205-208.

[8] المرسوم التنفيذي رقم 265/96 المؤرخ في 3 غشت سنة *1996* والمتضمن إنشاء سلك الحرس البلدي وتحديد مهامه وتنظيمه (الجريدة الرسمية،عدد 47).

[9] عبد الله أوهايبية ، المرجع السابق ، ص 206-207

[10] المرسوم الرئاسي 89/11 المؤرخ في 22 فبراير 2011 المتعلق بتحويل سلطة الوصاية على سلك الحرس البلدي الى وزارة الدفاع الوطني (الجريدة الرسمية العدد 26) .

[11] تم النص عليهم بموجب المادة 21 من قانون الاجراءات الجزائية.

[12] عبد الله أوهايبية المرجع السابق ، ص 211 .

[13] للتفصيل أكثر أنظر محمد محرز ، أصول الاجراءات الجزائية في القانون الجزائري ، على ضوء التعديلات لقانون الاجراءات الجزائية والاجتهاد القضائي ، دار هومة ، دون طبهة ، دون سنة ، ص 162 وما بعدها .

يمارس ضباط الشرطة القضائية مهامهم وصلاحياتهم وسلطاتهم المخولة لهم قانونا في نطاق خاص يمارسون فيه مهامهم وصلاحياتهم وسلطاتهم المخولة لهم قانونا ويترتب على التزامهم أو تجاوزهم لحدود هذا النطاق صحة أو بطلان ما يقومون به من اجراءات وأعمال.

ويحكم عملهم أو اختصاصهم ضابطان هما ، أولا الضابط المكاني ، وثانيا الضابط التوعي

الفرع الاول:الاختصاص المكاني

يتحدد مدى الاختصاص المكاني ونطاقه بحسب صفة الضبطية القضائية والتي يحملها وبحسب الجهة التي ينتمون اليها أو الجريمة ، فيكون الاختصاص اما محليا أو وطنيا

1 -**الاختصاص المحلي** : حسب نص المادة 16 في فقرتها الاولى من قانون الاجراءات الجزائية، يتحدد الاختصاص المحلي للضبطية القضائية في الحدود التي يباشرون فيهاوظائفهم المعتادة اعتمادا على المعايير الثلاث التقليدية وهي مكان وقوع الجريمة ومكان القبض على أحد المشتبه فيهم أو مكان اقامة احد المشتبه فيهم في ارتكابهم للجريمة .

وكل خروج على هذه الاحكام يعد باطلا وهذا حسب نص المادة 16 فقرة أولى من قانون الاجراءات الجزائية

2 -**الاختصاص الوطني** : يقصد بالاختصاص الوطني ممارسة الضبطية القضائية لمهامهم في كامل اقليم التراب الوطني ويكون اما في حالة الاستعجال أو بالنسبة للتابعين للأمن العسكري أو في حالة الجرائم المذكورة في قانون الاجراءات الجزائية حصرا.

أ -**حالة الاستعجال** : وهي الحالة التي تتطلب السرعة في اتخاذ الاجراءات الضرورية وخوفا من ضياع أثار ومعالم الجريمة ، يجوز لضباط الشرطة القضائية أن يباشروا مهامهم في كافة دوائر الاختصاص لمجلس القضاء الملحقين به وذلك حسب المادة 16 من قانون اجراءات جزائية في فقرتها الثانية ، كما يجوز لضباط الشرطة القضائية أن يباشروا مهمتهم في كافة الاقليم الوطني متى طلب منهم ذلك من القاضي المختص بشرط ان يساعدهم في ذلك ضباط الشرطة القضائية الذين يمارسون وظيفتهم في المجموعة السكنية المعنية ، وهنا يجب على ضابط الشرطة القضائية ان يخبرو وكيل الجمهورية الذي سيباشرون مهمتهم في دائرة اختصاصه [14].

ب -**التابعين للأمن العسكري** : اذ يمتد اختصاص هؤلاء الى كافة التراب الوطني دون قيد أو شرط وهذا ما جاء في نص المادة 16 من قانون الاجراءات الجزائية

ت -**الجرائم المحددة على سبيل الحصر** :تتمثلهذه الجرائم في جرائم الماسة بأنظمة المعالجة الالية للمعطيات وجرائم المخدرات والمنظمة العابرة للحدود الوطنية وجرائم تبييض الاموال وجرائم الارهاب وكذا جرائم قانون الصرف ، نص المشرع الجزائري على أن اختصاص ضباط الشرطة القضائية في هذه الجرائم يمتد

[14] عبد الرحمان خلفي ، الاجراءات الجزائية في التشريع الجزائري والمقارن ، دار بلقيس ، الجزائر طبعة 2015 ، ص 70 .

الى كامل الاقليم الوطني دون قيد أو شرط حسب المادة 16 السابقة الذكر ، على أن يتم اخطار كل من النائب العام ووكيل الجمهورية لدى المجلس القضائي المختص اقليما [15]، وكذلك تمديد عمليات مراقبة الاشخاص المذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه في ارتكابهم هذه الجرائم الخمس او مراقبة وجهة الاموال او الاشياء المستعملة في ارتكاب هذه الجرائم .

الفرعالثاني الاختصاص النوعي

ويختلف مجال الاختصاص النوعي للضبطية القضائيةحسب نوعية الجرائم التي يمارسون سلطاتهم بشأنها، ويتمثل في:

1 -**اختصاص نوعي عام وشامل** : وهو ما نصت عليه المواد 17، 18 ، 42 ، 50 ، 51 ، 52 ، 54 ، 62 ، 63 ، من قانون الاجراءات الجزائية ، التي تنص على انعقاد اختصاص الضبطية القضائية بممارسة سلطاتهم في كافة الجرائم مهما كانت جسامتها أو طبيعتها .

2 -**الاختصاص النوعي الخاص أو المحدد** : يتحدد هذاالاختصاص بنوعية معينة من الجرائم بموجب قوانين خاصة بفئات معينة من الاعوان والموظفين الذين خول لهم القانون بعض مهام الضبط القضائي ، مثال ذلك أعوان الجمارك لا يختصون الا بالجرائم الجمركية أو جرائم التهريب، ونفس الأمر فيما يخص مفتشي العمل يختصون فقط بمخالفات تشريع العمل والضباط التابعين للأمن العسكري حددت اختصاصاتهم بموجب المادة 15 مكرر [16]، وبالتالي فهؤلاء لا يجوز لهم القيام بالتحريات والاستدلالات حول كافة الجرائم ، مختصين فقط في الجرائم المرتبطة بالوظيفة التي يؤدونها .

المبحث الثاني : اجراءات الاستدلال في الجرائم الماسة بأنظمة المعالجة الالية للمعطيات

نص الدستور على الحق في حماية الحياة الخاصة وسرية الاتصالات والمراسلات، وعمل المشرع على اصدار قوانين متنوعة لحمايته ، الا أنه استثناء ومراعات لمقتضيات حماية النظام العام و ضرورات ومستلزمات التحقيقات التي تتطلب التطرق لهذه الحقوق ، نص المشرع على مجموعة من الترتيبات التقنية والاجراءات الاستثنائية التي خولها لضباط الشرطة القضائية خاصة من اجل الوقاية من الجرائم الالكترونية الاقتصادية ، هذا الى جانب الاجراءات التقليدية للبحث والتحري في كافة الجرائم .

سنتطرق في هذا المطلب الى كل من الترتيبات التقنية المخولة للضبطية القضائية في الفرع الاول وكذا الاجراءات التفتيش والحجز داخل المنظومة المعلوماتية .

المطلب الاول : الترتيبات التقنية على الاتصالات الالكترونية

تم النص على هذه الترتيبات في كل من قانون الاجراءات الجزائية وكذا القانون المتعلق بالقواعد الخاصة

[15] محمد حزيط ، مذكرات في قانون الاجراءات الجزائية الجزائري ، دار هومة ، الطبعة العاشرة ، 2015 ، ص 90 .
[16] تم اضافة هذه المادة من خلال تعديل قانون الاجراءات بموجب القانون رقم 07/17 المؤرخ في 28 جمادى الثانية 1438 الموافق ل 27 مارس 2017 (الجريدة الرسمية عدد 20).

للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وقانون الفساد، وتتمثل في المراقبة الإلكترونية التي تتم عن طريق اعتراض المراسلات وتسجيل الاصوات والتقاط الصور ، وعملية التسرب الذي تتم بمراقبة الاشخاص الذين يشتبه في ارتكابهم الجرائم الالكترونية الاقتصادية .

الفرع الاول:المراقبة الالكترونية للاتصالات

تطرق المشرع في المادة 56 من قانون الفسادللترصد الالكتروني والاختراق الذي يتمثل في المراقبة الالكترونية، وحدد اجراءاته وشروط اتخاذه من قبل الضبطية القضائية في المواد من 65 مكرر 5 الى 65 مكرر 10 من قانون الاجراءات الجزائية تحت عنوان الفصل الرابع في اعتراض المراسلات وتسجيل الاصوات والتقاط الصور ، حيث تم تحدي د شروط القيام بهذه التقنيات ، كما تم النص على الحالات التي يسمح فيها باللجوء الى هذه التقنيات في المادة 4 من القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها .

1 -شروط اللجوء الى المراقبة الالكترونية : نصت المادة 65 مكرر 5 من قانون الاجراءات الجزائية على هذه الشروط بما يلي :

- اذا اقتضت ضرورات التحري في الجريمة المتلبس بها،
- وجود تحقيق ابتدائي في جرائم المخدرات والجرائم المنظمة العابرة للحدود الوطنية والجرائم الماسة بالمعالجة الالية للمعطيات وجرائم تبييض الاموال أو الارهاب أو جرائك الصرف أو جرائم الفساد،
- الاذن باللجوء للمراقبة اذ نصت نفس المادة على جواز الاذن من وكيل الجمهورية او قاضي التحقيق المختص باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ، ووضع الترتيبات التقنية اللازمة لالتقاط وتثبيت وبث وتسجيل المكالمات في اماكن خاصة أو عامة أو التقاط الصور [17]،
- تنفيذ العمليا المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية في مرحلة البحث والتحري أو قاضي التحقيق في مرحلة التحقيق الابتدائي،

2 -الحالات التي يسمح باللجوء الى المراقبة الالكترونية

يمكن تصنيف الحالات التي جاءت بها المادة 4 من القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها الى 3 حالات

- حالة تتعلق بجرائم محددة وهي :

أ – الاولى أن يكون الهدف من المراقبة الوقاية من الافعال الموصوفة بجرائم الارهاب أو التخريب

[17] لصحة الاذن وجب ان يتوافر على مجموعة من البيانات وهي : ذكر كل العناصر التي تسمح لضابط الشرطة القضائية بالتعرف على الاتصالات والصور المطلوب التقاطها ، ذكر الاماكن المقصودة سكنية كانت أو غيرها ، أن يكون الاذن مكتوبا طبعا ، وأن يسلم الاذن في مدة اقصاها 4 اشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق .

أو الجرائم الماسة بأمن الدولة وهنا اشترط المشرع أن يتم تسليم الاذن بالمراقبة مكتوبا من السلطة القضائية المختصة كما رأينا ، الا أنه في الفقرتين الاخيرتين من المادة 4 السابقة الذكر نص المشرع في هذه الحالة أيضا على اختصاص النائب العام لدى مجلس قضاء الجزائر بمنح الاذن لضابط الشرطة القضائية اذا كانهذا الاخير منتميا للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المنصوص عليها في المادة 13 و 14 من نفس القانون ، وتكون مدة الاذن هنا 6 أشهر قابلة للتجديد ويكون التجديد على اساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها ، وان تكون هذه الترتيبات موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الافعال الارهابية والاعتداءات على أمن الدولة ومكافحتهما وذلك تحت طائلة العقوبات المقررة للمساس بالحياة الخاصة للغير .

ب – الثانية حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني ، وهنا اشترط ايضا ان يتم تسليم الاذن مكتوبا من السلطة القضائية المختصة

- حالة تتعلق بصعوبة التحقيق حيث نصت المادة 4 نفسها في الفقرة ج على أنه ولمقتضيات التحريات والتحقيقات القضائية وعندما يكون من الصعب الوصول الى نتيجة تهم الابحاث الجارية هنا يتطلب اللجوء الى المراقبة وأن يكون ايضا بإذن مكتوب من الجهة المختصة .
- حالة المساعدة القضائية الدولية ويكون اجراء المراقبة هنا تنفيذا لطلبات المساعدة القضائية الدولية ، في اطار النظر في جرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتكبة خارج الاقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني ، حسب المواد 15 حتى المادة 18 من القانون السابق .

الفرعالثاني: عملية التسرب

في نفس المادة 56 من قانون الفساد السابقة الذكر، نص المشرع على التسليم المراقب، والذي اصطلح عليه في قانون الاجراءات الجزائيةبـالتسرب ونضمهفي المواد 65 مكرر 11 الى 65 مكرر 18 منه، وقد أوردنا عملية التسرب كتقنية استحدثت هي ايضا وفق القانون 22/06 المؤرخ في 20 ديسمبر 2002 المعدل والمتمم لقانون الاجراءات الجزائية .

عندما تقتضي ضرورة التحري و التحقيق في الجرائم الخمس المنصوص عليهم في المادة 65 مكرر المذكورة سابقا[18]، يقوم ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، و بموجب إذن مكتوب و مسبب من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو متخف[19].

[18] المادة 65 مكرر 11 من قانون الاجراءات الجزائية .
[19] المادة 65 مكرر 12 من قانون الاجراءات الجزائية .

كما يسمح للضابط أو العون بإمكانية استعماله هوية مستعارة و ارتكاب الأفعال التالية دون اعتبارها تحريضاً على ارتكاب الاعتداءات، أو حتى مسؤولين جزائيا على هذه الافعال[20]:

– اقتناء أو حيازة أو نقل أو تسليم، أو إعطاء مواد أو أموال أو منتوجات أو وثائق، أو معلومات متحصل عليها من ارتكاب الاعتداءات، أو مستعملة في ارتكابها،

– استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم، الوسائل ذات الطَّابع القانوني أو المالي، و كذا وسائل النّقل أو التخزين أو الإيواء أو الحفظ أو الاتصال،

و يجب أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، و هوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته، و يحدد كذلك مدة عملية التَسرب التي لا يمكن أن تتجاوز 4 أشهر، إلا في حالة التمديد من طرف القاضي الذي رخص بها، و الذي يمكنه كذلك أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة ، وتوضع الرخصة في ملف الاجراءات بعد الانتهاء من عملية التسرب[21].

كما أنه وحفاظا على سلامة وامن العون المتسرب نصت المادة 65 مكرر 17 على مواصلة هذا العون رغم توقيف العملية أو انقضاء المهلة ، ولا يكون المتسرب هنا مسؤولا جزائياعلى أن لا تزيد المواصلة عن 4 أشهر ، وفي حال عدم تمكن المتسرب من توقيف نشاطه في ظروف تضمن أمنه ، عليه ان يخبر القاضي الذي اصدر الرخصة الذي بدوره يمكنه تمديدها ل 4 أشهر اخرى على الاكثر ، ويتم سماع المتسرب بصفته شاهدا على العملية دون سواه .

كما نص قانون الإجراءات الجزائية على عقوبات صارمة ضد من يكشف هوية ضابط أو عون الشرطة القضائية المتسرب، في أي مرحلة من مراحل الإجراءات طبقا للمادة 65 مكرر 16 من قانون الإجراءات الجزائية.

وبالتالي فقد أولى المشرع حماية بالغة لعملية التسرب وضمان سرية جريانها ، كما خص العون المتسرب بالحماية حفاظا على أمنه و سلامته خلال قيامه بالتسرب وحتى بعد الانتهاء منها.

ويمكن الاشارة أن كل من المراقبة الإلكترونيةوالتسرب يمكن استعمالهما في ان واحد في حالة ما توافرت شروطهما معا، واذا اقتضت متطلبات التحري والتحقيق ذلك ، اذ ان المراقبة الالكترونية قد تساعد كثيرا المتسرب في الكشف عن مرتكبي الجرائم ومنع وقوها ، وقد تم الاصطلاح على التسرب في المادة 56 من قانون الفساد[22]، بمصطلح التسليم المراقب كما نصت عليه المادة 16 مكرر من قانون الاجراءات الجزائية واصطلح عليه بمراقبة الاشخاص، ويكون ذلك كما رأينا في تمديد الاختصاص عبر كامل التراب الوطني.

المطلب الثاني : اجراءات التفتيش والحجز داخل المنظومة المعلوماتية

[20] المادة 65 مكرر 14 من قانون الاجراءات الجزائية .

[21] المادة 65 مكرر 15 من قانون الاجراءات الجزائية .

[22]القانون رقم 01/06 المؤرخ في 20 فيفري 2006 المتعلق بالوقاية من الفساد وكافحته، المعدل والمتمم (الجريدة الرسمية رقم 14 المؤرخة في 2006/3/8) .

تلعب الضبطية القضائية دورا بارزا في مجال الجرائم الالكترونية الاقتصادية خاصة بعد أن مكنها المشرع من العديد من الاختصاصات ذات الطابع الخاص وقيدها بمجموعة من الشروط والحالات نظرا لمساسها بالحياة الخاصة للأفراد ، فإضافة الى اجرائي المراقبة الالكترونية للمعلومات والتسرب ، نص المشرع على كل من التفتيش والحجز داخل المنظومة الالكترونية .

وعليه سنتطرق الى كل من التفتيش في المجال الالكتروني ، حجز المعلومات أو الانظمة أو المعطيات في المجال الإلكتروني

الفرع الاول: التفتيش داخل المنظومة المعلوماتية

اضافة الى التفتيش المادي لمسرح الجريمة والذي خصه المشرع بالعديد من الشروط والضمانات والذي يستعمل في الجرائم الماسة بالمعالجة الالية للمعطيات ، نص على التفتيش في نظم المعلوماتية .

ويمكن تعريف التفتيش على أنه : " البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها اليه أو هو البحث الدقيق أو الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه سواء كان مسكنا أو جهاز حاسوب أو أنظمة أو أنترانت " [23]

ومن خصائص التفتيش المعلوماتي أنه وسيلة من وسائل التحري في النظم المعلوماتية اطلاع عن المعطيات والمعلومات ، فيه تعرض للحياة الخاصة لأصحابها في بعض الحالات ، يسمح فيه باستعمال قواعد واساليب التحقيق الجنائي الفني عكس التفتيش الكلاسيكي المادي .نظرا لخصوصية هذا التفتيش ارتئينا أن نتطرق لشروطه واجراءاته وكذا أثار ه معتمدين في ذلك على النصوص القانونية المتعلقة به في كل من قانون اجراءات جزائية وقانون رقم 04/09 السابق الذكر، مع الاشارة أن القيام بالتفتيش الالكتروني يكون في نفس الحالات المشار اليها سابقا والمنصوص عليها بنص المادة 4 من القانون 04/09 .

1 -شروط التفتيش الالكتروني : لم تنص المادة 5 من القانون رقم 05/09 السابق الذكر على شروط التفتيش الالكتروني ، بل اكتفى المشرع بالإحالة فيها الى كل من قانون الاجراءات الجزائية ،و المادة 4 من نفس القانون التي تنص على الحالات التي يسمح فيها باللجوء الى المراقبة الالكترونية ،و من خلال هذه الاحالات وبالرجوع الى المواد المتعلقة بالتفتيش في قانون الاجراءات الجزائية نجد أن المشرع قد وسع من اختصاصات القائم به في الجرائم المحددة على سبيل الحصر وعليه لن نجد اشكال في تطبيق أحكامها على التفتيش الالكتروني :

- فبالنسبة لما يتعلق بالمكان كشرط فانه في التفتيش الالكتروني لا يكون بالانتقال الى مكان أو منزل يكفي الولوج الى المنظومة المعلوماتية أو جزء منها أو لمعطيات المعلوماتية المخزنة فيها ، أو منظومة تخزين معلومات حسب ما جاء في المادة 5 السابقة الذكر.

[23] رضا هميسي ، تفتيش المنظومات العملوماتية في القانون الجزائري ، مجلة العلوم القانونية والسياسية ، جامعة الوادي ، العدد 5 جوان 2012، 157-182 ، ص 160 .

وفي حال كانت المعلومات المبحوث عنها في منظومة أخرى يمكن الدخول اليها من خلال المنظومة الاولى والتي تم النص عليها في الفقرة أ من المادة 5 هنا يجوز تمديد التفتيش بسرعة بعد اعلام السلطة القضائية المختصة ، هنا التمديد لا يحتاج اذنا جديدا مجرد اعلام للسلطة المختصة .

واذا كانت المعلومات المبحوث عنها خارج الاقليم الوطني ، يكون الحصول عليها بمساعدة السلطات الاجنبية المختصة طبقا لاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل .

كما أضافت الفقرة الاخيرة من المادة 5 أنه يمكن للسلطة المكلف بالتفتيش تسخير أي شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها ، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها .

- شرط وقت التفتيش المادي محدد وفقا المادة 47 من قانون اجراءات جزائية والتي نصت على أنه يكون في كل وقت من الليل أو النهار اذا تعلق الامر بالجرائم الست منها جرائم الماسة بأنظمة المعالجة الالية للمعطيات .
- شرط أن يكون التفتيش بحضور صاحب المسكن فانه في الفقرة الاخيرة من المادة 45 من قانون الاجراءات الجزائية نصت على أن لا يطبق هذا الشرط في الجرائم الست بما فيها الجرائم محل دراستنا .

2 -أثار التفتيش الالكتروني : ان الهدف من اجراء التفتيش الالكتروني هو الحصول على معلومات للوقاية من الجرائم أو مكافحتها ، وهنا يتم حتى قبل وقوع الجريمة وذلك نظرا للخطورة الاجرامية التي يحدثها هذا النوع من الجرائم ، فاذا كانت نتائج التفتيش سلبية يكون الامر مفروغ منه ، أما اذا كانت النتائج ايجابية وتم العثور على دليل لإثبات معلومات محتمل استعمالها لارتكاب الجرم أو أن الجريمة قد وقعت فعلا ، فانه وجب ضبطها وحجزها .

الفرع الثاني:حجز المنظومة المعلوماتية

بعد التفتيش في الجرائم العادية يتم ضبط الاشياء التي تفيد في اثبات الجريمة وحجزها ، وتكون هذه الاشياء مادية اذ يتم جرد المنقولات ووضعها في احراز ونقلها للمكان المخصص للحجز عليها ، بينما يتم التحفظ على العقارات عن طريق تشميعها ووضع الاختام عليها حتى لا يتم تغيير أو اتلاف مسرح الجريمة ، الا أنه في الحجز المعلوماتي فالأمر يختلف ، اذ لا يتعلق الامر فقط بأجهزة الكمبيوتر ولواحقها والأقراصوالاشرطة التي تعتبر من قبيل الاشياء المادة وانما يتم الحجز حتى على الاشياء المعنوية ان صح التعبير والتي تتمثل في المنظومات المعلوماتية والمعطيات والبيانات .

1 -امكانية ضبط الاشياء الغير محسوسة :لقد اختلف الفقه في ضبط و حجز البيانات المعالجة والمعطيات المخزنة وانقسم الى موقفين :

- يرى أنصار الموقف الاول أنه لا يمكن تصور بأي حال من الاحوال اجراء الضبط والحجز على الكيانات المعنوية لانتفاء الكيان المادي لها ، الا ان هذه النظرية ومع التطور الحاصل في مجال

المعلوماتية اصبحت غير صالحة ولا تتماشى مع ما موجود حاليا ، ولا تتماشى ما يتطلب التفتيش الالكتروني وهو ما أداة بالفقهاء الى اجرها وعدم الأخذ بها لا في القانون ولا على مستوى القضاء .

- والاتجاه الثاني يرى أصحابه أنه لا يوجد ما يمنع حجز هذه المعطيات والبيانات المعالجة بنظام المعلوماتية وذلك عن طريق تمديد مفهوم ضبط وحجز الادلة المادية ليشمل البيانات الالكترونية ، ويرون أن هذه البيانات ايضا عبارة عن ذبذبات الكترونية واشارات أو موجات كهرومغناطيسية يمكن أن تسجل تخزن في وسائط معينة يمكن اعتبارها مادية أيضا .
- بالرجوع الى المادة 6 في فقرتها الاولى من القانون 04/09 نجد أن المشرع قد أخذ بالاتجاه الثاني القائل بإمكانية تفتيش البيانات المعالجة اليا وضبطها فقد اجاز حجز المعطيات المخزنة داخل المنظومة المعلوماتية ، كما يجيز نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احراز وفقا لقانون الاجراءات الجزائية ، مع السهر على سلامتها ، كما يجوز تشكيل أو اعادة تشكيل هذه المعطيات باستعمال وسائل تقنية قصد جعلها قابلة للاستغلال لأغراض التحقيق ، شرط ان لا يؤدي ذلك الى لمساس بمحتوى المعطيات .
- الحجز عن طريق منع الوصول الى المعطيات : يتم هذا الاجراء عند استحالة اجراء الحجز المذكور في المادة 6 لأسباب تقنية ، هنا تقوم السلطة القائمة بالتفتيش باستعمال تقنيات تعمل على نسخ أو منع الوصول الى المعطيات التي تحتويها المنظومة المعلوماتية التي تكون موضوعة تحت تصرف الاشخاص المرخص لهم باستعمال هذه المنظومة هذا حسب المادة 7 من القانون 04/09 ، كما نصت المادة 8 من نفس القانون على جواز منع الاطلاع على المعطيات التي يشكل محتواها جريمة في حد ذاتها عن طريق أمر تصدره السلطة التي تباشر التفتيش وذلك عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك .

كما شدد المشرع على عدم استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة والتفتيش والحجز الا في الحدود الضرورية للتحريات والتحقيقات القضائية .

هذا وقد أوكل المشرع سلطات القيام بعمليات المراقبة التفتيش الى العديد من الجهات من سلطات قضائ يةٍ كالنيابة و التحقيق ، والضبطية القضائية ، وكذا الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال ، اضافة الى مقدمي الخدمات مساعدة للسلطات المكلفة بالتحريات القضائية .

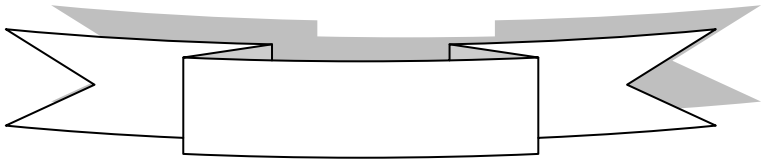
الخاتمة:

من خلال دراستنا للموضوع المتعلق بالأليات المستحدثة لمكافحة الجرائم الالكترونية الاقتصادية في مرحلة البحث والتحري المنصوص عليها في كل من قانون الإجراءات الجزائية وقانون الفساد، والقانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، نجد أن المشرع الجزائري قد وسع من اختصاصات الضبطية القضائية على حساب ضمانه للحقوق والحريات الفردية وهذا راجع للخطورة الاجرامية

للجرائم الاقتصادية ولمنع الافلات من العقاب، وتنحصر هذه الاليات في المراقبة الالكترونية والتسرب والتفتيش والحجز .

ولم يتوقف المشرع عند هذا الحد انما وسع من اختصاصات ضباط الشرطة القضائية محليا خاصة في جرائم محددة، الا أنه ورغم محاولة المشرع مسايرة التطور الحاصل في الاجرام الالكتروني، فان النصوص القانونية التي تنظمها لا تزال في حاجة الى الاثراء وذلك لسد النقائص التي تشوبها، والتي يتم اكتشافها ومعاينتها فعليا من الممارسة على أرض الواقع ولذلك نقترح من خلال هذا العمل مجموعة من التوصيات

- زيادة تكوين الجهات القضائية والامنية في مجال تكنولوجيات الاعلام والاتصال خاصة مجال التكنولوجي الاقتصادي.
- تحديث مستمر للتشريعات الخاصة بهذا النوع من الجرائم وانشاء هيئات بحثية وأمنية مثل الهيئة الوطنية للوقاية من الفساد ومكافحته ، مع تعزيز اختصاصات ونشاطاتها، ومنع تداخل الاختصاص بينها وبين الضبطية القضائية.
- تعديل النصوص الموضوعية وجعلها اكثر تحديدا ودقة لمنع الافلات من العقاب لمرتكبي مثل هذه الجرائم في مختلف الادارات والمؤسسات الاقتصادية، خاصة التابعة للدولة كونها تصيب اقتصاد الدولة في حد ذاتها ، خلق فضاء تعاوني وتكاملي بين المؤسسات الاقتصادية والجهات الامنية لمنع مثل هذه الاعتداءات.
- السعي الى عقد لقاءات علمية وفنية كنافذة مشتركة بين الباحثين والممارسين، يتم من خلالها تبادل الافكار والمعلومات هذه الجرائم وكيفية مكافحتهاوعرض تجارب الدول الاخرى في نفس المجال وتحليل مدى نجاعتها ، واستعمال وسائل تقنية اكثر جودة وفعالية لحماية الانظمة والخدمات على مستوى المؤسسات الاقتصادية .



حنان مسكين **فاطمة شيخ**
meskinehan1991@gmail.com *fatima.chikh@univ-mosta.dz*
جامعة الدكتور مولاي الطاهر – سعيدة – **جامعة مستغانم**

الجريمة الالكترونية وآليات التصدي لها في التشريع الجزائري

مقدمة:

إن التطورات الهائلة التي عرفتها التكنولوجيات الحديثة للإعلام والاتصال، ورغم ما وفرته من تسهيل في أمور حياتنا، إلا أنها في المقابل فتحت الباب على مصراعيها لتطور أدوات ووسائل وسبل تنفيذ الجريمة الالكترونية، وجعلها أكثر تعقيدا وصارت مكافحتها تبدو صعبة المنال إن لم تتضافر جهود الأطراف الفاعلة في الساحة المعلوماتية. وباعتبار الجرائم المعلوماتية من أخطر الجرائم وأعقدها فرضت على العالم ضرورة تكييف قوانينها للتعامل مع هذا النوع من الإجرام الذي بات يهدد أمن المجتمعات.

الجزائر وكغيرها من الدول ليست بمنأى عن الجريمة وتداعياتها على غرار الدول الأخرى حيث لم تسلم مواقع التواصل الاجتماعي وفضاء تبادل المعلومات من عمليات السطو على الصور والبيانات واستعمالها للابتزاز والمساومة والتشهير ، وأمام هذا الوضع الخطير من جهة، وعدم نجاعة الأساليب التقليدية من جهة أخرى سعت الجزائر لمواكبة الركب الحضاري لمواجهة الجريمة المعلوماتية ع ن طر يق سن آليات قانونية عملية لاحتواء الظاهرة والتصدي لها تماشيا مع متطلبات المنظومة الدولية والتزاماتها المنبثقة عن مصادقتها على عديد من الاتفاقيات المتعلقة بالجريمة المعلوماتية.

وعلى ضوء كل ما سبق يمكن أن نتساءل عن: ما مدى كفاية النصوص القانونية الحالية لمنع الجريمة المعلوماتية وردع مرتكبيها، ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة؟.

للإجابة عن التساؤل المطروح سيتم تقسيم موضوع دراسة إلى مبحثين أساسين على النحو التالي:

المبحث الأول: مفهوم الجريمة الالكترونية وخصائصها

المبحث الثاني الآليات القانونية لمكافحة الجرائم الالكترونية والحد منها

المبحث الأول: مفهوم الجريمة الالكترونية وخصائصها

تعتبر الجرائم الالكترونية من جرائم حديثة وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، ونتيجة لحداثتها فقد كانت هناك اتجاهات مختلفة في تعريفها، كما أنها تتميز بخصائص متفردة لا تتوفر في أي من الجرائم التقليدية ، لذا كان لزاما علينا تحديد الجريمة الالكترونية من خلال تحديد تعريفها(المطلب الأول) لنعرج بالبحث عن خصائصها(المطلب الثاني).

المطلب الأول: تعريف الجريمة الالكترونية

تعددت تعريفات الجريمة المعلوماتية وتباينت فيها بينها ضيقا واتساعا، وقد أسفر ذلك عن تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، وما استتبع ذلك من تسهيل التوصل إلى الحلول المناسبة لمواجهتها.

وفي هذا السياق لا يوجد مصطلح موحد للدلالة على هذه الظاهر، فهناك من يطلق ظاهرة الغش المعلوماتي أو الاختلاس لمعلوماتي أو الجريمة الالكترونية، جرائم الفضاء الافتراضي، جرائم كمبيوتر الانترنت، جرائم مجتمع ما بعد المعلومات وغيرها من المسميات ، وعلة هذا الاختلاف هو خشية حصر هذه الجريمة في نطاق ضيق فتعددت تعريف بشأنها وسنورد أهمها:[1]

01)-**الاتجاه الضيق في تعريف الجريمة الالكترونية:** من التعريفات التي وضعها أنصار الاتجاه الضيق أن الجريمة الالكترونية هي:"فعل غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها وحذفها أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه."([2])

وعرفها كلاوس تايدومان بأنها: "كافة أشكال السلوك غير المشروع أو الضار بالمجتمع ا لذي يرتكب باسم الحاسب الآلي"[3]

بينما عرفها الفقيه merwe إلى أن الجريمة المعلوماتية:" هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية". فيما عرفه الفقيه rosblat بأنها:" كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والى تحويل طريقته".

ولكن ما يلاحظ على تعاريف المقدمة جاءت قاصرة على الإحاطة بأوجه الظاهرة الإجرامية، أما تعريف كلاوس تايدومان فيؤخذ عليه أن بالغ في العمومية والاتساع لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع.

ويدخل في نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها: "الجرائم التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا". [4]

02)-**الاتجاه الموسع في تعريف الجريمة الالكترونية:** على عكس الاتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة وتختلف مواقفهم حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية.

وعليه فقد عرفت على أنها: "كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال أو الأشياء المعنوية الخبير الأمريكي Parker

(1)-طعباش أمين، الحماية الجنائية للمعاملات الالكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2015، ص15.
(2) نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2008،ص48.
(3) لمزيد من معلومات راجع:
Tiedemann (Klaus)، fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques، Rev.Dr.Pén.Crim n°7، Bruxelles، 1984، p 61 .
(4)-عبد العال الديربي، محمد صادق إسماعيل، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة، ط 1، المركز القومي للإصدارات القانونية ، القاهرة، 2012، ص 40-41.

عرف الجريمة المعلوماتية أنها:" كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل".

يعرف الأستاذ hestanc و vivant الجريمة المعلوماتية: "مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمك أن تكون جديرة بالعقاب".(5)

وفي ذات التوجه نجد أن منضمة التعاون الاقتصادي والتنمية (OECD) الخاص باستبيان الغش المعلوماتي عام1982والذي أوردته بلجيكا في تقريرها بان الجرائم المعلوماتية هي:" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".(6)

وعليه جرائم الكمبيوتر هو مصطلح شامل أشمل من المصطلح السابق ويقصد فيه كل الجرائم التي يستخدم فيها الكمبيوتر فهو سواء أداة الجريمة أو كان هدف الجريمة ويدخل من ضمنها جرائم معلوماتية وجرائم الإنترنت، كما يدخل من ضمنها الاعتداء على الشبكات المحلية خاصة بالهيئات والمنشات الخاصة والعامة.

03)-التعريف القانوني للجريمة الالكترونية: تبنى المشروع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث.(7)

ويجدر التنويه إلى أن المشرع الجزائري لم يتخلف بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات حيث أنه عرف من خلال نص المادة 2 من القانون رقم09-04 القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مسميا إياه":المنظومة المعلوماتية" وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين".(8)

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتي من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل وهذا دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم04-15 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات والذي أفرد القسم

(5)-نهلا عبد القادر الممني، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع ط1، 2008، ص 49 .

(6)-أحمد خليفة، الجرائم معلوماتية، دار الفكر الجامعي، ط2، 2006، ص87.

(7)-القانون رقم09-04 المؤرخ في 5غشت2009المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، جريدة رسمية ، عدد47، صادرة بتاريخ 16-08-2009.

(8)- نشناش منية، الركن المفترض في الجريمة المعلوماتية، مداخلة مقدمة بمناسبة الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة، المنظم يومي 16-17 نوفمبر2015، ص04 .

السابع مكرر منه تحت عنوان :المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 08 مواد من المادة 394مكرر وحتى المادة 394 مكرر07 .

وقد وفق المشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها، وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات .

المطلب الثاني: خصائص الجرائم معلوماتية

مما لاشك فيه أن الجرائم المعلوماتية تختلف عن الجرائم التقليدية من ناحية الأفعال الإجرامية ومن ثم ليس من المستغرب أن تختلف عنها في بعض الصفات التي تميزها عن غيرها من الجرائم بخلاف الصفات التي تطابق صفات الجرائم الأخرى.[9] وسوف نحاول إبراز أهم هذه الخصائص فيما يلي:

01) –الجرائم الالكترونية من الجرائم عابرة للحدود: إن الجريمة المعلوماتية هي شكل من أشكال الجرائم العابرة للحدود، فمسرح الجريمة لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد ماديا على مسرح الجريمة وهذا التباعد في المسافات بين الفعل المرتكب من خلال الحاسوب والفاعل وبين المعلومات التي كانت محل الاعتداء، فالجاني يستطيع القيام بجريمته بالدخول إلى ذاكرة الحاسوب الآلي الموجود في بلد آخر وهذا الفعل قد يضر شخصا ثالثا في بلد آخر.[10]

غير أنه طبيعة الدولية لهذا النوع من الجرائم يثير في كثير من الأحيان تحديات قانونية إدارية فنية بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.

02)–صعوبة اكتشاف واثبات الجرائم الالكترونية: تتميز الجريمة الالكترونية بصعوبة إثباتها وهذا راجع إلى طبيعتها اللامادية التي تجعل من محو الأدلة أمر سهلا إذ يمكن للمجرم الالكتروني محو آلاف من البيانات في ضغطة زر. وبهذا فالجريمة المعلوماتية لا تترك آثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية.

هذا وترجع صعوبة إثبات الجريمة الالكترونية إلى عدة الأسباب منها:

–صعوبة العثور على دليل مادي للجريمة وذلك راجع إلى استخدام الجاني وسائل فنية وتقنية معقدة مع سرعة محو الدليل والتلاعب بيه من قبل الجاني.

– وسيلة التنفيذ الجريمة تتسم غي غالب بالطالع التقني الذي يضفي عليها الكثير من التعقيد ، ومن ثم فإنها تحتاج خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب الماما بتقنيات الكمبيوتر ونظ م المعلومات.

03)– وقوع الجريمة الإلكترونية في بيئة المعالجة الآلية للبيانات : تقع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات والمعطيات خاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن

(9)-محمد سامي الشوا، ثورة المعلوماتية وانعكاساتها على قانون العقوبات، دار النهضة العربية، ط2، مصر، ب.س.ط، ص 58-60.
(10)-سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجستير في علوم القانونية، جامعة الحاج لخضرباتنةن2012-2013، ص32.

البحث عن قيام أو عدم قيام أركان الجريمة الالكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك انه في حالة تخلف هذا الشرط تنتفي الجريمة الالكترونية.[11]

وعليه يستلزم لقيام هذه الجريمة التعامل مع بيانا ت مجمعة ومجهزة للدخول للنظام المعلوماتي بغرض معالجتها الكترونيا، بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة، والتي يتوافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها وطباعتها، وهذه العمليات وثيقة الصلة بارتكاب الجرائم ولابد من فهم الجاني لها أثناء ارتكابها في حالات التزوير والتقليد.[12]

04)–قلة الإبلاغ عن وقوع الجريمة الالكترونية: غالبا لا يتم الإبلاغ عن وقوع الجريمة الالكترونية لعدم اكتشاف الضحية لها أو خوفا من التشهير، إذ تحجم الشركات والمؤسسات في مجتمعات الأعمال الإبلاغ عنها تجنبا للإساءة إلى السمعة وخوفا من التشهير.

المطلب الثالث: أنواع الجرائم المعلوماتية

تصنف الجريمة المعلوماتية(الالكتروني)إلى عدة أصناف فهناك من يصنفها تبعا لمرتكبها، وهناك الجرائم المعلوماتية التي صنفت تبعا لطريقة تنفيذها، وأخرى تبعا لغرض أو هدف الاعتداء[13] وتم تصنيفها وفق أسس متعددة بغرض تسهيل التعامل معها، ويمكن الإشارة إلى تصنفين رئيسيين:

التصنيف الشكلي: ويتضح من خلاله الشكل العام للجريمة والتغير الذي طرأ عليها بفعل التقنية المعلوماتية وينقسم إلى نوعين وهما :

▪ **الجرائم الالكترونية التقليدية** : وهي الجرائم المعروفة من السابق كالسرقة مثلا، ولكنها أصبحت ترتكب بتسخير قدرات التقنيات المعلوماتية كوسيلة لتنفيذها مما أعطاها مسميات أخرى كالسرقة الالكترونية تتفق وطبيعتها الجديدة.

▪ **الجرائم الالكترونية الجديدة** :وهي عبارة عن أشكال إجرامية مستحدثة لم تكن معروفة من السابق وتعتمد بشكل رئيسي في تنفيذها على التقنيات المعلوماتية أو الالكترونية كونها لم تعرف إلا بعد ظهور التقنيات الرقمية، كنشر الفيروسات الرقمية أو عمليات الاختراق لقواعد البيانات مثلا.

التصنيف العملي :ويعتمد على الدور الذي تلعبه تقنية المعلومات في الجريمة المنفذة ويندرج تحته ثلاثة أنواع وهي

▪ **الجرائم التي تستهدف النظام المعلوماتي** :وهي الجرائم الالكترونية التي تستهدف احد مكونات النظام المعلوماتي أو الالكتروني كجرائم الاختراق وجرائم إتلاف المعلومات.[14]

▪ **الجرائم المنفذة باستخدام النظام المعلوماتي** :وهي الجرائم التي يتم ارتكابها بواسطة التقنيات الرقمية كجرائم التعدي على البيانات وانتهاك الخصوصية.

(11)-خالد محمد كدفور المهيري، جرائم الكمبيوتر والانترنت والتجارة الالكترونية، دار الغرير للطباعة والنشر، دبي 2005،ص135.
(12) –أحمد خليفة الملط، الجرائم المعلوماتية ، دار الفكر الجامعي،الإسكندرية، د.س.ط، ص105.
(13)-منصور بن مصلح الجهني، أنواع الجرائم المعلوماتية وصفات مرتكبيها، مؤتمر الجرائم المعلوماتية، الرياض أكاديمية نايف العربية للعلوم الأمنية من 22 إلى 23 شوال 1430 الموافق 12-14 أكتوبر2009، ص06.
(14)-أسامة بن غانم العبيدي، جريمة إتلاف المعلومات، مجلة دراسات المعلومات، جزء 04، يناير2009، ص 93-123.

▪ **الجرائم المنفذة في بيئة النظام المعلوماتي** :وتتمثل في الجرائم التي تتم في البيئة الالكترونية دون الإضرار بالبيئة ذاتها، بل يكون الضرر على الأطراف المستخدمة أو المستفيدة من تلك البيئة كجرائم التشهير والجرائم الإباحية والأخلاقية.

المبحث الثاني: الآليات القانونية لمكافحة الجرائم الالكترونية والحد منها

إن موضوع الآليات القانونية لمكافحة الجريمة المعلوماتية أصبح هاجسا يؤرق رجال القانون بصفة خاصة، لذلك بات من المستعجل أن تتسع دائرة التعاون مع رجال العلم المتخصصين في التقنيات الرقمية ورجال القانون والمؤسسات الرسمية في الدولة، وعلى المستوى الدولي أيضا بغية سن قوانين تكافح مرتكبي تلك الجرائم. كما تبرز أهمية هاته الدراسة من الناحية النظرية في معرفة مدى كفاية النصوص القانونية الحالية لمنع الجريمة المعلوماتية وردع مرتكبيها ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة.[15]

المطلب الأول: آليات مكافحة الجريمة الالكترونية في قانون العقوبات

استحدث المشرع الجزائري القسم السابع مكرر من قانون العقوبات من الفصل الثالث الخاص بجرائم الجنايات وا لجنح ضد ا لأموال تحت عنوان" ا لمساس بأنظمة ا لمعالجة الآلية للمعطيات" بنص المواد 394مكرر-394مكرر7 من قانون العقوبات.[16]

ومن خلال هذه النصوص يتضح لنا أن المشرع الجزائري قسم الجرائم الالكترونية إلى أربع(4) طوائف تتعدد بحسب المصالح المحمية التي تتمثل أساسا في سرية هذه المعطيات أو تكاملها وف ي وفرتها وفي تكاملها وتتمثل في:

01)-تتضمن جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات.

02)-الجرائم الالكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي.

03)-الجرائم الالكترونية المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب.

04)-الجرائم الالكترونية للشخص المعنوي.

وفي سنة 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون رقم06-23 المؤرخ في20 ديسمبر2006[17] حيث مس ذلك التعديل القسم السابع مكرر منه والخاص بالجرائم الماسة

(15)-فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد2،2015،ص 08.

(16)-القانون رقم04-15 المؤرخ في 10-11-2004 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08-06-1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد71 لسنة 2004.

(17)-القانون رقم06-23 المؤرخ في 20-12-2006 المتضمن قانون العقوبات، الجريدة الرسمية، عدد 48، الصادرة في 24- 12- 2006 .

بأنظمة المعالجة الآلية للمعطيات، حيث تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالجرائم الواردة فيه، وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث عن الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الانترنت كوسيلة لنقل المعلومات وتزايد سريع لمستخدمي الانترنت.[18]

المطلب الأول: آليات مكافحة الجريمة الالكترونية في قانون الإجراءات الجزائية

لقد أدرك المشرع الجزائري بأن المواجهة الفعالة للإجرم الاالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شانها أن تتفادى وقوع الجريمة الالكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها.وهو ما استدركه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الالكترونية في مراقبة الاتصالات الالكترونية وتسجيلها والتسرب.

والجدير بالملاحظة أنه ونتيجة ارتفاع الجرائم الالكترونية في الجزائر ونظرا لسرعة تنفيذها تدخل المشرع الجزائري مرة أخرى من خلال إنشاء قطب جزائي وطني متخصص في محاربة الجريمة الالكترونية ومكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتشديد العقوبات على بعض الجرائم السيبرانية.[19]

المطلب الثالث: آليات مكافحة الجريمة الالكترونية في القوانين الخاصة

نظرا لعدم كفاية نصوص قانون العقوبات لحماية الحياة من مخاطر التكنولوجيا الحديثة ، سن المشرع الجزائري مجموعة من القوانين لحماية الحياة الخاصة في ظل الجرائم المعلوماتية، وذلك ابتدءا من سنة2009 إلى يومنا هذا.[20]

01)- آليات مكافحة الجريمة الالكترونية في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: كخطوة أولى للحكومة الجزائرية لمواجهة ما يعرف بالجريمة الالكترونية، صدر سنة 2009 القانون رقم 09-04 المؤرخ في 05 غشت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلا أن تجسيد بنوده على أرض الواقع ضعيف إلى حد الساعة، بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها، واقتصرت العقوبات في أغلب الأحيان على الغرامة المالي.[21]

ويتضمن القانون19 مادة موزعة على6 فصول، وعرف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في المادة02 على أنها:"الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة

(18)-سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، عدد52 ديسمبر2019،ص
(19) الباب السادس"القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"المواد من 211مكرر 22-211مكرر29 من الأمر رقم 21-11 المؤرخ في 25غشت2021 متمم للأمر رقم66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد65، الصادرة في26 غشت2021.
(20)- شيخ سناء، مكافحة الجرائم الالكترونية في القانون الجزائري، ص06.
(21)-حفوظة الأمير عبد القادر، غرادين حسام، الجريمة الالكترونية واليات التصدي لها، مداخلة بمناسبة الملتقى الوطني آليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، الجزائر العاصمة 29 مارس 2017.

الآلية للمعطيات المحددة قي قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية."

واستنادا لأحكام القانون رقم 09-04 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته نجده قد تضمن أحكاما خاصة بمجال التطبيق وأخرى خاصة بمراقبة الاتصالات الإلكترونية وعددت الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، بالإضافة إلى القواعد الإجرائية المتضمنة تفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الالكترونية، و نص القانون في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وتتكفل أيضا بتبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الالكترونية وتحديد مكان تواجدهم، كما أن هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية من إطار مبدأ المعاملة بالمثل.[22]

ويجدر التنويه أن أهمية هذا القانون تكمن كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين قواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

02)-**الحماية من خلال قانون الملكية الأدبية والفنية :** حاول المشرع الجزائري مواجهة الجريمة الالكترونية من خلال قانون الملكية الأدبية والفنية المتعلق بحق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم 03-05 المؤرخ في23-07-2003 المتعلق بحقوق المؤلف والحقوق المجاورة[23]حيث وسع قائمة المؤلفات المحمية، وذلك باندماج برامج المعلوماتية ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات برامج المعلوماتية , كما شدد العقوبات على المساس بحقوق المؤلفين خاصة المصنفات الرقمية التي تشملها الحماية.[24]

03)-آليات مكافحة الجريمة الإلكترونية في القانون المتعلق بالتوقيع والتصديق الإلكترونيين : أصدر المشرع الجزائري بتاريخ 1 فبراير 2015 القانون رقم 15-04 المحدد للقواعد المتعلقة بالتوقي ع التصديق الالكترونيين، وعرف التوقيع الالكتروني من خلال نص المادة 02منه، وبهذا نجد أن التوقيع والتصديق الالكترونيين يرتبط بمجموعة من البيانات ذات الطابع الشخصي التي يشكل الاعتداء عليها جريمة يعاقب مرتكبها بأحكام جزائية ومتمثلة في:

(22)-القانون رقم09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها السالف الذكر.
23- الأمر رقم 03- 05 المؤرخ في 19- 07- 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد 44 ، صادرة بتاريخ 13-07-2003 .
(24)-تجدر الإشارة إلى أن القانون الدستوري الجديد أكد هو الأخر في مادته 44 على حماية حقوق المؤلف وعدم جواز حجز على أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بأمر قضائي.

-الإخلال بسرية البيانات : طبقا لنص الماد 42 يجب على مؤدي خدمات التصديق الإلكتروني أن يحافظوا على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكترونية الممنوحة، فإذا أخلوا بهذا الواجب يعاقب طبقا لنص المادة 70 من نفس القانون بـ ا لحبس من ثلاثة (03)أشهر إلى سنتين(02) وبغارمة من200.000 دج إلى مليون دينار100.000 أو بإحدى هاتين العقوبتين.

-إفشاء البيانات الشخصية أو إساءة استعمالها :طبقا للمادة 68من هذا القانون يعاقب بالحبس من ثلاثة(03) أشهر إلى ثلاث (03)سنوات وبغرامة من مليون دينار 1000000 إلى خمسة ملايين دينار50000000 أو بإحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير.

-جمع البيانات الشخصية للمعني دون موافقته: طبقا لنص المادة 43 من هذا القانون فانه لا يمكن لمؤدي خدمات التصديق الإلكتروني أن يجمع البيانات الشخصية للمعني إلا بموافقته الصريحة، ومتى أ أخلّ بهذا الواجب يعاقب بالحبس من ستة (06)أشهر إلى ثلاث (03)سنواتوبغرامة2000000 إلى مليون دينار أو بإحدى هاتين العقوبتين فقط.

04)-آليات مكافحة الجريمة الإلكترونية في قانون القواعد العامة المتعلقة بالبريد والاتصالات الإلكتروني:أصدر المشرع القانون رقم 18-04 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية والذي ألغى بموجبه القانون رقم 2000-03 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية والذي أكد على وجوب عدم مساس استعمال شبكات وخدمات الاتصال الإلكترونية بحفظ الحياة الخاصة للأفراد، وفي حالة مخالفة يتم تعرض للأحكام الجزائية متعلق ة بانتهاك سرية معلومات المنصوص عليها في المادة 164 من هذا القانون، تحويل مراسلات الصادرة عن طريق البريد الالكتروني طبقا لنص المادة165 من نفس القانون.[25]

05)-مكافحة الجريمة الإلكترونية في قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي: مواكبة للتطورات والجرائم التي تمس خصوصية الأفراد اصدر المشرع الجزائري القانون رقم 18-07 والذي هدف منه تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وذلك في إطار احترام الحياة الخاصة للأفراد. وعرف المعطيات ذات الطابع الشخص من خلال نص المادة03 من هذا القانون، ومخالفة أحكتم هذا القانون يعرض المخالف لأحكام جزائية منصوص عليها في نصوص المواد54، 55،58،60، 62، 67من هذا القانون.[26]

المطلب الرابع: الهياكل الخاصة للتصدي للجرائم الالكترونية

نظرا لتفاقم الظاهرة الإجرامية المعلوماتية من يوم لآخر وبالنظر إلى الطبيعة الخاصة التي تتميز بها هذه

(25)-المواد164-165من القانون رقم 18-04 المؤرخ في10مايو2018 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، العدد27، الصادرة في 13مايو2018.

(26)-القانون رقم 18-07 المؤرخ في 10يونيو2018 المتعلق حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد34 ، الصادرة في 10يونيو2018.

الجرائم، كان من ضروري تدخل المشرع الجزائري لمكافحة هذه الظاهرة الإجرامية الحديثة وضع هيئات قانونية لمكافحة هذا النوع من الجرائم، ومن أهم هذه الأجهزة نخص بالذكر:

01)-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته: في سبيل مكافحة الجرائم المعلوماتية أو كما يسميها المشرع الجزائري جرائم تكنولوجيات الإعلام والاتصال استحد ث المشرع هيئة وطنية بموجب المادة 13 من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وحسب المادة 02 من مرسوم الرئاسي رقم 19-127 تعتبر:"الهيئة مؤسسة عمومية ذات الطابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع."[27] أما فيما يخص مهامها فنصت عليها المادة 14من قانون رقم 09-04 السالف الذكر.

02)-القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: إن الثورة التي حدثت في مجال المعلوماتية قد أدت إلى ارتكاب سلوكيات غير المروعة فرضت إضفاء الصفة الجرمية عليها سماها المشرع جرائم تكنولوجيات الإعلام والاتصال ، ولضمان فعالية متابعتها تم إنشاء قطب جزائي متخصص في هذا النوع من الجرام وزوده المشرع بمهمة المتابعة والتحقيق فيها وكذا حكم في الجنح المتعلقة بها.

واستنادا لأحكام القانون رقم 21-11متمم للأمر رقم 66-155 المؤرخ في 8يونيو1996المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 65، الصادرة في 26 غشت 2021 تم إنشاء قطب ذو اختصاص وطني مكلف بالجرائم مرتبطة بنشر معلومات الكاذبة التي من شانها أن تمس بالأمن العمومي واستقرار المجتمع والترويج لها طبقا لنص المادة 211مكرر22.

واستنادا لنصوص أحكام القانون رقم 21-11 السالف الذكر نجده حدد 5 جرائم رئيسية مرتبطة بتكنولوجيات الإعلام والاتصال يختص فيها وكيل الجمهورية لدى القطب وقاضي التحقيق ورئيس ذات القطب.[28]

خاتمة

ترتيبا لما سبق يتضح لنا أن انتشار تكنولوجيا الحديثة واستعمالاتها التي مست كل نواحي الحياة أفرز العديد من التحولات والتغيرات بشقيها الايجابي والسلبي، فالتقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى ظهور أشكال جديدة للإجرام اصطلح على تسميتها بالجريمة الالكترونية، رغبة من المشرع الجزائري في التصدي لظاهرة الإجرم الالكتروني وما يصاحبها من أضرر معتبرة على الأفارد وعلى مؤسسات الدولة من جهة، ومحاولة منه تدارك الفارغ التشريعي القائم في هذا المجال من جهة أخرى، عمد منذ الألفية الثانية إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على أرسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجية الإعلام والاتصال . وقام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الالكترونية. وعليه فان ه ـذا التنـوع

(27)-المادة 02 من المرسوم الرئاسي رقم 19-127 مؤرخ في 6يونيو2019 المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، جريدة رسمية، عدد37 ، الصادرة في 6يونيو2019.

(28)-لتفصيل أكثر راجع المواد 211 مكرر23 – 211مكرر 24-211مكرر25 من القانون رقم 21-11 السالف الذكر.

التشريعي من شانه أن يساهم بشكل فعال على الأقل في الوقت الراهن في الحد من تفاقم ظاهرة الإجرام الالكتروني في الدولة الجزائرية .

مع هذا ينبغي الاعتراف بحقيقة و هي انه ر غم الجهود الجبارة التي يبذلها المشرع الجزائري في سبيل التصدي لظاهرة الإجرم الالكتروني، إلا أنها غير كافية لبلوغ الهدف الذي يتطلع إليه، نظرا للتطورات السريعة والمستمرة التي تعرفها ظاهرة الإجرام الالكتروني م ن جهة، و نظرا للطالع العالمي والعابر للحدود الذي بها هذه الظاهر من جهة أخرى، لذلك لابد من التفكير في التوجه إلى التعاون التشريعي والقضائي والأمني مع الدول العربية ولما لا مع الدول الغربية الأكثر دارية بالجرائ الالكترونية والاستفادة من خبرتها في محال مكافحة هذه الجرائم.

ولتعزيز مكافحة الجرائم الالكترونية نوصي بجملة من توصيات يمكن إجمالها على نحو التالي:

01)-ضرورة إنشاء مركز بحث حول الجريمة المعلوماتية يعمل على دراسة تطورها والإجراءات الكفيلة للحد منها.

02)-ضرورة مراجعة التشريعات الوطنية التي لها علاقة بالجريمة المعلوماتية ونخص بالذكر قانون التجاري، المدني، قانون ملكية الفكرية.

03)-ضرورة التشدد في توقيع العقوبات عللا مرتكبي الجرائم الالكترونية سوا ء تعلق الأمر بمدة السجن المقررة أو الغرامات المالية.

04)-ضرورة إنشاء ضبطية خاصة ومحاكم متخصصة بالجرائم الالكترونية وتكوين أجهزة وشرطة جنائية مختصة في البحث والتحري عن جرائم الالكترونية.

05)-ضرورة خلق ثقافة اجتماعية جديدة تندد بجرائم الانترنت مع تفعيل أسلوب التوعية والتهذيب لدى مستخدمي شبكة الانترنت، وكذا نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية .

وفي الختام لابد من الإشارة إلى أنه لا يكفي أن يتم مواكبة نصوص تشريعية للتشريعات المقارنة بدون تجسيدها من الناحية التطبيقية ، إذ يجب العمل على تكوين فرق من الضبطية القضائية وقضاة مختصين في هذا النوع من الجرائم ومدها بكافة الوسائل المادية والتقنية اللازمة لأداء عملها.

قائمة المصادر والمراجع

أولا: قائمة المصادر

- الأمر رقم 03- 05 المؤرخ في 19- 07- 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد44 ، صادرة بتاريخ 13- 07-2003 .
- القانون رقم 04-15 المؤرخ في 10-11-2004 المعدل والمتمم للأمر 66-156 المؤرخ في08-06-1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71 لسنة 2004.
- القانون رقم 06-23 المؤرخ في 20-12-2006 المتضمن قانون العقوبات، الجريدة الرسمية، عدد 48 الصادرة في 24- 12-2006 .

▪ القانون رقم 09-04 المؤرخ في 5غشت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ولاتصال و مكافحتها ، جريدة رسمية ، عدد47 ، صادرة بتاريخ 16-08-2009.
▪ القانون رقم 18-04 المؤرخ في 10مايو2018 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، العدد27، الصادرة في 13مايو2018.
▪ القانون رقم 18-07 المؤرخ في 10يونيو2018 المتعلق حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد34 ، الصادرة في 10يونيو2018.
▪ الأمر رقم 21-11 المؤرخ في 25غشت2021 متمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد65 ، الصادرة في26 غشت2021.

المراسيم الرئاسية

▪ المرسوم الرئاسي رقم 19-127 مؤرخ في 6يونيو2019 المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، جريدة رسمية، عدد 37 ، الصادرة في6يونيو2019.

ثانيا: قائمة المراجع

01)-الكتب

▪ أحمد خليفة الملط، الجرائم المعلوماتية ،دار الفكر الجامعي،الإسكندرية،د.س.ط.
▪ أحمد خليفة، الجرائم معلوماتية، دار الفكر الجامعي، ط2، 2006.
▪ خالد محمد كدفور المهيري، جرائم الكمبيوتر والانترنت والتجارة الالكترونية، دار الغرير للطباعة والنشر دبي، 2005.
▪ الشوا، ثورة المعلوماتية وانعكاساتها على قانون العقوبات ،دار النهضة العربية،ط 2، مصر،بدون سنة الطبع..
▪ طعباش أمين، الحماية الجنائية للمعاملات الالكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية 2015.
▪ عبد العال الديربي، محمد صادق إسماعيل، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة، ط 1 المركز القومي للإصدارات القانونية، القاهرة، 2012.
▪ نهلا عبد القادر الممني، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع ط1، الإصدار الأول2008.
▪ نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2008.

ثانيا: أطروحات الدكتوراه ورسائل ومذكرات الماجستير

▪ سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجستير في علوم القانونية، جامعة الحاج لخضر باتنة، 2012-2013.

▪ **ثالثا: المقالات والمداخلات القانونية**

▪ أسامة بن غانم العبيدي، جريمة إتلاف المعلومات ، مجلة دراسات المعلومات، جزء 04، يناير 2009.

▪ سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، عدد 52 ديسمبر 2019.

▪ فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية،مجلة الحقوق والحريات، العدد2015،2

المداخلات القانونية

▪ حفوظة الأمير عبد القادر، غرادين حسام، الجريمة الالكترونية واليات التصدي لها، مداخلة بمناسبة الملتقى الوطني آليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، الجزائر العاصمة 29 مارس 2017.

▪ منصور بن مصلح الجهني، أنواع الجرائم المعلوماتية وصفات مرتكبيها، مؤتمر الجرائم المعلوماتية الرياض أكاديمية نايف العربية للعلوم الأمنية من 22 إلى 23 شوال 1430 الموافق 12-14 أكتوبر ،2009.

▪ نشناش منية ، الركن المفترض في الجريمة المعلوماتية ،مداخلة مقدمة بمناسبة الملتقى الوطني للجريمة المعلوماتية بين الوقاية و المكافحة، جامعة بسكرة يومي 16-17 نوفمبر 2015.

د. بورطال أمينة
amina.bourtal@univ-temouchent.edu.dz
جامعة بلحاج بوشعيب عين تموشنت

استحداث القطب الجزائي لمكافحة الجريمة الإلكترونية الاقتصاديّة في التشريع الجزائري

الملخص:

إنّ لظاهرة العولمة أثر بارز في تطوير الجريمة التقليدية إلى جريمة مستحدثة في جميع المجلات، الاجتماعية والثقافية والسياسية والاقتصادية، حيث انتشرت جرائم ذات طابع اقتصادي بوجه جديد، الّتي أصبحت تهدّد الفرد والمجتمع والدولة، نظرا لخطورتها، وهو ما جعل المشرع الجزائري يبحث عن حلّ متأثرا بالتشريعات الغربية، فحرص على ضرورة استحداث هيكل قضائي جديد للحدّ من آثارها السلبية، يتمثّل في القطب الجزائي الاقتصادي والمالي والقطب الجزائي الوطني الذي أنشأ خصيصا لمكافحة الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال.

الكلمات المفتاحية: الجريمة الاقتصادية، الجريمة الإلكترونية، قطب جزائي.

Abstract :

The phenomenon of globalization has a significant impact on the development of traditional crime, To a crime created in all magazines, social, cultural, political and economic, Where crimes of an economic nature have spread in a new way, That threatens the individual, society and the State, Because of its gravity, which caused Algerian legislature to seek a solution influenced by Western legislation, Emphasizing the need to introduce a new judicial structure to reduce its negative effects,Consisting of the National Economic and Financial Penal Pole and the National Penal Pole established specifically to combat crimes related to information and communication technology.

Keywords : *economic crime, cybercrime, Penal Pole.*

مقدّمة:

إنّ الاقتصاد يساهم بقدر كبير في تطوّر الدّولة، ويدفع بعجلة التّنمية الاقتصادية، بما أنّه يقوم على عمليّات الانتاج للسلع (زراعية أو صناعية أو حيوانية أو من مستخرجات الأرض أو البحر أو من ثورات طبيعية، أو معدنية)،[1] غير أنّه تميّز القرن العشرين باختراعات هائلة على المستوى التّقني، بظهور الحاسبات الالكترونية والّذي تطوّر بشكل أفضى لاستحداث شبكات المعلومات يطلق عليها النّظام المعلوماتي.

[1] محمد أحمد المشهداني، الجرائم الاقتصادية أنواعها وطرق مكافحتها والوقية منها، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، مجلد 20، عدد 1، 2020، ص 114.

غير أنّ تكنولوجيا الإعلام والاتّصال سلاح ذو حدّين، فبالرّغم من المحاسن الّتي تتميّز بها، أصبح من الممكن اختراق المعلومات عبر شبكة الأنترنيت وارتكاب جريمة واحدة عبر عدّة دول في آن واحد، وقد ترتّب عن التطوّر السّريع في مجال تقنيّة المعلومات والاتّصالات وشبكة الانترنيت ظهور أنماط جديدة من الجرائم المستحدثة ترتبط بنظم المعالجة الآلية للمعلومات، أفرزتها التغيّرات والتحوّلات الاقتصادية[1] تدعى بجرائم ذوي الياقات البيضاء،[2]التي ينتمي مرتكبوها إلى طبقة اجتماعية ذات مكانة، كالهواة، الهاكار، المهووسون.[3]

وغدا هذا النّوع من الجرائم أن تكون الكترونية نتيجة تحوّل البنى الاقتصادية إلى معلوماتية،[4]الّتي تؤثّر بشكل كبير على كيان الدّولة واستقرارها الأمني في جوانب شتّى منها الجانب الاقتصادي، الّتي تستهدف اقتصاديات الدّول، وانتهاك الموارد، وتدنّي معدّلات النمو ّالاقتصادي والدّخل القومي والاستثمار وتفشّي ظاهرتي الفقر والبطالة،[5]فأصبحت تشكّل عائق أساسي لبرنامج التنمية في الدول النامية، لاسيّما الدّول العربية،من جرّاء سوء استخدام التكنولوجيا، حيث تمثّل هاجسا مخيفا على الشّركات والمؤسّسات الاقتصادية الكبرى، الّتي تتعرّض لهجمات الكترونية على مدار السّاعة منذ عام 1999،[6]لتقدّر الجريمة الإلكترونية بنسبة حوالي 60 %للإدارات العامّة والمؤسّسات الصّناعية ونسبة 20 % للشركات الخاصة و 11 % الشّركات الأجنبية و06 % للأشخاص.[7]

وهو ما دفع المشرّع الجزائري يسعى جاهدا نحو الحدّ من الجرائم الإلكترونية الاقتصادية، بتوسيع الأجهزة الأمنية والقضائيّة، و فرض سياسات دوليّة وعقوبات على مرتكبيها، فتمّ انشاء أقطاب قضائية متخصّصة متكونة من قضاة متخصّصين ذوي خبرة وكفاءة لمكافحة هذه الجرائم وتزايدها السّريع، كتوجّه جديد تبنّاه المشرّع الجزائري بموجب نصوص قانونية، [8]بما أنّه أضعف هذا التقدّم التكنولوجي قدرات أجهزة الدّولة الّتي أصبحت عاجزة عن تطبيق القوانين ومواجهة هذه الجرائم المتصلة بتكنولوجيات الاعلام والاتّصال.[9]

---

[1] شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، عدد 1، يونيو 2020، ص 741.

[2] تعرف جرائم ذوي الياقات البيضاء تلك الجرائم غير العنيفة والمرتكبة لدوافع مالية من قبل رجال الأعمال وأصحاب النفوذ، حيث يعرفهاالمتخصص إدوين سذرلاند عام 1939 أنها جريمة يرتكبها فرد من ذوي الطبقات الاجتماعية العليا وله مكانة مرموقة في نطاق مهنته"، والتي تتمثل في الاحتيال، الرشوة، الاختلاس، الجرائم الالكترونية، انتهاك حقوق الطبع، غسيل الأموال، انتحال الشخصية والتزييف.

-www.wikipedia.org

[3]خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتيّة، دار الفكر الجامعي، مصر، طبعة أولى، 2019، ص 23.

[4] بوقال نسيم، المرجع السابق، ص 272.

[5] أمين جابر الشديفات، البطالة وعلاقتها بالجرائم الاقتصادية في العالم العربي (الأردن، السعودية، لبنان، مصر، المغرب)، مجلة دراسات، العلوم الإنسانية والاجتماعية، مجلد 44، عدد 1، 2017، ص 73.

[6] من بين الهجمات الإلكترونية انشاء مواقع الكترونية لنشر الشّائعات، تزوير المستندات الخاصة بالعملاء وابتزازهم مقابل تحصيل أموال، سرقة البيانات، الاحتيال.....الخ

- أبو بكر أحمد همام عبد المجيد، الآثار الاقتصادية للجرائم المعلوماتية وسبل مكافحتها، مجلة جامعة جنوب الوادي الدولية للدراسات القانونية، العدد السادس، 2021، ص 359.

[7]مزيود سليم، الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، العدد الأول، أفريل 2014، ص 103.

[8] القانون رقم 05-11 المؤرخ في 17 جويلية 2005 المتعلق بمراقبة مطابقة القانون العضوي المتعلق بالتنظيم القضائي، للدستور، ج ر عدد 51 المؤرخة في 20 يوليو 2005.

[9] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنيت، مذكرة ماجيستر في القانون العام، جامعة أبي بكر بلقايد تلمسان، 2011-2012، ص 47.

فكيفتصدّت هذه الآلية الاجرائية للجريمة الاقتصادية الالكترونية؟وهل يكفي القطب الجزائي الاقتصادي والمالي للنّظر في قضايا هذه الجريمة المستحدثة أم لا يتحقّق ذلك إلاّ بتدخّل القطب الجزائي الوطني المتخصّص لمكافحة الجرائم المتّصل بتكنولوجيا الإعلام والاتّصال؟

لنحاول الإجابة عن هذه التساؤلات من خلال المحورين الآتيين:

المحور الأول: مفهوم الجريمة الالكترونية الاقتصادية

المحور الثاني: دور القطب الجزائي المتخصّص في التصدّي للجريمة الالكترونية الاقتصادية

المحور الأوّل: مفهوم الجريمة الالكترونية الاقتصادية:

من أبرز الظّواهر الإجرامية الحديثة الجريمة الاقتصادية الالكترونية، الّتي تختلف عن الجريمة التقليدية في عدّة جوانب، الأمر الّذي يستدعي منّا تحديد مفهومها وخصوصيتها فيما يلي:

أولا: تعريف الجريمة الالكترونية الاقتصادية:

بادئ ذي بدء يجب التعرف على الجريمة الاقتصادية التي تعتبر "كلّ فعل غير مشروع ذا مظهر خارجي يخلّ بالنظام الاقتصادي والائتماني، يحضره قانون العقوبات أو القوانين الخاصة بخطط التنمية الاقتصادية الصادرة عن السلطة المختصة"، [1]فيمسّ بسلامة اقتصاد الدولة والتي تستهدف المصلحة العامة للكسب المادي على حساب الغير،[2]ليعرّفها المشرع الجزائري تحت تسميّة الجريمة الاقتصادية والمالية بموجب بموجب المادّة 211 مكرّر 2/3 من الأمر رقم 20-04 المتضمن قانون الإجراءات الجزائية [3] أنّها "تعتبر جريمة أكثر تعقيدا بالنّظر إلى تعدّد الفاعلين أو الشركاء أو المتضرّرين أو بسبب اتساع الرّقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة الأضرار المترتّبة عليها أو لصيغتها المنظّمة أو العابرة للحدود الوطنية أو لاستعمال تكنولوجيا الإعلام والاتصال في ارتكابها، تتطلّب اللّجوء إلى وسائل تحرّ خاصّة أو خبرة فنيّة متخصّصة أو تعاون قضائي دولي".

وبظهور عصر العولمة ظهرت أساليب تقنيّة جديدة للتّعامل الالكتروني، فأصبحت تُستخدم بشكل سلبي، فازدادت خطورة وتعقيد الجريمة الاقتصادية بتطور هذه التكنولوجيا ووسائل الاتصال، ونشاطات الدولة التجارية والاقتصادية والمالية،[4]الأمر الّذي ترتّب عنه لارتكاب أفعال اجرامية سيبرانية،[5]باستخدام أسلوب جديد جديد في ادارة مختلف المعاملات الاقتصادية والمالية، حيث يعرّفها المشرّع الجزائريالقانون رقم 09-04

[1] محمد أحمد المشهداني، الجرائم الاقتصادية أنواعها وطرق مكافحتها والوقية منها، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، مجلد 20، عدد 1، 2020، ص 110.

[2]بوقال نسيم، تطوّر الجريمة الاقتصادية وأهمّ خصائصها في العصر الحديث، ملتقى حول الجريمة المعاصرة في المجتمع الجزائري، أيام 25-26-27 ماي 2013، كلية العلوم الاجتماعية والانسانية، منشورات جامعة الطارف، 2013، ص 269.

[3]الأمر رقم 20-04 مؤرخ في 30 أوت 2020 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج. ر عدد 51 المؤرخة في 31 أوت 2020.

[4] رابح وهيبة، الإجراءات المتبعة أمام الأقطاب الجزائية المتخصصة، أطروحة دكتوراه، تخصص القانون الإجرائي، جامعة مستغانم، 2014-2015، ص 76.

[5] يصطلح على الجريمة الإلكترونية جرائم تكنولوجيا الإعلام والاتصال أو الجريمة الرقمية أو جرائم الحاسوب أو الجريمة السيبرانية أو جريمة الأنترنيت.

المؤرخ في 05 أوت 2009[1] في المادّة 02 /أ منه أنّها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدّدة في قانون العقوبات وأيّ جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتّصالات الالكترونية"، وفي ذات السياق تعرّفها المادّة 211 مكرّر 22 في فقرتها الثانية منالأمر رقم 21-11 المتضمن قانون الاجراءات الجزائية [2]"أيّ جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتّصالات الالكترونية، أو أيّ وسيلة أخرى أو آلية ذات صلة بتكنولوجيا الإعلام والاتّصال".

وتعرّف منظّمة التعاون الاقتصادي والتنمية التّابعة للأمم المتّحدة OCDE،[3] من خلال المؤتمر الّذي انعقد عام 1983 الجريمة الإلكترونية أنها كلّ فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية الجريمة الالكترونية أنها كلّ فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخّل التقنية الإلكترونية،[4]

ليتبيّن لنا من خلال هذا التعريف أنّه تكيّف الجريمة الكترونية باعتبارها كلّ سلوك إيجابي أو سلبي يقع باستخدام التقنية المعلوماتية على مصلحة مشروعة بالاعتداء، [5] متى تمّ الاعتداء على أموال مادّية أو معنوية،[6] غير أنّ ما يؤخذ عليه هو حصره الجرائم الالكترونية في تلك الجرائم الواقعة على الحاسب الآلي أو داخل نظامه، دون الجرائم الواقعة بواسطة الحاسب الآلي.[7]

ثانيا: خصوصية الجريمة الإلكترونية الاقتصادية:

تطرح الجريمة الإلكترونية الاقتصاديةالمرتبطة بشكل كبير بالأنشطة الاقتصادية، عدّة اشكالاتنتيجة خطورتها الّتي تستهدف فئات معيّنة تتمثّل في البنوك والمنشآت والمؤسسات المالية والمصرفيةالمُسيطرة على القيم الرأسمالية،التي أصبحت ضعيفة أمام المتغيّرات المُصاحبة لظاهرة العولمة والثّورة التقنية، حيث تباع المعلومات المالية والتّجارية والصّناعية المسروقة من ذويها الحقيقيين، [8]للتعرّف على أساليب إدارة المؤسّسات المالية والبنكية ومحاولة اختراقها أو تغيير نظمها.

ولا ينحصر تدخّل هذه الجرائم الاقتصادية الالكترونية المتطورة الهادفة نحو تحقيق أرباح أو سداد الديون،[9] داخل نطاق اقليم الدولة الجزائرية، بل يتعدّها باعتبارها من الجرائم العابرة للحدود، ممّا يؤثر على

---

[1] القانون رقم 09-04 مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، ج ر عدد 47 مؤرخة في 16 أوت 2009.

[2] الأمر رقم 21-11مؤرخ في 25 أوت 2021 يتمّم الأمر رقم 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج.ر عدد 65 المؤرخة في 26 أوت 2021.

[3] تعتبر منظّمةالتعاونالاقتصاديوالتنميةهيمنظّمةاقتصاديةدوليةتأسستعام 1961 منالدولالأوروبيةوأمريكاوكنداوتضمفيعضويتها 34 دولةمنهم 21منأصل 28 دولةهمأعضاءالاتحادالأوربيماعدابلغاريا،كرواتيا،قبرص،لاتفيا،استونيا،مالطا،رومانيا.

[4] www.oecd.org

[5] خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني، (دراسة مقارنة)، مجلد 7، عدد 26، 2018، ص 87.

[6] مزيود سليم، المرجع السابق، ص 96.

[7] خليل يوسف جندي، المرجع السابق، ص 87.

[8] معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة المفكر، جامعة محمد خيضر بسكرة، العدد 17، 2006، ص 410.

[9] كوثر حازم سلطان، موقف القانون والقضاء من الجريمة الالكترونية (السيبرانية) دراسة مقارنة، مجلة كلية التربية الأساسية، المجلد 22، عدد 96، 2016، ص 973، 974.

استقرارها، ويعرض حالتها الاقتصاديّة لخطر داهم،من قبل محترفين يتمتّعون بالقدرة على ارتكاب أفعال تستهدف الاحتيالعلى المصارفواعتراضبطاقاتالائتمانوسرقتهاواستخدامهاغيرالمشروع،والابتزازوالتزويروالتزييف،والتهرّبالضريبي، والاستيلاء على المال أو التجسّس أو الاستيلاء على البيانات السرية والاقتصادية،والمضاربة في الأسواق الماليّة والسّطو على الودائع بالبنوك وتدمير حساباتها للوصول للمعلومات الأمنية، [1]وقرصنة البرامج وتوزيعها غير مصرح به فتحوّل الأموال من القطاعات الأخرى، [2]وهم على علم مسبقا بالأضرار الّتي قد يتسبّبون بها لمؤسّسة أو شركة متمكّنة اقتصاديا، ولها كامل القدرة على تحمّل الخسارة من جرّاء تلاعباتهم الإلكترونية.[3]

ويترتّب عن ذلك المساس بالمركز الحسابي والإداري وتنقّل الأموال والاستثمارات في مختلف المنشآت، بالتسلل داخل النّظم المعلوماتية بهدف تدميرها أو الحصول على معلومات سريّة ذات طابع اقتصادي، والكشف عنالمعلومات الشخصية للأشخاص الطبيعيين بالحواسيب الآلية للبنوك والشركات، [4]والاستيلاء عليها، عليها، والتصرف فيها إما بدافع تنافسي، أو للابتزاز أو الحصول على مزايا ومكاسب اقتصادية، [5]فيتعرّض الأمن الاقتصادي لمخاطر عدم الاستقرار، ممّا يؤدّي إلى زعزعة ثقة المتعاملين الاقتصاديين، ويتوقّف النموّ الاقتصادي عند انتهاج سياسات الاقتصاد الحرّ الّذي يسعى نحو جذب رؤوس الأموال.

الأمر الّذي جعل من القوانين الّتي تحكمها قابلة للتّغيير السريع وان كانت المرونة والحركة من مقتضياتها حتى تواجه دائمًا الاحتمالات المضادة للسياسة الاقتصادية، وهي قوانين لا تحرص دائمًا على الوحدة في سياسة التّجريم والعقاب، فغالبا ما تخرج عن بعض القواعد العامّة العقابية، حيث تثار المسؤولية عن فعل الغير، والشخصالاعتباري،[6]بمعنىامتدّت آثارها لجميع الأشخاص الطبيعية والمعنوية.[7]

المحور الثاني: دور القطب الجزائي المتخصّص في التصدّي للجريمة الالكترونية الاقتصادية:

إنّ أول ظهور لمصطلح الأقطاب الجزائية كجهات قضائية متخصّصة تنظر في بعض الجرائم،[8]بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004،[9] والني تم الشروع في العمل بهذه الأقطاب منذ 2008، ليظهر في الوجود القطب الجزائي الوطني الّذي يلعب دور مهمّ جدا في التصدّي

[1] بوقال نسيم، المرجع السابق، ص 275، 276.

[2] كرم سلام عبد الرؤوف سلام، الجرائم الالكترونية في الفقه الاسلامي والقانون العضوي، المؤتمر الدولي العلمي الافتراض 2022، إصدارات المركز الديمقراطي العربي للدراسات الاستراتيجية السياسية والاقتصادية، ألمانيا / برلين، ص 62.

[3] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجنائية،مجلة مركز دراسات الكوفة، العراق، العدد السابع، 2008، ص 117.

[4] عادل يوسف عبد النبي الشكري، المرجع السابق، ص 116.

[5] مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، سلطة عمان، مجلي التعاون لدول الخليج العربية، ص 28.

[6] بوقال نسيم، المرجع السابق، ص 275، 276.

[7] بدرة لعور، الآليات المستجدة لمكافحة الجرائم الاقتصادية في التشريع الجزائري (الأقطاب الجزائية الاقتصادية والمالية: استحداث أم تجديد)، مجلة الرسالة للدراسات والبحوث الانسانية، جامعة العربي التبسي المسيلة، مجلد 6، عدد 3، سبتمبر 2021، ص 653.

[8] هامل محمد/ يوسفي مباركة، القطب الجزائي الاقتصادي والمالي كآلية لمكافحة جريمة التهريب، المجلة الاكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، مجلد 5، عدد 2، 2020، ص 869.

[9]القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج . ر عدد 71، 2004.

للجرائم ذات الاقتصادي والمالي، بما في ذلك الجرائم ذات صلة بتكنولوجيا الإعلام والاتّصال، وهو ما سنحاول التعرّض له فيما يلي:

أولا: الاطار التّنظيمي للقطب الجزائي الاقتصادي والمالي:

أما مخصوصيّة الجريمة الالكترونية الاقتصادية وخطورتها، الّتي باتت تهدّد الاقتصاد الوطني والدّولي،تسعىالجزائرمجابهةالجرائمالالكترونيةوسدّالنقصالحاصلفيالهيئاتالقضائيةالتيأصبحتغيرقادرةلوحدهامعالجةه ذه الجرائم المستحدثة، فأقرّ المشرّع الجزائري ضرورة انشاء هذه الهياكل الجديدة الّتي تتكون من قضاة مكونين في التخصّص.[1]

وتطبيقا لأحكام المادّة 32 من قانون الإجراءات المدنية والإدارية،[2]والمادة 24 من القانون رقم 05-11 المؤرخ في 17 جويلية 2005 المتعلق بمراقبة مطابقة القانون العضوي المتعلق بالتنظيم القضائي،[3]والمادة 21 في فقرتها الأخيرة من القانون العضوي رقم 22-10 المؤرخ في 09 جوان 2022 المتعلق بالتنظيم القضائي بقولها أنه "يمكن أن تضمّ المحكمة أقطاب قضائية متخصّصة تحدّد تشكيلتها في النصّ المنشئ لها"، [4]والمادة 329 في فقرته الخامسة، [5]أقرّ المشرّع الجزائي الجزائري بموجب أحكام قانون الإجراءات الجزائية انشاء القطب الجزائي الاقتصادي والمالي كهيئة قضائية جزائية على مستوى مقرّ مجلس قضاء الجزائر تختصّ بالنّظر في الجريمة الاقتصادية والمالية الأكثر تعقيدا، الّتي تتطلّب وسائل تحرّ خاصّة أو خبرة فنيّة متخصّصة أو تعاون قضائي دولي، لاسيّما تتبّع مسارات الجرائم الاقتصادية وقمع مخالفة التّشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج، حيث تنصّ المادّة 221 مكرّر من الأمر رقم 20-04 أنّه "ينشأ على مستوى محكمة مقرّ مجلس قضاء الجزائر قطب جزائي وطني متخصّص، لمكافحة الجريمة الاقتصادية والمالية".[6]

وأمام فعالية هذه الهيئة الوطنيّة للحدّ من انتشار الجريمة الاقتصادية والمالية، أكّد المشرّع الجزائري على استحداث بموجب الأمر رقم 21-11 المتعلّق بقانون الإجراءات الجزائية لأوّل مرّة في الجزائر القطب الجزائي صاحب الاختصاص الوطني في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال،حيث تنصّ

---

[1] تجدر الإشارة أنه تم تكوين هؤلاء القضاة في المدرسة العليا للقضاء والمدرسة العليا للمصرفة وتربض خارج الوطن، بالتعاون مع هيئات دول أجنبية منها الاتحاد الأوربي بهدف ضمان كفاءة مرفق القضاء.
- رابح وهيبة، المرجع السابق، ص 49، 50.

[2] تنصّ المادّة 32 من القانون رقم 08-09 المؤرخ في 25 فبراير 2008 المتضمن قانون الإجراءات المدنية والإدارية، ج ر عدد 21 المؤرخة في 23 أبريل 2008 أنّ "المحكمة هي الجهة القضائية ذات الاختصاص العام وتتشكّل من أقسام.
ويمكن أيضا أن تتشكّل من أقطاب متخصّصة"

[3] تنص المادة 24 من القانون رقم 05-11 المؤرخ في 17 جويلية 2005 المتعلق بالتنظيم القضائي: "أنّه "يمكن انشاء أقطاب قضائية متخصصة ذات اختصاص اقليمي موسّع لدى المحاكم.
يتحدد الاختصاص النوعي لهذه الأقطاب حسب الحالة، في قانون الإجراءات المدنية أو قانون الإجراءات الجزائية".

[4]القانون العضوي رقم 22-10 المؤرخ في 09 جوان 2022 المتعلق بالتنظيم القضائي، ج. ر عدد 41، المؤرخ في 16 جوان 2022.

[5] تنصّ المادّة 5/329 من الأمر رقم 66-155 المؤرخ في 08 يوليو 1966 المتضمن قانون الإجراءات الجزائية المعدّل والمتمّم أنه "يجوز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية **والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف"**

[6] الأمر رقم 20-04 المؤرخ في 30 أوت 2020 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج. ر عدد 51 المؤرخة في 31 أوت 2020.

المادّة 211 مكرّر 22 منه أنّه "ينشأ على مستوى مقرّ مجلس قضاء الجزائر قطب جزائي وطني متخصّص في المتابعة والتّحقيق في الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال والجرائم المرتبطة بها.

كما يختصّ بالحكم في الجرائم المنصوص عليها في هذا الباب اذا كانت تشكّل جنحا."

لنلاحظ أنّ هذا التطّور المؤسّساتي المستحدث يتماشى مع احدى الهيئات المكلّفة بمكافحة الجرائم الالكترونية، الّتي سبق للمشرّع الجزائري استحداثها عام 2009، المعروفة بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته بموجب القانون رقم 09-04 المؤرّخ في 05 أوت 2009، وهذا إن دلّ على شيء، فهو يوحي على مدى حرص المشرّع الجزائري على الوقاية من الجرائم المعلوماتية الاقتصادية.

ثانيا: اختصاص القطب الجزائي الاقتصادي والمالي:

وفق لأحكام الأمر رقم 20-04 المتضمّن قانون الإجراءات الجزائية، يمارس القطب الجزائي الاقتصادي اختصاصاته الاقليمي والنوعي، حيث منح القانون للقطب الجزائي اختصاص اقليمي موسع يشمل التراب الوطني،وهذا يعود لخصوصية الجريمة السيبرانية وعدم قدرة المحاكم على متابعة هذه الجرائم لتنوعها وكثرتها، كما حدد القانون للقطب الجزائي اختصاصات حصرية في الجرائم الواردة في المادة 211 مكرر 24. حيث يؤول الاختصاص النظر في الجرائم المذكورة في المادة 211 مكرر 24 الى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

1 -الاختصاص الاقليمي للقطب الجزائي الاقتصادي والمالي:

تخوّل المادّة 221 مكّرر 1 من الأمر رقم 20-40 لوكيل الجمهورية لدى القطب الجزائي الاقتصادي والمالي وقاضي التحقيق ورئيس القطب ممارسة كافة الصلاحيات في كامل التراب الوطني، نتيجة الخطورة التي تتسبّب فيها هذا النّوع من الجرائم الالكترونية العابرة للحدود، الأمر الّذي ينعكس بشكل سلبي على الاقتصاد المحلي والدولي.

وتجدر الإشارة أنّه أنشأ القطب الجزائي الاقتصادي والمالي المتخصّصعلى مستوى محكمة مقرّ مجلس قضاء الجزائر العاصمة، الّذي يختصّ أصلا في النظر في قضايا مكافحة الجريمة الاقتصادية والماليّة دون وجود أيّ محاكم أخرى على مستوى الجمهورية، حسبما تؤكّده المادّة 211 مكرّر من الأمر رقم 20-04 المتعلّق بقانون الإجراءات الجزائية، للنّظر في القضايا المتعلّقة بالجرائم المحدّدة على سبيل الحصر.

غير أنّه أصبح يحلّ محلّ هذا القطب الجزائي الاقتصادي والمالي، ما استحدثه الأمر رقم 21-11 والمعروف بالقطب الجزائي الوطني لمكافحة الجرائم المتصّلة بتكنولوجيا الاعلام والاتصال، والّذي ينشأ هو الآخر على مستوى مقرّ مجلس قضاء الجزائر، للمتابعة والتّحقيق فيها طبقا للمادّة 211 مكرّر 22، وذلك تطبيقا للأصل العام الّذي وسّع الاختصاص المحلّي لوكيل الجمهورية وقاضي التّحقيق والمحكمة لدائرة

اختصاص محاكم أخرىتطبيقا لأحكام المادّة 40/37،2/2، 5/329 من الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية.

غير أنّه لو ركّزنا على نصّ المادّة 329 فقرة 1 من قانون الإجراءات الجزائية الجزائري التي جاء في فحواها "تختص محليّا بالنظر في الجنحة محكمة محل الجريمة أو محكمة اقامة أحد المتهمين أوشركائهم أو محل القبض عليهم، ولوكان هذا القبض لسبب آخر"، لتستثني من نصّ المادّة 329 في فقرتها الخامسة مدى جوازية تمديد الاختصاص المحلي للمحكمة الى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

وهو مايؤكّده المرسوم التنفيذي رقم 06-384 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق المؤرخ في 05 أكتوبر 2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016،[1]الّذي حدّد أربع (04) محاكم على المستوى الوطني مع توسيع اختصاصها الاقليمي والتي تتمثّل في محكمة سيدي محمد ، محكمة قسنطينة ، محكمة وهران ، محكمة ورقلةتطبيقا لأحكام المواد 2، 3، 4، 5، وذلك للنّظر بشكل عام في قضايا الجرائم المتعلقة بالمتاجرة بالمخدّرات والجريمة المنظّمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتّشريع الخاصّ بالصّرف.[2]

والظّاهر أنّه وفقا لهذا الاختصاص المحلي لايتمّ النّظر في قضايا الجرائم الإلكترونية بشكل مستقلّ ، بخلاف القطب الجزائي الاقتصادي والمالي والقطب الجزائي الوطني، هذا الأخير الّذي يعمل على مكافحة الجرائم المتّصلة بتكنولوجيا الاعلام والاتّصالحسبما تؤكّدهلنا المادّة 211 مكرر 23 من الأمر رقم 21-11 أنه "يمارس وكيل الجمهورية لدى القطب الجزائي الوطني المختص لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الاقليم الوطني".

ومن المهّم التنويه لتدخّل القطب الجزائي الوطني والقطب الاقتصادي والمالي للنظر في قضايا الجرم ذات الطابع الاقتصادي والالكتروني إمّا حصرا أو على أساس مشترك أو تخويل الاختصاص لأحد القطبين بشكل وجوبي، لنتطرّق لهذه الحالات فيما يلي:

أ -الاختصاص الحصريللقطب الجزائي الوطني لمكافحة الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال:

---

[1]- المرسوم التنفيذي رقم 06-348 مؤرخ في 2006/10/05 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج رعدد 63، المؤرخة في 08 أكتوبر 2006، المعدل والمتمم بموجب المرسوم التنفيذي رقم 16-267 مؤرخ في 2016/10/17، ج ر عدد 62، المؤرخة في 23 أكتوبر 2016.

[2] تنص المادة 2 من المرسوم التنفيذي 06-384 أنه :
يمتدالاختصاصالمحليلمحكمةسيديامحمدووكيلالجمهوريةوقاضيالتحقيقبهاإلىمحاكمالمجالسالقضائيةلـ
الجزائروالشلفوالأغواطوالبليدةوالبويرةوتيزيوزووالجلفةوالمدية والمسيلة وبومرداسوتيبازةوعين الدفلى. وتنص المادة 3 أنه يمتد اختصاص المحلي لمحكمة قسنطينة إلى محاكم المجالس
القضائية:قسنطينةوأمالبواقيوباتنةوبجايةوبسكرةوتبسةوجيجلوسطيفوسكيكدةوعنابةوقالمةوبرجبوعريريجوالطارفوالواديوخنشلةوسوقأهراسو
ميلة، وتنص المادة 4 أنه يمتد الاختصاص المحلي لمحكمة ورقلة إلى محاكم المجالس القضائية
:ورقلةوأدراروتامنغستوإليزيوتندوفوغردايةة، وتنص المادة 5 أنّه يمتد الاختصاص المحلي إلى محاكم المجالس
القضائيةوهرانوبشاروتلمسانوتيارتوسعيدةوسيدبلعباسومستغانمومعسكروالبيضوتيسمسيلتوالنعامةوعينتيموشنتوغليزان. وهو ما تؤكّده المواد 3 و4 و5 من المرسوم التنفيذي رقم 16-267.

يمنح قانون الإجراءات الجزائية المعدّل الاختصاص الحصري للقطب الجزائي الوطني لمكافحة الجرائم المتّصلة بتكنولوجيات الاعلام والاتصال، المنصوص عليها في المادتين 211 مكرر 24 و 211 مكرر 25 منه، وتطبّق عليه الإجراءات المنصوص عليها في المواد 211 مكرّر 19 إلى 211 مكرّر 21 من هذا القانون.[1]

ب -الاختصاص المشترك للقطب الجزائي الوطني لمكافحةالجرائمالمتّصلةبتكنولوجياالإعلاموالاتّصال:

أماالخصوصيّةالّتيتشهدهاالجرائمالالكترونيةبشكلعاموالجرائمالالكترونيةالاقتصاديةبشكلأخصّ،أصبحمنال ضّروريتوحيدالعملبينسلطةالنّيابةوالتّحقيقورئيسذاتالقطبالجزائي،وهو ما تؤكّده المادّة 211 مكرّر 27من الأمر رقم 21-11 المتضمّن قانون الإجراءات الجزائية المعدّل، حيثيمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب، اختصاصا مشتركا مع الاختصاص النّاتج عن تطبيق المواد 37 و 40 و 329 من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيات الاعلام والاتصال والجرائم المرتبطة بها، لتطبّق ذات الإجراءات المنصوص عليها في المواد 211 مكرّر 4 و 15 امام القطب الجزائي الوطني لمكافحة الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال.[2]

ج -**الاختصاص الوجوبي للقطب الاقتصادي والمالي:**

يؤول الاختصاص وجوبا للقطب الاقتصادي والمالي متى تزامن مع اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال طبقا للمادة 211 مكرّر 28، وقد يؤول الاختصاصلمحكمة مقر مجلس قضاء الجزائر، متى تزامن اختصاصه مع اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتّصلة بتكنولوجيات الاعلام والاتصال طبقا للمادّة 211 مكرّر 29 من ق. إ. ج.ج.[3]

2 -**الاختصاص النوعي للقطب الجزائي الاقتصادي والمالي:**

تنصّ المادة 211 مكرّر 2 من الأمر رقم 20-04 أنّه "يمارس رئيس الجمهورية لدى القطب الجزائي الاقتصادي والمالي، وكذا قاضي التحقيق ورئيس ذات القطب اختصاصا مشتركا مع الاختصاص الناتج عن تطبيق المواد 37 و40 و 329 من هذا القانون بالنّسبة للجرائم المذكورة أدناه والجرائم المرتبطة بها".

ليتبيّن من خلال نصّ هذه المادّة أنه تتعدّد الجرائم التي تختصّ بها وكيل الجمهورية، قاضي التحقيق والمحكمة بين جرائم المخدرات والجريمة المنظّمة عبر الحدود الوطنية والجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلّقة بالتّشريع الخاصّ بالصّرف،[4] لنحاول التفصيل في هذه الجرائم كالآتي:

[1] طبقا للمادة 211 مكرّر 26 من الأمر رقم 21-11 المتضمّن قانون الإجراءات الجزائية المعدّل.
[2] طبقا للمادة 211 مكرّر 27 من الأمر رقم 21-11 المتضمّن قانون الإجراءات الجزائية المعدّل.
[3] المادة 211 مكرر 28 و211 مكرر 29 من الأمر 21-11.
[4] حسبما تؤكّده لنا المادة 2/37 والمادة 2/40 والمادة 5/329 من الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية.

أ –الجرائم المنصوص عليها في المواد 119 مكرر و 389 مكرّر و389 مكرر 1 و389 مكرر 2 و389 مكرر 3 من قانون العقوبات:

- جريمة الإهمال:

يعاقب بالحبس من ستة (6)أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 200.000 دج، آل موظف عمومي في مفهوم المادة 2 من القانون رقم 06 –01 المؤرخ في 20 فبراير سنة 2006 والمتعلق بالوقاية من الفساد ومكافحته، تسبب بإهماله الواضح في سرقة أو اختلاس أو تلف أو ضياع أموال عمومية أو خاصة أو أشياء تقوم مقامها أو وثائق أو سندات أو عقود أو أموال منقولة وضعت تحت يده سواء بحكم وظيفته أو بسببها.[1]

- جريمة تبييض الأموال:

تعرف هذه الجريمة أنّها أي فعل يرتكب لإيجاد تبرير كاذب لمصدر الأموال الناتجة بصورة مباشرة أو غير مباشرة عن نشاط غير مشروع، أو يساهم في عملية توظيف أو اخفاء أو تحويل مثل هذه العائدات غير المشروعة، فتهرب هذه الأموال عبر وسائل الكترونية عبر العالم لإدخالها في أنشطة استثمارية كموارد مشروعة،[2]ليعتبر تبييضا للأموال:

أ – تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات، على الإفلات من الآثار القانونية لفعلته.

ب – إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل أنها عائدات إجرامية.

ج– اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها، أنها تشكل عائدات إجرامية.

د– المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه ،[3] وهي ذات السلوكيات التي يجرمها القانون رقم 05–01 المؤرخ في 2005/02/06 المتعلق بالوقاية من تبييض وتمويل الإرهاب ومكافحتهما.[4]

وتوقع على هذه الأفعال المجرّمة عقوبات تتراوح بين عقوبة الحبس والغرامة، حيث يعاقب بالحبس من خمس (05) سنوات إلى عشر (10) سنوات كلّ من قام بتبييض الأموال وبغرامة تقدّر من 1.000.000 إلى 3.000.000 دج، ويعاقب بالحبس من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من

[1] المادة 119 مكرّر من الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة يونيو سنة 1966 المتضمن قانون العقوبات المعدل والمتمم.

[2] ساسي سفيان، الجريمة عابرة للحدود، ملتقى وطني أول حول الجريمة المعاصرة في المجتمع الجزائري، أيام 25/26/27 ماي 2013، كلية العلوم الاجتماعية والانسانية، جامعة الطارف، منشورات جامعة الطارف، 2013، ص 182.

[3] المادّة 389 مكرّر من قانون العقوبات الجزائري.

[4] القانون رقم 05-01 المؤرخ في 2005/02/06 المتعلق بالوقاية من تبييض وتمويل الإرهاب ومكافحتهما، ج. ر عدد 11، المؤرخة بـ 09 فيفري 2005.

4.000.000 دج إلى 8.000.000 دج كلّ من ارتكب جريمة تبييض الأموال على سبيل الاعتياد أو باستعمال التسهيلات التي يمنحها نشاط مهني أو في إطار جماعة ارهابية.[1]

ب الجرائم المنصوص عليه في القانون رقم 06-01 المؤرخ في 20 فبراير 2006 والمتعلق بالوقاية من الفساد ومكافحته:

يختصّ القطب الاقتصادي والمالي النّظر في القضايا المتعلقة بالفساد التي انشرت في الآونة الأخيرة المنصوص عليها في القانون رقم 06-01 المتعلّق بالوقاية من الفساد المتمم بالأمر رقم 05-10 حيث تنصّ المادّة 24 مكرّر 1 منه أنه تخضع الجرائم المنصوص عليها في هذا القانون لاختصاص الجهات القضائية ذات الاختصاص الموسع وفق لأحكام قانون الإجراءات الجزائية،[2] الأمر الذي دفع المشرع الجزائري يؤكّد ذلك بموجب نص المادة 211 مكرّر 2 من الأمر رقم 20-04 المتضمّن قانون الإجراءات الجزائية.

ت الجرائم المنصوص عليها في الأمر رقم 96-22 المؤرخ في 9 يوليو 1996 والمتعلّق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج:

أمام الخطورة الّتي تشهدها الجرائم الاقتصادية المهدّدةلاقتصاد الدولة وأموالها، منها جرائم الصرف وجرائم التحكم في رؤوس الأموال من داخل الجزائر وخارجها، فإنّه يتدخّل القطب الجزائي الاقتصادي والمالي للفصل فيها، تطبيقا لأحكام الأمر رقم 96-22 المتعلّق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج.[3]

ث الجرائم المنصوص عليها في المواد 11 و12 و 13 و 14 و 15 من الأمر رقم 05-06 المؤرخ في 23 أوت 2005 والمتعلق بمكافحة التّهريب:

حدّدت المادّة 211 مكرر 2 الأمر رقم 20-04 المتضمن قانون الإجراءات الجزائية المعدّل، بعض الأفعال المجرّمة التي يختصّ بالنّظر فيها القطب الجزائي الاقتصادي والمالي وهو ما سنوجزهفيما يلي:

- **جريمة التّهريبباستخدام المخازن ووسائل النقل:**

يعاقب بالحبس من سنتين (2) إلى عشر (10) سنوات وبغرامة تساوي عشر (10) مرات مجموع قيمتي البضاعة المصادرة ووسيلة النقل، كلّ شخص يحوز داخل النطاق الجمركي مخزنا معدا ليستعمل في التهريب أو وسيلة نقل مهيّأة خصيصا لغرض التّهريب.[4]

- **جريمة التّهريب باستخدام وسائل نقل:**

---

[1] المادتين 389 مكرّر 1 و2 من قانون العقوبات الجزائري.

[2] الأمر رقم 05-10 المؤرّخ في 26 أوت 2010 يتمّم القانون رقم 06-01 المؤرخ في 20 فبراير 2006 المتعلق بالوقاية من الفساد، ج ر عدد 50 المؤرخة في 01 سبتمبر 2010.

[3] الأمر رقم 96-22 المؤرخ في 23 صفر عام 1417 الموافق 9 يوليو سنة 1996 والمتعلق بقمع مخالفة التشريع والتنظيم الخاصبالصرف وحركة رؤوس الأموال من وإلى الخارج، ج ر عدد 43 المؤرخة في 10 يوليو 1996، المعدّل والمتمم بالأمر رقم 10-03 المؤرخ في 26 أوت 2010، ج ر عدد 50 المؤرخة في 01 سبتمبر 2010.
مع الإشارة أنه يتم معاينة مخالفات التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج في محاضر يحررها الموظفون أو الأعوان طبقا لأحكام المادة 02 من المرسوم التنفيذي رقم 11-34 المؤرخ في 29 يناير 2011 المعدل والمتمم للمرسوم التنفيذي رقم 97-257 المؤرخ في 14 يوليو 1997 الذي يضبط أشكال محاضر معاينة مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج وكيفيات إعدادها، ج.ر عدد 8 المؤرخة في 2011/02/06.

[4] طبقا للمادة 11 من الأمر رقم 05-06 المؤرخ في 23 أوت 2005 والمتعلق بمكافحة التهريب المعدل والمتمم بالقانون رقم 06-20 المؤرخ في 11 ديسمبر 2006.

يعاقب على أفعال التهريب التي ترتكب باستعمال أي وسيلة نقل بالحبس من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة تساوي عشر (10) مرات مجموع قيمتي البضاعة المصادرة ووسيلة النقل.[1]

- **جريمة التّهريب باستعمال سلاح ناري:**

يعاقب بالحبس من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة تساوي عشر (10) مرات قيمة البضاعة المصادرة على أفعال التهريب التي ترتكب مع حمل سلاح ناري.[2]

- **جريمة تهريب الأسلحة:**

يعاقب بالسجن المؤبد كلّ من يهرّب الأسلحة.[3]

- **جريمة التهريب الماسة بالأمن والاقتصاد والصحّة:**

يعاقب بالسّجن المؤبّد كلّ من يرتكب أفعال التهريب على درجة من الخطورة تهدّد الأمن الوطني أو الاقتصاد الوطني أو الصحة العمومية.[4]

ونظرا للدّور الإيجابي الّذي يؤدّيه هذا القطب الجزائي الاقتصادي والمالي، ليحدّد المشرع الجزائري بموجب نصّ المادّة 211 مكرّر 24 من الأمر رقم 21-11 طبيعة هذه الجرائم الّتي يختص بالفصل فيها القطب الجزائي الوطني، بقولها "معمراعاةأحكامالفقرة 2 منالمادة 211 مكرر 22 أعلاه،يختصّوكيلالجمهوريةلدىالقطبالجزائيالوطنيلمكافحةالجرائمالمتّصلةبتكنولوجياتالإعلاموالاتّصالوقاضيالتّحقيقو رئيسذاتالقطبحصريابالمتابعةوالتّحقيقوالحكمفيالجرائمالمتّصلةبتكنولوجياتالإعلاموالاتصالالمذكورةأدناهوكذاالجرائما لمرتبطةبها منها الجرائم التي نكيفها أنها ذات طابع اقتصادي
جرائمالمساسبأنظمةالمعالجةالآليةللمعطياتالمتعلقةبالإداراتوالمؤسّساتالعمومية.

ضف إلى ذلك، يختصّ وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال الأكثرتعقيداوالجرائمالمتصلة بها،على بما أنّ هذه الجريمة يُنظرلها على أساس تعدّد الفاعلين أوالشركاء أو المتضررينأوبسببباتّساعالرقعةالجغرافيةلمكانارتكابالجريمةأوجسامةاثارهاأوالأضرارالمترتّبةعليهاأولطابعهاالمنظمالعا برللحدودالوطنيةأولمساسهابالنظامالعاموالأمنالعموميين،حيثتتطلباستعمالوسائلتحريخاصةأوخبرةفنيةمتخصصةأوالل جوءالتعاونقضائيدولي.[5]

خاتمة:

وفي ختام هذه المداخلة نقول، أنّالجرائم الاقتصادية في ثوبها الجديد، أصبحتمنأهمّالتحدّياتالّتييواجههاأعضاء المجتمعالدولي،نتيجةالأخطار الاجتماعية والسّياسية والاقتصادية

[1] طبقا للمادة 12 من نفس الأمر.
[2] طبقا للمادة 13 من نفس الأمر.
[3] طبقا للمادة 14 من نفس الأمر.
[4] طبقا للمادة 15 من نفس الأمر.
[5] المادّة 211 مكرّر 25 من الأمر رقم 21-11.

الّتيتهدّدجميعالمؤسّساتالوطنيةوالشعوبوالأفراد، أمامنقص خبرة الأجهزة الأمنية والقضائية لمواكبة سرعة تطوّر التكنولوجيا نتيجة نقص المعارف التّقنية، لنستنتج في هذا الشّأن:

– مدى خصوصية الجريمة الالكترونية الاقتصادية وتعقيدها وخطورتهاوسرعةتنفيذهاوصعوبةاثباتها.

–مدى أهميّة انشاء الأقطاب المتخصّصة الاقتصادية والمالية ذات الأولوية في متابعة الجرائم الخطرة بالنّظر إلى نوعيتها، للحدّ من انتشار هذه الجرائم الاقتصادية الالكترونية ذات طابع عابر للحدود الوطنيّة.

– الاختصاص الوطني ل لقطب الجزائي الوطني المختص بمكافحة الجرائم المتّصلة بتكنولوجيات الاعلام والاتصال، في ممارسة صلاحياته.

ومن أهمّ التّوصيات الّتي يُستحسن الأخذ بها:

– نشر ثقافة المعلوماتية وكيفيّة استخدام الحواسيب الآلية.

– نشر التوعية في المجتمعات حول الجرائم الالكترونية ومخاطرها وتعريف الافراد بكيفية الحفاظ على معلوماتهم الخاصة.

– البحث عن سبل للكشف عن الجرائم الالكترونية الاقتصادية، للتقليل من الصعوبة التي تنتابها بخصوص الكشف عنها.

–توجيه وتحديث التّشريعات والقوانين بما يتماشى مع التطوّرات التكنولوجية.

– الزامية تكوين قضاة متخصّصين في الأقطاب الجزائية، وتزويدها بأحدث التقنيات للنظر في قضايا المتعلقة بالجرائم الإلكترونية.

– ندعو نحو انشاء مرصد جزائري لترقّب السلوكات الإجرامية التقليدية بشكل عام والإلكترونية بشكل خاص.

– توحيد نصوص قانون العقوبات الاقتصادي في تقنين مستقل، لتسهيل مهمّة الفصل في القضايا الإجرامية ذات الطّابع الاقتصادي.

– تعزيز أولوية الاختصاص للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والتعاون المشترك مع القطب الجزائي المالي والاقتصادي للفصل في القضايا الإجرامية ذات الطابع المالي والاقتصادي.

– يمارس القطب الجزائي الوطني مهامه على مستوى محلي للنظر في القضايا ذات الطابع الاقتصادي والمالي.

– ضرورة استحداث أقطاب جزائية جهوية على مستوى الوطن لمكافحة الجرائم الالكترونية الاقتصادية.

قائمة المراجع والمصادر:

أولا: الكتب والمؤلفات:

– خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتيّة، دار الفكر الجامعي، مصر، طبعة أولى، 2019.

ثانيا: المذكرات والأطروحات:

– رابح وهيبة، الإجراءات المتبعة أمام الأقطاب الجزائية المتخصصة، أطروحة دكتوراه، تخصص القانون الإجرائي، جامعة مستغانم، 2014–2015.

– رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنيت، مذكرة ماجيستر في القانون العام، جامعة أبي بكر بلقايد تلمسان، 2011–2012.

ثالثا: المقالات العلمية:

– أبو بكر أحمد همام عبد المجيد، الآثار الاقتصادية للجرائم المعلوماتية وسبل مكافحتها، مجلة جامعة جنوب الوادي الدولية للدراسات القانونية، العدد السادس، 2021.

– أمين جابر الشديفات، البطالة وعلاقتها بالجرائم الاقتصادية في العالم العربي (الأردن، السعودية، لبنان، مصر، المغرب)، مجلة دراسات، العلوم الإنسانية والاجتماعية، مجلد 44، عدد 1، 2017.

– بدرة لعور، الآليات المستجدة لمكافحة الجرائم الاقتصادية في التشريع الجزائري (الأقطاب الجزائية الاقتصادية والمالية: استحداث أم تجديد)، مجلة الرسالة للدراسات والبحوث الانسانية، جامعة العربي التبسي المسيلة، مجلد 6، عدد 3، سبتمبر 2021.

– خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني، (دراسة مقارنة)، مجلد 7، عدد 26، 2018.

– شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، عدد 1، يونيو 2020.

– محمد أحمد المشهداني، الجرائم الاقتصادية أنواعها وطرق مكافحتها والوقية منها، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، مجلد 20، عدد 1، 2020.

– مزيود سليم، الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، العدد الأول، أفريل 2014.

– معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة المفكر، جامعة محمد خيضر بسكرة، العدد 17، 2006.

– عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجنائية،مجلة مركز دراسات الكوفة، العراق، العدد السابع، 2008.

– كوثر حازم سلطان، موقف القانون والقضاء من الجريمة الالكترونية (السيبرانية) دراسة مقارنة، مجلة كلية التربية الأساسية، المجلد 22، عدد 96، 2016.

–هامل محمد/ يوسفي مباركة، القطب الجزائي الاقتصادي والمالي كألية لمكافحة جريمة التهريب، المجلة الاكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، مجلد 5، عدد 2، 2020.

– مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، سلطة عمان، مجلة التعاون لدول الخليج العربية.

رابعا: مداخلات علمية:

– بوقال نسيم، تطوّر الجريمة الاقتصادية وأهمّ خصائصها في العصر الحديث، ملتقى حول الجريمة المعاصرة في المجتمع الجزائري، أيام 25–26–27 ماي 2013، كلية العلوم الاجتماعية والانسانية، منشورات جامعة الطارف، 2013.

– ساسي سفيان، الجريمة عابرة للحدود، ملتقى وطني أول حول الجريمة المعاصرة في المجتمع الجزائري، أيام 27/26/25 ماي 2013، كلية العلوم الاجتماعية والانسانية، جامعة الطارف، منشورات جامعة الطارف، 2013.

– كرم سلام عبد الرؤوف سلام، الجرائم الالكترونية في الفقه الاسلامي والقانون العضوي، المؤتمر الدولي العلمي الافتراض 2022، إصدارات المركز الديمقراطي العربي للدراسات الاستراتيجية السياسية والاقتصادية، ألمانيا / برلين.

خامسا: النصوص القانونية:

– الأمر رقم 66–155 المؤرخ في 08 يوليو 1966 المتضمن قانون الإجراءات الجزائية المعدّل والمتمّم.

– الأمر رقم 20–04 المؤرخ في 30 أوت 2020 المعدل والمتمم للأمر رقم 66–155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج. ر عدد 51 المؤرخة في 31 أوت 2020.

– الأمر رقم 21–11 المؤرّخ في 25 أوت 2021 المتعلّقبقانونالإجراءاتالجزائية، ج. ر عدد 65، المؤرخة في 26 أوت 2021.

– الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة يونيو سنة 1966 المتضمن قانون العقوباتالمعدل والمتمم.

– الأمر رقم 05–10 المؤرّخ في 26 أوت 2010 يتمّم القانون رقم 06–01 المؤرخ في 20 فبراير 2006 المتعلق بالوقاية من الفساد، ج ر عدد 50 المؤرخة في 01 سبتمبر 2010.

– الأمر رقم 96–22 المؤرخ في 23 صفر عام 1417 الموافق 9 يوليو سنة 1996 والمتعلق بقمع مخالفة التشريع والتنظيم الخاصبالصرف وحركة رؤوس الأموال من وإلى الخارج ، ج ر عدد 43 المؤرخة في 10 يوليو 1996، المعدّل والمتمم بالأمر رقم 10–03 المؤرخ في 26 أوت 2010، ج ر عدد 50 المؤرخة في 01 سبتمبر 2010.

– الأمر رقم 05–06 المؤرخ في 23 أوت 2005 والمتعلق بمكافحة التهريب المؤرخ المعدل والمتمم بالقانون رقم 06–20 المؤرخ في 11 ديسمبر 2006.

– المرسوم التنفيذي رقم 11–34 المؤرخ في 29 يناير 2011 المعدل والمتمم للمرسوم التنفيذي رقم 97–257 المؤرخ في 14 يوليو 1997 الذي يضبط أشكال محاضر معاينة مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج وكيفيات إعدادها، ج. ر عدد 8 المؤرخة في 2011/02/06.

– المرسوم التنفيذي رقم 06–348 مؤرخ في 2006/10/05 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج رعدد 63، المؤرخة في 08 أكتوبر 2006، المعدل والمتمم

بموجب المرسوم التنفيذي رقم 16-267 مؤرخ في 2016/10/17، ج ر عدد 62، المؤرخة في 23 أكتوبر 2016.

- القانون العضوي رقم 22-10 المؤرخ في 09 جوان 2022 المتعلق بالتنظيم القضائي، ج. ر عدد 41، المؤرخ في 16 جوان 2022.

- القانون رقم 08-09 المؤرخ في 25 فبراير 2008 المتضمن قانون الإجراءات المدنية والإدارية، ج ر عدد 21 المؤرخة في 23 أبريل 2008

- القانون رقم 09-04 مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، ج ر عدد 47 مؤرخة في 16 أوت 2009.

-القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج . ر عدد 71، 2004.

- القانون رقم 05-11 المؤرخ في 17 جويلية 2005 المتعلق بمراقبة مطابقة القانون العضوي المتعلق بالتنظيم القضائي، للدستور، ج ر عدد 51 المؤرخة في 20 يوليو 2005.

- القانون رقم 05-01 المؤرخ في 2005/02/06 المتعلق بالوقاية من تبييض وتمويل الإرهاب ومكافحتهما، ج. ر عدد 11، المؤرخة بـ 09 فيفري 2005.

سادسا: المواقع الالكترونية:

- www.wikipedia.org
-www.oecd.org

مقلاتي مونة
meguellati.mouna@univ-guelma.dz
جامعة 8 ماي 1945 قالمة

إستراتيجية مواجهة الجريمة من خلال خيار المدن الآمنة

مقدمة:

يعد قانون التهيئة والتعمير من بين الوسائل القانونية التي يمكن بموجبها مراقبة وتنظيم حركة البناء وتنظيم الفضاءات في المحيط العمراني للتجمعات السكنية والريفية، وتطوير وتنمية الشبكة العمرانية بشكل متوازن، مع الأخذ بعين الاعتبار جميع المقومات والعناصر الوسيطة للمجال الذي يقع فيه النسيج العمراني، هذا الأخير لن يتحقق بدون تطبيق قواعد تنظيمية للبنايات وأخرى تخطيطية للشوراع وخطوط المواصلات، إذ يجب أن تتوافق عملية البناء مع القواعد الهندسية والمعمارية والقانونية المطلوبة، حفاظا على النظام العام في مجال التهيئة والتعمير بمدلولاته الثلاث: الأمن العام، الصحة العامة، السكينة العامة، ويعد التخطيط في مجال التهيئة العمرانية بصفة عامة، والتعمير بصفة خاصة أسلوبا متبعا للحد من الفوضى العمرانية بإخضاع التوسع الحضري ونمو المدن إلى التخطيط العمراني المدروس، لتنظيم عملية البناء والتعمير وفقا للقواعد المنصوص عليها واحترام مختلف أدوات التهيئة والتعمير، تحقيقا لهذا الغرض أولى المشرع حماية خاصة لعمليات البناء وقيدها بضرورة الحصول على الرخص، حيث يتطلب التخطيط العمراني للمدن توافر مقاييس معينة تتعلق بعرض وطول الشوارع وتنظيمها ، إذ يعد التخطيط المسؤول المباشر عن توفير القاعدة العمرانية لحياة اجتماعية أفضل والحد من مسار حركة الجريمة، وهذا لن يتأتى إلا من خلال دراسة المصمم العمراني والمعماري وفهمه وربطه للمحددات التخطيطية والتصميمية المؤثرة على تحقيق الأمن في الأحياء السكنية، حتى لا يتحول التخطيط إلى سبب رئيسي في ارتفاع معدلات الجريمة وإضعاف الأمن بها، لأن ارتفاع معدلات الجريمة مرتهن بمستوى جودة البيئة العمرانية، إذ يسأل جزائيا كل من يخالف الأحكام المنظمة لرخص البناء، حيث أثبت الواقع العملي حقيقة ارتكاب الكثير من المخالفات، إذ رغم وجود ترسانة قانونية في مجال التعمير إلا أنها لم تحد من تفشي ظاهرة البناءات اللاواعية وغير المشروعية، أو غير المطابقة لمواصفات البناء المطلوبة، مما استوجب على المشرع إعادة النظر بالقواعد الضابطة للتهيئة والتعمير من خلال تضمينها أحكام جديدة وعقوبات صارمة بغرض التصدي لهذه الظاهرة، لخطورة العمليات التي يقوم بها الأشخاص الذين يخالفون أحكام قانون العمران، لذا حرص المشرع على تكييف تلك الأفعال على أنها مخالفات عمرانية توقع المعني تحت طائلة العقوبات المدنية والجزائية

بناءا على ذلك تثار الإشكالية المحورية التي يمكن صياغتها على النحو التالي: **كيف يمكن لجهود مواجهة الجريمة في الوسط الحضري أن تتحقق عبر خيار المدن الأمنة كإستراتيجية تعمل عليها الدول؟**

لمناقشة الإشكالية المطروحة، سيتم تنظيم المادة العلمية المتصلة بالموضوع ضمن محورين، وذلك على النحو التالي

المحور الاول: جرائم رخص البناء ومتابعتها:

بالرجوع لنصوص قانون التهيئة والتعمير 90-29 والمراسيم التطبيقية له، نجد أن المشرع الجزائري حدد جرائم رخص البناء على النحو التالي.

أولا: جرائم رخص البناء:

01: جريمة البناء بدون رخصة:

يقصد بها تنفيذ أشغال أو إستعمال أرض دون رخصة بناء، في مجال يفرض فيه الحصول على رخصة بناء مسبقة كما عرفت بأنها إنشاء مبان جديدة أو إقامة أعمال مثل التعلية والتوسيع أو التعديل أو إجراء تعديلات للواجهة قبل الحصول على رخصة بذلك من الجهة الإدارية المختصة وفقا لما تمليه قوانين التهيئة والتعمير [1]، وقد كيف المشرع الجزائري هذه الجريمة على أنها مخالفة بنص المادة 50 من المرسوم التشريعي 07/94 إذ حدد أقصى عقوبة لها بألفي دج أما القانون رقم 15/08 فأعتبرها جنحة تقوم على ركن شرعي ، مادي ومعنوي وهي كذلك مركبة لأن القانون يستلزم لوقوعها توافر عدة أعمال مادية وقرر لها عقوبة قد تصل إلى الحبس من 06 أشهر إلى سنة مع تشديد الغرامة في حالة العود، كما جرم المشرع من خلال نص المادة 79 من قانون 15/08 المحاولة في إرتكاب جريمة البناء بدون رخصة [2]بقولها: " يعاقب بغرامة .... كل من يشيد أو يحاول تشييد بناية دون رخصة، وتبدأ مرحلة التنفيذ في البناء بدون رخصة بعمليات التهيئة كافتتاح ورشة الحفر واستخدام مواد البناء والآلات الحديثة أو إنجاز حاجز فاصل على محيط العقار المراد البناء عليه، أو وجود عقد مقاولة يتضمن تاريخ البدء في تنفيذ البناء فهذه الأفعال لا لبس في أنها ستؤدي مباشرة إلى البناء [3].

02: جريمة القيام بأعمال بناء غير مطابقة لمواصفات رخصة البناء:

هناك حالات أين يمنح رئيس البلدية رخصة البناء لطالبها، من أجل إنجاز بناية لكن هذا الأخير لا يحترم المخططات والمساحة المحددة في الرخصة، وينجز بناية تختلف تماما عن الرخصة المسلمة له ففي هذه الحالة يعتبر قد ارتكب مخالفة عمرانية[4] عملا بنص المادة 76 مكرر قانون 29/90 التي نصت على أنه:" في حالة التأكد من عدم مطابقة البناء لرخصة البناء المسلمة، يحرر العون المخول قانونا محضر معاينة المخالفة ويرسله إلى الجهة القضائية المختصة، كما ترسل أيضا نسخة منه إلى رئيس المجلس الشعبي البلدي والوالي المختصين في أجل لا يتعدى 72 ساعة"

وتعرف هذه الجريمة على أنها جريمة إقامة الأعمال دون مراعاة الأصول الفنية المقررة قانونا، في تصميم أعمال البناء أو تنفيذها أو الإشراف على التنفيذ أو في متابعة عدم مطابقة التنفيذ للرسومات والبيانات والمستندات التي منح الترخيص على أساسها، أما بالنسبة لمخالفات قرار الترخيص بسبب عدم مراعاة المواصفات التقنية والمادية لمشروع البناء، فقد يكون مثلا بتجاوز معامل شغل الأرضية بنسبتها المئوية

المقررة ، تجاوز معامل شغل الطريق، عدم احترام مستوى الارتفاع المرخص له، إنجاز منفذ بطريقة غير قانونية[5].

03: إنجاز تجزئة أو مجموعة سكنية دون رخصة تجزئة أو تشييد بناية داخل تجزئة لم يتحصل لها على رخصة تجزئة:

بالنسبة لمن ينشئ تجزئة أو مجموعة سكنية دون رخصة، فتتم معاقبته بعقوبة الحبس من 06 أشهر إلى سنتين وبغرامة من 100.000 دج إلى 1000.000 دج وفي حالة العود تضاعف العقوبة، أما الشخص الذي يقوم بتشييد بناية داخل تجزئة لم يتحصل لها على رخصة تجزئة، فيعاقب بغرامة مالية من 100.000 دج إلى 1000.000 دج وفي حالة العود تضاعف الغرامة، إلا أنه بالنسبة للمقاول الذي أنجز الأشغال والمهندس المعماري والمهندس الطبوغرافي أو كل صاحب دراسة الذي أعطى أوامر تسببت في إحدى الجنح سالف ذكرها، فإنه تطبق على من أعطى الأمر العقوبات المذكورة أعلاه [6].

04: مخالفات عدم القيام بإجراءات التصريح والإشهار:

وهي المخالفة التي لا يقوم فيها الجاني بوضع لافتة مرئية من الخارج، توضح مراجع رخصة البناء الممنوحة ونوع البناء وتاريخ افتتاح الورشة والتاريخ المتوقع لإنهاء الأشغال وكذا إسم صاحب المشروع ومكتب الدراسات والمؤسسة المكلفة بالإنجاز [7] والهدف من وضع اللافتة في مكان ظاهر عن الشروع في عمليات البناء هو ضمان قيام المقاول والمهندس بالتنفيذ طبقا لما هو موجود في الرسومات والمواصفات، وهو إجراء يزرع الطمأنينة لدى أصحاب الشأن، ويسمح للهيئات الإدارية المختصة بالمراقبة، وفي حالة عدم وضع لافتة تدل على أشغال إتمام الإنجاز، يعاقب المخالف طبقا لنص المادة 89 من قانون 15/08 بغرامة مالية من خمسة ألاف دج " إلى عشرة ألاف دج وفي حالة العود تضاعف العقوبة.

05: مخالفة الربط غير القانوني لشبكات الانتفاع العمومي بدون رخصة:

ويقصد بها قيام المالك أو المقاول أو القائم بالأشغال بربط البناية بشبكات الإنتفاع العمومي من غاز، كهرباء، مياه الصرف، دون إستخراج رخصة البناء لإقامة البناء، أو دون الحصول على شهادة مطابقة بعد إتمامه من أجل الربط، وقد حدد المشرع العقوبة لهذه المخالفة بموجب نص المادة 88 من قانون 15/08 المتمثلة في الغرامة من خمسين ألف إلى مئة ألف دج، سواء تم إرتكابها من طرف المالك أو المقاول أو القائم بالأشغال وسواء كان الربط مؤقتا أو نهائيا، وعند العود تضاعف الغرامة مع إمكانية إصدار الجهات القضائية أمرا بإعادة الأماكن إلى حالتها الأصلية مع تحمل مرتكبها المصاريف، إضافة إلى هذه المخالفات فقد جرم المشرع من خلال القانون رقم 15/08 بعض التصرفات حفاظا على النظافة العامة والصحة العامة وكذا المظهر الجمالي للمحيط الحضري منها، وضع مواد البناء أو الحصى أو الفضلات في الطريق العمومي[8].

ثانيا: معاينة ومتابعة جرائم رخص البناء:

01- إجراءات معاينة رخص البناء:

جرائم رخص البناء شأنها شأن بقية الجرائم الأخرى المتعلقة بالعمران، تتطلب المعاينة والإثبات ومتابعة مرتكبيها مما يستوجب لأجل قيام دليل بشأنها معاينة الجريمة معاين مادية وإثباتها عن طريق هيئات إدارية تتولى مهمة المحافظة على النظام العام العمراني، من طرف أعوان مؤهلون قانونا لتقصي مخالفات رخص البناء[9].

أ- الأعوان المؤهلون قانونا لمراقبة مخالفات العمران:

نظرا لأهمية مجال الرقابة وسع المشرع دائرة المكلفين بها حتى يتمكن من السيطرة على ظاهرة التعدي على أنظمة التعمير والتشريعات المتعلقة بها، وقد نصت المادة 76 مكرر من قانون 29/90 على هؤلاء كمايلي:

- مفتشو التعمير- أعوان البلدية المكلفين بالتعمير- موظفي إدارة التعمير والهندسة المعمارية- فرق المتابعة والتحقيق- شرطة العمران- أعوان مراقبة المناطق المحمية

ب- السلطات التي يتمتع بها الأعوان المؤهلون لمعاينة جرائم رخص البناء:

*** مراقبة الوثائق:**

يتعين على هؤلاء الأشخاص المؤهلين قانونا لمعاينة مخالفات البناء، أن يقوموا بزيارة الورشات والمنشأت الأساسية والبنايات الجاري إنجازها، وكذا الفحص والمراقبة التي يرونها مفيدة وطلب الوثائق التقنية الخاصة وذلك لأجل معرفة مدى تطابقها مع التشريعات والتنظيم المعمول بهما، ويمكن أن تتم المراقبة ليلا وأثناء أيام الراحة والعطل وتكون بشكل فجائي

***تسخير القوة العمومية للقيام بعملهم:**

يمكن للأعوان المؤهلون قانونا لمعاينة مخالفات البناء والتعمير، الإستعانة بالقوة العمومية" الشرطة، الدرك" لأجل إنجاز مهامهم في حالة عرقلتها وعدم إحترامهم من طرف المواطنين" المادة 76 مكرر 1 من قانون 29/90.

***تحرير محاضر المعاينة:**

تنتهي الزيارة الميدانية لورشات أشغال البناء بتحرير محاضر يتم فيها إثبات مختلف أنواع مخالفات البناء غير القانوني وكل التجاوزات المسجلة إخلال بقواعد التعمير، وعندما ينتهي العون من تحرير محضر المعاينة يقوم بإرساله إلى رئيس المجلس الشعبي البلدي والوالي المختصين في أجل لا يتعدى 72 ساعة من تاريخ تحريره وفي حالة التأكد من عدم مطابقة البناء لرخصة البناء المسلمة، يحرر العون المحضر ويرسله مباشرة إلى الجهة القضائية المختصة، ونسخة أخرى إلى رئيس المجلس الشعبي البلدي أو الوالي المختصين إقليميا في أجل لا يتعدى كذلك 72 ساعة[10]، وفي هذه الحالة تقرر الجهة القضائية المختصة البت في الدعوى العمومية إما الأمر بمطابقة البناء لمواصفات رخصة البناء، أو هدمه كليا أو جزئيا في أجل تحدده وفي حالة عدم امتثال المخالف للحكم الصادر عن العدالة في الآجال المحددة، يقوم رئيس المجلس الشعبي البلدي أو الوالي المختصين إقليميا تلقائيا، بتنفيذ الأشغال المقررة على نفقة المخالف[11].

ثالثا: الجزاءات المترتبة عن البناء بدون رخصة:

1- الجزاء الإداري" الهدم"

منح المشرع من خلال نص المادة 76 مكرر ف 2 من قانون 29/90 لرئيس المجلس الشعبي البلدي والوالي المختصين إقليميا سلطة إصدار قرار إداري بهدم البناء، الذي تم دون رخصة بناء، وهذا في أجل 08 أيام من تاريخ إستلام محضر إثبات المخالفة المحرر من طرف العون المختص، وفي حالة قصور رئيس المجلس الشعبي البلدي عن إصدار قرار الهدم في الأجل المحدد أنفا، تعهد مهمة إصدار قرار الهدم للوالي في أجل لا يتعدى 30 يوما من تاريخ إستلام المحضر المثبت للمخالفة.

02- المتابعة القضائية" تحريك الدعوى العمومية"

أ- تحريك الدعوى العمومية عن طريق النيابة العامة:

للنيابة العامة أن تحرك الدعوى العمومية الناتجة عن جرائم رخص البناء" المادة 18 من المرسوم التنفيذي 55/06 المؤرخ في 30جانفي 2006 المحدد لشروط وكيفات تعيين الأعوان المؤهلين للبحث عن مخالفات التشريع والتنظيم في مجال التهيئة والتعمير ومعاينتها، وكذا إجراءات المراقبة، كما نصت المادة 76 مكرر 5 من قانون 29/90 على أنه:" في حالة التأكد من عدم مطابقة البناء لرخصة البناء المسلمة يحرر العون المخول قانونا محضر معاينة المخالفة ويرسله إلى الجهة القضائية المختصة"

إذ يقوم وكيل الجمهورية بمباشرة الدعوى الجزائية، بعد تلقي محضر المخالفة ويقوم باستدعاء المخالفين مباشرة أمام محكمة الجنح على أساس أن هذه القضايا لا تحتاج إلى تحقيق قضائي كون معاينة هذه المخالفات هي معاينة مادية ، وأغلب المحاضر التي تحتويها لها نماذج محددة قانونا، وتكون صحيحة إلى غاية إثبات عكسها[12].

ب- تحريك الدعوى عن طريق الإدعاء المدني الأصلي:

يمكن الإدعاء مدنيا من طرف أي شخص متضرر من أي جريمة، أمام قاضي التحقيق لكن المشرع الجزائري منح حق الإدعاء في جرائم البناء طبقا لنص المادة 74 من قانون 90-29 لكل جمعية تشكلت بصفة قانونية تنوي بموجب قانونها الأساسي أن تعمل من أجل تهيئة إطار الحياة وحماية المحيط، أن تطالب بالحقوق المعترف بها في مجال التهيئة والتعمير ، فجميع الجمعيات التي تعمل في إطار تهيئة الحياة وحماية المحيط أن ترفع شكوى أمام الجهات القضائية المختصة، إذا لم تقم الإدارة بتحرير محاضر تثبت مخالفات البناء، فلها حق المطالبة بذلك والتأسيس كطرف مدني للمطالبة بالتعويضات عن المخالفات المرتكبة[13]

المحور الثاني: دور البيئة العمرانية في الحد من الجريمة :

إن وضع البرامج والخطط للتعامل مع البيئة العمرانية، سواء بتصميمها أو إعادة تصميمها سوف يؤدي في نهاية المطاف إلى التقليل من فرص ارتكاب الجريمة .

أولا: الحد من حركة دخول المشاة وإقفال الشوارع:

01- الحد من حركة دخول المشاة:

لقد اقترح نيومان لتحقيق بيئة أمنة أربعة عناصر عند التصميم الإنساني الطبيعي وهذه العناصر هي :

01-العمل على اختيار المواقع السكنية الجديدة في مناطق أمنة، إذ يؤدي ذلك إلى انخفاض معدلات الجريمة .

02- تصميم نوافذ المباني السكنية على نحو يمكن السكان من ملاحظة من يتواجد بالخارج[14].

02-إقفال الشوارع:

تزيد الفضاءات شبه العامة من جرائم العنف الشخصي، وخلق بيئة مناسبة للرصد الإجرامي، إذ يكون استعمالها للسكان والغرباء على حد السواء، مما يصعب السيطرة عليها، ويستغلها المجرم كنقطة رصد أو اختباء لارتكاب جريمته[15]لذا فإن استعمال التصميم المعماري والعمراني بكفاءة، مهم لإلغاء المناطق السكنية والفراغات والتشكيلات المكانية، التي تخفض مستوى الأمن وتشجع على حدوث الأنشطة الإجرامية إذ يستطيع المصمم أو العمراني أن يلغي في تصميمه، تلك الفراغات وأن ينشأ بيئة غير مشجعة على ارتكاب الجريمة، كما أنه كلما زاد الترابط الاجتماعي، بين السكان في الحي كلما انخفض مستوى الجريمة به، خصوصا في السكنات الحضرية الجديدة، التي تتجه نحو الفردية والنفعية وضعف التماسك الاجتماعي مما يساعد على تطور الجريمة[16].

ثانيا: مشاركة السكان في المراقبة وتخطيط الموقع:

01-مشاركة السكان في المراقبة:

للسكان دور رئيسي في مكافحة الجريمة والوقاية منها، ذلك أن تلاحم أفراد المجتمع مع جهاز الأمن وتحقيق مستوى لا بأس به من التعاون على نحو يجعل التصدي للجريمة قبل وقوعها والوقاية منها، وبذلك يتضح أن دور السكان لا يقل أهمية عن دور الأمن في تحقيق الحد من الجريمة وإلقاء القبض على مرتكبيها، وتقديمهم للعدالة ، ويمكن تحديد دور السكان في مكافحة الجريمة من خلال:

- اتخاذ احتياطات كفيلة لوقوع الجريمة سواء على أنفسهم أو ممتلكاتهم من خلال الحيطة والحذر واتخاذ التدابير اللازمة لذلك.

-الإبلاغ عن الأشخاص المسيئة فيهم، أو الأشخاص الذين يرتكبون جرائم أو التي يخططون لإرتكابها .

- التعاون مع الأجهزة الأمنية في كشف ما يحيط بالجرائم غير المكتشفة وتزويدهم بالمعلومات والبيانات التي تفيد في إكتشافها والقبض على مرتكبيها..

- التعاون مع الجهات القضائية خاصة في تقديم الشهادة[17]

حيث وجد أن المجرمون يترددون في ارتكاب جرائمهم في المناطق التي يدركون أنها تحت سيطرة مراقبة سكان المنطقة

02- تخطيط الموقع :

إن تخطيط الغرباء والمستخدمين العاديين للفراغ العمراني، يلاحظون ويميزون الإشارات البيئية التي توحي بأن هذا المكان أمن أو غير أمن وإذا توافرت البيئة التي تعطي إشارات عن توفر الأمن، بشكل إيجابي تنتفي الحاجة إلى أجهزة المراقبة ذات التقنية المتقدمة لتوفير الأمن ففاعلية المراقبة تزداد عندما يعرف السكان بعضهم البعض ويربطهم حيز مشترك، ويلعب تخطيط الموقع دورا هاما في المساعدة على المراقبة الطبيعية

من خلال مراعاته مداخل ونوافذ الأبنية، مواقف السيارات والمواد الشفافة والعاكسة التي يمكن أن تحسن الرؤية، ومن الضروري الإشراف على الأماكن الأكثر عرضة للجريمة بأبنية مشغولة في كل الأوقات أو تحوي عددا من الفعاليات والأنشطة في الطوابق الأرضية من خلال وجود نوافذ كبيرة تشرف على الشوارع العادية، وإلغاء الاقبية التي يمكن أن تستخدم لاختباء المرجمين أو هروبهم، كما قد يعرقل الغطاء النباتي الرؤية الجيدة، أو قد يكون عاملا مساعدا وذلك وفقا لموقعه وارتفاع مغروساته [18]

ثالثا:الاهتمام بالجوانب البيئية واستخدام الكاميرات:

01- الاهتمام بالجوانب البيئية:

إن استقرار الفرد مرهون، بإحساسه بالأمن وسلامته في نفسه وماله وحياته وأهله، ورغم أن هناك العديد من الأليات الوقائية والعقابية، المطبقة للحد من الجريمة، إلا أن البيئة العمرانية تؤدي دورا بارزا في التشجيع على حصول الجريمة أو الحد منها، وازدياد حجم قوة الأمن لن يكون له تأثير يذكر على خفض مستوى الجريمة داخل هذه التجمعات، مالم تكن الأحياء مصممة بشكل يساعد على الرفع من مستوى الأمن بها، وتعتبر معالجة الجوانب البيئية، المؤدية لوقوع الجريمة أو المشجعة عليها أو الموفرة للمناخ المناسب لها، أحد الجوانب التي يجب أن تعنى بالاهتمام وتؤخذ بالاعتبار، وقد وجد أن تكاليف التصميم المعماري والعمراني للحد من الجريمة، أقل من تكليف زيادة قوات الأمن. [19]لذ يمكن القول بأن تخطيط وتصميم البيئة السكنية، وطريقة تشكيلها يؤدي دورا هاما وفعالا للغاية في تقوية العلاقات الاجتماعية بين السكان وإحساسهم بالأمن ومشاركتهم الفعالة في إيجاده، وفي تقليص الفرص المتاحة للجريمة، وبالتالي الرفع من مستوى الأمن بالأحياء السكنية، فالبيئة العمرانية المحيطة بالفرد لها دور رئيسي، ذو تأثير مباشر في تشكيل شخصية الفرد وسلوكه، إما إيجابا أو سلبا لذا وجب أن تكون هذه الأخيرة ملائمة لساكنيها ، وهو ما يحتاج إلى تخطيط محكم لتهيئتها بالشكل الآمن والسليم، فارتفاع معدلات الجريمة مرتهن بمستوى جودة البيئة العمرانية، إذ تمثل المناطق العشوائية وغير المخططة بؤرا خصبة لتوليد الجريمة، فالحد من مستوى ارتكاب الجريمة مرتبط بالاهتمام بالجانب العمراني للمدينة جنب إلى جنب مع المجهودات الأمنية، وذلك من خلال متابعة ورصد المستجدات والتحولات في العلاقة بين النواحي الأمنية، وتأثيراتها على عمران المدينة، والعمل على رفع مستوى البيئة العمرانية للأماكن العشوائية، وتحسين ظروف المعيشة فيها، وتفعيل مستوى الرقابة البلدية لتحديد الأجزاء المتدهورة في المدن للحد من الاستيطان العشوائي فيها.[20].

02-إستخدام الكاميرات :

أدى تزايد عدد ساكني المدن إلى تضاعف الاحتياجات اليومية للأفراد، خاصة في ظل كثافة النشطة الاقتصادية والمستويات العالية من الازدحام والأعمال غير المشروعة ، واتضح أنّه لأجل تحسين مستويات السلامة والأمن ينبغي التعامل مع احتمالات حدوث الجرائم ضد الافراد والممتلكات والنظام العام، على مستوى كل شارع، وعلى مدار كل الأوقات، ولتحقيق هذا المبتغى يجري استخدام كاميرات المراقبة بالفيديو، للمساهمة في تكريس الأمن ورصد الجرائم والمساعدة في التحقيقات [21]، وقد زادت الأجهزة الأمنية الجزائرية

من الاعتماد على أنظمة المراقبة بالفيديو لمواجهة الجرائموقد ساعدت كاميرات المراقبة في توقيف عدد من المطلوبين أمنيا، وأيضا في تأمين الممتلكات في التجمعات الحضرية المختلفة.

رابعا–**الفضاء الوقائي ومراعاة الكثافة السكانية والإسكانية:**

01– الفضاء الوقائي:

توجد هناك أنواع من الفراغات والتشكيلات المكانية في الأحياء السكنية مثل المناطق المتوارية والمظلمة، تشجع على حدوث الأنشطة الإجرامية، ويستطيع المعماري المطلع على أسلوب المجرمين، في الإقدام على الجريمة أن يتحاشى في تصميمه تلك الفراغات التي تدعم الأنشطة الإجرامية، فالمجرم في بحث مستمر عن بيئة غير حصينة وغير مشجعة، على ارتكاب الجريمة لذا فإن استعمال التصميم المعماري والعمراني بكفاءة مهم لإلغاء المناطق السكنية المعيبة أو غير الحصينة، فالفضاء الوقائي يعد نموذجا جيدا للحلول التي تمنع الجريمة في البيئة السكنية[22].

02–**مراعاة الكثافة السكانية والإسكانية:**

إنّ الكثافة السكانية هي أحد العوامل التخطيطية المهمة المثيرة للجدل، وذلك لارتباطها بوقوع الجريمة، وأغلب العلماء الاجتماعيين والمخططين العمرانيين، يؤمنون بأن الكثافة والازدحام مرتبطة ارتباطا وثيقا بوقوع الجريمة، حيث ينظرون إلى المناطق السكنية المزدحمة على أنها مناطق ذات معدلات عالية للجريمة ويعتبر المخططون العمرانيون أن الكثافة السكانية والإسكانية، من المواضيع الأساسية والمهمة حيث لها أهمية كبيرة في تهيئة بيئة سكنية صالحة ومريحة ، فلو نظرنا إلى الأمن الاجتماعي داخل المناطق السكنية لوجدنا أن الكثير من الأشخاص يحددون بعض الشروط الرئيسية الواجب توافرها عند اختيارهم سكنا ما، ومن بين تلك الشروط هو مدى مقاومة تلك المنطقة للجرائم ونوع المشكلات الاجتماعية التي تتعرض إليها ومدى استتباب الأمن فيها [23]، ومن خلال ذلك يمكن توظيف عملية التخطيط لخدمة أهداف الأمن الاجتماعي، وبالتالي خدمة المجتمع والتخلص من الانحرافات والعمليات الإجرامية بمعالجتها قبل وقوعها، ولن يتم ذلك إلا بواسطة وضع تصاميم للمناطق السكنية تهدف لإزالة وتقليل العوامل المخلخلة ، وبهذا فإن للمخطط الحضري دورا في عملية المحافظة والمشاركة لخدمة المواطن في توفير الراحة والأمان والإستقرارله[24].

خاتمة:

نصل في نهاية هذه الورقة البحثية إلى القول بأن:

01– رغم وجود المخططات التوجيهية للتهيئة والتعمير، والتي تحدد بوضوح القطاعات القابلة للتعمير وغير القابلة للتعمير، وتحديد مقاييس شغل الأراضي سواء بالمنع أو فرض أشكال معينة لاستغلال الأراضي إلا أنه اتضحت محدودية هذه المخططات التي نتج عنها غياب سياسة عمرانية واعية نتج عنها العديد من المشاكل التي مست النسيج العمراني

02- نلمس اليوم وبكل أسف الآثار السلبية التي تركها انعدام سياسية محكمة في تسيير المدن وأشكال توسعها الداخلي من تعمير مخطط وأخر عشوائي خاصة أمام وجود مماطلة الإدارة وعدم اتخاذها الإجراءات اللازمة لفرض إحترام قواعد العمران.

03- إن عدم فعالية القوانين الزجرية في قطاع العمران وعدم تطبيقها في ظل ضعف التأطير العمراني وعجز المصالح المسؤولة محليا وإقليميا عن الاستجابة للطلب المتزايد عن السكن، فتح المجال لبروز مسلك غير قانوني عبر الحصول على أراضي في إطار تجزئات غير قانونية بمعمار لا يراعي الخصوصيات المحلية، إذ ساهم هذا الأمر في إحتدام المضاربة العقارية لضعف إهتمام الدولة وتدخلها.

04- أمام التجاهل التام لأبسط قواعد التعمير استدعى الأمر ضرورة اضطلاع أجهزة الدولة بالتنظيم العمراني والتهيئة العمرانية، قصد وضع حد للتجاوزات في حركة البناء وفق قواعد مرسومة بعيدا عن أهواء الأفراد لضمان صلاحية المباني من الناحية الفنية والصحية وسلامتها.

05-أمام عجز السلطات العمومية عن الاستجابة لكل الحاجيات السكنية بالرغم من المجهودات التي تقوم بها في الزمان والمكان ، عمدت الإدارة مرغمة تارة ومخيرة تارة أخرى إلى التساهل مع انتشار البناء غير القانوني والذي تتجلى أبرز تداعياته السلبية في تشويه النسيج العمراني وبقاء البناية في شكل ورشة مفتوحة ودائمة لسنوات طويلة.

06- يؤدي سوء التصميم والتخطيط العمراني إلى تأثير كبير على ضعف وفقدان الروابط الاجتماعية بين السكان ، وبالتالي ازدياد الفرص المتاحة لارتكاب مختلف الجرائم.

07- نظرا لخصوصية جرائم رخص البناء وبسبب طابعها المادي والتقني، فقد حرص المشرع أن يتم إثبات المخالفات أيا كانت طبيعتها في شكل محاضر يتم تحديدها من قبل الأعوان المؤهلين قانونا.

07-إن هدف تخطيط أية مدينة، هو خلق بيئة عمرانية اجتماعية متوازنة مطمئنة، أما إذا فقدت المقومات الاجتماعية والفلسفية والمدنية لمفهوم المدينة، أي حصول خطأ في تخطيط استخدامات الأرض وسوء توزيع النشاطات والوظائف الحضرية في المدينة، سيؤدي حتما إلى وقوع نتائج مؤذية للمجتمع الحضري قد تسبب في انهيار عناصر النظام الأمني فيه.

الهوامش

([1])-**سبتي محمد ، رخصة البناء في القانون الجزائري** ، مذكرة ماجيستر فرع الإدارة والمالية، كلية الحقوق ، جامعة الجزائر، 2002، ص: 86.

([2])-بالة عبد العالي، **الدليل العملي في إجراءات تسوية البنايات غير القانونية**، النشر الجامعي الجديد، 2021، ص: 200.

([3])-قزاتي ياسمين، **النزاع الجزائي الناتج عن رخصة البناء بدون رخصة**، دار هومه، 2016، ص: 66.

([4])-بلول فهيمة، متابعة المخالفات العمرانية في مجال البناء، مسؤولية من؟ مجلة القانون والمجتمع، المجلد 09 ، العدد 01، 2021،

([5])-عبد الحليم بن بادة، **مخالفات رخص البناء في التشريع الجزائري بين التجريم والمتابعة الجزائية**، مجلة تشريعات التعمير والبناء، العدد 07 سبتمبر 2018، ص:06

([6])-كيحل سلسبيل، **آليات الرقابة على عمليات البناء في التشريع الجزائري** ، مذكرة ماجيستر فرع الإدارة العامة وتسيير الاقاليم، جامعة الإخوة منتوري قسنطينة، 2015، 2016، ص: 157.

([7])-خمار فاضل، **الجرائم الواقعة على العقار**، دار هومه، الجزائر، 2006، ص: 108.

([8])-بالة عبد العالي، المرجع السابق، ص: 203، 204.

([9])-بوط سفيان، **تجريم أعمال البناء بدون رخصة ودوره في الرقابة على البناء والتعمير** ، مجلة البحوث والدراسات القانونية، العدد 11، ص: 82.

([10])- عبد الحليم بن بادة، المرجع السابق، ص: 16.

([11])- المرجع نفسه، ص: 16

([12])- عبد الحكيم بادة، المرجع السابق، ص: 19.

([13])-بوط سفيان، المرجع السابق، ص: 87.

([14])- بن عايض أحمد عسيري، **المرجع السابق**، ص: 164.
([15])- ريهام عايض، **المرجع السابق**، ص: 49.
([16])- عبد الله بوصنوبرة، جمال حواوسة،**المرجع السابق**، ص: 46.
([17])- محمد السعيد تركي، نسيغة فيصل ، **سياسة الوقاية والمنع من الجريمة**، مجلة البحوث والدراسات ، العدد 01، المجلد 15، 2018، ص: 244.
([18])- ليليان أحمد دلالة، المرجع الاسبق، ص: 450.
([19])-علي بن سالم بن عمر باهمام، **المرجع السابق**، ص:11
([20])- فهد الصالح، **المناطق العشوائية والجريمة** ، جريدة الرياض، مقال منشور بتاريخ 18 يوليو 2020، اطلع عليه بتاريخ : 20 أفريل2022م، متوفر على الربط الإلكتروني: www.alriyadh.com/15811084
([21])-محمد بيضا، **المدن الذكية تحتاج نظام المراقبة الشبكية** ، جريدة البيان منشور بتاريخ 06 يونيو 2015 ، اطّلع عليه يوم : 21-04-2022م، متوفر على الرابط الإلكتروني التالي:
https://www.albayan.ae/economy/companies-businesses/2015-06-06-1.2389804
([22])- علي بن سالم، بن عمر باهمام، المرجع السابق، ص: 13.
([23])-محمد توفيق محمد الحاج حسن، **أهمية ودور الأمن الحضري في الحد من الجريمة في المدن الفلسطينية ، دراسة تحليلية لمدينة** نابلس ، كلية الدراسات العليا، جامع النجاح الوطنية، 2007ن ص: 54.
([24])-**المرجع نفسه، ص: 55.**

العايب سامية
samialaib@hotmail.fr
جامعة 8 ماي 1945 قالمة

لعرابة منال
araba.manel@univ-guelma.dz
جامعة 8 ماي 1945 قالمة

قراءة في أحكام غرامة الصلح كآلية لحماية المستهلك الإلكتروني على ضوء قانون التجارة الإلكترونية 18_05.

A Reading of the provisions of the conciliation fine as a mechanism to protect e-consumer in the light of the E-Commerce Act 05-18.

الملخص

غرامة الصلح وسيلة وقائية غير قضائية جاء بها المشرع الجزائري في قانون التجارة الإلكترونية 18_05 كجزاء يقع على المورد الإلكتروني المرتكب لإحدى مخالفات قانون التجارة الإلكترونية.

تمثل آليةغرامة الصلح أحد تطبيقات العدالة التصالحية، إذ تعد الطريق الفعال لتسوية المخالفة لقانون التجارة الإلكترونية، تعبر أحد أهم بدائل الدعوى العمومية في ظل السياسة الجنائية المعاصرة يترتب وراء إبرامها عدم ملاحقة الشخص المخالف مقابل امتثاله إلى جملة من الشروط المكفولة والمتضمنة بموجب قانونالتجارة الإلكترونية.

الكلمات المفتاحية: غرامة الصلح _ التجارة الإلكترونية_ المستهلك الإلكتروني _ المورد الإلكتروني.

Abstract :

The conciliation fine is a non-judicial preventive method introduced by the Algerian legislator in the E-Commerce Law 05-18 as a penalty for the electronic supplier who commits one of the violations of the E-Commerce Law.

The conciliation fine mechanism represents one of the applications of restorative justice, as it is the effective way to settle the violation of the electronic commerce law. It expresses one of the most important alternatives to the public lawsuit in light of the contemporary criminal policy, the conclusion of which entails the non-prosecution of the violator in return for his compliance with a set of guaranteed conditions included under e-commerce Law.

Keywords: *Conciliation fine - e-commerce - e-consumer - e-supplier.*

مقدمة

لقد أدى التطور التكنولوجي واتساع استخدام شبكة الانترنيت إلى حدوث تغييرات مست جميع المجالات، وامتد استخدام الرسائل الإلكترونية وشبكة الانترنيت إلى المجال الاقتصادي والتجاري ما أدى إلى حدوث تغيرات جوهرية وخلق بيئة أعمال تجارية رقمية، وظهر نمط جديد من أنماط التجارة الذي أطلق عليه بالتجارة الإلكترونية[1].

تعتبر التجارة الإلكترونية [2] من مظاهر ونتائج التحولات التي شهدها العالم منذ التسعينيات في القرن الماضي في شتى المجالات، إذ أصبحت المعاملات التجارية تتم عبر وسائط إلكترونية، فهي تقنية جديدة للبيع أكثر من أي عقد توزيع مواد أو تقديم خدمات [3] ومن ثم أصبحت التجارة الإلكترونية أحد أهم دعائم النظام الاقتصادي العالمي الجديد، وأحد الآليات الهامة التي تعتمد عليها عولمة المشروعات التجارية والإنتاجية[4]، وتبعا لذلك بادر المشرع الجزائري إلى وضع قانون خاص جديد رقم 18_05[5]المؤرخ في 10 ماي 2018 يتعلق بالتجارة الخارجية الذي يحدد القواعد العامة المتعلقة بالتجارة الإلكترونية للسلع والخدمات، الذي يعتبر جديد و مازال في خطواته الأولى، وذلك للمراقبة الفعالة للسوق الالكترونية التي تعرف اضطرابات ناجمة عن حداثة الموضوع بالنسبة للمجتمع الجزائري، وتحديد التزامات و حقوق كل من طرفي عقود التجارة الالكترونية[6].

وقد حدد قانون التجارة الالكترونية الأفعال التي تعتبر مخالفات وحدد عقوبتها، ومنه في حال قيام المورد الالكتروني بأحد هذه الأفعال يتوجب على الأعوان المؤهلين إما إرسال المحضر إلى الجهة القضائية المختصة أو اقتراح غرامة صلح على المخالفين حسب ما جاءت به المادة 45 من قانون التجارة الإلكترونية، والتي تسمح في حالة تسديد مبلغ الغرامة المقترحة بإنهاء النزاع وبالتالي المتابعات القضائية.

ولما كانت المصالحة إجراء قانونيا في مجال الممارسات التجارية الإلكترونية،تتبلور إشكالية الدراسة حول: كيفية تطبيق هذه الطريقة الودية للفصل في مختلف المخالفات المتعلقة بقانون التجارة الإلكترونية؟

---

[1]كمال بلارو، الحماية الجنائية للمستهلك الإلكتروني في ظل التشريع الجزائري، مجلة البحوث في العقود وقانون الأعمال، جامعة منتوري- قسنطينة، العدد 2، ديسمبر2019، الصفحات .73

[2]يقصد بالتجارة الإلكترونية النشاط الذي يقوم بموجبه مور إلكتروني باقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك إلكتروني، عن طريق الاتصالات الإلكترونية.

[3] Philipe, le Tourneau, contrats informatique et électroniques, édition Dalloz référence, 2012-2013, PARIS p371.

[4]عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، مصر، 2015، ص 7.

[5]قانون رقم18-05 المؤرخ في 10ماي2018 المتعلق بالتجارة الالكترونية، جريدة رسمية عدد28، مؤرخةفي 16 ماي 2018.

[6]صبرينة كدام، وسيلة بوحية، غرامة الصلح حماية للمورد الالكتروني من المتابعات القضائية في قانون التجارة الالكترونية، المجلة الجزائرية للعلوم القانونية، السياسية والاقتصادية، مجلد 57، العدد 2، 2020، ص 76.

وبغية الإلمام والإحاطة بجوانب الموضوع وتحليل أبعاده القانونية ومحاولة شرح الإجراءات القانونية ذات الصلة وتبسيطها، استلزم البحث اعتماد المنهج الوصفي والمنهج التحليلي، وذلك بعرض وصفي للظاهرة مع تحليل دقيق للبيانات والمعلومات.

لتحليل إشكالية الدراسة قسم البحث إلى مبحثين إثنين:

المبحث الأول: نطاق تطبيق غرامة الصلح في قانون التجارة الإلكترونية

المبحث الثاني: سير إجراءات غرامة الصلح في قانون التجارة الإلكترونية

المبحث الأول: نطاق تطبيق غرامة الصلح في قانون التجارة الإلكترونية

اهتم المشرع الجزائري بحماية المستهلك الإلكتروني[7] من أشكال الممارسات التجارية غير المشروعة، التي لا تراعي الشروط المطلوبة قانونا في صناعة المنتجات وتسويقها، والتي لا يمكنها أن تعرض المستهلك لمخاطر ومضَار قد لا تحمد عقباها في بعض الحالات، حيث يمكن لهذه التجاوزات أو المخالفات أن تفوت مصلحة المستهلك وتمس باحتياجاته المرعية قانونا وراء عملية الاستهلاك [8]، وقصد تعزيز حماية المستهلك الإلكتروني من أي شكل من أشكال الممارسة غير المشروعة استحدث المشرع آلية غرامة الصلح لحماية المستهلك الإلكتروني من تجاوزات الموردين الإلكترونيين في عرض المنتوج الموجه للاستهلاكوذلك من خلال القانون رقم 18_05 المؤرخ في 16 ماي 2018 المتعلق بالتجارة الإلكترونية.

وبذلك تعتبر آلية غرامة الصلح في مجال الممارسات التجارية إجراء استثنائي، يلتزم من طرفاه باحترام شروطه ولا يجوز لأحدهما تعديلها، كونه إجراء محدد بنصوص القانون وليس من طرف الإدارة المتصالحة [9]، ومن ثم اشترط القانون لإجراء المصالحة في جرائم التجارة الإلكترونيةنطاقا محددا لجواز إجرائه منه ما تعلق بالنطاق الموضوعي (المطلب الأول) ومنها ما تعلق بالنطاق الشخصي (المطلب الثاني).

المطلب الأول: محل غرامة الصلح

نقصد هنا بمحلغرامة الصلح المجال الموضوعي بمعنى آخر الجرائم التي يجوز عليها تطبيق هذه الآلية، وقد حددت المادة 45 من قانون رقم 18_05 المتعلق بالتجارة الإلكترونية محلغرامةالصلح حيث تنصالمادة 45 منالقانونرقم 18-05 علىأنه:

---

[7] المستهلك الإلكتروني هو كل شخص طبيعي أو معنوي يقتني بعوض سلعة أو خدمة عن طريق الاتصالات الإلكترونية من المورد ٱلإلكتروني بغرض الاستخدام الإلكتروني وهذا التعريف جاءت به المادة الثانية من القانون 05/18.

[8] رانية دخير، خصوصية غرامة الصلح في قانون حماية المستهلك وقمع الغش، مجلة القانوني الدولي والتنمية، المجلد 07، العدد 01، جوان 2019، ص 45.

[9] Naar Fatiha, LA TRANSACTION PÉNALE EN MATIÈRE ÉCONOMIQUE, THESE de DOCTORAT EN SCIENCES SPECIALITE, FACULTÉ DE DROIT ET SCIENCES POLITIQUES, DROIT, UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU, 2013, p 35.

"دونالمساسبحقوقالضحاياأوفيالتعويض،تؤهلالإدارةالمكلفةبحمايةالمستهلكبالقيامبإجراءاتغرامةالصلحمعالأشخاصالمتابعينبمخالفةأحكامهذاالقانون.

يجبعلىالأعوانالمنصوصعليهمفيالمادة 36 منهذاالقانوناقتراحغرامةصلحعلىالمخالفين.

لايمكنإجراءغرامةالصلحفيحالةالعودأوالمخالفاتالمنصوصعليهافيالمادتين 37 و38 منهذاالقانون".

أولا: الجرائم المخالفةقانون التجارة الإلكترونية

بالرجوع إلى نصوصقانون رقم 18_05 المتعلق بالتجارة الإلكترونية نجد أن المشرع قد صنف الجرائمالمخالفةلقواعده ووضع العقوبات المقررة في حال ارتكابها وذلكمن خلال المواد من 37 إلى 41وتتمثل في الجرائم التالية:

تعتبر جريمة حسب المادة 37 من قانون التجارة الالكترونية كل من يعرض للبيع، أو يبيع عن طريق الاتصال الالكتروني، المنتجات أوالخدمات المذكورة في المادة 03 من نفس القانون وهي: "لعب القمار والرهان واليانصيب، المشروباتالكحولية والتبغ، المنتجات الصيدلانية، المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أوالتجارية، كل سلعة أو خدمة محظورة بموجب التشريع المعمول به، كل سلعة أو خدمة تستوجب إعدادعقد رسمي".

كما يعتبر جريمة حسب المادة 38 من قانون التجارة الإلكترونية كل مخالفةلأحكام المادة 5 وبالرجوع إلى نص المادة 5 نجدها تنص على أنه : "تمنع كل معاملة عن طريق الاتصالات الإلكترونية في العتاد والتجهيزات والمنتجات الحساسة المحددة عن طريق التنظيم المعمول به، وكذا كلالمنتجات و/أو الخدمات الأخرى التي من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمنالعمومي "[10].

كما تعتبر جريمة من هذا القانون حسب ما جاءت بها لمادة 39 من نفس القانونكل مورد إلكتروني يخالف أحدالالتزامات المنصوص عليها في المادتين 11 و12 من هذا القانون.

كما عاقبت المادة 40 من نفس القانون كل من يخالف أحكام المواد 30،31،32،34 من هذا القانون.

ثانيا: المخالفات الموجبةلغرامة الصلح

بعد التعرض للجرائم المخالفة لقانون التجارة الإلكترونية و باستقراء نص المادة 45 من نفس القانون السابق ذكرها نجد أن المشرع جعل من غرامة الصلح حق للمخالفين حيث أن قانون التجارة الالكترونيةأوجب على الأعوان المؤهلين اقتراحها على المورد الالكتروني المخالف ويبقى قبولها من عدمه اختيارا له.

[10]المادة 05 من قانون رقم 18_05 المتعلق بالتجارة الإلكترونية، المرجع السابق، ص 5.

ويجوز إعمال آلية غرامة الصلحفي كل المخالفات المنصوص عليها في قانون رقم 18_05 المتعلق بالتجارة لإلكترونيةماعدا المخالفات المنصوص عليها في المادتين 37 و38.

إذتستثني المادة 37 من قانون رقم 18_05 المتعلق بالتجارة الإلكترونية المصالحة في حال وجود مخالفات متعلقة بمعاملات لعب القمار والرهان واليانصيب، المشروبات الكحولية والتبغ، المنتجات الصيدلانية، المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية، كل سلعة أو خدمة محظورة بموجب التشريع المعمول به، وبكل سلعة أو خدمة تستوجب إعداد عقد رسمي، كونها معاملات محضورة بموجب المادة 3 من القانون رقم 18-05.

كما تستثنى من المصالحة حسب المادة 38 من القانون 18-05 المتعلق بالتجارة الإلكترونية كل المعاملات المحظورة بموجب المادة 5 من نفس القانون والتي تتعلق بكل معاملة عن طريق الاتصالات الإلكترونية في العتاد والتجهيزات والمنتجات الحساسة المحددة عن طريق التنظيم المعمول به، وكذا كل المنتجات و/أو الخدمات الأخرى التي من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمن العمومي.

المطلب الثاني: أطراف غرامة الصلح

تتمثل أطراف اتفاق غرامة الصلح في مجال قانون التجارة الإلكترونية في كل من الإدارة المتصالحة والمورد الإلكتروني مرتكب المخالفة.

أولا: الأشخاص المرخص لهم بالتصالح مع الإدارة (مرتكب الجريمة)

يعتبر المورد الإلكتروني الشخص المرخص له بالتصالح مع الإدارة في قانون التجارة الإلكترونية فيحال ارتكابه المخالفة من المخالفات المنصوص عليها في القانون المطبق على قانون التجارة الإلكترونية ،وقد عرفت المادة 03 من القانون رقم 18-05المورد الإلكتروني بأنه: "كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توفي السلع أو الخدمات عن طريق الاتصالات الإلكترونية"[11].

لذلك فالأشخاص المرخص لهم بالتصالح مع الإدارة في قانون التجارة الإلكترونية هم كل مرتكب المخالفة من المخالفات المنصوص عليها في القانون المطبق على قانون التجارة الإلكترونية مهما كانت طبيعته سواء شخص طبيعي متمتع بالأهلية الكاملة، أو كان شخص معنوي تابع للقطاع العام أو للقطاع الخاص فإنه يمكن التصالح مع الإدارة بواسطة الممثل الشرعي له، وحتى يستفيد مرتكب جريمة الممارسات التجارية الإلكترونية من المصالحة يجب أن لا يكون في حالة عود وهذا شرط نصت عليه المادة 45فقرة 03

[11] المادة 03 من القانون رقم 18_05، المرجع السابق، ص 5.

من القانون 18-05 السالف الذكر على أنه: "... لا يمكن إجراء غرامة الصلح في حالة العود أو المخالفات المنصوص عليها في المادتين 37 و38 من هذا القانون".

يعد في حالة عود كل من يكرر نفس الجريمة خلال مدة لا تتجاوز 12 شهرا من تاريخ العقوبة المتعلقة بالجريمة السابقة ويضاعف حينها مبلغ الغرامة حسب ما جاءت به المادة 48 من قانون 18-05.[12]

ثانيا: الجهة المؤهلة لإجراء غرامة الصلح

يخول المشرع الجزائري بنص المادة 45 من القانون 18-05 السابق ذكره للإدارة المكلفة بحماية المستهلك إمكانية فرض غرامة الصلح في حالة وجود مخالفة لأحكام هذا القانون، وقد حددت المادة 36[13]من هذا القانون الجهة المكلفة بفرض غرامة الصلح المتمثلة في الجهة المؤهلة لمعاينة مخالفات أحكام هذا القانون وهم: ضباط وأعوان الشرطة القضائية المنصوص عليهم في ق.إ.ج، وكذا الأعوان المنتمون للأسلاك الخاصة بالرقابة التابعون للإدارة المكلفة بالتجارة.

أ) ضباط وأعوان الشرطة القضائية

وتجدر الإشارة إلى أن المادة 15 من قانون الإجراءات الجزائية[14] قد حدد الأشخاص التي تتمتع بصفة الضبطية القضائية كالآتي:

-رؤساء المجالس الشعبية البلدية،

- ✓ ضباط الدرك الوطني،
- ✓ الموظفون التابعون للأسلاك الخاصة للمراقبين، ومحافظي وضباط الشرطة للأمن الوطني،
- ✓ ضباط الصف الذين أمضوا في سلك الدرك ثلاث (3) سنوات على الأقل، وتم تعيينهم بموجب قرار مشترك صادر عن وزير العدل حافظ الأختام، ووزير الدفاع الوطني، بعد موافقة لجنة خاصة .
- ✓ الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ وأعوان الشرطة للأمن الوطني الذين أمضوا ثلاث (3) سنوات على الأقل بهذه الصفة والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية، بعد موافقة لجنة خاصة،

[12]تنص المادة 48 من قانون رقم 18_05 على أنه: " يضاعف مبلغ الغرامة في حالة تكرار نفس الجريمة خلال مدة لا تتجاوز اثني (12) شهرا من تاريخ العقوبة المتعلقة بالجريمة السابقة".

[13]المادة 36 من قانون رقم 18_05 المتعلق بالتجارة الإلكترونية، المرجع السابق، ص 9.

[14]قانون الإجراءات الجزائية الصادر بموجب القانون رقم 155/66 المؤرخ في 1966/03/04 والمتمم بالأمر رقم 15-12 المؤرخ في 28 يوليو سنة 2015، جريدة رسمية العدد 41، الصادر في 19 يوليو 2015.

- ✓ ضباط وضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع ووزير العدل.

أما المادة 19 من نفس القانون فقد حددت من يتمتع بصفة الضبط القضائي وهم:

- ✓ موظفو مصالح الشرطة وضباط الصف في الدرك الوطني ومستخدمو المصالح العسكرية للأمن الذين ليست لهم صفة ضباط الشرطة القضائية.

أ) الأعوان المنتمـون إلى الأسلاك الخاصة بالرقابة التابعون للإدارات المكلفة بالتجارة

حيث تم تنظيم مهام هذه الفئة بمقتضى المرسوم التنفيذي رقم 09_415[15] المؤرخ في 16 ديسمبر 2009 يتضمن القانون الأساسي الخاص المطبق على الموظفين المنتمين للأسلاك الخاصة بالإدارة المكلفة بالتجارة، وحسب المادة 02 من المرسوم السابق [16] ذكره تعتبر الأسلاك الخاصة بالرقابة التابعون للإدارات المكلفة بالتجارة، الأسلاك المنتمية إلى الشعبتين الآتيتين:

_ شعبة قمع الغش[17]،

_ شعبة المنافسة والتحقيقات الاقتصادية[18].

المبحث الثاني: سير إجراءات غرامة الصلح في قانون التجارة الإلكترونية

لكل نظام قانوني نطاقه الخاص الذي يطبق فيه، وكذلك هو الحالبالنسبة للمصالحة في المواد التجارية عامة وفي قانون التجارة الإلكترونية خاصة، لها نطاق قانوني لا تتجاوزه، ويظهر ذلك من خلالتحديد المراحل التي يمر بهاإجراءالمصالحة (المطلبالأول)،وما يترتب عن هذا الإجراء من آثار (المطلب الثاني).

المطلب الأول: مراحل فرض غرامة الصلح

[15] مرسوم تنفيذي رقم 09-415 مؤرخ في 29 ذي الحجة عام 1430 الموافق ل 16 ديسمبر سنة 2009، يتضمن القانون الأساسي الخاص المطبق على الموظفين المنتمين للأسلاك الخاصة بالإدارة المكلفة بالتجارة، ج ر ج عدد 20، المؤرخ في 20 ديسمبر 2009.

[16] المادة 3 من المرسوم التنفيذي رقم 09_415 السابق ذكره، ص 21.

[17] تضم شعبة قمع الغش حسب المادة 4 من المرسوم أعلاه الأسلاك الآتية:

- سلك مراقبي قمع الغش، عن طريق الزوال،
- سلك محققي قمع الغش،
- سلك مفتشي قمع الغش.

[18] تضم شعبة المنافسة والتحقيقات الاقتصادية حسب المادة 5 من المرسوم أعلاه الأسلاك الآتية:

_ سلك مراقبي المنافسة والتحقيقات الاقتصادية، عن طريق الزوال،

_ سلك محققي المنافسة والتحقيقات الاقتصادية،

_ سلك مراقبي المنافسة والتحقيقات الاقتصادية.

لما كانت المصالحة إجراء قانونيا في مجال الممارسات التجارية الإلكترونية، تجري المصالحة في حال مخالفة قواعد قانون التجارة الإلكترونية 18_05 عن طريق إجراءات معينة حددها القانون وهي: الإجراءات المتعلقة باقتراح غرامة الصلح(الفرع الأول)، الإجراءات المتعلقة بتحصيل غرامة الصلح(الفرع الثاني).

الفرع الأول: الإجراءات المتعلقة باقتراح غرامة الصلح

في حالة ثبوت إحدى المخالفات المذكورة في هذا القانون ماعدا المخالفات المنصوص عليها في المادتين 37 و38 من هذا القانون، وجب على الجهة المؤهلة لمعاينة مخالفات أحكام هذا القانون اقتراح غرامة صلح مع المخالفين.

وبالرجوع إلىالفقرةالأخيرمنالمادة 45 منننفسالقانون يفهم من خلالاستعمالهامصطلح " يجب" أنالأعوانمجبرينعلىاقتراحغرامةالصلحعلىالمخالفينحيثأنالصلحفيهذهالحالةيعتبرحقللمخالفينيجبعلىالأعوانقتراحهولهمال حقوالحريةفياللجوءاليهأوتركه.

ويحددالأعوانالمؤهلينعندتحريرالمحضرمبلغالغرامةبالرجوعإلىالمخالفةالمعاينةوبحضورالمخالفالذييمكنهأنيمار سالحقالمخولله،بعدالإحاطةالكاملةبكلالوقائع،بقبولأورفضالمبلغالمقترح،مبلغغرامةالصلح[19].

وقد حددت المادة 46 من نفس القانون أن مبلغ غرامة الصلح يمثل الحد الأدنى من الغرامة المنصوص عليها في أحكام هذا القانون، وفي حالة قبول المورد الالكتروني لغرامة الصلح، تقوم الإدارة المؤهلة بتخفيض 10%.[20]

الفرع الثاني: الإجراءات المتعلقة بتحصيل غرامة الصلح

تبلغ المصالح التابعة لإدارة الجمارك المورد الإلكتروني المخالف خلال مدة لا يتعدى (7) أيام ابتداءا من تاريخ تحرير المحضر، الأمر بالدفع عن طريق جميع الوسائل المناسبة مصحوبا بإشعار بالاستلام، يتضمن هوية المرد الإلكتروني، عنوان بريده الإلكتروني، وتاريخ وسبب المخالفة، ومراجع والنصوص المطبقة ومبلغ الغرامة المفروضة بالإضافة إلى مواعيد وكيفيات الدفع.

استنادا إلى نص المادة 47 من القانون رقم 18-05 السابق ذكره إذا لم يتم دفع الغرامة أو لم يمتثل المخالف للأحكام التشريعية والتنظيمية المعمول بها في أجل 45 يوما، يرسل المحضر على الجهة القضائية المختصة.

المطلب الثاني: الآثار المترتبة عن فرض غرامة الصلح

[19] صبرينة كدام، وسيلة بوحية، المرجع السابق، ص 83.

[20] المادة 46 من القانون رقم 18-05، ص 10.

لاشك أن الفائدة من غرامة الصلح في مادة قانون التجارة الإلكترونية تكمن في الآثار الهامة التي تترتب عنها حينما تتم صحيحة، ولعل أهم أثر يسعى إلى تحقيقه طرفي المصالحة هو حسم النزاع دون اللجوء إلى القضاء[21].

فبعد تمام إجراءات غرامة الصلح في مادة قانون التجارة الإلكترونية تصدر الجهة المكلفة بفض غرامة الصلح قرار نهائي يترتب عنه جملة من الآثار، وعليه نتناول في هذا الصدد آثار غرامة الصلح بالنسبة لأطرافها (الفرع الاول)، ثم نتطرق إلى آثار غرامة الصلح بالنسبة للغير.

الفرع الأول: الأثار المصالحة بالنسبة لأطراف الخصومة

يترتب على غرامة الصلح في حال إبرامها صحيحة، وفق ما تم النص عليه في القواعد القانونية والتنظيمية عدة آثار بالنسبةلأطرافه ولعل أهمها تتمثل في حسم وإنهاء النزاع ويترتب على ذلك نتيجتين أساسيتين تمثلتا في أثرين:

أولا: أثر الانقضاء

لمينص القانون صراحة في نصوص قانون التجارة الإلكترونية على انقضاء الدعوى العمومية بالصلح ولكن من خلال ما ذكر في المادة 47 منهوبمفهوم المخالفة إذا تم دفع الغرامة واحترام الأحكام القانونية لا يرسل المحضر إلى الجهة القضائيةوتنقضي الدعوى العمومية، وزيادة على ذلك فالمصالحة حسب القوانين الجزائية تؤدي إلى انقضاء الدعوى العمومية، سواءتمت قبل المتابعة القضائية أو بعدها أو حتى بعد صدور حكم قضائي ما لم يحز على قوة الشيءالمقضي فيه، فإذا تمت المصالحة قبل إحالة الملف على وكيل الجمهورية، يحفظ الملف على مستوىالإدارة المعنية، أما إذا حصلت المصالحة بعد إرسال الملف إلى وكيل الجمهورية ، فالأمر يختلف حسبالمرحلة التي وصلت إليها الإجراءات[22].

ثانيا: أثر التثبيت

تؤدي المصالحة الجزائية إلى تثبيت الحقوق سواء تلك التي اعترفت بها المؤسسة المخالفةللإدارة، أو تلك التي اعترفت بها الإدارة للمؤسسة المخالفة، وغالبا ما يكون أثر تثبيت الحقوقمقصور على الإدارة ذلك أن آثار الصلح النسبة للإدارة تتمثل أساسا في الحصول على غرامة الصلحالتي تم الاتفاق عليها، وحينئذ تنتقل ملكيتها إلى الإدارة بالتسلم فيتحقق بذلك الأثر الناقل للمصالحة[23].

---

[21] مونية مسمة، المصالحة في مادة الممارسات التجارية، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون العام للأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي، جيجل، 2010-2011، ص 53.

[22] صبرينة كدام، وسيلة بوحية، المرجع السابق، ص 84.

[23] أحسن بوسقيعة، المصالحة في المادة الجزائية بوجه عام وفي المادة الجمركية بوجه خاص، دار هومة، الجزائر، 2013، ص ص 286-287

الفرع الثاني: أثار المصالحة بالنسبة للغير

تتفق التشريعات الجزائية التي تجيز المصالحة على حصر آثار المصالحة في المخالف مع الإدارة وحده، ولا يمتد أثرها للفاعلين الآخرين الذين ارتكبوا معه نفس المخالفة ولا إلى شركائه، تثور التساؤل هنا حول ما إذا كان آثار المصالحة ذات تطبيق نسبي تشمل أطرافها دون أن تتعدى أثارها إلى الغير مثلما هو معمول به في بقية التشريعات التي تجيز المصالحة أم تنصرف آثارها أيضا للغير بالنسبة لقانون التجارة الإلكترونية؟

أولا: لا ينتفع الغير من المصالحة.

يقصد بالغير في مجال قانون التجارة الإلكترونية الفاعلون والشركاء فما مدى تطبيق قاعدة عدم انتفاع الغير بالمصالحة بالنسبة لجرائم مخالفة قواعد انون التجارة الإلكترونية على الفاعلين الآخرين والشركاء؟

كأصل عام، فإن التشريعات الجزائية تحصر آثار المصالحة في المؤسسة المتصالحة مع الإدارةبحيث لا تنصرف هذه الآثار للغير والذي يقصد به الفاعلون الآخرون والشركاء[24].

ولذا فإن المصالحة التي تتم مع إحدى المؤسسات المخالفة لا تقف حائلا أمام متابعة مؤسسة أخرى ساهمت أو شاركت مع الأولى في ارتكاب المخالفة.

ثانيا: لا يضار الغير من المصالحة.

إذا كان الغير لا ينتفع بالمصالحة فإنه في ذات الوقت لا يلحقه ضررا من إجرائها، حيث أنه مع لا ينصرف أثر المصالحة إلا بالنسبة لعاقديها [25]،فإذا تصالحت إحدى المؤسسات مع الإدارة، فإن شركائها لا يلتزمون بما يترتب عن تلكالمصالحة من آثار في ذمة المؤسسة التي أبرمتها، حيث لا يجوز للإدارة الرجوع على أي منهم عندإخلال المؤسسة المتصالحة بالتزاماتها. كما أنه لا يمكن للإدارة أن تحتج باعتراف المؤسسة التيتصالحت معها بارتكابها المخالفة المنسوبة إليها لإثبات تورط شركائها فمن حق هؤلاء نفي الجريمةعنهم بكل طرق الإثبات ولا يكون للضمانات التي قدمتها المؤسسة المتصالحة مع الإدارة أي أثر علىباقي المؤسسات المخالف.

أما بالنسبة للمضرور من جريمة المرتكبة فإن السؤال يثور حولإمكانية حقه في المطالبة بالتعويض أم لا؟ من حق المضرور الحصول على تعويض اللازم لإزالة الضررالذي أصابه بسبب المخالفة وبما أنه لم يكن

[24]أحسن بوسقيعة، المنازعات الجمركية (تصنيف الجرائم ومعاينتها–المتابعة والجزاء)، الطبقة الثانية، دار هومه للطباعة والنشر والتوزيع، الجزائر 2005،ص296.

[25]عمر عدوني، المصالحة في المادة الجمركية، مذكرة لنيل شهادة الماجستير في القانون، فرع منازعات جمركية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، 2013–2014، ص 164.

طرفا في هذه المصالحة فهي لا تلزمه ولا تسقط حقه فيالتعويض وله أن يلجأ للقضاء لاستيفائه، ونتيجة لهذا، فقد منحه المشرع الحق في اللجوء إلى القضاءالمدني وذلك بموجب المادة 45 من القانون 18_15[26].

خاتمة

ختاما عما سبق التقدم به، تهدف إجراء غرامة الصلح إلى توجيه السياسة العقابية من طابعها الردعي إلى تسوية النزاع القائم بين أطراف الدعوى العمومية بإنهاء الدعوى العمومية بطرق رضائية بسلك طريق الإصلاح، وبالتالي الخروج قليلا عن المسالك المعتادة لتوقيع الجزاء الجنائي.

من خلال ما تمّ تحليله باقتضاب في هذه الدراسة **توصلنا إلى أهم النتائج التالية:**

– تعد غرامة الصلح حق للمخالفين حيث أن القانون التجارة الالكترونية يجب الأعوان المؤهلين

على اقتراحها للمورد الالكتروني المخالف ويبقى قبولها من عدمه اختيارا له.

_ لا يمكن فرض غرامة الصلح على كل المخالفات فقد منع القانون رقم 18_05 صراحة التصالح في حالة العود وفي حالةالمخالفات المتعلقة بمعاملات لعب القمار والرهان واليانصيب، المشروبات الكحولية والتبغ، المنتجاتالصيدلانية، المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية، كل سلعة أو خدمةمحظورة بموجب التشريع المعمول به، وبكل سلعة أو خدمة تستوجب إعداد عقد رسمي، كذلك استثنى منالمصالحة كل معاملة عن طريق الاتصالات الإلكترونية في العتاد والتجهيزات والمنتجات الحساسةالمحددة عن طريق التنظيم المعمول به، وكذا كل المنتجات و/أو الخدمات الأخرى التي من شأنهاالمساس بمصالح الدفاع الوطني والنظام العام والأمن العمومي.

– لم ينص القانون صراحة في نصوص قانون التجارة الإلكترونية على انقضاء الدعوى العمومية بالصلح ولكن من خلال ما ذكر في المادة 47 منه وبمفهوم المخالفة إذا تم دفع الغرامة واحترام الأحكام القانونية لا يرسل المحضر إلى الجهة القضائية وتنقضي الدعوى العمومية.

– منح المشرع للضحاياالحقفي التعويض من خلال اللجوء إلى القضاء المدني وذلك بموجب المادة 45 من القانون 18_15 كاستثناء نص عليه سوى هذا القانون.

انطلاقا مما تم تسجيله من نتائج نقترح **أهم التوصيات التي قد تسهم في تفعيل آلية غرامة الصلح والتي يمكن حصرها في:**

– تأهيل أعوان مخصصة لمتابعة إجراءات المصالحة غير الأعوان المعاينون للمخالفة.

[26] صبرينة كدام، وسيلة بوحية، المرجع السابق، ص ص 85–86.

– إنشاء هيئة قضائية أو قضاء مستقل للنظر فقط في المنازعات التي تنشأ بمناسبة المخالفاتالمتعلقة بالممارسات التجارية، وذلك بسبب كثرة ملفات المتابعات على مستوى المحا كم ._

قائمة المصادر والمراجع

القوانين:

– قانون الإجراءات الجزائية الصادر بموجب القانون رقم 155/66 المؤرخ في 1966/03/04 والمتمم بالأمر رقم 15–12 المؤرخ في 28 يوليو سنة 2015، جريدة رسمية العدد 41، الصادر في 19 يوليو 2015.
– قانون رقم18–05 المؤرخ في 10ماي2018 المتعلق بالتجارة الالكترونية، جريدة رسمية عدد 28، مؤرخة في 16 ماي 2018.
– مرسوم تنفيذي رقم 09–415 مؤرخ في 29 ذي الحجة عام 1430 الموافق ل 16 ديسمبر سنة 2009، يتضمن القانون الأساسي الخاص المطبق على الموظفين المنتمين للأسلاك الخاصة بالإدارة المكلفة بالتجارة، ج ر ج عدد 20، المؤرخ في 20 ديسمبر 2009.

الكتب:

– أحسن بوسقيعة، المنازعات الجمركية (تصنيف الجرائم ومعاينتها–المتابعة والجزاء)، الطبقة الثانية، دار هومه للطباعة والنشر والتوزيع، الجزائر 2005.
– أحسن بوسقيعة، المصالحة في المادة الجزائية بوجه عام وفي المادة الجمركية بوجه خاص، دار هومة، الجزائر، 2013.

–عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، مصر، 2015.

المقالات:

– رانية دخير، خصوصية غرامة الصلح في قانون حماية المستهلك وقمع الغش، مجلة القانوني الدولي والتنمية، المجلد 07، العدد 01، جوان 2019.

– صبرينة كدام، وسيلة بوحية، غرامة الصلح حماية للمورد الالكتروني من المتابعات القضائية في قانون التجارة الالكترونية، المجلة الجزائرية للعلوم القانونية، السياسية والاقتصادية، مجلد 57، العدد 2، 2020.

– كمال بلارو، الحماية الجنائية للمستهلك الإلكتروني في ظل التشريع الجزائري، مجلة البحوث في العقود وقانون الأعمال، جامعة منتوري–قسنطينة، العدد 2، ديسمبر2019.

الرسائل العلمية:

- عمر عدوني، المصالحة في المادة الجمركية، مذكرة لنيل شهادة الماجستير في القانون، فرع منازعات جمركية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، 2013-2014، ص 164.
- مونية مسمة، المصالحة في مادة الممارسات التجارية، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون العام للأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي، جيجل، 2010-2011، ص 53.

مراجع باللغة الأجنبية:

- Philipe, le Tourneau, contrats informatique et électroniques, édition Dalloz référence, 2012-2013, PARIS.

- Naar Fatiha, LA TRANSACTION PÉNALE EN MATIÈRE ÉCONOMIQUE, THESE de DOCTORAT EN SCIENCES SPECIALITE, FACULTÉ DE DROIT ET SCIENCES POLITIQUES, DROIT, UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU, 2013, p 35.