تاريخ استقبال المقال: 25-02-2018 تاريخ قبول نشر المقال: 09-05-2018 تاريخ نشر المقال: 2018/7/10

النظـــام القانونـــي للجريمـــة المعلوماتيـــة و صعوبات تحقيق الأمن الإلكتروني

فريجــة محمــد هشام
كليــة الحقــوق والعلوم السياسية
جامعة المسيلة- الجزائر
E.mail: hichem.fridja@yahoo.fr

الملخّــص:

تعتبر كل من الأنترنيت، شبكات الكمبيوتر وأنظمة المعالجة الآلية للمعطيات، مجالاً خصباً لارتكاب العديد من الجرائم في مختلف الأقاليم، كالجرائم المعلوماتية وجرائم الكمبيوتر، والتي تستعمل فيها كل من وسائل الكمبيوتر وشبكات الأنترنيت، بهدف سرقة المعلومات الشخصية للأفراد والشركات، وارتكاب جرائم إلكترونية أخرى. ومنه فهذا المقال يهدف إلى دراسة الجريمة المعلوماتية وتوضيح خصائص هاته الجريمة، وكذا تبيان مختلف العراقيل التي تمنع مكافحة هاته الجرائم.

الكلمات المفتاحية: الأمن الإلكتروني-شبكة الأنترنيت – جهاز الكمبيوتر– الجريمة المعلوماتية – نظام المعالجة الآلية للمعطيات.

Résumé :

L'internet, les réseaux informatiques et les systèmes de traitement automatique des données, offrent une nouvelle opportunité de commettre de nombreuses activités criminelles dans de nombreux pays, comme les cyber-crimes et les délits informatiques, qui sont des actes criminels visant les ordinateurs et les réseaux, en vue de pirater les informations privées d'une entreprise, individu, ou commettre d'autres crimes informatiques. Cet article a pour but de définir le Crime électronique, de clarifier ses caractéristiques et de nous montrer les déférents obstacles pour combattre ce fléau.

Mots clés : Sécurité électronique - Réseau d'internet - Informatique - Cybercriminalité - Systèmes de traitement automatique des données.

Abstract:

The Internet, computer networks, and the automatic data processing systems, presents an enormous new opportunity for committing many criminal activities in many

countries, such as cyber crimes and computer crimes, wich are a criminal acts dealing with computers and networks, in order to steal a company's or individual's private information, or to do other computer crimes. this article aimes to defin the Electronic Crime and clarify its characteristic and to show us the deferent obstacles to fight this scourge.

Keywords: Electronic security- Internet network - Computer- cyber crime - Automatic data processing systems.

مقدمة :

أضحت الجريمة تهدد الاستقرار والأمن العالميين وليس فقط الأمن الداخلي، نتيجة لتشعبها عبر الحدود الوطنية، وذلك نظرا لظهور أنماط جديدة أو مستحدثة لم يعرفها العالم من قبل، حيث أصبح المجرمون يستغلون مختلف الوسائل التي أنتجها هذا العصر في تطوير وتوسيع نشاطاتهم الإجرامية، ومن بين ما يستعملونه كوسائل لارتكاب جرائمهم، شبكات الأنترنيت وأجهزة الكمبيوتر.

1/ أهمية الدراسة:

لقد أدى الاستخدام المتزايد للأنظمة المعلوماتية وأجهزة الكمبيوتر، إلى كثير من المخاطر رغم ما حققته من فوائد جمّة وعظيمة في مجال الرقي والتقدم التكنولوجي والإنساني وتتمثل هذه المخاطر في إمكانية تدمير برامجه وبياناته أو معرفة أسرارها والاحتيال عليها أو إتلافها وهو ما يطلق بالإجرام المعلوماتي.

ولذلك فإن أهمية الدراسة تكمن في تناولها لظاهرة مستحدثة وهي ظاهرة جرائم التطور الإلكتروني، التي تهدد أمن واستقرار المجتمع بل العالم بأسره، خاصة وإن علمنا بأن عمليات التعارف على شبكة المعلومات الدولية أدت إلى حدوث جرائم الانتحار الجماعي التي نفذها بعض المراهقين في أمريكا، وكذا مختلف الدول العربية، هذا بالإضافة إلى جرائم خطف

الأشخاص والطلاق والسرقة والتهديد والقذف وتشويه السمعة وغيرها من الجرائم التي وقعت في مختلف بلدان العالم، إلاّ أنه سوف نركز في دراستنا هذه على مختلف الجهود المبذولة، من أجل وضع حد لارتكاب مثل هاته الجرائم، التي أصبح من السهل تحقيق نتيجتها وسط هذا العالم الرقمي الافتراضي.

2/ أسباب اختيار الدراسة:

تطورت الجريمة المرتكبة عبر الأنترنيت بشكل رهيب في الآونة الأخيرة، وذلك للتطور المستمر والمتسارع لشبكة الأنترنيت، مما جعل هذه الشبكة سبب ووسيلة مثالية لتنفيذ العديد من الجرائم بعيدا عن مرأى الجهات الأمنية، مما دعا بها إلى إفراز نماذج جديدة من السلوك الإجرامي الإلكتروني، تبدو النصوص القائمة والتي وضعت لمواجهة الجريمة في ثوبها التقليدي، عاجزة عن أن تواجه هذه الجرائم المعلوماتية المستحدثة، والتي يرجع العامل الأكبر في ظهورها إلى تزايد وتنامي الاستعمال للحاسب الآلي وشبكاته وتطبيقاته، واستعمال الشبكة المعلوماتية في كافة المجالات الاقتصادية والاجتماعية والسياسية والأمنية وغيرها، مما يدعوا بنا الأمر إلى دراسة هذه النقاط بشيء من التفصيل.

3/ أهداف الدراسة:

بالرجوع إلى مدى خطورة هذا النوع من الإجرام العصري وحداثته النسبية والطابع التقني الذي يستخدم في ارتكابه، والمحاولات الفقهية العديدة من أجل جعل النصوص التقليدية القائمة قادرة على مواجهة هذا الشكل المستحدث من الإجرام، قبل أن يتم المطالبة بضرورة استحداث نصوص جديدة لمواجهة تلك الجرائم المستحدثة التي تعتمد على التقنية المتطورة

الحديثة "New Advanced Technology" ونظرا لطبيعة تلك الجرائم فإن البحث في مدى مواجهتها جنائيا و كيفيته هو ما تهدف إليه هذه الدراسة، كما تسعى هذه الدراسة هادفة إلى تعريف الجريمة المعلوماتية وبيان خصائصها ومحاولة الكشف عن العلاقة التي تربط بين التطور التكنولوجي والجريمة. وكذا دراسة هذا النوع من الجريمة في الدول العربية والصعوبات المواجهة لمكافحة الجريمة المعلوماتية من خلال العقبات المتعلقة باكتشافها وإثباتها، وكذا الصعوبات المتعلقة بالجانب القانوني ومشكلة الاختصاص القضائي في الجرائم المعلوماتية.

4/ إشكالية الدراسة:

تحاول هذه الدراسة جاهدة استبيان أوجه القصور التشريعي في الدول العربية عن مواكبة مثل هذه الجرائم سريعة التطور، وذلك سعيا للتوصل لآليات قادرة على احتوائها ومواجهتها، فالتعرف على ماهية الجريمة المعلوماتية وآثارها وطرق مكافحتها يعد من بين تساؤلات هذه الدراسة كمحاولة للوصول إلى الآلية المثلى للتعاطي مع هذه الجريمة، وبذلك يمكن طرح الإشكالية التالية: "ما هي أهم الطرق الواجب اتباعها من أجل منع وقوع الجرائم المعلوماتية (الجرائم الإلكترونية)؟ و كيف يمكن جعل الأنترنيت وسيلة أكثر أمان؟

5/ المنهج المتبع في الدراسة:

من أجل الإجابة عن الإشكالية المطروحة، ومعالجة الموضوع فقهيا وقانونيا تم الاعتماد على المنهج الوصفي التحليلي حتى يتم تعريف الجريمة المعلوماتية، والتطرق للصعوبات المواجهة أثناء محاولة إثباتها وكذا أثناء

اكتشافها ومحاولة مكافحة هذه الجريمة المعلوماتية التي أصبحت تهدد أمن واستقرار المجتمع وحتى مؤسسات الدولة.

6/ خطة الدراسة:

تم تقسيم الدراسة إلى مبحثين تناول الأول منها مفهوم الجريمة المعلوماتية وبيان خصائصها وذلك في المبحث الأول. أما الصعوبات المواجهة لمكافحة هذه الجريمة فقد تم التطرق إليها في المبحث الثاني من هذه الدراسة من خلال محاولات إظهار الصعوبات المتعلقة باكتشاف وإثبات الجريمة الإلكترونية، ثم الصعوبات المتعلقة بالجانب القانوني ومعوقات تحديد القانون الواجب التطبيق وكذا مشكل الاختصاص القضائي.

المبحث الأول: تعريف الجريمة المعلوماتية وبيان خصائصها.

سنتناول في هذا المبحث تعريف الجريمة المعلوماتية، من الزاوية الفنية والزاوية القانونية، وكذا حسب نظام مكافحة جرائم المعلوماتية للمملكة العربية السعودية في المطلب الأول، ثم نتناول خصائص الجريمة المعلوماتية في المطلب الثاني.

المطلب الأول: تعريف الجريمة المعلوماتية.

إن للجريمة المعلوماتية عدة مسميات، فهي جريمة الكمبيوتر والأنترنيت، وهناك من يطلق عليها اسم الجريمة الإلكترونية، وهناك من يسميها بالجرائم المستحدثة، ولكن عند التطرق إلى تعريف الجريمة المعلوماتية فيجب تناولها من جانب فني وجانب قانوني.

الفرع الأول: تعريف الجريمة المعلوماتية من زاوية فنية.

إن من يتناول التعريف الفني للجريمة المعلوماتية يميل إلى القول إلى أن الجريمة المعلوماتية هي: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة، كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[1].

كما يعرفها جانب من الفقه الجنائي بأنها: "الاستخدام غير المشروع للحاسبات، والتي تتخذ صورة فيروس"Virus" يهدف إلى تدمير الثروة المعلوماتية"[2].

الفرع الثاني: تعريف الجريمة المعلوماتية من زاوية قانونية.

ثمة جانب من الفقه القانوني، عرّف الجريمة المعلوماتية بأنها: "الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الأنترنيت".[3]

إن هذا التعريف يعتبر واضح و بسيط، ولكن عدم إشارته إلى إمكانية وقوع الجريمة المعلوماتية أيضا على شبكة الأنترنيت، هو لقصور يكمن في صلب هذا التعريف، كما في حالة تعطيل الشبكة عن العمل، أو العمل على الإبطاء من سرعتها، أو إتلاف المواقع على شبكة الأنترنيت.

وقد عرّفت الجريمة المعلوماتية كذلك بأنها:" الاستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المعتمد الضار لأجهزة الكمبيوتر أو ملفات البيانات"[4].

كما تعتبر الجريمة المعلوماتية بالنظر إلى الوسيلة المستخدمة فيها: "بأنها الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية

داخل نظام حاسب، و بعبارة أخرى، هي تلك الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا".[5]

لكن ما يعاب على ما سبق من التعريفات هو اعتمادها على "الوسيلة" في تعريف الجريمة المعلوماتية، وما رآه البعض هو أن تعريف الجريمة المعلوماتية يقوم في الأساس على العمل الرئيسي المكون لها، و ليس فقط الوسائل المستخدمة فيها. ذلك أنه لا يمكن أن يطلق على جريمة ما، أنها من جرائم الحاسب الآلي، لمجرد أن الحاسب قد استخدم في ارتكابها.[6]

ومن أجل ذلك فقد أوجدت تعريفات أخرى تناولت الجانب "الموضوعي" للجريمة المعلوماتية، فهذه الجريمة ليست الجريمة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها، بل تقع على الحاسب الآلي أو في داخل نظامه.

ولذلك فقد عرفت من قبل أنصار هذا الاتجاه بأنها: "نشاط غير مشروع موجه للنسخ أو التغيير أو الحذف أو الوصول إلى المعلومات المخزنة داخل الحاسب، أو التي تُحوّل عن طريقه"[7]. وعرفت كذلك بأنها: "غش (Fraud) معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها".[8]

ومن خلال كل هاته التعريفات فيمكن الإجماع على أن الجريمة المعلوماتية من شأنها أن تتسبب في تهديد الحريات الفردية، بسبب اعتمادها على تقنية متطورة تتمثل في شبكة الأنترنيت والحاسبات الآلية الصغيرة، ولذلك لابد من إيجاد الوسيلة المناسبة لمكافحتها والحد منها، لتجنب هذا الخطر المهدد في الوقت المحدد.

المطلب الثاني: خصائص الجريمة المعلوماتية.

حيث سنستعرض خصائص الجريمة المعلوماتية/الإلكترونية في كل من الفروع التالية:

الفرع الأول: خفاء الجريمة والسرعة والتطور في ارتكابها.

قد لا يلحظ الضحية بأنه قد وقع في شراك الجريمة المعلوماتية رغم أنها وقعت أثناء وجوده على الشبكة، ذلك أن الجاني يتمتع بقدرات تمكنه من ارتكاب جريمته بدقة متناهية كسرقة الأموال بعد إرسال مجموعة من الفيروسات المدمرة لجهاز الحاسوب، وجرائم التجسس وسرقة المكالمات وغيرها، مما ينبئنا بأن الجرائم الناشئة عن استخدام الأنترنت (الجرائم الإلكترونية)، في أغلبها جرائم خفية ومستترة.[9]

ومنه فإن الجريمة المعلوماتية أسرع تطورا من التشريعات، ويرجع الأمر في ذلك إلى التطور التكنولوجي الهائل لشبكة الأنترنيت، تزامنا مع مختلف الخطط الإجرامية التي يعقدها المجرمين المعلوماتيين، والتي تسمح لهم بإبتكار وسائل وطرق معقدة لم تعرفها التشريعات من قبل وذلك من أجل ارتكابهم لجرائمهم[10].

الفرع الثاني: لا مادية الجريمة المعلوماتية وسرعة محو الدليل.

من بين الخصائص المميزة للجريمة المعلوماتية، طابعها اللامادي، حيث لا تدع المجال لتحديد الفعل من عدمه، مما يجعل الأمر يزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي بيئة الحاسوب والأنترنيت تكون البيانات عبارة عن عالم إلكتروني غير مرئي، ينساب عبر النظام المعلوماتي، مما يجعل طمس الدليل ومحوه كليا أمرا في غاية السهولة من قبل الفاعل.[11]

فمعظم جرائم المعلوماتية تم اكتشافها بالصدفة بعد ارتكابها، ويمكن أن تعود أسباب صعوبة إثبات الجرائم المعلوماتية إلى خمسة أمور كالتالي:

1- الجريمة المعلوماتية لا تترك أثرا لها بعد ارتكابها.

2- تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.

3- صعوبة الاحتفاظ الفني بآثارها إن وجدت.

4- تعتمد على الخداع في ارتكابها.

5- تعتمد الجريمة المعلوماتية على قمة الذكاء في ارتكابها.[12]

الفرع الثالث: هدوء الجريمة المعلوماتية أثناء التنفيذ.

إن جرائم الأنترنيت تعتبر الأكثر هدوء أثناء ارتكابها من حيث طبيعتها، ولا تحتاج إلى العنف تماما، وكل ما تحتاج إليه هو القدرة الفعالة والذكاء الإجرامي الخارق في ارتكاب الأفعال غير المشروعة عن طريق الكمبيوتر و/أو باستعمال الأنترنيت، ومنه فتعتبر هذه الجريمة أثناء تنفيذها من الجرائم التي لا تدعو إلى العنف أو الدماء أو الجهد العضلي، بل هي من الجرائم النظيفة، التي تتم عن طريق تغيير في أرقام بيانات مخزنة داخل الكمبيوتر.[13]

الفرع الرابع: الجريمة المعلوماتية جريمة عابرة للحدود.

إن السهولة في حركة المعلومات عبر التقنيات الحديثة، جعل بإمكان المجرم المعلوماتي ارتكابه لجريمته المعلوماتية عن طريق حاسوب موجود في دولة معينة، بينما يتحقق فعله الإجرامي في دولة أخرى غير الدولة المرتكب فيها الفعل الإجرامي.[14]

المبحث الثاني: صعوبات مكافحة الجريمة المعلوماتية.

هناك العديد من الجهود المبذولة للحد من الجريمة المعلوماتية، إمّا من قبل المشرعين أو من قبل سلطات التحقيق والضبطية القضائية، دولية كانت أو داخلية، إلاّ أن هذه الجهود تصطدم بالعديد من العراقيل والصعوبات من بينها صعوبات اكتشاف وإثبات الجريمة الإلكترونية وذلك يرجع إلى طبيعتها اللاّمادية أساسا، والصعوبات المتعلقة بالجانب القضائي والمتعلقة بالقانون الواجب التطبيق، وماهي الجهة القضائية المختصة بالنظر في هذه الجريمة والتي يمكن أن تتعدد أماكن وزمن ارتكاب هذه الجريمة.

المطلب الأول: الصعوبات المتعلقة باكتشاف وإثبات الجريمة المعلوماتية.

سنتناول في هذا المطلب دراسة الصعوبات المواجهة من أجل اكتشاف الجريمة المعلوماتية في الفرع الأول، ثم نتناول في الفرع الثاني صعوبات إثبات الجريمة المعلوماتية، كغياب الدليل المادي للجريمة المعلوماتية وقلة الإبلاغ عن وقوعها.

الفرع الأول: صعوبات اكتشاف الجريمة المعلوماتية.

إن اكتشاف الجرائم المعلوماتية أمر في غاية الصعوبة، مما يحتم على المشرع أو المحقق القضائي تدارك هاته المعوقات من أجل درء هاته الجريمة وكذا حماية الأفراد منها، ومن هاته الصعوبات كالتالي:

أولا: فقدان الآثار التقليدية للجريمة المعلوماتية: وهو من بين ما يميزها عن باقي الجرائم، أي لا مادية الجريمة المعلوماتية، وارتكابها يتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية، مما يبقي هاته الجريمة مجهولة ما لم يبلغ عنها للجهات المعنية بالتحقيق الجنائي.[15] كما أن البيانات

والمعلومات التي تشتمل عليها، لا تتضمن آثار أو بصمات يمكن التعرف من خلالها على مرتكب هذه الجريمة.[16]

ثانيا: تعمد الجناة إلى فرض تدابير أمنية من أجل إخفاء جرائمهم: وإزالة آثارها عن طريق التلاعب بالقواعد والبيانات والبرامج في الكمبيوتر، خاصة وأن التخزين الإلكتروني غير مرئي ومكتوب بلغة الأرقام، أو فرض تدابير احترازية من أجل عدم تسهيل إجراءات التفتيش التي يتوقع الجناة حدوثها كاستخدام كلمات السر، أو إعطاء تعليمات خفية بين هذه البيانات أو تشفيرها حتى يستحيل على جهات التحري والبحث الوصول إلى كشف هاته الأفعال غير المشروعة، مما يشكل عقبة أمام إقامة الدليل على الجريمة الإلكترونية وإثباتها[17].

ثالثا: التكتم على الجريمة المعلوماتية من قبل الجهات المجني عليها: بحيث تحرص هاته الجهات المجني عليها، والتي غالبا ما تكون مصرفا أو مؤسسة مالية أو شركة، على التكتم وعدم الإبلاغ على مثل هذه الجرائم التي راحت ضحيتها، خوفا من الخسائر التي يمكن أن تتكبدها جرّاء هذا الإبلاغ، أو بسبب نقص ثقة العملاء في هذه المؤسسات، أو حتى قد يتوخى بعض المجني عليهم من وراء العزوف عن الإبلاغ عدم إتاحة الفرصة للأجهزة الأمنية من الاطلاع على معلومات لم يجر الإبلاغ عنها.[18]

ومنه فعدم تبليغ السلطات المختصة في مكافحة هذه الجريمة يبقيها مستترة ما لم يتم الإبلاغ عنها، ومن ثم فالصعوبات التي تواجه أجهزة الأمن والمحققين هو أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة التي تحكم الجريمة التقليدية.

رابعا: نقص الخبرة لدى جهات التحقيق والتحري: هي مسألة في غاية الأهمية والصعوبة وخاصة إذا نظرنا إلى التكوين والخبرات المكتسبة لرجال الضبط القضائي، وسلطات التحقيق والتحري مقارنة بحداثة الجرائم وتقنياتها العالية، نجدها تتطلب من القائمين على البحث والتحري إلمام كافي بها، وخبرة فنية في مجال الجريمة المعلوماتية والنظم الإلكترونية والبيانات، ولا يكفي أن تكون لهم الخلفية القانونية فقط، بل هذا الأخير يمكن أن يكون بدوره العنصر المحفز والمساعد لمرتكبي الجرائم المعلوماتية.[19]

كما أنه من بين التحديات والمشاكل التي تواجه أجهزة الأمن وأجهزة العدالة الجنائية في جرائم الأنترنيت، أن الجناة في هذه الجرائم لهم مفردات ومصطلحات خاصة بهم، لدرجة أنهم يطلقون على أنفسهم اسم "النخبة" بدعوى أنهم الأكثر دراية ومعرفة بعالم الأنترنيت وأسرار الكمبيوتر ولغاته المتميزة. [20]

الفرع الثاني: صعوبات إثبات الجريمة المعلوماتية.

تتصف الجريمة المعلوماتية بالخفاء وعدم تركها لآثار مادية يمكن متابعتها، كما تتسم بالخطورة وصعوبة الاكتشاف، ثم إن ما يميز الجريمة المعلوماتية هو صعوبة تحديد مكان وقوعها أو مكان التعامل معها، بسبب اتساع نطاقها المكاني وتعدد مرتكبيها ووسائل استعمالها وضخامة بياناتها، وترجع صعوبة إثبات الجريمة المعلوماتية إلى عدة أمور كالتالي:

أولا: غياب الدليل المادي للجريمة المعلوماتية:

إن الطبيعة غير المرئية للجريمة المعلوماتية/الإلكترونية أو الأدلة المتحصل عليها من خلال هاته الجريمة، تعتبر أحد أبرز المشكلات التي تلقي بظلالها على جهات الأمن والملاحقة والمحققين، خاصة إن قلنا بأن

أغلب المعلومات والبيانات التي يتم تداولها عبر الكمبيوتر والتي من خلالها تتم العمليات الإلكترونية تكون في صورة رموز وأرقام مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلاّ من خلال جهاز الكمبيوتر، ومنه فالجرائم التي ترتكب على العمليات الإلكترونية، والتي تعتمد في موضوعها على التشفير والأرقام السرية والتخزين الإلكتروني، يصعب أن تخلّف وراءها آثار مرئية تكشف عنها أو يُستدَل من خلالها على المجرمين المعلوماتيين.[21]

ثانيا: سهولة إخفاء الدليل وإعاقة الوصول إليه.

حيث أنه يمكن للمجرم المعلوماتي أن يجعل من الصعب الاحتفاظ بدليل الجريمة الإلكترونية، كما يمكنه في أقل من ثانية بل في لمحة من البصر أن يمسح أو يغير البيانات والمعلومات الموجودة في الكمبيوتر[22]. على خلاف الجرائم التقليدية المادية التي لا يمكن محو آثارها أو من الصعب جدا أن يتم إخفاء الدليل، هذا من جهة.

ومن جهة أخرى فإن الجريمة المعلوماتية تحتاج إلى خبرة فنية، ويصعب على المحقق التقليدي أن يتوصل إليها، إذ تتطلب إلمام خاص بتقنيات الكمبيوتر ونظم المعلومات سواء لارتكابها أو التحقيق فيها أو حتى من أجل ضمان ملاحقة قضائية فعّالة[23].

ثالثا: صعوبات إثبات الجريمة المعلوماتية في قلة الإبلاغ عن وقوعها.

في الغالب الأعم لا يتم الإبلاغ عن الجرائم المعلوماتية، إمّا لعدم اكتشاف الضحية لها، وإما خشيته من التشهير، بل ويصعب حتى كشفها وحصرها ومتابعة مرتكبيها.

كما أن الصعوبة تتمثل في الاعتماد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها، وهو يزيد فرص مجرم الأنترنيت في الإفلات من العقاب ثم إن الخاصية التي تميزها، هو الذكاء في ارتكابها، فالجريمة المعلوماتية من النوع الذي يمكن أن نطلق عنه وصف "جرائم الذكاء"، كما أنها ليست جريمة منظمة، ذلك أن الإجرام الإلكتروني هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، كما أن المجرم الإلكتروني ذو مهارات تقنية عالية وإلمام بتكنولوجيا النظم المعلوماتية وهو ما يزيد من صعوبة الأمر[24].

المطلب الثاني: الصعوبات المتعلقة بالجانب القانوني والاختصاص القضائي.

إن الصعوبات التي تواجه مكافحة الجرائم المعلوماتية، لم تبق تلك المتعلقة باكتشافها ومحاولات إثباتها فقط، بل تعدّت ذلك بكثير وانبثق عن الطابع العالمي للجريمة المعلوماتية صعوبات أخرى تتمثل في القانون الواجب التطبيق والجهة القضائية المختصة، حيث ترى كل دولة أن لها الحق في متابعة مرتكب هذه الجريمة لعدة اعتبارات، ذلك أن ميزة الجريمة المتعدية خلقت إشكالاً حاداً انجر عنه تنازع قوانين أكثر من دولة في هذا المجال.

وكنتيجة حتمية لذلك وبما أن الجريمة المعلوماتية تخترق كل الحدود الإقليمية المعمول بها، وجب تعاون أكثر من دولة، غير أن ما يلاحظ في حقيقة الأمر هو قصور هذا التعاون الدولي مقارنة بالتطور الهائل للجريمة من جهة، ومن جهة أخرى أن الإجراءات التقليدية المطبقة في مجال التعاون الدولي للحد من الإجرام العابر للحدود لم تتطور بتطور التقنية.

الفرع الأول: معوقات تحديد القانون الواجب التطبيق.

إن تحديد القانون الواجب التطبيق، والجهة القضائية المختصة في النظر في الجرائم المعلوماتية، يكتسي أهمية بالغة بالنظر إلى أبعادها ووصفها كجريمة عابرة للحدود، ذلك أن غالبية الأفعال ترتكب من خارج الحدود، أو أنها تمر عبر شبكة الأنترنيت، الأمر الذي يبرز أهمية اختبار مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق، وما إذا كانت القواعد القانونية القائمة في هذا المجال تحكم هذا النوع من الجرائم، أم يتعين إفراد قواعد خاصة بها، جرّاء ما تثيره من مشكلات وصعوبات في مجال الاختصاص القضائي.

إن المبادئ التقليدية في تحديد القانون الواجب التطبيق تنقسم إلى مبدأ إقليمية النص الجنائي، مبدأ عينية النص الجنائي والذي يقصد به اتباع التشريع الجنائي الوطني للدولة، ليطبق على بعض الجرائم بعينها والعقاب عليها، رغم عدم وقوعها على الإقليم الوطني، بصرف النظر عن جنسية مرتكبيها[25]، وكذا المبدأ الثالث وهو مبدأ شخصية النص الجنائي. إلاّ أن هذه المبادئ خاصة وأنها تحكم الجريمة التقليدية فهي تنتفي أمام خصوصية الجريمة المرتكبة عبر الأنترنيت.

ويترتب على عدم تبعية شبكة الأنترنيت لأي جهة أو شخص محدد ولعدم وجود مقر لها في دولة معينة، تخضع لرقابتها أو سيطرتها، ونظرا لعدم وجود قانون جنائي موحد يحكم هذه الشبكة، فإن القوانين الجنائية التي تطبق عليها تتعدد بتعدد الدول المرتبطة بها، باعتبار أن القانون الجنائي يتعلق بسيادة الدولة.

الأصل في القوانين هو إقليمية النص الجنائي، فإذا ما ارتكب شخص ما جريمة عن طريق الأنترنيت بداخل الدولة، وتحققت نتيجتها بذات الدولة،

فالقانون الواجب التطبيق بلا منازع هو قانون هذه الدولة بغض النظر عن جنسية الجاني أو المجني عليه، فقط يكفي أن تكون هذه الجريمة على إقليم الدولة سواء كان إقليماً برياً، أو بحرياً، أو جوياً.[26]

يترتب على تطبيق مبدأ إقليمية قانون العقوبات عدم اهتمام الدولة إلاّ بالجرائم التي تقع على إقليمها، فلا يمتد إلى ما يرتكب خارجه من جرائم ولو كان مرتكبوها من رعايا هذه الدولة، غير أن هذه النتيجة قد لا تتفق مع حماية مصالح الدولة، خاصة فيما يتعلق بالجرائم التي ترتكب عبر الأنترنيت، وذلك راجع إلى البعد الدولي، بل العالمي لنشاط الشبكة، حيث يضع دول مختلفة في حالة اتصال دائم والبيانات والمعلومات التي يتم إدخالها وتحميلها على الشبكة تنتشر في ثوان معدودة في كل الدول المرتبطة بها، بحيث تكون متاحة لأي مستخدم في تلك الدول[27].

كذلك الأمر بالنسبة لمبدئي عينية وشخصية النص الجنائي اللّذان لا يمكن تطبيقهما في هذا النطاق، فإذا كان هذان المبدءان وضعا لكي يغطيا القصور الذي تميز به مبدأ إقليمية النص الجنائي في الجرائم التقليدية، فالأمر غير ذلك في الجرائم المرتكبة عبر الأنترنيت خاصة في ظل عالمية الشبكة، حيث أن السلوك في هذه الجريمة يمر عبر عدة دول، الشيء الذي يخلق إشكالاً كبيرا في تحديد القانون الواجب التطبيق نظراً لاختلاف تشريعات هذه الدول، وعدم وجود اتفاقات فيما بينها، فمثلاً دولة تأخذ بمبدأ الإقليمية والأخرى بمبدأ العينية، ودولة أخرى تأخذ بمبدأ الشخصية، الأمر الذي يثير نزاع فيما يتعلق بالقانون الواجب تطبيقه، فكل دولة ترى نفسها الأحق بمتابعة الجاني.

الفرع الثاني: مشكلة الاختصاص القضائي في الجرائم المعلوماتية.

أثارت الجرائم المرتكبة عبر الأنترنيت مسألة الاختصاص على المستوى المحلي والدولي، بالرغم من أنه لا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك.

ينجم عن اختلاف التشريعات والنظم القانونية تنازع في الاختصاص بين الدول خاصة في إطار الجرائم المتعلقة بالأنترنيت التي تتميز بكونها عابرة للحدود، فقد يحدث أن تُرتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي، وقد تكون هذه الجريمة من الجرائم التي تهدّد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية، كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الاطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقاً لمبدأ الإقليمية لكل دولة من الدول التي مسّتها الجريمة[28].

يلاحظ أن اختصاص القضاء بنظر الجرائم التي تتم عبر شبكة الأنترنيت والقانون الواجب تطبيقه على الفعل، لا يحظى بالوضوح أو القبول أمام حقيقة أن غالبية هذه الأفعال من قبل أشخاص من خارج حدود الدولة، أو أنه تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، وهو ما يبرز أهمية اختبار مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق وما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشاكل في حقل

الاختصاص القضائي، ويرتبط بمشكل الاختصاص وتطبيق القانون مشكل امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود.

أدى هذا البعد عبر الوطني للجريمة المرتكبة عبر الإنترنيت إلى تشتت الجهود وإعاقة التعاون الدولي في مجال التصدي لهذا النوع من الإجرام، وذلك لاختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق[29].

الخاتمـــــة:

إن مبدأ الشرعية الجنائية يفرض قاعدة أساسية وهي عدم جواز التجريم والعقاب عند غياب النص، الأمر الذي يمنع معاقبة مرتكبي الأفعال الضارة والخطرة على المجتمع بواسطة الكمبيوتر أو عند الاتصال بالأنترنيت، خاصة وأن المشرع الجنائي في عديد من الأقطار العربية لم يقم بسن التشريعات اللاّزمة لإدخال هذا السلوك ضمن دائرة التجريم والعقاب.

كما أن وضع قوانين وأنظمة خاصة للمعاقبة على جرائم المعلومات، دون اللّجوء إلى تطبيق قواعد القانون الجنائي التقليدي، من شأنه أن يفرض حماية جنائية من الأفعال المكونة لأركان الجريمة المعلوماتية، واتخاذ إجراءات فورية اتجاه المخالفين في المواقع الإلكترونية ويتم تدميرها إذا ثبت إضرارها بالأمن القومي والآداب العامة.

وفي ختام هذه الدراسة تم التوصل إلى مجموعة من النتائج والاقتراحات أملاً في الوصول إلى حلول للتحديات التي تقف أمام تحقيق الأمن الإلكتروني في الدول العربية كالتالي:

أولا: النتائـــج.

1/ إن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلى تنظيم قانوني، يضع إطارا للعلاقات التي تترتب على استخدامه بما يكفل حماية الحقوق المترتبة على هذا الاستعمال ويحدد الواجبات اتجاهها.

2/ مبدأ إقليمية النص الجنائي يفقد صلاحيته من حيث التطبيق بالنسبة للجرائم المعلوماتية التي تتجاوز حدود المكان، فالجرائم المعلوماتية عابرة للحدود.

3/إن التقدم التكنولوجي أفرز أنماطا جديدة من الجريمة، وكذا من المجرمين، فكان للتقدم في العلوم المختلفة أثره على نوعية الجرائم، واستغل المجرم ثمرات هذه العلوم في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية، بحيث أن المشكلة لا تكمن في استغلال المجرمين للأنترنيت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون لهم.

ثانيا: الاقتراحات.

1/ رفع مستوى الوعي والإدراك لدى مستعملي الأنترنيت وخاصة الأطفال، تجاه ما يمكن أن يصلهم من محتوى غير لائق، مع ضرورة تعزيز الحوار الودّي بين الآباء و الأبناء.

2/ ضرورة وضع تشريعات وقوانين تعاقب مرتكبي جرائم الأنترنيت والمعلومات وتطوير التشريعات الموجودة حاليا وتحيينها بما يواكب التطور العلمي والتكنولوجي، وبما يكفل حقوق المواطنين المستخدمين لشبكة المعلومات الدولية، وتحديد واجباتهم.

3/ ضرورة التنسيق والتعاون الدولي، قضائياً وإجرائياً في مجال مكافحة الجرائم المعلوماتية.

4/ ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية وتدريبهم على كيفية التعامل مع أجهزة الحاسوب وشبكات الأنترنيت، مع تدريب وتحديث رجال الادعاء العام والنيابة العامة ورجال القضاء بشأن التعامل مع أجهزة الحاسوب والأنترنيت.

5/ إتاحة الفرصة للمواطنين وإشراكهم في مكافحة الجرائم المعلوماتية، من خلال توفير الخط الساخن، الذي يختص بتلقي البلاغات المتعلقة بهذه الجرائم، ولا سيما الجرائم الأخلاقية، كالاستغلال الجنسي للأطفال عبر الأنترنيت.

6/ ضرورة إنشاء أقسام بكليات الحقوق بالجامعات العربية لدراسة "الحماية القانونية للمعلوماتية" أو "قانون المعلوماتية والأنترنيت"، مع وجوب إدخال مادة "أخلاقيات استخدام الأنترنيت والمعلوماتية" ضمن المناهج الدراسية في التعليم الجامعي وما قبله.

قائمة الهوامش :

1/ د. محمد الأمين البشرى، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنيت، كلية الشريعة والقانون، جامعة الإمارات، مايو2005، ص03.

2/ د. هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنيت، كلية الشريعة والقانون، جامعة الإمارات، مايو2005، ص07.

3/ د. محمد عبد الرحيم سلطان العلماء، جرائم الأنترنيت والاحتساب عليها، بحث مقدم لمؤتمر القانون والكمبيوتر والأنترنيت، كلية الشريعة والقانون، جامعة الإمارات، مايو2005، ص 05.

4/ د. ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية، الجريمة عبر الأنترنيت، منظور أمني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنيت، كلية الشريعة والقانون، جامعة الإمارات، مايو 2005، ص03.

5 / Richard Totty and Anothony Hardcastle, crime in computer, related "information technology and the law", chris edwards and nigle savage, Macmillan publishers, UK, 1986, p169.

6/ د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنيت في القانون العربي النموذجي، دراسة قانونية متعمقة في القانون المعلوماتي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 24.

7 / Michael Alexander, computer crime, Ugly secret for business , computer world, vol xxiv, No11, 1990, p: 104.

8/ د. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الإسكندرية، 1997، ص02.

9/ د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنيت، دار النهضة العربية، القاهرة، ص 32؛ د. تركي بن عبد الرحمن،(بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة مقدمة استكمالاً لمتطلبات الحصول على درجة دكتوراه الفلسفة الأمنية، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية، الرياض، 2009)، ص:20.

10/ د. أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار نشر، 2005، ص: 26.

11/ حيث يقوم المجرم المعلوماتي بإعاقة سلطات التحقيق لعدم الوصول إلى الدليل بشتى الوسائل، كمسح البرامج، أو محو الدليل من شاشة الكمبيوتر أو وضع كلمات ورموز سرية لمنع إيجاد أي دليل يدينه. (أنظر: د. محمد عبد الرحيم سلطان العلماء، المرجع السابق، ص 09).

12/ د. عبد الفتاح مراد، شرح جرائم الكمبيوتر والأنترنيت، شركة البهاء للبرمجيات والكمبيوتر والنشر الإلكتروني، الإسكندرية، جمهورية مصر العربية، دون سنة نشر، ص:42.

13/ د. عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص52؛ د. ذياب موسى البداينة، دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية، المنعقدة بكلية التدريب، قسم البرامج التدريبية، القنيطرة المملكة المغربية، أيام:9-13 أفريل 2006، ص:20.

14 / Mascala Corinne, criminalité et contrat électronique, IN, le contrat électronique, travaux de l'association CAPITANT Henri, journées national, Paris, 2000, P119.

15/ د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنيت، دراسة متعمقة في جرائم الحاسب الآلي والأنترنيت، بهجات للطباعة والتجليد، مصر، 2009، ص: 41.

16/ د. أحمد آيت الطالب، العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة، الدورة التدريبية لمكافحة الجرائم الإرهابية المعلوماتية، كلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية، 9- 2006/4/13، ص: 16.

17/ د. فريد منعم صبور، حماية المستهلك عبر الأنترنيت ومكافحة الجرائم الإلكترونية، دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010، ص: 32؛

- كما أن الاستعانة بالخبرة في مجال الجرائم الإلكترونية، تظهر عند غيابه، فقد تعجز الشرطة عن كشف غموض الجريمة، وقد تعجز هي أو جهة التحقيق عن جمع الأدلة حول الجريمة، وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه.

(See :Robert Taylor, Computer Crime in Criminal Investigation, edited by Charles Swanson, n.chamelin and L.Territto, Hill, inc .5 edition, 1992, P.1).

18/ د. موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص 05.

19/ د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنيت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص: 122.

20/ د. حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنيت، مقال منشور على الموقع الإلكتروني: http://www.eastlaws.com، ص:6-7.

21/ د. غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب والأنترنت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص: 539.

22 / John Eaton and Jermy Smithers, A managers guide to information Technology, London, philip Allan, 1982, P 263.

23/ د. هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنيت، المنعقد بجامعة الإمارات العربية المتحدة، خلال الفترة: 01-03 مايو 2000.

24/ د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، 2005، بدون بلد نشر، ص 28؛ د. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2008، ص47.

25/ د. غازي عبد الرحمن هيان الرشيد، المرجع السابق، ص499.

26/ د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنيت، دار النهضة العربية، القاهرة، دون سنة النشر، ص69.

27/ د. أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة، طبعة كلية الحقوق، جامعة بنها، 2009، ص58.

28/ د. حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الأنترنيت، مقال منشور على الموقع الإلكتروني: http://www.minshawi.com، ص52-53.

29/ محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005، ص35.