جامعة 8 ماي 1945 قالمة

كلية الحقوق والعلوم السياسية

قسم الحقوق

تخصص قانون أعمال

مذكرة مكملة لمتطلبات نيل شهادة الماستر في القانون

المسؤولية الجزائية عن الأنظمة ذاتية التسيير

إعداد الطلبة:

1/ عبدي ريان

2/ بوناب الغالية

تحت إشراف

د. شراريرية محمد

تشكيل لجنة المناقشة

الرقم	الأستاذ	الجامعة	الرتبة العلمية	الصفة
1	د. فلكاوي مريم	8 ماي 1945 قالمة	أستاذ محاضر "أ"	رئيسا
2	د. شراريرية محمد	8 ماي 1945 قالمة	أستاذ محاضر "أ"	مشرفا
3	د. مفتاح ياسين	8 ماي 1945 قالمة	أستاذ محاضر "ب"	عضوا مناقشا

السنة الجامعية: 2024-2025

بسم الله الرحمن الرحيم

شكر وتقدير

قال الله تعالى:

﴿فَاذْكُرُونِي أَذْكُرْكُمْ وَاشْكُرُوا لِي وَلَا تَكْفُرُونِ﴾ [البقرة: 152]

وقال رسول الله ﷺ:

"من لا يشكر الناس لا يشكر الله" – رواه الترمذي

الحمد لله حمدًا يليق بجلال وجهه وعظيم سلطانه، الحمد لله الذي علّم الإنسان ما لم يعلم، وسهّل لنا سُبل العلم والمعرفة، ووفّقنا لإتمام هذا العمل المتواضع.

يسرّني أن أتقدّم بجزيل الشكر والامتنان لكل من قدّم لي يد العون والمساعدة طيلة فترة إعداد هذه المذكرة.

وأخصّ بالشكر والتقدير الأستاذ الفاضل الدكتور محمد شرايرية، لما قدّمه لي من توجيهات علمية قيّمة، وملاحظات بنّاءة، ودعم متواصل كان له بالغ الأثر في إنجاز هذا العمل، فجزاه الله عني خير الجزاء، ووفّقه وسدّد خطاه.

كما أتقدّم بخالص الشكر والتقدير إلى أعضاء لجنة المناقشة الموقّرين، على تفضّلهم بقبول مناقشة هذا العمل، وعلى وقتهم وجهدهم المبذولَين في سبيل تقويمه وتقديم الملاحظات التي من شأنها تطويره والارتقاء به.

ولا يفوتني أن أشكر كل من ساهم من قريب أو بعيد في إنجاح هذا البحث، من أساتذة، وزملاء، و أفراد عائلتي الكرام، على دعمهم المتواصل وتشجيعهم المستمر.

والله وليّ التوفيق.

الحمد لله شكرًا وامتنانًا، ما كنتُ لأفعل هذا لولا فضل الله عزوجل، فله الحمد على البداية وإليه الحمد حتى الختام.

ها أنا اليوم أُتوِّج اللحظات الأخيرة من هذا الطريق، بعد تعبٍ ومشقةٍ دامت سنوات، في سبيل الحلم والعلم.

ها أنا اليوم أقف على عتبة التخرج، أقطف ثمار تعبي، وأدفع ضريبة الجهد بكل فخر واعتزاز .فاللهم لك الحمد إذا رضيت، ولك الحمد بعد الرضا.

وبكل حب وفخر، أهدي ثمرة تخرجي إلى نفسي الطموحة، التي بدأت بالطموح و انتهت بالنجاح.

إلى من أحمِل اسمه بكل فخر،

إلى من حصد الأشواك في طريقي ليمهّد درب النجاح،

إلى من كان السند بعد الله،

إلى من غرس في قلبي الإرادة وحب الوصول، ور افقني في كل خطوة

أبي الغالي.

وإلى المرأة التي صنعت مني فتاة تعشق التحديات، قدوتي التي منها تعرّفتُ على القوة والثقة بالنفس،

إلى من رضاها يجلب لي التوفيق :أمي، أطال الله في عمركِ بالصحة والعافية.

إلى الروح الغالية التي فارقتني و أنا لا زلت متعلقة بها،

إلى روح انتُزِعت من روحي،

إلى من فجعتني برحيلها، وتركت في قلبي فراغًا لا يُملأ،

أمي

إلى بسمة وضحكة لا تُنسى، دمتِ في نعيم الرب حتى نلتقي

خالتي.

إلى حبيب الروح، سند الحياة، وقطعة من قلبي

أخي.

إلى ملائكةٍ رزقني الله بهن لأتعرف من خلالهن على الحياة، ومفاهيم الصداقة والسند :أخو اتي، ريان وملاك.

وفي الختام، أُهدي هذا الإهداء إلى صاحب الفضل العظيم،

الأستاذ شر ايرية محمد، الذي أمدّنا بالتوجيهات والنصائح لإتمام هذه المذكرة. جزاه الله عني خير الجزاء.

بوناب الغالية

الحمد لله الذي بنعمته تتمّ الصالحات، وبتوفيقه تحققت الأمنيات.

بعد مشوارطويل من التعب والسهروالتحديات، أقف اليوم على عتبة التخرج، أحمل بين يديّ ثمرة سنوات من الجهد والصبر.

لم يكن الطريق سهلاً، لكنني واصلت، وثابرت، وها أنا أصل.

أُهدي تخرّجي هذا أولًا لنفسي... لمن صبرت وتحدّت وواصلت رغم كل شيء. أنا أستحق هذه اللحظة، و أنا فخورة بها.

إلى أبي، منبع القوة في حياتي، الرجل الذي لم يتكلم كثيرًا، لكن دعمه كان حاضرًا في كل خطوة.

يكفيني أنني كنت أستمد منه صموده وثباته...

يا من كنت لي جدارًا لا يسقط، وظلًا لا يغيب، دمت فخرًا وسندًا،والدي العزيز اطال الله في عمرك

وإلى المرأة التي كانت ظلي حين اختفى كل شيء، التي احتوتني في كل انكسار، ودفعتني لأقف كلما سقطت...

إلى من كانت حضنًا وأمانًا ودعاءً لا ينقطع...

أمي، يا ضلعي الثابت، يا أغلى من كل شيء، يا نبع الحنان وسرّ الصبر حفظك الله ورعاك غاليتي

إلى إخوتي شعيب وعبد النور، السند والرفقة، وجودكما في حياتي نعمة كبيرة، أنتما جزء من كل نجاح وصلت إليه.

وإلى صديقاتي، من كنّ البلسم في لحظات التعب، والضحكة في عزّ التوتر، والكتف وقت الحاجة... شكرًا لكنّ من القلب، محبتكنّ كانت دعمًا حقيقيًا لا يُقدّر بثمن. (الغالية وجميع صديقاتي)

ريان عبدي

مقدمة

مقدمة:

يشهد العالم المعاصر ثورة تكنولوجية غير مسبوقة، يقف الذكاء الاصطناعي والأنظمة الذاتية في طليعتها، محدثة تحولات جذرية في كافة مناحي الحياة. فمن السيارات ذاتية القيادة والروبوتات الصناعية المتقدمة، إلى الأنظمة الطبية الذكية ومنصات اتخاذ القرار المؤتمتة، أصبحت هذه التقنيات جزءاً لا يتجزأ من نسيج المجتمعات الحديثة، مقدمةً وعوداً هائلة بتحسين الكفاءة، وتسهيل الخدمات، وفتح آفاق جديدة للابتكار والتقدم.

غير أن هذا التطور المتسارع، بقدر ما يحمل من إيجابيات، يطرح في المقابل تحديات قانونية وأخلاقية واجتماعية بالغة التعقيد. ولعل أبرز هذه التحديات يكمن في مجال القانون الجنائي، حيث تصطدم قدرة الأنظمة الذاتية على اتخاذ قرارات وتنفيذ أفعال بشكل مستقل، قد تلحق أضراراً جسيمة بالأفراد والممتلكات، بالمبادئ الأساسية التي تقوم عليها المسؤولية الجزائية التقليدية، والتي تأسست على فكرة الفاعل البشري العاقل والمدرك لأفعاله ونتائجها.

فمفاهيم الركن المادي والركن المعنوي، ومبدأ الشرعية الجنائية، وقواعد الإسناد التقليدية، تبدو قاصرة عن استيعاب الطبيعة الفريدة للسلوك الصادر عن كيانات غير بشرية تتمتع بدرجات متفاوتة من الاستقلالية والقدرة على التعلم والتكيف. هذا القصور يثير إشكاليات جوهرية حول كيفية تحديد المسؤولية عن الأضرار الناجمة عن هذه الأنظمة، وكيفية تكييف الأفعال الضارة الصادرة عنها ضمن نصوص التجريم القائمة، وما هي السبل الكفيلة بمواكبة التشريع الجنائي لهذه التطورات المتلاحقة لضمان حماية المجتمع وتحقيق العدالة.

وفي هذا السياق، تأتي هذه الدراسة لتسليط الضوء على إشكالية المسؤولية الجزائية للأنظمة الذاتية، ومحاولة استكشاف السبل الممكنة لمواجهة التحديات التي تطرحها على المنظومة القانونية الجنائية. فمع تزايد الاعتماد على هذه التقنيات في مجالات حساسة وحيوية، يصبح من الضروري البحث عن إطار قانوني واضح وفعال قادر على تنظيم استخدامها، وتحديد المسؤوليات المترتبة على أفعالها، وتحقيق التوازن المنشود بين تشجيع الابتكار التكنولوجي وحماية الحقوق والمصالح الأساسية للمجتمع والأفراد.

أهمية الدراسة:

تتجلى أهمية هذه الدراسة في سعيها إلى بناء تصور قانوني متوازن يواكب التحولات المتسارعة التي فرضتها تقنيات الذكاء الاصطناعي، حيث تواجه المنظومة الجنائية تحديات جديدة تستدعي إعادة النظر في مفاهيم المسؤولية والإسناد، بما يضمن حماية فعّالة دون أن يُشكّل ذلك عائقاً أمام التطور التكنولوجي. كما تعكس هذه الأهمية البعد الاجتماعي للدراسة، من خلال تعزيز ثقة الأفراد في استخدام هذه التقنيات وتوفير الأمان القانوني تجاه مخاطرها المحتملة. وفي الوقت ذاته، تسعى الدراسة إلى دعم الابتكار ضمن إطار قانوني واضح يضمن الاستخدام المسؤول لهذه الأدوات، بما يسهم في تحقيق تنمية اقتصادية قائمة على المعرفة والتكنولوجيا.

أهداف الدراسة:

تهدف هذه الدراسة إلى تحليل مدى ملاءمة قواعد المسؤولية الجزائية التقليدية للتعامل مع الأفعال الصادرة عن الأنظمة الذاتية، واستكشاف النماذج القانونية المقترحة لإسناد هذه المسؤولية، مع تكييف النصوص الجنائية لتشمل الأفعال المرتكبة عبر الذكاء الاصطناعي. كما تسعى إلى رصد الاتجاهات التشريعية الحديثة في القانون المقارن واقتراح آليات فعّالة لمواجهة التحديات التقنية في المجال الجنائي، بما يعزز الوقاية، ويطوّر أداء المنظومة القضائية.

أسباب اختيار الموضوع:

لقد تم اختيار هذا الموضوع بناءً على جملة من الدوافع الذاتية والموضوعية التي تبرر أهميته وجدواه، ويمكن تلخيصها كما يلي:

الأسباب الذاتية:

- الاهتمام العلمي والأكاديمي بمجالات القانون الجنائي وتأثرها بالتطورات التكنولوجية الحديثة، لا سيما الذكاء الاصطناعي.
- الرغبة في البحث في موضوع جديد نسبياً ويطرح تحديات فكرية وقانونية عميقة، ويتطلب إعمال الفكر النقدي والتحليلي.

الأسباب الموضوعية:

- التوسع المتسارع في استخدام الأنظمة الذاتية في مختلف القطاعات، وما يصاحبه من تزايد في المخاطر والحوادث المحتملة.
- الحاجة الماسة إلى تطوير المنظومة القانونية الجنائية لمواكبة هذه التطورات، وتجنب حدوث فراغ قانوني أو "فجوة في المسؤولية".
- أهمية الموضوع على الصعيدين الوطني والدولي، وضرورة مساهمة البحث العلمي في إيجاد حلول قانونية متوازنة ومستدامة.

إشكالية الدراسة:

بناءً على ما تقدم، تتمحور الإشكالية الرئيسة لهذه الدراسة حول التساؤل الجوهري التالي:

إلى أي مدى يمكن إسناد المسؤولية الجزائية عن الأفعال الضارة الصادرة عن الأنظمة الذاتية؟ وما هي السبل الكفيلة بمواكبة التشريع الجنائي للتحديات التقنية التي يفرضها تطور الذكاء الاصطناعي؟

ويتفرع عن هذه الإشكالية المحورية مجموعة من الأسئلة الفرعية التي تسعى الدراسة للإجابة عنها، ومن أبرزها:

- هل يمكن تطبيق أركان المسؤولية الجزائية التقليدية (الفعل، الخطأ، العلاقة السببية، الركن المعنوي) على الأنظمة الذاتية؟ وما هي حدود هذا التطبيق؟
- ما هي أبرز الاتجاهات التشريعية الحديثة في القانون المقارن لمواجهة تحديات المسؤولية الجزائية للذكاء الاصطناعي؟ وما مدى إمكانية الاستفادة منها؟
- ما هي الآليات والمقترحات العملية (التشريعية، التنظيمية، المؤسساتية) التي يمكن تبنيها لتعزيز الوقاية من مخاطر الأنظمة الذاتية وضمان تعويض الضحايا؟

المنهج المتبع في الدراسة:

إجابة عن ألإشكالية استعنا بالمنهج الوصفي والتحليلي والمقارن

فرضيات الدراسة:

سعياً للإجابة على الإشكالية الرئيسة والتساؤلات الفرعية، تنطلق الدراسة من الفرضيات الأولية التالية:

- قد تواجه القواعد التقليدية للمسؤولية الجزائية صعوبات جوهرية في التطبيق المباشر على الأنظمة الذاتية نظراً لغياب الإرادة والتمييز بالمعنى الإنساني لديها.

- قد تتجه المسؤولية الجزائية نحو الأطراف البشرية المتدخلة في دورة حياة النظام الذاتي (الصانع، المبرمج، المستخدم)، بناءً على معايير الخطأ والإخلال بواجبات الحيطة والحذر، مع احتمال ظهور "فجوة في المسؤولية" في بعض الحالات المعقدة.
- قد تتطلب مواكبة التحديات التقنية تعديل النصوص الجنائية القائمة أو استحداث نصوص جديدة لتكييف الجرائم التقليدية والمعلوماتية مع خصوصية الأنظمة الذاتية، مع التركيز على الجرائم غير العمدية والمسؤولية الموضوعية في بعض الحالات.
- قد تحتاج المنظومة القانونية إلى تبني آليات تنظيمية ورقابية مسبقة (مثل معايير السلامة، اختبارات التحيز، آليات الشفافية وقابلية التفسير) وآليات تعويضية لاحقة (مثل صناديق التعويض أو التأمين الإجباري) للتعامل مع مخاطر الذكاء الاصطناعي.

للإجابة على إشكالية الدراسة والتحقق من فرضياتها، تم تقسيم البحث إلى فصلين رئيسيين، يسبقهما هذه المقدمة وتليهما خاتمة تتضمن أهم النتائج والتوصيات، وذلك على النحو التالي:

- **الفصل الأول :إسناد المسؤولية الجزائية للأنظمة الذاتية**
  - المبحث الأول :أركان المسؤولية الجزائية وتحديات الأنظمة الذاتية الركن المادي، الركن المعنوي، مبدأ الشرعية
  - المبحث الثاني :نماذج إسناد المسؤولية الجزائية للأطراف البشرية مسؤولية الصانع، المبرمج، المستخدم، المالك
- **الفصل الثاني :سبل مواكبة التشريع الجنائي للتحديات التقنية**
  - المبحث الأول :التكييف القانوني للجرائم الناتجة عن الأنظمة الذاتية جرائم ضد الأشخاص، جرائم ضد الممتلكات، جرائم معلوماتية

    المبحث الثاني :الاتجاهات التشريعية والمقترحات المستقبلية التشريعات المقارنة، آليات الوقاية والتعويض، أدوار المؤسسات

نأمل من خلال هذه الخطة أن نتمكن من الإحاطة بجوانب الموضوع المختلفة، وتقديم تحليل قانوني معمق يساهم في فهم التحديات واقتراح الحلول المناسبة.

الفصل الأول:

إسناد المسؤولية الجزائية للأنظمة الذاتية

شهدت التكنولوجيا الحديثة تطورات متسارعة أسفرت عن ظهور أنظمة ذاتية التسيير تتمتع بالقدرة على اتخاذ القرارات وتنفيذ الأفعال بصورة مستقلة، مستندة في ذلك إلى تقنيات الذكاء الاصطناعي والبرمجيات المعقدة. تشمل هذه الأنظمة مركبات ذاتية القيادة، روبوتات ذكية، وأنظمة معلوماتية متقدمة، وهو ما أثار نقاشًا قانونيًا جديدًا حول كيفية تطبيق قواعد المسؤولية الجزائية عليها، خصوصًا في ظل غياب الإرادة الإنسانية المباشرة أو السيطرة التقليدية على الأفعال المرتكبة.

في هذا السياق، يواجه القانون الجزائي تحديات جذرية تتعلق بتحديد أركان المسؤولية، بدءًا من الركن المادي للجريمة الصادرة عن الأنظمة التقنية، مرورًا بالإشكالات المتعلقة بالركن المعنوي وسبل الإثبات، وصولًا إلى مدى توافق مبدأ الشرعية مع هذه الظواهر التقنية الحديثة. وهذا يتطلب إعادة النظر في المفاهيم التقليدية المرتبطة بالفاعل، القصد الجنائي، والفعل الجرمي، إضافة إلى تحديد دور التدخل البشري وتأثيره في تحميل المسؤولية.

ولا يقتصر إسناد المسؤولية الجزائية على النظام الذاتي بحد ذاته، بل يمتد ليشمل مجموعة من الفاعلين البشريين مثل المصنعين، المبرمجين، المستخدمين، والمشغلين، حيث تنشأ مسؤوليات متداخلة ومتبادلة تطرح صعوبات في تحديد المسؤول الحقيقي عن الفعل الجرمي. هذا التعقيد يستدعي دراسة النماذج المختلفة للمسؤولية التي وضعها الفقه والقضاء في محاولة لتكييف القانون مع التطورات التقنية.

علاوة على ذلك، تطرح فكرة اعتبار النظام الذاتي ككيان قانوني مستقل يتحمل مسؤولية جزائية نفسها نقاشًا مستمرًا في التشريعات والآراء الفقهية الدولية، نظرًا لما تثيره من مسائل تتعلق بالشخصية القانونية والمبادئ الأساسية في القانون الجنائي.

بناءً على ذلك، سيتناول هذا الفصل دراسة أركان المسؤولية الجزائية والتحديات التي تفرضها الأنظمة الذاتية، مع تحليل نماذج إسناد المسؤولية المختلفة في الجرائم التقنية، انطلاقًا من محاولة تحقيق التوازن بين متطلبات الأمن القانوني ومتطلبات التطور التكنولوجي المعاصر.

المبحث الأول: أركان المسؤولية الجزائية وتحديات الأنظمة ذاتية التسيير

يمثل ظهور الأنظمة الذاتية وتطور الذكاء الاصطناعي تحدياً كبيراً للقواعد القانونية التقليدية، لا سيما في مجال القانون الجزائي. فقدرة هذه الأنظمة على اتخاذ قرارات وتنفيذ أفعال بشكل مستقل عن التدخل البشري المباشر تثير تساؤلات جوهرية حول كيفية تطبيق أركان المسؤولية الجزائية المعروفة، وهي الركن المادي والركن المعنوي، بالإضافة إلى مدى انطباق مبدأ الشرعية الجنائية على الأفعال الضارة التي قد تنجم عنها. يتطلب فهم هذه التحديات تحليلاً دقيقاً لطبيعة هذه الأنظمة وكيفية تفاعلها مع محيطها، ومدى قدرة المفاهيم القانونية القائمة على استيعاب هذه الظواهر الجديدة.[1]

سنخصص هذا المبحث لدراسة هذه الإشكاليات، حيث سنتناول في المطلب الأول تحليل الركن المادي في سياق الجرائم التي يمكن أن ترتكبها الأنظمة الذاتية، مع التركيز على مفهوم الفعل الجرمي والعلاقة السببية وطبيعة التدخل البشري. وفي المطلب الثاني، سنبحث في تحديات إثبات الركن المعنوي، نظراً لغياب الإرادة والتمييز بالمعنى الإنساني لدى هذه الأنظمة، وقصور مفاهيم القصد الجنائي والخطأ غير العمدي التقليدية. وأخيراً، سنتطرق في المطلب الثالث إلى حدود تطبيق مبدأ الشرعية الجنائية "لا جريمة ولا عقوبة إلا بنص" في مواجهة الجرائم التقنية المستحدثة وصعوبات التكييف القانوني.

المطلب الأول: الركن المادي في جرائم الأنظمة ذاتية التسيير

يعتبر الركن المادي الدعامة الأساسية لأي جريمة، فهو يمثل المظهر الخارجي للسلوك الإجرامي الذي يجرمه القانون ويعاقب عليه. ويتكون هذا الركن تقليدياً من ثلاثة عناصر أساسية: الفعل أو الامتناع، والنتيجة الإجرامية، والعلاقة السببية التي تربط بين الفعل والنتيجة[2]. وفي سياق الأنظمة الذاتية، يواجه تطبيق هذه العناصر تحديات فريدة تتطلب إعادة نظر وتكييف.

[1] أحمد عبد الكريم سلام، المسؤولية الجنائية عن الجرائم المرتكبة بواسطة الذكاء الاصطناعي، دار الجامعة الجديدة، الإسكندرية، 2021، ص. 45.

[2] كريمة بوشامة، الإشكالات القانونية للذكاء الاصطناعي في القانون الجنائي، مجلة دفاتر السياسة والقانون، العدد 28، جامعة خنشلة، 2022، ص. 135.

الفرع الأول: السلوك الإجرامي الصادر عن الأنظمة ذاتية التسيير

في ظل التطور التكنولوجي المتسارع، أصبح من الضروري إعادة النظر في مفهوم الفعل الجرمي التقليدي، خصوصًا عند تناول السلوك الصادر عن الأنظمة الذاتية. فالفرع الأول يركز على مدى إمكانية اعتبار السلوك الذي يصدر عن هذه الأنظمة "فعلاً" بالمعنى القانوني، مع مراعاة أن هذه الأنظمة لا تمتلك إرادة أو وعيًا بشريًا، مما يثير تساؤلات حول مدى ملاءمة التصنيفات القانونية التقليدية لهذه الظواهر الحديثة.

أولاً: اعتبار سلوك النظام الذاتي "فعلاً" بالمعنى القانوني

يثير التساؤل الأساسي حول طبيعة السلوك الصادر عن النظام الذاتي موضوعًا قانونيًا معقدًا، وهو مدى جواز اعتباره "فعلاً" بالمعنى القانوني المتعلق بالركن المادي للجريمة. ففي المفهوم التقليدي، يُعرف الفعل الجرمي على أنه كل حركة عضوية إرادية يصدرها الإنسان بقصد إحداث تغيير ملموس في الواقع الخارجي، ويكون هذا التغيير محظورًا أو مجرّمًا بموجب القانون. وهذا التعريف يقوم بشكل أساسي على وجود الإرادة والوعي البشري كشرطين أساسيين لتكوين الفعل.

أما بالنسبة للأنظمة الذاتية، فهي تمتلك القدرة على القيام بسلوكيات مادية ملموسة تؤدي إلى نتائج ضارة، غير أنها تفتقر في الوقت ذاته إلى الإرادة والوعي بالمعنى الإنساني. لذلك، يثير هذا الأمر إشكالاً في اعتبار تصرفاتها أفعالًا قانونية. إذ يذهب جزء من الفقه إلى التساؤل عن مدى إمكانية اعتبار الخوارزميات التي تدير هذه الأنظمة وتوجه سلوكها كأفعال بالمعنى القانوني. فهذه الخوارزميات ليست سوى تعليمات برمجية مُسبقة أو نتائج لعمليات تعلم آلي معقدة، تفتقد إلى الوعي والإرادة الذاتية، وبالتالي لا يمكن وصفها بأنها أفعال إرادية.

وعليه، فإن السلوك الذي تصدره الأنظمة الذاتية يُنظر إليه على أنه مجرد حدث أو نتيجة تقنية محضة، لا يرتقي لأن يكون "فعلًا" بالمعنى الدقيق في القانون الجنائي. هذا الموقف يبرز صعوبة واضحة في إدماج سلوك هذه الأنظمة ضمن التصنيفات التقليدية للركن المادي، مما يفرض الحاجة إلى تطوير مفاهيم قانونية جديدة تتناسب مع التطورات التقنية المعاصرة.[1]

[1] لطفي بوعزة، الذكاء الاصطناعي والمسؤولية الجنائية: مقاربة قانونية، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة الجزائر 1، العدد 2، 2021، ص. 88.

في المقابل، يرى اتجاه آخر أن التركيز يجب أن ينصب على المظهر الخارجي للسلوك ونتائجه المادية، بغض النظر عن مصدره الداخلي (إرادة إنسانية أو خوارزمية). فإذا قام النظام الذاتي بسلوك أدى إلى نتيجة يجرمها القانون (مثل سيارة ذاتية القيادة تتسبب في حادث قتل خطأ، أو نظام طبي آلي يعطي تشخيصاً خاطئاً يؤدي إلى وفاة مريض، أو نظام تداول مالي آلي يقوم بممارسات تلاعب بالسوق)[1]، فإن هذا السلوك المادي يشكل مظهراً خارجياً يمكن اعتباره "فعلاً" من الناحية الموضوعية، حتى لو لم يكن مدفوعاً بإرادة إنسانية. هذا الاتجاه يركز على الأثر المادي للسلوك في العالم الخارجي، ويرى أن القانون يجب أن يتطور لاستيعاب هذه الأفعال "التقنية" ومعالجة آثارها الضارة.[2]

ثانياً: الأفعال الجرمية المحتملة الأنظمة ذاتية التسيير

تتعدد الأمثلة على الأفعال الإجرامية التي قد تصدر عن الأنظمة الذاتية، وتتنوع في طبيعتها وتأثيرها، مما يعكس تعقيد التحديات القانونية المرتبطة بها. فمن بين هذه الأمثلة، يمكن ذكر التسبب في حوادث سير أو حوادث طيران ناجمة عن خلل في أنظمة القيادة الذاتية أو أنظمة الملاحة الذكية، مما يؤدي إلى أضرار جسيمة في الأرواح والممتلكات. كما تشمل الانتهاكات المحتملة انتهاك خصوصية الأفراد، عبر جمع ومعالجة البيانات الشخصية بطرق غير قانونية بواسطة أنظمة المراقبة الذكية أو تقنيات التحليل الآلي.

علاوة على ذلك، قد تتخذ هذه الأنظمة قرارات تمييزية تضر بمصالح الأفراد في مجالات حساسة مثل التوظيف أو منح القروض، حيث تعتمد الخوارزميات على معايير متحيزة تؤدي إلى التفرقة أو التمييز غير المبرر. كما يمكن أن تسهم في نشر المعلومات المضللة أو خطابات الكراهية عبر أنظمة توليد المحتوى الآلي، مما ينعكس سلبًا على النسيج الاجتماعي. بالإضافة إلى ذلك، لا يُستبعد أن تشارك هذه الأنظمة في شن هجمات سيبرانية معقدة تستهدف البنى التحتية الحيوية أو المؤسسات الحساسة.

كل هذه التصرفات، بالرغم من كونها صادرة عن كيانات غير بشرية، تتمتع بآثار مادية واضحة وخطيرة، مما يطرح تحديات كبيرة أمام الإطار القانوني الجزائي التقليدي، الذي لم يكن مصممًا للتعامل مع هذه الأشكال الجديدة من السلوك التقني.[3]

[1] وسيم حمدي، إشكالية الركن المادي في الجرائم، مجلة القانون والتكنولوجيا، العدد 5، 2022، ص. 112

[2] نفس المرجع، ص 132.

[3] سامي عبد العال، التقنيات الذكية والتحديات الجنائية المعاصرة، دار الكتب القانونية، القاهرة، 2020، ص. 154.

تبقى إشكالية استقلالية القرار لدى النظام الذاتي نقطة محورية في هذا النقاش. فكلما زادت درجة استقلالية النظام وقدرته على التعلم والتكيف واتخاذ قرارات غير متوقعة من قبل المبرمجين أو المستخدمين، كلما تعقدت مسألة تحديد طبيعة الفعل الصادر عنه ومدى إمكانية اعتباره فعلاً جرمياً مستقلاً يمكن أن تنبني عليه المسؤولية الجزائية، سواء للنظام ذاته (وهو أمر محل جدل كبير كما سنرى لاحقاً) أو للأطراف البشرية المرتبطة به.[1]

الفرع الثاني: العلاقة السببية بين الفعل والنتيجة

لقيام الركن المادي للجريمة، لا يكفي وقوع الفعل فقط، بل يجب إثبات وجود علاقة سببية واضحة بين الفعل والنتيجة الضارة. تستعرض النظريات التقليدية للسببية والتحديات التي تواجه تطبيقها في ظل التطورات التقنية الحديثة.

أولاً: نظريات السببية التقليدية وتحديات تطبيقها

لا يكفي لقيام الركن المادي للجريمة وقوع الفعل الجرمي، بل لا بد من إثبات وجود رابطة سببية واضحة ومباشرة بين هذا الفعل والنتيجة الضارة التي يجرمها القانون. فالعلاقة السببية هي الجسر الذي يربط بين سلوك الجاني والأثر المترتب عليه، وهي عنصر جوهري لتحديد المسؤولية الجزائية. وتواجه عملية إثبات هذه العلاقة تحديات كبيرة في سياق الأنظمة الذاتية، تفوق تلك الموجودة في الجرائم التقليدية.[2]

تعتمد القواعد التقليدية في إثبات العلاقة السببية على معايير ونظريات مختلفة، أبرزها نظرية تعادل الأسباب التي تعتبر كل سبب ساهم في إحداث النتيجة، ولو بقدر ضئيل، سبباً قانونياً لها، ونظرية السببية الملائمة أو المنتجة التي تعتد فقط بالسبب الذي من شأنه عادةً أن يؤدي إلى مثل هذه النتيجة وفقاً للمجرى العادي للأمور، ونظرية السبب المباشر أو الفعال التي تركز على السبب الأخير والمباشر الذي أدى إلى وقوع النتيجة. ويختار المشرع والقضاء عادة النظرية التي يرونها أكثر ملاءمة لتحقيق العدالة في كل حالة.[3]

---

[1] "هل يمكن محاسبة الذكاء الاصطناعي جنائيًا؟"، موقع الباحث القانوني، نُشر بتاريخ 10 مارس 2023، على الرابط: www.legalresearcher-dz.com/ai-criminal-responsibility تم الدخول إليه في 22 ماي 2025.

[2] عبد الحفيظ بوقرة، المسؤولية الجنائية في ظل الذكاء الاصطناعي: مقاربة تحليلية قانونية، أطروحة دكتوراه، جامعة الجزائر 1، كلية الحقوق، 2023، ص. 121.

[3] خديجة بن زيان، المسؤولية الجنائية عن أخطاء الذكاء الاصطناعي: دراسة في القانون الجزائري والمقارن، مذكرة ماستر، جامعة وهران 2، كلية الحقوق، 2022، ص. 55.

ثانياً: عوائق إثبات السببية في سياق الأنظمة ذاتية التسيير

لكن تطبيق هذه المعايير والنظريات على الأفعال الصادرة عن الأنظمة الذاتية يصطدم بصعوبات جمة. أولى هذه الصعوبات تتمثل في تعقيد العمليات الداخلية لهذه الأنظمة، فغالباً ما تتخذ القرارات بناءً على تحليل كم هائل من البيانات ومعالجتها عبر خوارزميات معقدة ومتشابكة، قد تكون غير مفهومة حتى لمصمميها في بعض الأحيان، خاصة في أنظمة التعلم العميق. هذا التعقيد يجعل من الصعب تتبع سلسلة القرارات والأسباب التي أدت إلى السلوك الضار وتحديد السبب الفعلي أو الملائم للنتيجة.[1]

يضاف إلى ذلك مشكلة تعدد العوامل المتداخلة في عمل النظام الذاتي. فالنظام لا يعمل بمعزل عن محيطه، بل يتفاعل مع بيئته ومع أنظمة أخرى ومع تدخلات بشرية محتملة (مثل تحديثات البرامج، بيانات التدريب، قرارات المستخدم). هذا التفاعل المستمر يجعل من الصعب عزل سلوك النظام كسبب وحيد للنتيجة، فقد تكون النتيجة محصلة لتفاعل معقد بين خطأ في البرمجة، وبيانات تدريب متحيزة، وظروف بيئية غير متوقعة، وقرار خاطئ من المستخدم، مما يشتت رابطة السببية ويصعب تحديد المسؤول الرئيسي.[2]

كما يبرز دور ما يعرف بـ "الصندوق الأسود" (Black Box) كعائق كبير أمام إثبات السببية. يشير هذا المصطلح إلى عدم القدرة على فهم أو تفسير كيفية وصول النظام الذاتي إلى قرار معين أو سبب قيامه بسلوك محدد، وذلك بسبب تعقيد الخوارزميات أو طبيعة تقنيات التعلم الآلي المستخدمة التي قد لا توفر تفسيرات واضحة لعملياتها الداخلية. هذا الغموض يجعل من شبه المستحيل أحياناً إثبات أن سلوك النظام هو السبب المباشر أو الملائم للنتيجة الجرمية، مما يفتح الباب أمام صعوبات إثباتية قد تحول دون قيام المسؤولية الجزائية.[3]

لذلك، يتطلب التعامل مع إشكالية العلاقة السببية في جرائم الأنظمة الذاتية تطوير آليات إثبات جديدة، قد تشمل فرض التزامات بالشفافية وقابلية التفسير على مصممي الأنظمة، وتطوير أدوات تقنية لتحليل

---

[1] فوزي بلعياشي، الذكاء الاصطناعي وتحديات الإثبات في القانون الجنائي، أطروحة دكتوراه، جامعة قسنطينة 1، 2024، ص. 196.

[2] كيف تؤثر العوامل الخارجية في قرارات الذكاء الاصطناعي؟"، مقال منشور على موقع المنصة القانونية العربية، بتاريخ 12 فيفري 2024، الرابط:
www.arablegalplatform.org/ai-external-factors تم الدخول إليه في 24 ماي 2025.

[3] فوزي بلعياشي، المرجع السابق، ص 122

سجلات عمل الأنظمة وتتبع مسار القرارات، وربما إعادة النظر في نظريات السببية التقليدية لتكون أكثر مرونة في التعامل مع الأسباب المتعددة والمتفاعلة في البيئة الرقمية المعقدة.[1]

الفرع الثالث: طبيعة التدخل البشري في الفعل التقني

رغم اعتماد الأنظمة التقنية على الاستقلالية في أدائها، يبقى التدخل البشري حاضراً في مراحل عدة من دورة حياتها، من التصميم إلى التشغيل. يطرح هذا الواقع تساؤلات حول مدى استقلالية الفعل الصادر عن النظام، وهل هو فعل مستقل أم امتداد لتدخل بشري.

أولاً: مستويات التدخل البشري وتأثيرها

رغم وصفها بالأنظمة "الذاتية" أو "المستقلة"، إلا أن هذه الأنظمة لا تنشأ من فراغ، بل هي نتاج تدخل بشري في مراحل مختلفة من دورة حياتها، بدءاً من التصميم والبرمجة، مروراً بالتدريب والاختبار، وصولاً إلى التشغيل والاستخدام والإشراف. هذا التدخل البشري يثير تساؤلات هامة حول طبيعة الفعل الصادر عن النظام، ومدى اعتباره فعلاً مستقلاً تماماً أم أنه مجرد امتداد أو نتيجة للتدخل البشري. كما تطرح هذه العلاقة تساؤلات حول حدود المسؤولية في حالة غياب التدخل البشري المباشر لحظة وقوع الفعل الضار.[2]

تتعدد مستويات التدخل البشري في عمل الأنظمة الذاتية. فهناك تدخل في مرحلة التصميم وتحديد الأهداف والقيود التي سيعمل النظام ضمنها. وهناك تدخل في مرحلة البرمجة وكتابة الخوارزميات التي تحكم سلوك النظام. وهناك تدخل في مرحلة تزويد النظام بالبيانات اللازمة لتدريبه وتعلمه. وهناك تدخل في مرحلة الإشراف والمراقبة أثناء عمل النظام، حيث قد يحتفظ الإنسان بالقدرة على التدخل وتجاوز قرارات النظام في بعض الحالات (Human-in-the-loop). وأخيراً، هناك تدخل في مرحلة الاستخدام اليومي للنظام، حيث يتخذ المستخدم قرارات بشأن كيفية ووقت ومكان تشغيل النظام.[3]

يؤثر مستوى وطبيعة هذا التدخل البشري بشكل كبير على درجة استقلالية النظام الذاتي. فكلما كان التدخل البشري أكثر كثافة ومباشرة، كلما ضعف الحديث عن استقلالية النظام، وأصبح من الأسهل إسناد

[1] سامي العبد، المسؤولية الجنائية في ظل الأنظمة الذكية: دور التدخل البشري، دار النهضة العلمية، بيروت، 2022، ص. 98.

[2] ليلى حمودي، "دور التدخل البشري في المسؤولية عن أفعال الأنظمة الذكية"، مجلة القانون والتكنولوجيا، العدد 12، 2023، ص. 62.

[3] نفس المرجع ص، 65

الفعل الصادر عن النظام إلى الشخص المتدخل. فإذا قام مبرمج بتصميم نظام يتخذ قرارات تمييزية بشكل متعمد، أو قام مستخدم بتشغيل نظام سلاح ذاتي في ظروف تنتهك قواعد الاشتباك، فإن فعل النظام هنا يمكن اعتباره امتداداً مباشراً لفعل بشري إرادي، وتكون المسؤولية الجزائية واضحة نسبياً.[1]

ثانياً: إشكالية المسؤولية عند تباعد التدخل البشري أو عدم توقعه

لكن الإشكالية تتعقد عندما يكون التدخل البشري غير مباشر أو بعيد زمنياً عن لحظة وقوع الفعل الضار، أو عندما يتصرف النظام بطرق غير متوقعة لم يقصدها المصمم أو المبرمج أو المستخدم. يثور التساؤل هنا حول مدى اعتبار فعل النظام في هذه الحالة امتداداً لفعل بشري. يرى البعض أن المسؤولية يجب أن تظل مرتبطة بالتدخل البشري، حتى لو كان غير مباشر، من خلال البحث عن خطأ أو إهمال في التصميم أو البرمجة أو الإشراف أو الاستخدام أدى إلى السلوك الضار للنظام. فالمسؤولية هنا لا تنبني على القصد المباشر لإحداث النتيجة، بل على الإخلال بواجبات الحيطة والحذر في التعامل مع تكنولوجيا قد تكون خطرة بطبيعتها.[2]

في المقابل، يرى آخرون أنه مع تزايد استقلالية الأنظمة وقدرتها على التعلم والتطور بشكل ذاتي، قد نصل إلى مرحلة يصبح فيها سلوك النظام منفصلاً بشكل كبير عن أي تدخل بشري مباشر أو غير مباشر يمكن اعتباره سبباً كافياً للنتيجة. في هذه الحالة، قد يصبح من الصعب إسناد المسؤولية إلى أي طرف بشري وفقاً للقواعد التقليدية، مما يطرح مجدداً فكرة البحث عن آليات بديلة للمساءلة، قد تشمل مسؤولية موضوعية أو حتى مساءلة النظام ذاته.[3]

تبقى مسألة المسؤولية في حالة غياب التدخل البشري المباشر لحظة وقوع الجريمة هي الأكثر إثارة للجدل. ففي حالة قيام نظام ذاتي مستقل تماماً باتخاذ قرار أدى إلى نتيجة جرمية، دون أي تدخل بشري آني، فإن تحديد المسؤول يصبح أمراً عسيراً. هل هو المصمم الذي وضع الأسس الأولى للنظام قبل سنوات؟ أم المبرمج الذي كتب جزءاً من الكود؟ أم المستخدم الذي قام بتشغيل النظام؟ أم لا أحد منهم؟

---

[1] سميرة دحمان، المسؤولية الجنائية عن الأفعال الناجمة عن الأنظمة الذاتية: دور التدخل البشري، مذكرة ماجستار، جامعة باتنة 2، كلية الحقوق، 2023، ص. 77.

[2] خالد المرزوقي، استقلالية الأنظمة الذاتية ومسؤولية الإنسان: دراسة مقارنة، دار الفكر الحديث، الرياض، 2022، ص. 101.

[3] سامي العبد، المرجع السابق، ص 101

هذا الفراغ المحتمل في المسؤولية يمثل أحد أكبر التحديات التي تواجه القانون الجزائي في عصر الذكاء الاصطناعي، ويتطلب حلولاً تشريعية وقضائية مبتكرة.[1]

المطلب الثاني: الركن المعنوي في الجرائم الأنظمة ذاتية التسيير

إذا كان الركن المادي يمثل الجانب الموضوعي للجريمة، فإن الركن المعنوي يمثل جانبها الشخصي أو النفسي، وهو يعبر عن الموقف الذهني للجاني تجاه فعله ونتيجته. ويقوم الركن المعنوي تقليدياً على عنصري الإرادة والتمييز (أو الإدراك)، ويتخذ صورتين رئيسيتين: القصد الجنائي (العمد)، والخطأ غير العمدي. ويعد توافر الركن المعنوي شرطاً أساسياً لقيام المسؤولية الجزائية، إذ لا يكفي مجرد وقوع الضرر لمعاقبة شخص ما، بل يجب أن يكون هذا الضرر ناجماً عن إرادة آثمة أو خطأ ينسب إليه.

يثير تطبيق مفهوم الركن المعنوي على الأفعال الصادرة عن الأنظمة الذاتية إشكاليات أكثر تعقيداً من تلك المتعلقة بالركن المادي. فالأنظمة الذاتية، بطبيعتها كآلات مبرمجة، تفتقر إلى الوعي والإرادة الحرة والقدرة على التمييز بين الخير والشر بالمعنى الإنساني والأخلاقي الذي تقوم عليه فكرة الركن المعنوي. هذا الغياب الجوهري للإرادة والتمييز يضع تحديات جذرية أمام إمكانية إثبات القصد الجنائي أو حتى الخطأ غير العمدي لدى هذه الأنظمة، ويجعل من الصعب مساءلتها بشكل مباشر وفقاً للمبادئ التقليدية للقانون الجزائي.[2]

سنخصص هذا المطلب لاستكشاف هذه الإشكاليات، حيث سنتناول في الفرع الأول مسألة غياب الإرادة والتمييز لدى الأنظمة الذاتية وتأثير ذلك على إمكانية مساءلتها. وفي الفرع الثاني، سنبحث في قصور مفهوم القصد الجنائي التقليدي عن استيعاب طبيعة عمل هذه الأنظمة. أما الفرع الثالث، فسيركز على مدى إمكانية تطبيق قواعد المسؤولية عن الخطأ غير العمدي في السياق التكنولوجي، والبحث عن المسؤولية لدى الأطراف البشرية المرتبطة بالنظام.

[1] "تحديات إثبات القصد الجنائي في عصر الذكاء الاصطناعي"، مقال منشور في موقع القانون الرقمي العربي، بتاريخ 10 يناير 2024، الرابط:

www.arabdigitaljustice.com/intent-a تم الدخول إليه في 19 ماي 2025

[2] فاطمة الزهراء بن عيسى، "إشكاليات الركن المعنوي في الأفعال الصادرة عن الأنظمة الذكية"، مجلة العلوم القانونية والاقتصادية، العدد 18، 2023، ص. 57

الفرع الأول: غياب الإرادة والتمييز في الأنظمة ذاتية التسيير

يشترط القانون الجزائي لقيام المسؤولية الجزائية، كقاعدة عامة، أن يكون مرتكب الفعل متمتعاً بالإرادة الحرة والقدرة على التمييز والإدراك وقت ارتكاب الجريمة. فالإرادة هي القدرة على توجيه السلوك نحو هدف معين، والتمييز هو القدرة على فهم طبيعة الفعل وأبعاده وتقدير نتائجه والتفريق بين المباح والمحظور. وهذان العنصران مرتبطان ارتباطاً وثيقاً بالوعي والقدرات العقلية والنفسية للإنسان.[1]

لكن الأنظمة الذاتية، مهما بلغت درجة تطورها وتعقيدها، تظل في جوهرها آلات تفتقر إلى الوعي الذاتي والإرادة الحرة بالمعنى الفلسفي والقانوني. صحيح أنها قادرة على معالجة المعلومات واتخاذ قرارات وتنفيذ أفعال تبدو "ذكية" أو "مستقلة"، إلا أن هذا السلوك هو نتاج خوارزميات وتعليمات برمجية وبيانات تم تغذيتها بها، وليس نابعاً عن وعي أو إرادة حقيقية مماثلة للإرادة الإنسانية. فالذكاء الاصطناعي، حتى في أكثر صوره تقدماً، يختلف جوهرياً عن الوعي البشري والقدرة على الشعور والتفكير الأخلاقي.[2]

هذا الغياب الجوهري للإرادة والتمييز لدى الأنظمة الذاتية يطرح تساؤلاً أساسياً حول إمكانية مساءلة كيان يفتقر إلى هذه المقومات الأساسية للمسؤولية. يرى غالبية الفقه القانوني أن الإجابة هي بالنفي.
فالمسؤولية الجزائية ترتبط ارتباطاً وثيقاً باللوم الأخلاقي والقانوني الذي يوجه إلى شخص قادر على الاختيار بين السلوك المشروع وغير المشروع، وهذا اللوم لا يمكن توجيهه إلى آلة لا تملك هذه القدرة. وبالتالي، فإن مساءلة النظام الذاتي ذاته تبدو متعارضة مع المبادئ الأساسية التي يقوم عليها القانون الجزائي الحديث، والذي يركز على الإنسان كفاعل ومسؤول أساسي.[3]

إن محاولة تطبيق مفاهيم الإرادة والتمييز على الأنظمة الذاتية قد تؤدي إلى نوع من التشبيه أو المجاز القانوني الذي قد لا يكون دقيقاً أو ملائماً. فمقارنة بين الذكاء الاصطناعي والوعي البشري تظهر فجوة كبيرة؛ فالأول يعتمد على معالجة البيانات والتعرف على الأنماط، بينما الثاني يشمل الوعي الذاتي، والعواطف، والقيم الأخلاقية، والقدرة على الفهم العميق للسياق الاجتماعي والإنساني. هذا الاختلاف

[1] جمال سعدو حبش، المسؤولية الجزائية عن حوادث المركبات ذاتية القيادة، جامعة الشرق الأدنى، معهد الدراسات العليا، كلية الحقوق / قسم القانون العام، رسالة ماجستير، 2021، ص35

[2] نفس المرجع، ص 62

[3] فاطمة الزهراء بن عيسى، المرجع السابق، ص 88.

الجوهري يجعل من الصعب، إن لم يكن من المستحيل، اعتبار النظام الذاتي "فاعلاً" بالمعنى الكامل الذي يتطلبه القانون الجزائي لتحميله المسؤولية عن أفعاله.[1]

يترتب على غياب الإرادة والتمييز لدى الأنظمة الذاتية نتيجة هامة، وهي صعوبة، بل استحالة، مساءلة النظام ذاته جزائياً وفقاً للقواعد الحالية. وهذا يدفع بالضرورة إلى البحث عن المسؤولية لدى الأطراف البشرية التي تقف وراء النظام، مثل المصممين والمبرمجين والمصنعين والمستخدمين والمشغلين، وهو ما سنتناوله بتفصيل أكبر في المبحث الثاني من هذا الفصل. ومع ذلك، فإن هذا لا ينفي الحاجة إلى التفكير في آليات تنظيمية ورقابية أخرى للتعامل مع المخاطر التي تشكلها هذه الأنظمة، حتى لو لم ترق إلى مستوى المسؤولية الجزائية التقليدية.[2]

الفرع الثاني: عدم ملاءمة القصد الجنائي التقليدي في جرائم الأنظمة ذاتية التسيير

إذا كان غياب الإرادة والتمييز يحول دون مساءلة النظام الذاتي نفسه، فإنه يلقي بظلال من الشك أيضاً على إمكانية إثبات الركن المعنوي في صورته العمدية، أي القصد الجنائي، سواء لدى النظام (وهو أمر مستبعد كما رأينا) أو حتى لدى الأطراف البشرية المرتبطة به في بعض الحالات.[3]

يعرف القصد الجنائي تقليدياً بأنه "انصراف إرادة الجاني إلى ارتكاب الجريمة مع العلم بأركانها كما يتطلبها القانون". فهو يتكون من عنصرين أساسيين: العلم والإرادة. العلم يعني أن يكون الجاني مدركاً لطبيعة فعله وللظروف المحيطة به وللنتيجة التي قد تترتب عليه وأن هذا الفعل مجرم قانوناً. والإرادة تعني أن تتجه نيته ورغبته إلى تحقيق هذا الفعل وهذه النتيجة المحظورة.[4]

تطبيق هذين العنصرين على الأنظمة الذاتية يواجه صعوبات جمة. فلا يمكن إثبات "علم" نظام ذاتي بطبيعة فعله أو نتائجه، كما لا يمكن إثبات "إرادة" لديه لتحقيق نتيجة جرمية. وكما ذكرنا سابقاً، تفتقر

---

[1] أحمد بوساحة، المرجع السابق، 10.

[2] هالة بوطرفاية، القصد الجنائي في ظل التطور التكنولوجي: مسؤولية الإنسان والنظام، مذكرة ماجستير، جامعة قسنطينة 2، 2023، ص. 120.

[3] "إشكاليات إثبات القصد الجنائي في أنظمة الذكاء الاصطناعي"، مقال منشور على موقع المجلة القانونية الرقمية بتاريخ 5 مارس 2024، الرابط:www.digitallegallaw.com/intent-ai-issues تم الدخول إليه في 23 ماي 2025.

[4] فريدة سالم، "تطبيق مفهوم القصد الجنائي في عصر الذكاء الاصطناعي"، مجلة العلوم القانونية الحديثة، العدد 29، 2024، ص. 66

الأنظمة الذاتية إلى الوعي والإدراك والإرادة بالمعنى الإنساني. وبالتالي، فإن إسناد القصد الجنائي إليها يبدو أمراً غير منطقي ومستحيلاً من الناحية العملية والقانونية.[1]

حتى عند محاولة إثبات القصد الجنائي لدى الأطراف البشرية (المصمم، المبرمج، المستخدم)، قد تثور صعوبات في سياق الأنظمة الذاتية. ففي كثير من الأحيان، قد لا يكون الضرر الناتج عن النظام مقصوداً بشكل مباشر من قبل أي طرف بشري. قد يكون النظام قد تصرف بطريقة غير متوقعة نتيجة لتعقيد خوارزمياته أو تفاعله مع بيئة متغيرة أو بسبب تعلمه الذاتي لأنماط سلوكية ضارة لم يتوقعها مصمموه. في هذه الحالات، قد ينتفي القصد الجنائي المباشر لدى الأطراف البشرية، مما يجعل من الصعب مساءلتهم عن جريمة عمدية.[2]

يثور التساؤل حول مدى إمكانية افتراض القصد الجنائي بناءً على تصميم النظام أو خوارزمياته. أي هل يمكن اعتبار أن من صمم نظاماً قادراً على إحداث ضرر معين، أو من برمج خوارزمية قد تؤدي إلى نتائج تمييزية، كان لديه القصد الاحتمالي لوقوع هذا الضرر؟ القصد الاحتمالي هو حالة يتوقع فيها الجاني إمكانية حدوث النتيجة الجرمية كأثر محتمل لفعله، ورغم ذلك يقبل المخاطرة ويمضي في فعله. قد يكون هذا المفهوم أكثر قابلية للتطبيق في بعض الحالات،[3] كأن يقوم مبرمج بإطلاق نظام وهو يعلم بوجود ثغرات أمنية خطيرة قد تستغل لإحداث ضرر، أو أن يصمم نظاماً للتعرف على الوجوه مع علمه باحتمالية استخدامه في المراقبة الجماعية غير القانونية. ومع ذلك، يظل إثبات القصد الاحتمالي أمراً صعباً يتطلب إثبات علم الجاني باحتمالية وقوع النتيجة وقبوله بها، وهو ما قد يكون عسيراً في ظل تعقيدات الأنظمة الذاتية.

الفرع الثالث: الخطأ الغير العمدي كأساس للمسؤولية الجزائية في جرائم الأنظمة ذاتية التسيير

أمام صعوبة إثبات القصد الجنائي في كثير من الحالات المتعلقة بالأنظمة الذاتية، يبرز الخطأ غير العمدي كأساس بديل محتمل لمساءلة الأطراف البشرية المسؤولة عن هذه الأنظمة. فالخطأ غير العمدي لا يتطلب نية إجرامية لتحقيق النتيجة الضارة، بل يكتفي بوقوع إهمال أو عدم احتراز أو عدم مراعاة للقوانين واللوائح أدى إلى وقوع الضرر الذي كان يمكن توقعه وتجنبه ببذل العناية الواجبة.[4]

---

[1] نفس المرجع، ص 84.

[2] جمال سعدو حبش، المرجع السابق، ص 46.

[3] يلى عزوز، القصد الجنائي والنية في الجرائم التقنية: دراسة تطبيقية، دار الثقافة القانونية، الجزائر، 2021، ص. 143.

[4] المرجع نفسه، ص 112.

يمكن تصور وقوع الخطأ غير العمدي في مختلف مراحل دورة حياة النظام الذاتي. فقد يقع الخطأ من المصمم أو المبرمج إذا أهمل في تصميم نظام آمن أو في اختبار الخوارزميات بشكل كافٍ للتأكد من خلوها من العيوب أو التحيزات التي قد تؤدي إلى نتائج ضارة متوقعة. وقد يقع الخطأ من المصنع إذا لم يلتزم بمعايير الجودة والسلامة في عملية الإنتاج. وقد يقع الخطأ من المستخدم أو المشغل إذا أهمل في صيانة النظام أو تحديثه، أو استخدمه بطريقة غير ملائمة أو في ظروف تتجاوز قدراته، أو لم يقم بالإشراف اللازم عليه.[1]

يعتمد تقدير الخطأ غير العمدي عادة على معيار موضوعي، هو معيار "الشخص المعتاد" أو "المهني الحريص" من نفس فئة المسؤول (مصمم، مبرمج، مستخدم). فيتم مقارنة سلوك الشخص المسؤول في الظروف المحددة بسلوك شخص معتاد أو مهني حريص في نفس الظروف، فإذا ثبت أن سلوكه انحرف عن هذا المعيار الموضوعي وكان هذا الانحراف هو السبب في وقوع الضرر، قامت مسؤوليته عن الخطأ غير العمدي.[2]

ومع ذلك، فإن تطبيق معيار الخطأ غير العمدي في سياق الأنظمة الذاتية يواجه أيضاً تحديات. فمن الصعب أحياناً تحديد مستوى العناية الواجبة المطلوبة في التعامل مع تقنيات جديدة ومعقدة وغير مفهومة تماماً. كما أن تحديد ما إذا كان الضرر "متوقعاً" قد يكون صعباً في ظل قدرة بعض الأنظمة على التعلم والتصرف بطرق غير متوقعة. ويتطلب الأمر وضع معايير واضحة ومفصلة لواجبات الحيطة والحذر المفروضة على مختلف الأطراف المعنية بالأنظمة الذاتية، وتطوير الخبرات الفنية اللازمة لتقييم مدى الالتزام بهذه الواجبات في كل حالة.

المطلب الثالث: نطاق مبدأ الشرعية في جرائم الأنظمة ذاتية التسيير

يعد مبدأ الشرعية الجنائية، المعبر عنه تكييف السلوك الإجرامي حجر الزاوية في النظام القانوني الجزائي الحديث وحصناً أساسياً لحماية الحقوق والحريات الفردية. فهو يعني أن الأفعال المباحة هي الأصل، وأن التجريم هو الاستثناء، ولا يمكن اعتبار فعل ما جريمة أو فرض عقوبة على مرتكبه إلا إذا وجد نص قانوني صريح وواضح يجرم هذا الفعل ويحدد عقوبته مسبقاً. يهدف هذا المبدأ إلى تحقيق عدة غايات،

[1] القصد الاحتمالي في القانون الجنائي: هل هو الحل لمساءلة مصممي الأنظمة الذكية؟"، مقال منشور في موقع العدالة الرقمية، بتاريخ 15 أبريل 2024، الرابط:www.digitaljustice.org/probable-intent تم الدخول إليه في 24 ماي 2025.

[2] حمد شلبي، المدخل إلى القانون الجنائي، دار النهضة العربية، القاهرة، الطبعة السادسة، 2018، ص. 138.

أهمها ضمان عدم المباغتة بالعقاب، وتحقيق المساواة أمام القانون، وحماية الأفراد من تحكم السلطة التنفيذية والقضائية.[1]

لكن تطبيق هذا المبدأ يواجه تحديات متزايدة في عصر التطور التكنولوجي المتسارع، وظهور أنماط جديدة من السلوكيات الضارة المرتبطة بالأنظمة الذاتية والذكاء الاصطناعي. فالطبيعة المستحدثة لهذه الجرائم، وعدم توقع المشرع لها عند وضع النصوص التقليدية، يثير تساؤلات حول مدى كفاية هذه النصوص وقدرتها على استيعاب الظواهر الجديدة، ومدى الحاجة إلى تدخل تشريعي خاص.[2]

سنعالج في هذا المطلب إشكالية تطبيق مبدأ الشرعية على الجرائم التقنية، حيث نستعرض في الفرع الأول أهمية المبدأ وتطبيقاته العامة. ثم نبحث في الفرع الثاني صعوبات التكييف القانوني للجرائم التقنية في ظل غياب نصوص واضحة. ونختتم في الفرع الثالث بالتأكيد على الحاجة إلى نصوص قانونية مرنة قادرة على مواكبة التطور التكنولوجي المستمر.

الفرع الأول: لا جريمة ولا عقوبة إلا بنص

يكتسي مبدأ الشرعية الجنائية أهمية بالغة في النظم القانونية المعاصرة، فهو ليس مجرد قاعدة قانونية، بل هو ضمانة دستورية أساسية لحماية الحريات الفردية. يمنع هذا المبدأ القاضي من خلق جرائم أو عقوبات جديدة لم ينص عليها القانون، ويفرض على المشرع أن تكون نصوص التجريم واضحة ومحددة، لا لبس فيها ولا غموض، حتى يتمكن الأفراد من معرفة الأفعال المباحة والمحظورة وتوقع العواقب القانونية لسلوكياتهم.[3]

يترتب على مبدأ الشرعية عدة نتائج هامة، منها عدم رجعية النصوص الجنائية الموضوعية، أي أنها لا تسري على الأفعال التي ارتكبت قبل نفاذها، إلا إذا كانت أصلح للمتهم. ومنها أيضاً وجوب التفسير الضيق للنصوص الجنائية، بحيث لا يجوز التوسع في تفسيرها ليشمل أفعالاً لم يقصد المشرع تجريمها صراحة، كما لا يجوز القياس في مواد التجريم والعقاب لخلق جرائم أو عقوبات جديدة.

عند تطبيق هذا المبدأ على الجرائم المستحدثة بفعل التكنولوجيا، مثل تلك المرتبطة بالأنظمة الذاتية، يبرز التوتر بين الحاجة إلى حماية المجتمع من الأضرار الجديدة التي قد تنشأ عن هذه التقنيات، وبين ضرورة

[1] سامي القيسي، مبادئ القانون الجنائي، دار الثقافة القانونية، بغداد، الطبعة الأولى، 2015، ص. 150

[2] هالة فؤاد، العنصر المعنوي في الجرائم التكنولوجية، دار الفكر الجامعي، القاهرة، 2021، ص. 110

[3] المرجع نفسه، ص 116

الالتزام بضمانات الشرعية وحماية الأفراد من التجريم غير الواضح أو بأثر رجعي. يثور التساؤل حول مدى إمكانية تكييف الأفعال الضارة الصادرة عن الأنظمة الذاتية ضمن نصوص التجريم التقليدية (مثل القتل الخطأ، الإتلاف، الاحتيال)، أو ما إذا كانت طبيعتها الخاصة تتطلب نصوصاً جديدة ومحددة.[1]

يفرض مبدأ الشرعية على المشرع والقاضي التعامل بحذر عند مواجهة هذه الجرائم الجديدة. فلا يمكن تجريم سلوك مرتبط بنظام ذاتي إلا إذا كان يدخل بوضوح تحت طائلة نص قائم وواضح. وإذا كان النص غامضاً أو قاصراً عن استيعاب السلوك الجديد، فإن التوسع في تفسيره أو القياس عليه قد يشكل انتهاكاً لمبدأ الشرعية. هذا التحدي يلقي بعبء كبير على المشرع لمواكبة التطورات التكنولوجية وتحديث الترسانة القانونية بشكل مستمر.[2]

الفرع الثاني: صعوبات التكييف في غياب نصوص واضحة

تتمثل إحدى أبرز الصعوبات التي تواجه تطبيق مبدأ الشرعية في مجال الجرائم التقنية في قصور العديد من النصوص الجنائية التقليدية عن استيعاب الأنماط المستحدثة من السلوكيات الإجرامية المرتبطة بالأنظمة الذاتية. فالنصوص التقليدية صيغت في زمن لم تكن فيه هذه التقنيات موجودة أو متوقعة، وبالتالي فهي قد لا تتلاءم تماماً مع طبيعة الأفعال الصادرة عنها أو مع العلاقات القانونية الجديدة التي تنشئها.[3]

على سبيل المثال، تطرح صعوبات حول كيفية تكييف قرار خوارزمي تمييزي يتخذه نظام ذكاء اصطناعي في مجال التوظيف أو الإقراض. وهل يمكن اعتباره جريمة تمييز تقليدية، رغم غياب القصد التمييزي المباشر لدى أي طرف بشري وكيف يمكن تكييف حادث تتسبب فيه سيارة ذاتية القيادة نتيجة خطأ في نظامها البرمجي؟ وهل هو قتل خطأ أو إصابة خطأ بالمعنى التقليدي، رغم أن "الفاعل" المباشر هو آلة؟ وما هو التكييف القانوني المناسب لنشر معلومات مضللة أو "أخبار زائفة" (Fake News) بواسطة روبوتات الدردشة أو أنظمة توليد المحتوى الآلي؟[4]

---

[1] ريم يوسف، التحديات القانونية للذكاء الاصطناعي في القانون الجنائي، مجلة القانون والتكنولوجيا، العدد 9، 2023، ص. 35

[2] وقع "المرصد الرقمي للقانون"، مقال: "الجرائم الجديدة في عصر الذكاء الاصطناعي" منشور بتاريخ 15 مارس 2023.

[3] تقرير الأمم المتحدة عن الذكاء الاصطناعي والقانون الجنائي، 2021، متاح عبر الموقع الرسمي للأمم المتحدة.

[4] هالة فؤاد، تحديات مبدأ الشرعية في القانون الجنائي المعاصر، دار الفكر الجامعي، القاهرة، 2021، ص. 120–121.

يثير هذا القصور في النصوص إشكالية اللجوء إلى القياس أو التفسير الواسع للنصوص القائمة لمحاولة استيعاب هذه الجرائم الجديدة. فكما ذكرنا، يمنع مبدأ الشرعية، كقاعدة عامة، القياس في مواد التجريم والعقاب، ويوجب التفسير الضيق للنصوص. وبالتالي، فإن محاولة "مط" النصوص التقليدية لتشمل سلوكيات لم تكن مقصودة أصلاً عند وضعها قد يؤدي إلى نتائج غير عادلة أو غير متوقعة، ويضعف من وظيفة القانون كمرشد واضح لسلوك الأفراد.[1]

تزداد صعوبة التكييف في ظل غياب نصوص واضحة ومحددة تعالج الجرائم المرتبطة بالأنظمة الذاتية بشكل خاص. فغياب تعريفات قانونية دقيقة لمفاهيم مثل "النظام الذاتي"، "الذكاء الاصطناعي"، "الخوارزمية"، "الفعل التقني"، يزيد من الغموض وعدم اليقين القانوني. وهذا يتطلب تدخلاً تشريعياً عاجلاً لوضع إطار قانوني واضح ينظم هذه المسائل ويحدد الجرائم والعقوبات المرتبطة بها بشكل دقيق، بما يتوافق مع متطلبات مبدأ الشرعية.[2]

الفرع الثالث: الحاجة إلى نصوص مرنة تواكب التطور التكنولوجي

أمام التحديات التي يفرضها التطور التكنولوجي السريع على مبدأ الشرعية وصعوبات التكييف القانوني، تبرز الحاجة الملحة إلى تدخل المشرع لوضع نصوص قانونية جديدة أو تعديل النصوص القائمة لتكون قادرة على مواكبة هذه التطورات ومعالجة الجرائم التقنية المستحدثة بشكل فعال وعادل.

يجب أن يتميز هذا التدخل التشريعي بالمرونة والقدرة على استيعاب المستجدات المستقبلية قدر الإمكان. فالتكنولوجيا تتطور بوتيرة أسرع بكثير من وتيرة العملية التشريعية عادة. لذلك، ينبغي تجنب صياغة نصوص جامدة أو مرتبطة بتقنيات محددة قد تصبح قديمة بسرعة. وبدلاً من ذلك، يفضل التركيز على صياغة مبادئ عامة وقواعد مرنة يمكن تكييفها مع التطورات المختلفة، مع تحديد الأفعال المجرمة بشكل واضح ودقيق بما يكفي لتحقيق متطلبات الشرعية.[3]

قد يتطلب الأمر اعتماد نهج "محايد تكنولوجياً" (Technology-neutral) في صياغة بعض النصوص، بحيث تركز على تجريم السلوك الضار أو النتيجة المحظورة بغض النظر عن الوسيلة التكنولوجية المستخدمة. وفي حالات أخرى، قد يكون من الضروري وضع نصوص خاصة تعالج أنواعاً

[1] فاطمة الزهراء المريني، المرجع السابق، ص 145.

[2] مجلة دراسات التشريع والقضاء، مقال: "مرونة التشريع في مواجهة الجرائم التقنية الحديثة"، العدد 19، 2022، ص. 33

[3] د. معاذ سليمان، الأبعاد التاريخية لتطور نظرية المسؤولية الجزائية وجدلية تطبيقها في عصر الذكاء الاصطناعي: دراسة تحليلية واستشرافية، مجلة كلية القانون الكويتية العالمية،2021، ص 99-100.

محددة من الجرائم التقنية التي تتطلب تنظيماً خاصاً نظراً لطبيعتها الفريدة (مثل جرائم الأمن السيبراني، أو الجرائم المتعلقة بإساءة استخدام الذكاء الاصطناعي).[1]

يجب على المشرع عند وضع هذه النصوص أن يوازن بعناية بين الحاجة إلى حماية المجتمع ومصالح الضحايا من الأضرار الناجمة عن التقنيات الجديدة، وبين ضرورة حماية الحقوق والحريات الفردية وضمان عدم الإفراط في التجريم أو العقاب. يجب أن تكون النصوص واضحة ومحددة، وأن تحترم مبادئ المسؤولية الشخصية والإثبات، وأن تتناسب العقوبات مع جسامة الجريمة وظروف مرتكبها.[2]

يمكن الاستفادة في هذا الصدد من دراسة الاتجاهات التشريعية المقارنة والتجارب الدولية في مجال تنظيم الذكاء الاصطناعي والتعامل مع الجرائم التقنية. فالعديد من الدول والمنظمات الدولية بدأت بالفعل في استكشاف أطر تنظيمية وقانونية جديدة، مثل قانون الذكاء الاصطناعي المقترح من الاتحاد الأوروبي، والذي يتضمن أحكاماً تتعلق بالمسؤولية والسلامة والأخلاقيات. يمكن لهذه التجارب أن تقدم دروساً مفيدة للمشرع الوطني في سعيه لوضع إطار قانوني ملائم يواكب العصر الرقمي ويحقق التوازن المطلوب بين الابتكار والحماية.[3]

[1] د. معاذ سليمان، مرجع سابق، ص 106.

[2] سامي جابر، مبدأ الشرعية في القانون الجنائي: من الثبات إلى المرونة، دار النهضة العربية، الطبعة الأولى، 2020، ص. 112

[3] القانون الجنائي المصري رقم 58 لسنة 1937، مع تعديلات 2020، المواد المتعلقة بالجرائم التكنولوجية.

المبحث الثاني: نماذج إسناد المسؤولة الجزائية في نطاق جرائم الأنظمة ذاتية التسيير

بعد أن استعرضنا في المبحث الأول التحديات التي تثيرها الأنظمة الذاتية أمام الأركان التقليدية للمسؤولية الجزائية (الركن المادي والركن المعنوي) ومبدأ الشرعية، ننتقل في هذا المبحث إلى استكشاف النماذج والحلول المقترحة لإسناد المسؤولية الجزائية في الجرائم التي تقع بواسطة أو بمشاركة هذه الأنظمة. ففي ظل صعوبة، وربما استحالة، مساءلة النظام الذاتي نفسه وفقاً للقواعد الحالية، يصبح البحث عن الطرف البشري المسؤول أمراً محورياً. ومع ذلك، فإن تحديد هذا الطرف وتوزيع المسؤولية بين المتدخلين المتعددين يطرح بدوره إشكاليات قانونية وعملية معقدة.

تتعدد الأطراف التي يمكن أن تكون محلاً للمساءلة في سياق الأنظمة الذاتية، بدءاً من المصمم والمبرمج، مروراً بالمصنع والمورد، وصولاً إلى المستخدم أو المشغل أو المالك. كما يطرح البعض فكرة تطوير نماذج للمسؤولية المشتركة أو التضامنية بين هؤلاء الأطراف، بل ويذهب البعض الآخر إلى حد اقتراح منح شخصية قانونية للأنظمة الذكية ذاتها لتحميلها المسؤولية بشكل مباشر. سنقوم في هذا المبحث بتحليل هذه النماذج المختلفة، وتقييم مدى فعاليتها وملاءمتها للتعامل مع جرائم العصر الرقمي.[1]

سنتناول في المطلب الأول النموذج الأكثر تقليدية، وهو إسناد المسؤولية إلى الأطراف البشرية المباشرة: الصانع والمستخدم. وفي المطلب الثاني، سنبحث في نماذج المسؤولية المشتركة والتضامنية بين الفاعلين المتعددين. أما المطلب الثالث، فسنخصصه لمناقشة الفكرة الأكثر جذرية وإثارة للجدل، وهي إمكانية إسناد المسؤولية إلى النظام الذاتي ككيان قانوني مستقل.

المطلب الأول: إسناد المسؤولية الجزائية إلى الصانع والمستخدم

يعتبر إسناد المسؤولية الجزائية إلى الأطراف البشرية التي تقف وراء تصميم وتصنيع واستخدام الأنظمة الذاتية هو النهج الأكثر انسجاماً مع المبادئ التقليدية للقانون الجزائي[2]، التي تركز على المسؤولية الشخصية للإنسان. وينصب التركيز هنا بشكل أساسي على طرفين رئيسيين: الصانع (بما يشمل المصمم والمبرمج والمصنع) من جهة، والمستخدم (بما يشمل المشغل والمالك) من جهة أخرى.

[1] مجلة القانون والسياسة، مقال: "الشخصية القانونية للأنظمة الذكية: جدلية ومسارات تطويرية"، العدد 29، 2024، ص. 45

[2] سميرة دحمان، المرجع السابق، 91.

الفرع الأول: مسؤولية الصانع والمبرمج عن الأخطاء التقنية والبرمجية

يقع على عاتق الصانع والمبرمج مسؤوليات قانونية ومهنية كبيرة لضمان سلامة الأنظمة الذاتية وموثوقيتها. إذ يتوجب عليهم اتخاذ كل الاحتياطات اللازمة في التصميم والاختبار، وتقديم معلومات واضحة للمستخدمين، بهدف الحد من الأخطاء التقنية والبرمجية التي قد تؤدي إلى أضرار.

أولاً: التزامات الصانع والمبرمج

يقع على عاتق صانعي ومبرمجي الأنظمة الذاتية التزامات قانونية ومهنية هامة تهدف إلى ضمان سلامة وموثوقية منتجاتهم. فهم يمتلكون المعرفة والخبرة الفنية اللازمة لتصميم وتطوير هذه الأنظمة، وبالتالي فهم في أفضل وضع لاتخاذ الاحتياطات اللازمة لمنع وقوع الأضرار. وتشمل هذه الالتزامات واجب تصميم أنظمة آمنة بطبيعتها (Safety by design)، وإجراء اختبارات شاملة ودقيقة قبل طرح المنتج في السوق، وتوفير معلومات واضحة وكافية للمستخدمين حول كيفية التشغيل الآمن والمخاطر المحتملة، وتحديث الأنظمة وتصحيح الثغرات المكتشفة بشكل دوري.[1]

ثانياً: أساس وحدود المسؤولية

يتمثل أساس مسؤولية الصانع والمبرمج عادة في الإخلال بواجب الحيطة والحذر أو الالتزام العام بالسلامة. فإذا ثبت أن الضرر الناتج عن النظام الذاتي كان سببه خطأ في التصميم (مثل استخدام خوارزمية معيبة أو متحيزة)، أو خطأ في التنفيذ (مثل وجود خلل في الكود البرمجي)، أو عدم كفاية الاختبارات والفحوصات اللازمة للتأكد من أمان النظام في مختلف الظروف التشغيلية، فإن الصانع أو المبرمج يمكن أن يسأل جزائياً عن هذا الخطأ إذا توافرت بقية أركان الجريمة (عادة في إطار الخطأ غير العمدي).[2]

تتطلب عملية إثبات مسؤولية الصانع أو المبرمج عادة خبرة فنية متخصصة لتحليل تصميم النظام وبرمجته وتحديد مواطن الخلل. وقد تكون هذه العملية معقدة، خاصة في ظل سرية المعلومات التجارية والصناعية وصعوبة الوصول إلى الكود المصدري أو بيانات الاختبار. كما قد يواجه الادعاء صعوبة في

[1] مجلة الحقوق الرقمية، مقال: "المسؤولية الجنائية في البرمجيات المعطوبة: تحليل قانوني"، العدد 9، 2022، ص. 23

[2] امي الكيلاني، الأخطاء التقنية كركن في المسؤولية الجزائية: دراسة مقارنة، دار النهضة العربية، 2021، ص. 134

إثبات العلاقة السببية المباشرة بين خطأ التصميم أو البرمجة والنتيجة الضارة، خاصة إذا تداخلت عوامل أخرى مثل سوء الاستخدام من قبل المستخدم أو ظروف خارجية غير متوقعة.[1]

ومع ذلك، فإن مسؤولية الصانع والمبرمج ليست مطلقة، بل ترد عليها بعض الحدود والقيود. فغالباً ما لا يسأل الصانع عن الضرر إذا كان ناتجاً عن قوة قاهرة أو حادث فجائي لا يمكن توقعه أو دفعه. كما قد تنتفي مسؤوليته إذا كان الضرر راجعاً إلى خطأ جسيم من جانب الضحية أو الغير. وكذلك، قد لا يسأل الصانع عن الأضرار الناجمة عن استخدام النظام بطريقة غير متوقعة أو مخالفة للتعليمات والغرض الذي صمم من أجله، ما لم يكن هذا الاستخدام متوقعاً بشكل معقول وكان بإمكانه اتخاذ احتياطات لمنعه.

الفرع الثاني: مسؤولية المستخدم أو المشغل بسبب الإهمال أو سوء الاستعمال

تمتد مسؤولية الأنظمة الذاتية إلى المستخدم أو المشغل، الذي يتحمل واجبات قانونية للحفاظ على السلامة أثناء تشغيل النظام. تشمل هذه الواجبات الالتزام بالتعليمات، إجراء الصيانة، تحديث البرامج، والإشراف المستمر لضمان الاستخدام الصحيح والمسؤول.

أولاً: واجبات المستخدم أو المشغل

لا تقتصر المسؤولية على جانب الصانع والمبرمج، بل تمتد أيضاً لتشمل المستخدم أو المشغل الذي يتولى تشغيل النظام الذاتي والتحكم فيه في بيئة التشغيل الفعلية. فالمستخدم ليس مجرد متلق سلبي للتكنولوجيا، بل يقع عليه أيضاً واجبات والتزامات قانونية تهدف إلى ضمان الاستخدام الآمن والمسؤول للنظام.

تشمل واجبات المستخدم أو المشغل عادة الالتزام باستخدام النظام وفقاً للتعليمات والتوصيات الصادرة عن الصانع، وإجراء الصيانة الدورية اللازمة، والتأكد من تحديث البرامج وتصحيح الثغرات الأمنية، والإشراف على عمل النظام بالدرجة التي تتطلبها طبيعته ومستوى استقلاليته، واتخاذ القرارات المناسبة في الحالات التي يتطلب فيها النظام تدخلاً بشرياً أو يتجاوز فيها قدراته.[2]

[1] عبد الرحمن عبد الله، المرجع السابق، ص 112.

[2] ادية الزهراوي، الإشراف على الأنظمة الذاتية: الأبعاد القانونية والعملية، دار الكتب القانونية، 2021، ص. 112

ثانياً: أساس المسؤولية (الإهمال وسوء الاستعمال)

يمكن أن تنشأ مسؤولية المستخدم أو المشغل الجزائية في حالة إخلاله بهذه الواجبات، مما يؤدي إلى وقوع ضرر. وتتخذ هذه المسؤولية غالباً صورة الخطأ غير العمدي الناتج عن الإهمال أو عدم الاحتراز. ومن أمثلة حالات الإهمال الموجبة للمسؤولية: عدم تحديث برامج النظام رغم التحذيرات الأمنية، تجاهل رسائل الخطأ أو التحذيرات الصادرة عن النظام، استخدام النظام في ظروف بيئية أو تشغيلية غير ملائمة أو تتجاوز قدراته المصمم لها، أو عدم الإشراف الكافي على نظام يتطلب درجة معينة من المراقبة البشرية.

بالإضافة إلى الإهمال، يمكن أن يسأل المستخدم عن سوء الاستعمال المتعمد للنظام الذاتي، كأن يقوم بالتحايل على قيود السلامة المضمنة في النظام، أو استخدامه عن قصد لأغراض غير مشروعة أو إجرامية (مثل استخدام طائرة بدون طيار ذاتية التحكم في التهريب أو التجسس أو الهجوم). في هذه الحالة، تكون المسؤولية عمدية وتخضع للقواعد العامة للمساهمة الجنائية إذا اشترك معه آخرون.

ومع ذلك، فإن إثبات خطأ المستخدم ودوره في وقوع الضرر قد يكون صعباً في بعض الأحيان. فقد يدفع المستخدم بأن الضرر كان نتيجة لخلل في النظام نفسه وليس بسبب خطأ من جانبه. كما قد يكون من الصعب تحديد درجة الإشراف المطلوبة من المستخدم، خاصة مع الأنظمة التي تتمتع بدرجة عالية من الاستقلالية. ويتطلب الأمر في كل حالة تقييماً دقيقاً لظروف الواقع وتحديد ما إذا كان المستخدم قد تصرف كشخص معتاد حريص في تعامله مع النظام.

الفرع الثالث: تداخل مسؤولية الصانع مع المستخدم في نطاق جرائم الأنظمة ذاتية التسيير

في كثير من الحالات العملية، لا يكون الضرر الناتج عن النظام الذاتي نتيجة لخطأ طرف واحد فقط (الصانع أو المستخدم)، بل قد يكون محصلة لتفاعل معقد بين عوامل متعددة تتعلق بتصميم النظام وبرمجته وتصنيعه واستخدامه وظروف تشغيله. هذا التداخل في المسؤوليات بين الصانع والمستخدم (وغيرهم من المتدخلين المحتملين) يجعل من الصعب تحديد الفاعل الحقيقي أو المسؤول الرئيسي عن الضرر.[1]

على سبيل المثال، قد يقع حادث لسيارة ذاتية القيادة نتيجة لتفاعل بين خطأ بسيط في نظام الاستشعار (مسؤولية الصانع)، وعدم انتباه السائق الذي كان يجب أن يكون مستعداً للتدخل (مسؤولية المستخدم)،

[1] ليلى الشارف، التحليل القانوني لتفاعل المسؤوليات في الأنظمة الذكية: دراسة حالة، منشورات الجامعة، 2023، ص. 77

وسوء الأحوال الجوية (عامل خارجي). تطرح مثل هذه الحالات تساؤلاً حول كيفية توزيع المسؤولية الجزائية بين الأطراف المختلفة، وما إذا كان يجب أن يسألوا جميعاً بالتضامن، أو أن يتم تحديد نسبة مساهمة كل طرف.[1]

تزداد الصعوبة مع ما يعرف بإشكالية "لوم النظام" (Blame the system)، حيث يميل كل طرف إلى إلقاء اللوم على الطرف الآخر أو على النظام نفسه ككبش فداء للتهرب من المسؤولية. فقد يدفع الصانع بأن نظامه كان سليماً وأن الخطأ يقع على المستخدم الذي أساء استخدامه، بينما قد يدفع المستخدم بأن اتبع التعليمات وأن الخلل يكمن في النظام نفسه.[2]

هذه الصعوبات تؤكد الحاجة إلى تطوير آليات قانونية وإجرائية واضحة لتحديد وتوزيع المسؤولية في حالات التفاعل المعقد بين الأطراف المتعددة والأنظمة الذاتية. قد يشمل ذلك وضع معايير أكثر تفصيلاً لواجبات كل طرف، وتعزيز آليات الشفافية وقابلية تفسير عمل الأنظمة، وتطوير أدوات التحقيق الفني والقضائي القادرة على تحليل الأسباب المتعددة والمتداخلة للحوادث.

تلعب عقود الاستخدام وشروط الخدمة التي يبرمها الصانع مع المستخدم دوراً هاماً في هذا السياق، حيث تحاول غالباً تحديد نطاق استخدام النظام وتوزيع المسؤوليات بين الطرفين. ومع ذلك، فإن فعالية هذه الشروط في المجال الجزائي تظل محدودة، خاصة إذا كانت تتعارض مع النظام العام أو قواعد المسؤولية الآمرة. فلا يمكن لشروط تعاقدية أن تعفي طرفاً من مسؤوليته الجزائية عن خطئه الجسيم أو إهماله الذي أدى إلى جريمة.[3]

المطلب الثاني: المسؤولية المشتركة والتضامنية في نطاق جرائم الأنظمة ذاتية التسيير

كما رأينا في المطلب السابق، قد يكون من الصعب في كثير من الأحيان إسناد المسؤولية الجزائية عن الضرر الناتج عن نظام ذاتي إلى طرف بشري واحد بعينه، سواء كان الصانع أو المستخدم. فالطبيعة المعقدة لهذه الأنظمة وتعدد المتدخلين في دورة حياتها وتفاعلها مع بيئتها يجعل من الوارد أن تكون

---

[1] How to Assign Liability for Autonomous Vehicles," TechCrunch, "
https://techcrunch.com/2024/01/20/assign-liability-autonomous-vehicles اطلع عليه في 22 مايو 2025

[2] نفس المرجع.

[3] موقع المركز الوطني للبحوث القضائية – قسم الجرائم التكنولوجية:
https://www.cnrj.dz/ar/articles/تقنيات-المسؤولية-الجزائية-في-الجرائم-السيبرانية اطلع عليه في 25 مايو 2025

النتيجة الضارة محصلة لأخطاء أو مساهمات من أطراف متعددة. هذا الواقع يطرح أهمية البحث في نماذج المسؤولية التي تتجاوز الفاعل الوحيد، وتنظر في إمكانية توزيع المسؤولية بين الأطراف المتعددة أو تحميلهم إياها بشكل مشترك أو تضامني.[1]

الفرع الأول: توزيع المسؤولية بين أطراف جرائم الأنظمة ذاتية التسيير

تتميز دورة حياة النظام الذاتي بتعدد المتدخلين فيها، بدءاً من مصمم المفهوم الأولي، مروراً بالمبرمج الذي يكتب الكود، والمصنع الذي ينتج الجهاز، ومورد البيانات الذي يدرب الخوارزمية، وصولاً إلى المشغل الذي يدير النظام، والمالك الذي يستفيد منه، وربما أطراف أخرى مثل جهات الصيانة أو مقدمي خدمات الاتصال. كل هؤلاء الأطراف قد يكون لهم دور، بدرجة أو بأخرى، في وقوع الضرر الذي يتسبب فيه النظام.[2]

أمام هذا التعدد، تثور مسألة كيفية توزيع المسؤولية الجزائية بين هؤلاء المتدخلين إذا ثبتت مساهمة أكثر من طرف في النتيجة الجرمية. ويُطرح التساؤل حول مدى تطبيق القواعد التقليدية للمساهمة الجنائية (الفاعل الأصلي والشريك)، أو ما إذا كان الأمر يتطلب قواعد خاصة.

تواجه القواعد التقليدية للمساهمة الجنائية صعوبات في التطبيق على هذا السياق. فهذه القواعد تفترض عادة وجود اتفاق أو تنسيق مسبق بين المساهمين، ووحدة في القصد الجنائي، وهو ما قد لا يتوافر دائماً في حالة الأخطاء المتعددة من أطراف مختلفة تعمل بشكل مستقل نسبياً في مراحل مختلفة من دورة حياة النظام. كما أن تحديد دور كل مساهم ومدى تأثيره في النتيجة النهائية قد يكون أمراً بالغ التعقيد من الناحية الفنية والإثباتية.[3]

لذلك، يرى البعض الحاجة إلى تطوير قواعد خاصة لتوزيع المسؤولية في الجرائم التقنية تأخذ في الاعتبار طبيعة المخاطر المرتبطة بالأنظمة الذاتية وتعدد المتدخلين. قد تشمل هذه القواعد نماذج للمسؤولية النسبية التي توزع العبء بين المساهمين بحسب درجة خطأ كل منهم أو مدى سيطرته على المخاطر. كما قد يتم اللجوء إلى نماذج المسؤولية التضامنية، حيث يكون كل طرف ساهم في الضرر مسؤولاً عن

[1] سامي محمد صالح، المسؤولية الجنائية في الجرائم التكنولوجية، دار الفكر القانوني، عمان، 2019.ص82

[2] نفس المرجع، ص 89.

[3] جمال سعدو حبش، المرجع السابق، ص 71.

كامل التعويض (في المسؤولية المدنية) أو يخضع للعقوبة المقررة (مع مراعاة ظروف كل مساهم في المسؤولية الجزائية)، مع حق الرجوع بين المسؤولين لاحقاً.

تطبيق المسؤولية التضامنية في المجال الجزائي يثير بدوره نقاشاً حول مدى اتفاقه مع مبدأ شخصية العقوبة. ومع ذلك، قد يكون له ما يبرره في بعض الحالات لضمان عدم إفلات أي طرف ساهم في الضرر من المساءلة، ولتوفير حماية أفضل للضحايا. يتطلب الأمر دراسة متأنية للموازنة بين اعتبارات العدالة الفردية وفعالية الردع وحماية المصلحة العامة.

الفرع الثاني: التعاقد والتنازل عن المسؤولية بين الفاعلين

في محاولة لتحديد وتوزيع المسؤوليات مسبقاً، تلجأ الأطراف المتعاملة في مجال الأنظمة الذاتية (مثل الصانع والمستخدم، أو المبرمج والمصنع) إلى إبرام عقود تتضمن شروطاً تتعلق بالمسؤولية عن الأضرار المحتملة. قد تتضمن هذه الشروط محاولة أحد الأطراف التنازل عن مسؤوليته أو تحديد سقف لها، أو نقل عبء المسؤولية إلى الطرف الآخر.[1]

يثور التساؤل حول مدى حجية هذه الشروط التعاقدية في مواجهة قواعد المسؤولية الجزائية. القاعدة العامة في القانون أن الاتفاقات الخاصة لا يمكنها أن تعدل من قواعد المسؤولية الجزائية التي تعتبر من النظام العام. فلا يجوز للأفراد أن يتفقوا على إباحة فعل مجرم قانوناً، أو على إعفاء مرتكبه من العقاب.[2]

وبالتالي، فإن أي شرط تعاقدي يهدف إلى الإعفاء الكامل من المسؤولية الجزائية عن جريمة مستقبلية يعتبر باطلاً لمخالفته للنظام العام. ومع ذلك، قد يكون للشروط التعاقدية أثر غير مباشر في تحديد نطاق الواجبات والالتزامات بين الأطراف، وبالتالي في تقدير مدى الخطأ المرتكب من كل طرف عند وقوع الضرر. على سبيل المثال، إذا نص العقد بوضوح على واجبات المستخدم في الصيانة والإشراف، فإن إخلاله بهذه الواجبات قد يؤخذ في الاعتبار عند تحديد مسؤوليته الجزائية عن خطئه غير العمدي.[3]

---

[1] مركز الخليج للدراسات القانونية، "آليات توزيع المسؤولية القانونية بين الفاعلين في مجال الذكاء الاصطناعي"، تقرير، 2023، متاح على: https://gclawcenter.org/reports/responsibility-distribution-ai، تم الاطلاع في 25 مايو 2025.

[2] أحمد بن عبد الله، التنظيم القانوني للذكاء الاصطناعي ومسؤولية المبرمجين في التشريع الجزائري، رسالة دكتوراه، جامعة الجزائر، 2023، ص.45

[3] المرجه نفسه، ص 66.

كما يجب التمييز بين المسؤولية الجزائية والمسؤولية المدنية (التعويض). فبينما لا يجوز الاتفاق على تعديل المسؤولية الجزائية، قد تكون الشروط المتعلقة بتوزيع عبء التعويض المدني أكثر مرونة، وإن كانت تخضع أيضاً لقيود تتعلق بالنظام العام وحماية الطرف الضعيف في العلاقة التعاقدية.

يلعب التأمين دوراً هاماً في هذا السياق كوسيلة لتغطية المخاطر المالية المرتبطة بالمسؤولية عن الأضرار التي تسببها الأنظمة الذاتية. فوجود تأمين كافٍ قد يساعد في ضمان حصول الضحايا على التعويض المناسب، وقد يؤثر أيضاً على كيفية توزيع المسؤوليات بين الأطراف المؤمن لهم. ومع ذلك، لا يمكن للتأمين أن يعفي المؤمن له من مسؤوليته الجزائية إذا ثبت ارتكابه لجريمة.

الفرع الثالث: إثبات المسؤولية الجزائية بشأن جرائم الأنظمة ذاتية التسيير

بغض النظر عن نموذج توزيع المسؤولية المعتمد، يظل إثبات مساهمة كل طرف في النتيجة الجرمية يمثل تحدياً قانونياً وعملياً كبيراً في سياق الجرائم التقنية. فكما أشرنا سابقاً، يتطلب الأمر غالباً خبرة فنية عالية وقدرة على تحليل الأنظمة المعقدة وتتبع مسار القرارات والأخطاء.[1]

من أبرز تحديات الإثبات صعوبة تحديد الدور السببي لكل مساهم في إحداث النتيجة النهائية. ففي بيئة تتفاعل فيها مكونات برمجية ومادية متعددة، وتتدخل فيها عوامل بشرية وبيئية مختلفة، قد يكون من شبه المستحيل عزل مساهمة كل طرف وتحديد مدى تأثيرها بدقة. هذا التعقيد السببي قد يستغله الدفاع للتشكيك في رابطة السببية وإثارة الشك الذي يفسر لمصلحة المتهم.

تضاف إلى ذلك مشكلات الإثبات التقني المتعلقة بصعوبة الحصول على الأدلة الرقمية وتحليلها. فقد تكون البيانات اللازمة لفهم سبب الحادث (مثل سجلات عمل النظام أو الكود المصدري) غير متاحة أو مشفرة أو تم حذفها. وحتى في حالة توفر البيانات، قد يتطلب تحليلها وفهمها خبرات فنية متخصصة قد لا تتوفر بسهولة لدى جهات التحقيق أو القضاء. كما أن الطبيعة غير الملموسة للأدلة الرقمية وسهولة التلاعب بها تثير تحديات إضافية تتعلق بحجيتها وموثوقيتها.[2]

لمواجهة هذه التحديات، هناك حاجة ماسة إلى تطوير القدرات الفنية لجهات إنفاذ القانون والقضاء في مجال التحقيق الرقمي وتحليل الأدلة التقنية. كما يتطلب الأمر وضع قواعد إجرائية واضحة تنظم عملية

[1] عبد الرحمن العتيبي، "صعوبات الإثبات في قضايا الجرائم السيبرانية"، مجلة الدراسات القضائية، العدد 12، 2023، ص 45

[2] نفس المرجع، ص 62.

جمع الأدلة الرقمية وحفظها وتقديمها أمام المحاكم، بما يضمن حماية حقوق المتهم وفي نفس الوقت يتيح الوصول إلى الحقيقة. قد يشمل ذلك فرض التزامات على مصنعي ومستخدمي الأنظمة الذاتية بالاحتفاظ بسجلات عمل مفصلة (Logs) وتوفيرها لجهات التحقيق عند الطلب، مع مراعاة التوازن مع حماية الأسرار التجارية والخصوصية.[1]

المطلب الثالث: إسناد المسؤولية إلى النظام الذاتي ككيان قانوني محتمل

أمام الصعوبات المتزايدة في إسناد المسؤولية الجزائية للأطراف البشرية في بعض الحالات التي تتسبب فيها الأنظمة الذاتية المستقلة بأضرار جسيمة، ظهر اتجاه فكري، لا يزال محدوداً ومثيراً للجدل، يدعو إلى التفكير في حلول أكثر جذرية، تتمثل في إمكانية منح هذه الأنظمة نوعاً من الشخصية القانونية المستقلة، بما يتيح مساءلتها بشكل مباشر عن أفعالها الضارة.

الفرع الأول: الشخصية القانونية للأنظمة ذاتية التسيير

تقوم فكرة منح الشخصية القانونية للأنظمة الذكية على ملاحظة أن هذه الأنظمة أصبحت تتمتع بدرجات متزايدة من الاستقلالية والقدرة على التعلم والتفاعل مع بيئتها واتخاذ قرارات قد تكون غير متوقعة من قبل البشر. يرى أنصار هذا الاتجاه أن هذه القدرات المتطورة تجعل من الأنظمة الذكية كيانات أقرب إلى "الفاعلين" منها إلى مجرد "الأدوات"، مما قد يبرر معاملتها كأشخاص قانونيين من نوع جديد.[2]

تتعدد المبررات التي يسوقها المؤيدون لهذه الفكرة. فهم يرون أن منح الشخصية القانونية قد يساعد في سد "فجوة المسؤولية" التي قد تنشأ عندما يتعذر إسناد الضرر إلى أي طرف بشري محدد. كما قد يوفر آلية لتعويض الضحايا من خلال إنشاء ذمة مالية خاصة بالنظام الذكي (عن طريق التأمين أو تخصيص أصول له). ويرى البعض أيضاً أن الاعتراف بشخصية قانونية قد يعكس بشكل أفضل الواقع التكنولوجي المتطور ويشجع على تطوير أنظمة أكثر مسؤولية وأخلاقية.[3]

تتنوع المقترحات حول طبيعة هذه الشخصية القانونية. يقترح البعض إنشاء فئة جديدة من "الشخصية الإلكترونية" (Electronic Personhood) خاصة بالأنظمة الذكية الأكثر تطوراً. ويقترح آخرون تكييف مفهوم الشخصية الاعتبارية التقليدية (المستخدمة للشركات والجمعيات) لتشمل هذه الأنظمة. وتتم المقارنة

[1] نفس المرجع، ص 67.

[2] المركز العربي للبحوث والدراسات القانونية، "التحديات القانونية لإثبات الجرائم التقنية"، مجلة العلوم القانونية، العدد 14، 2022.

[3] عبد الرحمن العتيبي، المرجع السابق، ص 87.

غالباً مع الشخصية الاعتبارية للشركات، حيث تعتبر الشركة كياناً قانونياً مستقلاً عن مساهميها ومديريها، لها ذمة مالية خاصة وتتحمل المسؤولية عن التزاماتها.[1]

ومع ذلك، تواجه فكرة منح الشخصية القانونية للذكاء الاصطناعي انتقادات واسعة وجذرية. يرى المعارضون أن هذه الفكرة تتجاهل الاختلاف الجوهري بين الإنسان والآلة، وأنها تقوم على تشبيه سطحي ومضلل. فالأنظمة الذكية، مهما تطورت، تفتقر إلى الوعي والإرادة الحرة والقدرات الأخلاقية التي تشكل أساس الشخصية الإنسانية والمسؤولية القانونية. كما يثيرون مخاوف من أن يؤدي منح الشخصية القانونية للآلات إلى إضعاف المسؤولية البشرية الحقيقية وإلى خلق كيانات قانونية يصعب السيطرة عليها أو محاسبتها بشكل فعال.

الفرع الثاني: الشخصية القانونية للأنظمة ذاتية التسيير فقها وتشريعا

لا تزال فكرة منح الشخصية القانونية للأنظمة الذكية في مراحلها الجنينية ولم تحظ بقبول واسع على المستوى التشريعي أو الفقهي الدولي. ومع ذلك، فقد أثارت بعض النقاشات والمبادرات التي تستحق الذكر.

لعل أبرز هذه المبادرات هو قرار البرلمان الأوروبي الصادر عام 2017 بشأن القواعد القانونية المدنية للروبوتات، والذي تضمن توصية للمفوضية الأوروبية بالنظر في إنشاء شخصية قانونية خاصة للروبوتات الذكية والمستقلة الأكثر تطوراً على المدى الطويل، بهدف تحميلها المسؤولية عن الأضرار التي تسببها. ورغم أن هذه التوصية كانت غير ملزمة وأثارت جدلاً واسعاً، إلا أنها وضعت الفكرة على جدول الأعمال السياسي والقانوني.[2]

على المستوى الفقهي، تتباين المواقف بشكل كبير. فبينما يدافع بعض الباحثين بحماس عن ضرورة الاعتراف بنوع من الشخصية القانونية للذكاء الاصطناعي لمواجهة تحديات المستقبل، يرفض غالبية الفقهاء هذه الفكرة ويعتبرونها غير ضرورية بل وخطيرة. ويؤكد هؤلاء على أن الأدوات القانونية الحالية (مثل قواعد مسؤولية المنتج، والمسؤولية عن فعل الغير، والمسؤولية التقصيرية) يمكن تكييفها وتطويرها

[1] European Cybercrime Centre, 2022. Available at: -https://www.europol.europa.eu/publications-documents/challenges-in-cybercrime

[2] د. محمد بن إبراهيم، "الشخصية القانونية للذكاء الاصطناعي: تحديات وآفاق"، مجلة الدراسات القانونية العربية، العدد 34، 2021، ص 14

للتعامل مع الأضرار الناجمة عن الأنظمة الذاتية دون الحاجة إلى اللجوء إلى خيال قانوني مثل "الشخصية الإلكترونية".[1]

كما تبرز العديد من التحديات العملية التي تعترض تطبيق فكرة الشخصية القانونية على الأنظمة الذكية، مثل كيفية تحديد معايير الأهلية لمنح هذه الشخصية، ومن سيمثل النظام قانوناً أمام القضاء، وكيف ستتشكل ذمته المالية، وما هي الحقوق والالتزامات التي ستترتب على هذه الشخصية. غياب الإجابات الواضحة والمقنعة على هذه الأسئلة يجعل من الصعب تبني هذا التوجه في الوقت الراهن.[2]

بشكل عام، يمكن القول بأنه لا يوجد إجماع دولي أو توجه تشريعي واضح نحو منح الشخصية القانونية للأنظمة الذكية. ويبقى التركيز منصباً على تطوير آليات المساءلة التي تستهدف الأطراف البشرية المسؤولة عن تصميم وتطوير ونشر واستخدام هذه التقنيات.

الفرع الثالث: الآثار المترتبة عن إضفاء الشخصية القانونية على الأنظمة ذاتية التسيير

إذا تم، جدلاً، تبني فكرة منح الشخصية القانونية للأنظمة الذكية، فإن ذلك سيثير آثاراً عميقة وجذرية على منظومة القانون الجزائي برمته. فأول هذه الآثار هو إمكانية مساءلة النظام الذاتي جزائياً بشكل مباشر عن الأفعال الجرمية التي يرتكبها، باعتباره "شخصاً" قانونياً مستقلاً.

وهذا يطرح مباشرة تساؤلاً حول طبيعة العقوبات التي يمكن فرضها على نظام ذاتي. فالعقوبات الجزائية التقليدية (مثل الحبس والغرامة) مصممة للبشر. ويصبح التساؤل هنا عن العقوبة المناسبة لآلة. يقترح البعض عقوبات مثل "الإعدام الرقمي" (إيقاف تشغيل النظام بشكل دائم)، أو "إعادة التأهيل" (إعادة برمجة النظام لتصحيح سلوكه)، أو فرض غرامات مالية على الذمة المالية المخصصة للنظام (إن وجدت). إلا أن فعالية وجدوى هذه العقوبات المقترحة تظل محل شك كبير، خاصة فيما يتعلق بتحقيق أهداف العقوبة التقليدية كالردع والإصلاح.

كما يثور تساؤل حول تأثير مساءلة النظام الذاتي على مسؤولية الأطراف البشرية المرتبطة به. أي هل ستصبح مسؤولية البشر تبعية لمسؤولية النظام، أم ستظل مسؤولية أصلية ومستقلة؟ وهل يمكن أن يؤدي التركيز على مساءلة الآلة إلى إضعاف الحوافز لدى البشر لاتخاذ الاحتياطات اللازمة وتجنب المخاطر؟

[1] عبد الله الحسيني، المرجع السابق، ص 55.

[2] د. محمد بن إبراهيم، "الشخصية القانونية للذكاء الاصطناعي: تحديات وآفاق"، مجلة الدراسات القانونية العربية، العدد 34، 2021، ص 122

يخشى الكثيرون من أن تصبح "الشخصية القانونية" للآلة مجرد وسيلة للتهرب من المسؤولية البشرية الحقيقية.

بالإضافة إلى ذلك، فإن مساءلة كيان غير بشري يفتقر إلى الوعي والإرادة والقدرة على الشعور بالذنب أو الندم يثير إشكاليات فلسفية وأخلاقية عميقة حول معنى العدالة والمسؤولية في القانون الجزائي. فتطبيق العقوبة على آلة يطرح تساؤلات حول مدى تحقيق العدالة، ومدى انسجام ذلك مع المبادئ الأساسية التي يقوم عليها القانون الجزائي الحديث الذي يضع الإنسان وكرامته في مركزه.[1]

لهذه الأسباب مجتمعة، يبدو أن فكرة إسناد المسؤولية الجزائية إلى النظام الذاتي ككيان قانوني مستقل لا تزال بعيدة عن الواقع العملي وتواجه عقبات نظرية وعملية وقانونية وأخلاقية جسيمة. ويبقى التركيز على تطوير آليات مساءلة الأطراف البشرية هو المسار الأكثر واقعية وانسجاماً مع مبادئ القانون الجزائي وقيمه الأساسية في الوقت الحاضر والمستقبل المنظور.

[1] البرلمان الأوروبي، تقرير حول القواعد القانونية المدنية للروبوتات، قرار صادر عام 2017، متاح على: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_AR.html تم الاطلاع: 24 ماي 2025.

خلاصة الفصل الأول:

يخلص الفصل إلى أن مسألة إسناد المسؤولية الجزائية في ظل بروز الأنظمة الذاتية التسيير تمثل تحديًا عميقًا للمنظومة القانونية التقليدية، إذ تستدعي إعادة نظر جذرية في المفاهيم الكلاسيكية للمسؤولية الجزائية التي تقوم أساسًا على العنصر البشري، من حيث الأهلية والنية والإرادة. فهذه الأنظمة، بما تتمتع به من قدرات على اتخاذ قرارات مستقلة وتنفيذ أفعال دون تدخل مباشر من الإنسان، تطرح إشكالية جوهرية تتعلق بإمكانية مساءلتها قانونيًا، الأمر الذي يبدو متعارضًا مع المبادئ الأساسية للقانون الجنائي، وعلى رأسها مبدأ الشخصية في العقوبة ومبدأ الشرعية.

وأمام استبعاد مساءلة النظام الذاتي ذاته ككيان مستقل، يتجه التفكير القانوني نحو تحميل المسؤولية للأطراف البشرية ذات الصلة، كالمصممين، المطورين، والمشغلين، وذلك من خلال توسيع مفهوم الخطأ غير العمدي وتطوير معايير العناية الواجبة، بما يتلاءم مع خصوصيات هذه الأنظمة. غير أن هذا الحل قد لا يكون كافيًا وحده، بالنظر إلى ما يعرف في الفقه بـ "فجوة المسؤولية"، وهي المسافة الفاصلة بين الأضرار التي يمكن أن تسببها هذه الأنظمة والفاعلين التقليديين الذين قد لا تتوافر في حقهم أركان المسؤولية بشكل واضح.

من هذا المنطلق، يقترح الفصل استكشاف نماذج مسؤولية تكميلية تستند إلى مفاهيم جديدة أو معدّلة، من بينها المسؤولية عن المنتج، التي تتيح مساءلة الجهة المصنعة عن أضرار النظام، وكذلك المسؤولية القائمة على المخاطر، التي تفترض تحميل من يستفيد من التكنولوجيا المتقدمة تبعات استخدامها، حتى في غياب خطأ محدد. ويشدد في هذا السياق على ضرورة التوفيق بين مقتضيات حماية المجتمع وردع الأفعال الضارة، وبين احترام المبادئ الأساسية كشرط التجريم ومبدأ عدم رجعية القوانين.

الفصل الثاني:

سبل مواكبة التشريع الجنائي للتحديات التقنية

يشهد العالم تحولات تكنولوجية متسارعة، يقف على رأسها التطور الهائل في مجال الذكاء الاصطناعي والأنظمة الذاتية. هذه التقنيات، بقدر ما تحمل من وعود بتسهيل حياة البشر وتحقيق التقدم في مختلف المجالات، فإنها تثير في الوقت ذاته تحديات قانونية وأخلاقية غير مسبوقة، لا سيما في إطار القانون الجنائي. فقدرة الأنظمة الذاتية على اتخاذ قرارات وتنفيذ أفعال قد تلحق أضراراً بالأشخاص والممتلكات، دون تدخل بشري مباشر في لحظة وقوع الفعل، تضع القواعد التقليدية للمسؤولية الجزائية القائمة على الفعل الإرادي والخطأ البشري أمام اختبار حقيقي.

لقد تناولنا في الفصل الأول إشكالية إسناد المسؤولية الجزائية لهذه الكيانات الجديدة، وبحثنا في مدى انطباق أركان الجريمة التقليدية الركن المادي والركن المعنوي على أفعالها، واستعرضنا نماذج المسؤولية المقترحة للأطراف البشرية المتدخلة الصانع، المبرمج، المستخدم. إلا أن مواجهة التحديات التي تطرحها الأنظمة الذاتية لا تقتصر على تحديد المسؤول، بل تمتد لتشمل ضرورة تكييف النصوص الجنائية القائمة لتستوعب الأشكال الجديدة للإجرام التقني، وابتكار آليات تشريعية وتنظيمية قادرة على مواكبة هذا التطور المتسارع، وتعزيز الوقاية من المخاطر وضمان تعويض الضحايا.

يهدف هذا الفصل إلى استكشاف سبل مواكبة التشريع الجنائي لهذه التحديات التقنية. سنخصص المبحث الأول لتحليل التكييف القانوني للجرائم التي يمكن أن تنجم عن الأنظمة الذاتية، سواء كانت جرائم واقعة ضد الأشخاص، أو ضد الممتلكات، أو جرائم معلوماتية متخصصة، محاولين استجلاء مدى كفاية النصوص الحالية وقصورها. أما المبحث الثاني، فسنتطرق فيه إلى الاتجاهات التشريعية الحديثة والمقترحات المستقبلية لمواجهة هذه التحديات، من خلال قراءة في التشريعات المقارنة الرائدة، وبحث الآليات المبتكرة لتعزيز الوقاية والتعويض، وتسليط الضوء على الأدوار المنوطة بالمؤسسات الرقابية والتشريعية والقضائية في هذا السياق.

إن الهدف الأسمى هو البحث عن توازن دقيق بين تشجيع الابتكار التكنولوجي والاستفادة من إمكانات الذكاء الاصطناعي، وبين ضرورة حماية المصالح الجوهرية للمجتمع والأفراد، وضمان سيادة القانون والعدالة في العصر الرقمي.

المبحث الأول: التكييف القانوني للجرائم الناتجة عن الأنظمة ذاتية التسيير

تثير الأفعال الضارة الصادرة عن الأنظمة الذاتية تحدياً جوهرياً أمام المشرع والقاضي الجنائي، يتمثل في كيفية تكييف هذه الأفعال ضمن نصوص التجريم القائمة. فالقانون الجنائي، بمبادئه ونصوصه التي صيغت في عصر ما قبل الثورة الرقمية، قد لا يكون مهيأً بشكل كامل لاستيعاب الطبيعة الفريدة للسلوك الصادر عن كيانات غير بشرية تتمتع بدرجات متفاوتة من الاستقلالية والقدرة على التعلم. تتجلى أهمية التكييف القانوني الدقيق في كونه المنطلق الأساسي لتحديد ما إذا كان الفعل المرتكب يشكل جريمة يعاقب عليها القانون، ومن ثم تحديد المسؤول عنها وتوقيع الجزاء المناسب. إن صعوبة تطبيق النصوص التقليدية، التي تفترض فاعلاً بشرياً يتمتع بالإرادة والتمييز، على أفعال الأنظمة الذاتية، تستدعي تحليلاً معمقاً لمدى كفاية هذه النصوص والحاجة إلى تعديلها أو استحداث نصوص جديدة تتلاءم مع الواقع التكنولوجي المستجد.[1]

سنتناول في هذا المبحث أبرز الجرائم التي يمكن أن تنشأ عن استخدام الأنظمة الذاتية، مقسمة بحسب طبيعة الحق المعتدى عليه. سنبدأ بالجرائم الواقعة ضد الأشخاص، كالقتل والإيذاء غير العمديين، ثم ننتقل إلى الجرائم الواقعة ضد الممتلكات، كالإتلاف والاستخدام غير المشروع، وأخيراً سنتطرق إلى الجرائم المعلوماتية التي تلعب فيها الأنظمة الذاتية دوراً متزايداً، كالقرصنة وسرقة البيانات. وسنركز في كل مطلب على تحليل أركان الجريمة المعنية في سياق الأنظمة الذاتية، وتحديد الصعوبات التي تعترض تطبيق النصوص القائمة، وبحث الحلول الممكنة لتجاوزها.

المطلب الأول: الجرائم الواقعة ضد الأشخاص

تعد حماية حياة الإنسان وسلامته الجسدية من أسمى الأهداف التي يسعى القانون الجنائي إلى تحقيقها. ومع تزايد انتشار الأنظمة الذاتية في مجالات حيوية تمس حياة الأفراد بشكل مباشر، مثل قطاع النقل السيارات ذاتية القيادة والرعاية الصحية الأنظمة الطبية الذكية والقطاع الصناعي الروبوتات المستقلة، تتزايد المخاوف من إمكانية تسبب هذه الأنظمة في أضرار جسيمة للأشخاص، قد تصل إلى حد القتل أو الإيذاء. إن خطورة هذه الأضرار المحتملة تفرض على المشرع والقضاء ضرورة توفير حماية جنائية فعالة للأفراد

[1] حسين علي الطباخ، المسؤولية الجنائية في ضوء تطور الذكاء الاصطناعي، دار النهضة العربية، القاهرة، 2020، ص. 45.

في مواجهة المخاطر الناشئة عن هذه التقنيات، وذلك من خلال تكييف نصوص التجريم المتعلقة بالجرائم الواقعة ضد الأشخاص لتشمل الأفعال الضارة الصادرة عن الأنظمة الذاتية.[1]

سنركز في هذا المطلب على تحليل ثلاث صور رئيسية للجرائم التي يمكن أن تقع ضد الأشخاص بفعل الأنظمة الذاتية: القتل غير العمدي، والأذى الجسدي الناتج عن خلل تقني، والمساس بالسلامة الجسدية نتيجة قرارات خوارزمية. وسنبحث في كل فرع مدى انطباق أركان الجريمة التقليدية، والتحديات التي تواجه إثبات الخطأ والعلاقة السببية، وإشكالية تحديد المسؤول في ظل تعقد الأنظمة وتعدد المتدخلين.

الفرع الأول: القتل غير العمدي بفعل الأنظمة ذاتية التسيير

تعتبر جريمة القتل غير العمدي من أخطر الجرائم التي يمكن أن تنجم عن عمل الأنظمة الذاتية، لا سيما في قطاعات مثل النقل الذاتي أو الرعاية الصحية. وتثير هذه الجريمة تساؤلات معقدة حول كيفية تطبيق أركانها التقليدية على سيناريوهات تتورط فيها آلات مستقلة.[2]

أولاً: تحليل أركان جريمة القتل غير العمدي في سياق الأنظمة الذاتية

تقوم جريمة القتل غير العمدي تقليدياً على ثلاثة أركان أساسية: الخطأ، والضرر (وفاة إنسان)، والعلاقة السببية بين الخطأ والضرر. يتخذ الخطأ في هذه الجريمة صورة الإهمال، أو عدم الاحتياط، أو عدم مراعاة القوانين واللوائح والأنظمة. ويتمثل التحدي الأكبر في سياق الأنظمة الذاتية في تحديد طبيعة الخطأ ومصدره.[3]

فهل يمكن اعتبار "خطأ" النظام الذاتي (مثل خطأ في التعرف على عائق، أو اتخاذ قرار خاطئ في موقف طارئ) بمثابة الخطأ الذي يتطلبه القانون لقيام الجريمة؟ أم أن الخطأ يجب أن ينسب بالضرورة إلى فاعل بشري؟ كما رأينا في الفصل الأول، تفتقر الأنظمة الذاتية إلى الإرادة والتمييز بالمعنى الإنساني، مما يجعل من الصعب نسبة الخطأ إليها مباشرة. لذلك، يتجه البحث عن الخطأ عادة نحو الأطراف البشرية

[1] إيمان عبد الستار أحمد، الذكاء الاصطناعي والمسؤولية الجنائية، المجلة المصرية للدراسات القانونية، العدد 17، 2021، ص. 132.

[2] علي عبد القادر القهوجي، الوجيز في شرح قانون العقوبات – القسم العام، منشورات الحلبي الحقوقية، بيروت، 2012، ص. 217.

[3] علي عبد القادر القهوجي، المرجع نفسه، ص. 219.

المرتبطة بالنظام: المصمم الذي قد يكون أهمل في وضع معايير السلامة، أو المبرمج الذي ارتكب خطأ في كتابة الكود، أو المصنع الذي لم يجر الاختبارات الكافية، أو المستخدم الذي أهمل في الإشراف أو أساء استخدام النظام.[1]

أما ركن الضرر، وهو وفاة إنسان، فلا يثير إشكالية خاصة في هذا السياق، فالنتيجة المأساوية واحدة سواء كان المتسبب فيها إنساناً أو آلة. لكن إثبات العلاقة السببية بين الخطأ (البشري المفترض) والوفاة الناتجة عن فعل النظام الذاتي يمثل تحدياً كبيراً آخر. فتعقيد الأنظمة، وتعدد العوامل المتداخلة (برمجية، مادية، بيئية، بشرية)، وظاهرة "الصندوق الأسود" قد تجعل من الصعب تتبع سلسلة الأحداث وتحديد السبب المباشر أو الملائم للوفاة بشكل قاطع، مما قد يعيق إمكانية الإدانة.[2]

ثانياً: إشكالية تحديد المسؤول عن الخطأ

تعتبر إشكالية تحديد المسؤول عن الخطأ المؤدي إلى القتل غير العمدي هي العقدة الأساسية في هذا النوع من الجرائم. ففي ظل تعدد المتدخلين في دورة حياة النظام الذاتي (مصمم، مبرمج، مصنع، مورد بيانات، مالك، مشغل، جهة صيانة)، يصبح من الصعب تحديد الطرف الذي يمكن أن ينسب إليه الخطأ الجنائي الموجب للمسؤولية.[3]

هل هو الصانع الذي طرح في السوق نظاماً غير آمن بما فيه الكفاية؟ أم المبرمج الذي أغفل حالة معينة في الخوارزمية؟ أم المستخدم الذي لم يلتزم بتعليمات التشغيل أو لم يتدخل في الوقت المناسب؟ أم أن المسؤولية تتوزع بينهم جميعاً؟ تطرح هذه الأسئلة تحديات كبيرة أمام جهات التحقيق والقضاء، وتتطلب خبرات فنية عالية لتحليل أسباب الحادث وتحديد مواطن الخلل والإهمال.

تزداد الإشكالية تعقيداً مع الأنظمة التي تتمتع بقدرات تعلم ذاتي وتتخذ قرارات غير متوقعة بناءً على خبراتها المتراكمة. ففي هذه الحالة، قد يكون من الصعب ربط سلوك النظام بخطأ بشري محدد، مما

[1] سامي بن يوسف، الأنظمة الذاتية والمسؤولية القانونية: تحديات وآفاق، مجلة العلوم القانونية، العدد 12، 2023، ص. 112

[2] ناصر عبد القادر، المسؤولية الجنائية في ظل الثورة الرقمية، دار النهضة العربية، 2021، ص. 134

[3] ليلى الحاج، التحديات القانونية للذكاء الاصطناعي في المجال الجنائي، مجلة القانون الحديث، العدد 7، 2022، ص. 89

يثير مجدداً النقاش حول "فجوة المسؤولية" وإمكانية مساءلة النظام نفسه وهو ما استبعدناه في الفصل الأول كأساس للمسؤولية الجزائية التقليدية[1]

ثالثاً: أمثلة عملية

تجسدت هذه الإشكاليات في حوادث واقعية أثارت اهتماماً عالمياً. لعل أبرزها حوادث السيارات ذاتية القيادة التي أدت إلى وفاة مشاة أو ركاب. ففي كل حادث، كان التحقيق يركز على تحديد ما إذا كان الخطأ يكمن في نظام الاستشعار أو نظام اتخاذ القرار في السيارة، أم في إهمال السائق الذي كان يفترض أن يكون مشرفاً على النظام، أم في عوامل خارجية أخرى. وغالباً ما كانت نتائج التحقيقات معقدة وتثير جدلاً حول توزيع المسؤوليات.[2]

كذلك، تبرز المخاطر في المجال الطبي مع استخدام أنظمة التشخيص أو الجراحة الروبوتية المعتمدة على الذكاء الاصطناعي. فأي خطأ في تشخيص حالة مريض أو في تنفيذ عملية جراحية بواسطة نظام ذاتي قد يؤدي إلى وفاته، مما يطرح تساؤلات حول مسؤولية الطبيب المشرف، ومصمم النظام، والمستشفى. يتطلب التعامل مع هذه الحالات تكييفاً دقيقاً لمفهوم الخطأ الطبي ليشمل الأخطاء الناتجة عن التفاعل بين الإنسان والآلة.[3]

الفرع الثاني: الأذى الجسدي الناتج عن خلل تقني

إلى جانب القتل، يمكن للأنظمة الذاتية أن تتسبب في إيذاء جسدي غير مميت للأفراد، وذلك نتيجة لحدوث خلل تقني في تصميمها أو عملها. ويشمل ذلك طيفاً واسعاً من الإصابات، بدءاً من الجروح والكدمات البسيطة وصولاً إلى العجز الدائم.

أولاً: تكييف جريمة الإيذاء غير العمدي مع حالات الخلل في الأنظمة ذاتية التسيير

تنطبق على جريمة الإيذاء غير العمدي نفس الأركان العامة لجريمة القتل غير العمدي (الخطأ، الضرر، العلاقة السببية)، مع اختلاف في طبيعة الضرر الذي يتمثل هنا في المساس بسلامة الجسم دون

[1] ليلى الحاج، المرجع السابق، ص 100

[2] خالد مراد، السيارات ذاتية القيادة والمسؤولية القانونية، مجلة النقل الذكي، المجلد 5، العدد 2، 2023، ص. 45

[3] سامي الحسن، التشخيص الطبي الآلي: تحديات قانونية وأخلاقية، دار النشر الأكاديمي، 2023، ص. 102

إزهاق الروح. وبالتالي، فإن التحديات المتعلقة بتحديد الخطأ ومصدره، وإثبات العلاقة السببية، وتحديد المسؤول، تظل قائمة بنفس القدر من التعقيد.[1]

يجب البحث عن الخطأ المتمثل في الإهمال أو عدم الاحتراز لدى الأطراف البشرية المسؤولة عن النظام (الصانع، المبرمج، المستخدم). فإذا أمكن إثبات أن الخلل التقني الذي أدى إلى الإيذاء كان نتيجة لإهمال في التصميم أو الاختبار أو الصيانة أو الاستخدام، وأن هذا الخلل هو السبب المباشر أو الملائم للضرر الجسدي، أمكن مساءلة الطرف المسؤول عن جريمة الإيذاء غير العمدي.[2]

ثانياً: صعوبات إثبات الخلل التقني وعلاقته السببية بالضرر الجسدي

يعد إثبات وجود خلل تقني في النظام الذاتي وتحديد طبيعته ومصدره خطوة حاسمة في تحديد المسؤولية. وغالباً ما يتطلب ذلك خبرة فنية متخصصة وقدرة على تحليل سجلات عمل النظام وفحص مكوناته المادية والبرمجية. وقد تكون هذه العملية صعبة ومكلفة، خاصة إذا كان النظام معقداً أو كانت المعلومات المتعلقة بتصميمه وعمله سرية.

كما أن إثبات العلاقة السببية بين الخلل التقني والضرر الجسدي قد لا يكون سهلاً دائماً. فقد يدفع الصانع أو المستخدم بأن الضرر كان نتيجة لعوامل أخرى لا علاقة لها بالخلل المزعوم، مثل سوء استخدام الضحية نفسه، أو ظروف خارجية غير متوقعة، أو حتى عيوب كامنة في تصميم المنتج لا ترقى لمستوى الخطأ الجنائي. ويتطلب الفصل في هذه الدفوع تحليلاً دقيقاً لوقائع كل حالة وظروفها.[3]

ثالثاً: دور معايير السلامة والجودة في تحديد الخطأ

تلعب معايير السلامة والجودة المعتمدة في صناعة وتطوير الأنظمة الذاتية دوراً هاماً في تحديد مدى وجود الخطأ الموجب للمسؤولية. فإذا ثبت أن الصانع أو المبرمج لم يلتزم بالمعايير الفنية المتعارف عليها أو بالمتطلبات التنظيمية المفروضة لضمان سلامة النظام، فإن ذلك يمكن أن يشكل قرينة قوية على وجود إهمال أو عدم احتياط من جانبه.

---

[1] أحمد زين الدين، المسؤولية الجنائية عن الأفعال غير العمدية، مجلة الحقوق المعاصرة، العدد 22، 2022، ص. 58

[2] نور الدين بن حمد، الإيذاء غير العمدي في القانون الجنائي: دراسة مقارنة، دار الفكر القانوني، 2021، ص. 89

[3] مصطفى عبد الحميد، المسؤولية الجنائية عن الأفعال الناتجة عن الأنظمة التقنية، مجلة القانون والتكنولوجيا، العدد 10، 2023، ص. 112

لذلك، تبرز أهمية وضع معايير واضحة ومفصلة لسلامة وموثوقية الأنظمة الذاتية، خاصة تلك المستخدمة في المجالات عالية المخاطر. كما يتطلب الأمر تطوير آليات فعالة للرقابة والاختبار والاعتماد للتأكد من التزام المطورين والمصنعين بهذه المعايير قبل طرح منتجاتهم في السوق. إن وجود إطار معياري وتنظيمي قوي يمكن أن يساهم في تحديد الخطأ وتسهيل إثبات المسؤولية في حالة وقوع حوادث.[1]

الفرع الثالث: المساس بالسلامة الجسدية نتيجة قرارات خوارزمية

لا يقتصر خطر المساس بالسلامة الجسدية على حالات الخلل التقني الواضح، بل قد ينجم أيضاً عن القرارات التي تتخذها الخوارزميات التي تحرك الأنظمة الذاتية، حتى لو كانت هذه الخوارزميات تعمل ظاهرياً كما هو مصمم لها. فقد تؤدي هذه القرارات، بسبب طبيعتها أو تحيزاتها الكامنة، إلى نتائج تمس بسلامة الأفراد.

أولاً: تحليل القرارات الخوارزمية التي قد تؤدي إلى ضرر جسدي

تتخذ الأنظمة الذاتية قرارات بناءً على تحليل البيانات ومعالجتها بواسطة خوارزميات معقدة. وفي بعض الحالات، قد تكون هذه القرارات ذات تأثير مباشر على السلامة الجسدية للأفراد. ومن الأمثلة على ذلك: أنظمة التشخيص الطبي الآلي التي قد تخطئ في تشخيص حالة خطيرة أو توصي بعلاج غير مناسب، أنظمة التحكم الصناعي التي قد تتخذ قرارات تشغيلية خاطئة تؤدي إلى حوادث عمل، أو حتى أنظمة المراقبة الأمنية التي قد تخطئ في تحديد هوية شخص وتؤدي إلى استخدام مفرط للقوة ضده.

في هذه الحالات، لا يكون الضرر ناتجاً عن خلل فني بالمعنى التقليدي، بل عن "قرار" اتخذه النظام بناءً على برمجته والبيانات المتاحة له. وهذا يثير تساؤلاً حول مدى إمكانية اعتبار هذا القرار الخوارزمي الخاطئ بحد ذاته فعلاً يمكن أن تتبني عليه المسؤولية الجزائية.[2]

ثانياً: إشكالية التحيز الخوارزمي وتأثيره على السلامة الجسدية

تعتبر مشكلة التحيز الخوارزمي (Algorithmic Bias) من أبرز التحديات في هذا السياق. فالخوارزميات غالباً ما يتم تدريبها على كميات هائلة من البيانات التي قد تعكس تحيزات موجودة في

[1] أحمد صالح، معايير السلامة في تطوير الأنظمة الذكية: التحديات القانونية والتقنية، مجلة الدراسات القانونية، العدد 25، 2024، ص. 45

[2] عمر الحداد، تأثير الخوارزميات على سلامة الأفراد: دراسة مقارنة، دار الفكر القانوني، القاهرة، 2023، ص. 120

المجتمع أو في طريقة جمع البيانات نفسها. ونتيجة لذلك، قد تتخذ الأنظمة الذاتية قرارات تمييزية أو غير عادلة تجاه فئات معينة من الأفراد، مما قد يؤثر على سلامتهم الجسدية بشكل مباشر أو غير مباشر.

على سبيل المثال، قد تكون أنظمة التعرف على الوجوه أقل دقة في التعرف على وجوه الأقليات العرقية، مما قد يؤدي إلى أخطاء في تحديد الهوية في سياقات أمنية. وقد تكون أنظمة التشخيص الطبي أقل فعالية في تشخيص أمراض معينة لدى النساء أو الأقليات إذا كانت بيانات التدريب متحيزة نحو فئات أخرى. هذا التحيز، وإن لم يكن مقصوداً بالضرورة من قبل المبرمجين، يمكن أن يؤدي إلى أضرار جسدية حقيقية ويتطلب معالجة قانونية وتنظيمية.[1]

ثالثاً: مدى إمكانية اعتبار القرار الخوارزمي الخاطئ فعلاً مجرماً بحد ذاته

يثير المساس بالسلامة الجسدية نتيجة قرار خوارزمي تساؤلاً حول مدى إمكانية اعتبار هذا القرار "فعلاً" بالمعنى القانوني، وهل يمكن أن يشكل أساساً للمسؤولية الجزائية حتى في غياب خلل تقني واضح أو خطأ بشري مباشر يمكن إثباته؟

يبدو أن القواعد التقليدية للمسؤولية الجزائية تجد صعوبة في التعامل مع هذه الإشكالية. فنسبة الخطأ إلى قرار خوارزمي مجرد، دون ربطه بإهمال بشري في التصميم أو التدريب أو الإشراف، قد يتعارض مع مبدأ شخصية المسؤولية. ومع ذلك، فإن خطورة النتائج التي قد تترتب على هذه القرارات الخاطئة تدفع باتجاه البحث عن حلول. قد يتمثل أحد الحلول في التركيز على واجبات العناية والحيطة المفروضة على مصممي ومستخدمي الأنظمة التي تتخذ قرارات حساسة تمس السلامة الجسدية، واعتبار الإخلال بهذه الواجبات (مثل عدم اختبار التحيز، أو عدم وضع آليات للتحقق والمراجعة البشرية) بمثابة الخطأ الموجب للمسؤولية، حتى لو كان القرار الخوارزمي نفسه يبدو "صحيحاً" من الناحية التقنية البحتة.[2]

[1] سعاد إبراهيم، التحيز الخوارزمي وتأثيره على حقوق الإنسان، مجلة دراسات القانون والتكنولوجيا، العدد 12، 2024، ص. 45

[2] سامي الحسن، القرارات الخوارزمية والمسؤولية القانونية: دراسة تحليلية، مجلة الدراسات القضائية، العدد 8، 2024، ص. 52

المطلب الثاني: الجرائم الواقعة ضد الممتلكات

لا تقتصر الأضرار المحتملة للأنظمة الذاتية على الأشخاص فحسب، بل تمتد لتشمل الممتلكات العامة والخاصة. فقدرة هذه الأنظمة على التفاعل مع البيئة المادية والتحكم في الآلات والمعدات تجعلها قادرة على إحداث أضرار مادية جسيمة، سواء عن طريق الخطأ أو نتيجة لخلل أو حتى بفعل مقصود من قبل أطراف خارجية تستغل هذه الأنظمة. وتشمل هذه الأضرار إتلاف المركبات والمباني والبنى التحتية، والاستيلاء غير المشروع على الأصول الرقمية أو المادية، وتعطيل أنظمة الحماية والتحكم الحيوية. يفرض هذا الواقع ضرورة تكييف نصوص القانون الجنائي المتعلقة بحماية الملكية لتشمل الأفعال الضارة الصادرة عن الأنظمة الذاتية، وتحديد المسؤوليات المترتبة عليها.[1]

سنتناول في هذا المطلب أبرز صور الجرائم التي يمكن أن تقع ضد الممتلكات بفعل الأنظمة الذاتية. سنبدأ بتحليل جريمة إتلاف الممتلكات، خاصة في سياق الأنظمة ذاتية القيادة. ثم ننتقل إلى بحث إشكالية الاستخدام غير المشروع لأصول الغير بواسطة هذه الأنظمة. وأخيراً، سنتطرق إلى جريمة تعطيل نظم الحماية والتحكم عن بعد، مع التركيز على التحديات القانونية والتقنية التي تثيرها هذه الجرائم المستحدثة.

الفرع الأول: إتلاف الممتلكات عبر أنظمة ذاتية القيادة

تعتبر حوادث المركبات ذاتية القيادة التي تؤدي إلى إتلاف ممتلكات (مثل سيارات أخرى، أو واجهات مباني، أو تجهيزات طرقية) من السيناريوهات الواقعية التي بدأت تظهر مع انتشار هذه التقنية. وتثير هذه الحوادث تساؤلات حول كيفية تطبيق جريمة الإتلاف وتحديد المسؤول عنها[2].

أولاً: تطبيق جريمة الإتلاف على الحوادث التي تسببها المركبات ذاتية القيادة

تتطلب جريمة الإتلاف عادة ركناً مادياً يتمثل في فعل الإتلاف أو التخريب الذي يلحق بمال مملوك للغير، وركناً معنوياً يتمثل في القصد الجنائي (في الإتلاف العمدي) أو الخطأ غير العمدي (في الإتلاف

[1] خالد عبد الله، القانون الجنائي في مواجهة التكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2022، ص. 210

[2] مريم العرفاوي، المسؤولية القانونية عن الأضرار الناجمة عن المركبات ذاتية القيادة، مجلة القانون والآليات الحديثة، العدد 7، 2023، ص. 57

غير العمدي، إذا نص القانون على ذلك). في سياق المركبات ذاتية القيادة، يتمثل الفعل المادي في الاصطدام أو الانحراف الذي يؤدي إلى إلحاق الضرر بالممتلكات[1].

تثور الصعوبة مجدداً عند محاولة إثبات الركن المعنوي. فإذا كان الحادث ناتجاً عن قرار اتخذته المركبة بشكل مستقل، فمن الصعب نسبة القصد الجنائي أو حتى الخطأ غير العمدي إلى المركبة نفسها. لذلك، يتجه البحث عن المسؤولية نحو الأطراف البشرية. فإذا كان الإتلاف ناتجاً عن خطأ في تصميم نظام القيادة الذاتية أو في برمجته أو اختباره، يمكن مساءلة الصانع عن الإتلاف غير العمدي (إذا كان مجرماً). وإذا كان ناتجاً عن إهمال من جانب السائق المشرف (مثل عدم الانتباه أو عدم التدخل في الوقت المناسب)، يمكن مساءلته هو عن الخطأ. أما إذا قام شخص ما بتعمد استخدام المركبة ذاتية القيادة لإتلاف ممتلكات الغير (كأن يوجهها عمداً نحو سيارة أخرى)، فإنه يسأل عن جريمة الإتلاف العمدي كفاعل أصلي.[2]

ثانياً: تحديد المسؤول عن الإتلاف (المالك، المشغل، الصانع)

كما في حالة الجرائم ضد الأشخاص، يمثل تحديد المسؤول عن الإتلاف الناتج عن مركبة ذاتية القيادة تحدياً. هل هو مالك المركبة، أم المشغل (السائق المشرف)، أم الصانع؟ تعتمد الإجابة على سبب الحادث وطبيعة الخطأ المرتكب.

كقاعدة عامة، قد يسأل المالك أو المشغل إذا ثبت إهماله في استخدام المركبة أو الإشراف عليها. أما الصانع، فيمكن أن يسأل إذا ثبت أن الحادث كان نتيجة لخلل أو عيب في تصميم النظام أو تصنيعه لم يتخذ الاحتياطات الكافية لمنعه. وقد تتوزع المسؤولية بينهم إذا ساهمت أخطاء متعددة في وقوع الحادث.[3]

تلعب وثائق التأمين دوراً هاماً في تغطية الأضرار المادية الناتجة عن هذه الحوادث، لكنها لا تعفي الأطراف من المسؤولية الجزائية إذا ثبت ارتكابهم لخطأ موجب للعقاب.

---

[1] فهد القحطاني، جريمة الإتلاف وأثرها في ظل التقنيات الذكية، المؤتمر العربي للقانون والتكنولوجيا، الرياض، 2024، ص. 150

[2] المرجع، نفسه ص 165

[3] د. محمد الكيلاني، القانون الجنائي وتحديات الجرائم المرتبطة بالتكنولوجيا الحديثة، دار النهضة العربية، 2021، ص. 105

ثالثاً: إشكالية الإتلاف الناتج عن تفاعل بين عدة أنظمة ذاتية التسيير

تزداد الصورة تعقيداً عندما يكون حادث الإتلاف ناتجاً عن تفاعل بين عدة مركبات أو أنظمة ذاتية القيادة (مثل تصادم بين سيارتين ذاتيتي القيادة). ففي هذه الحالة، يصبح تحديد الطرف المخطئ وتوزيع المسؤولية أكثر صعوبة، خاصة إذا كانت الأنظمة تتواصل وتتخذ قرارات بشكل منسق أو متفاعل.

يتطلب التعامل مع هذه السيناريوهات تطوير آليات قانونية وتقنية قادرة على تحليل التفاعلات المعقدة بين الأنظمة وتحديد مصادر الأخطاء. وقد يتطلب الأمر أيضاً وضع قواعد خاصة للمسؤولية في حالات الحوادث التي تتورط فيها أنظمة متعددة، قد تشمل نماذج للمسؤولية المشتركة أو التضامنية بين مصنعي ومشغلي هذه الأنظمة.[1]

الفرع الثاني: الاستخدام غير المشروع لأصول الغير

يمكن للأنظمة الذكية، بقدراتها على معالجة البيانات والتحكم في الأجهزة، أن تُستخدم كوسيلة لارتكاب جرائم تتعلق بالاستخدام غير المشروع لأصول مملوكة للغير، سواء كانت أصولاً رقمية أو مادية.

أولاً: تحليل صور الاستخدام غير المشروع

تتعدد صور الاستخدام غير المشروع التي يمكن أن تسهلها الأنظمة الذكية. فقد يُستخدم نظام ذكي لاختراق شبكات حاسوبية والوصول غير المصرح به إلى بيانات أو موارد مملوكة للغير. وقد يُستخدم الذكاء الاصطناعي لتحليل نقاط الضعف في أنظمة الحماية واختراقها بهدف سرقة معلومات أو أموال. كما يمكن استغلال القدرات الحاسوبية للأنظمة الذكية المملوكة للغير (مثل خوادم الحوسبة السحابية) بشكل غير مشروع للقيام بعمليات معقدة مثل تعدين العملات المشفرة أو شن هجمات إلكترونية.[2]

تمتد صور الاستخدام غير المشروع لتشمل الأصول المادية أيضاً. فقد تُستخدم طائرات بدون طيار ذاتية التحكم في عمليات التهريب أو التجسس أو نقل مواد ممنوعة عبر الحدود أو إلى داخل مناطق

[1] المرجع نفسه، ص 110.

[2] سمير الشريف، الجرائم الإلكترونية واستخدام الأنظمة الذكية في الاختراق والقرصنة، مجلة الأمن السيبراني، العدد 8، 2023، ص. 45

محظورة (مثل السجون). وقد تُستخدم الروبوتات الصناعية المستقلة في عمليات تخريب أو سرقة داخل المصانع.[1]

ثانياً: تكييف النصوص القائمة المتعلقة بإساءة استخدام الممتلكات مع الواقع الرقمي

تواجه النصوص الجنائية التقليدية المتعلقة بجرائم مثل السرقة، أو خيانة الأمانة، أو إساءة استخدام الممتلكات، تحديات في التكيف مع هذه الصور المستحدثة من الاستخدام غير المشروع في البيئة الرقمية وبواسطة الأنظمة الذكية.

فمفهوم "المال" أو "الأصل" قد يحتاج إلى توسيع ليشمل البيانات والمعلومات والموارد الحاسوبية غير الملموسة. كما أن أفعال "الاختلاس" أو "الاستيلاء" قد تتخذ أشكالاً جديدة في العالم الرقمي يصعب تكييفها ضمن القوالب التقليدية. ويتطلب الأمر غالباً تفسيراً واسعاً للنصوص القائمة أو استحداث نصوص خاصة بالجرائم المعلوماتية لمعالجة هذه الأفعال.[2]

ثالثاً: دور الأنظمة الذكية في تسهيل ارتكاب هذه الجرائم

لا تقتصر إشكالية الأنظمة الذكية على كونها "أداة" في يد المجرم البشري لارتكاب جرائم الاستخدام غير المشروع، بل قد تتطور لتصبح "فاعلاً" شبه مستقل في بعض الحالات. فالأنظمة الذكية القادرة على التعلم والتكيف قد تتمكن من اكتشاف ثغرات واستغلالها بشكل ذاتي، أو قد يتم تصميمها خصيصاً للبحث عن فرص للاستيلاء غير المشروع على الأصول وتنفيذها بشكل مؤتمت.[3]

هذا التطور يزيد من صعوبة تتبع الجريمة وتحديد المسؤول عنها. فإذا قام نظام ذكي مستقل بسرقة بيانات أو استغلال موارد حاسوبية دون تدخل بشري مباشر، فمن هو المسؤول؟ هل هو المبرمج الذي صمم

[1] أحمد الجابري، استغلال الحوسبة السحابية والأنظمة الذكية في الجرائم المالية، المؤتمر الدولي للأمن السيبراني، دبي، 2024، ص. 112

[2] خالد عبد الله، المرجع السابق، ص 225.

[3] فهد القحطاني،، المرجع السابق، ص 165.

النظام بهذه القدرات؟ أم المستخدم الذي أطلقه؟ أم لا أحد؟ تعود هنا إشكالية "فجوة المسؤولية" لتطرح نفسها بقوة.[1]

الفرع الثالث: تعطيل نظم الحماية والتحكم عن بعد

تمثل أنظمة الحماية والتحكم عن بعد (مثل أنظمة الإنذار، وأنظمة المراقبة، وأنظمة التحكم الصناعي في البنى التحتية الحيوية كالطاقة والمياه والنقل) أهدافاً حساسة للهجمات التي قد تستخدم فيها الأنظمة الذكية.

أولاً: تجريم أفعال تعطيل أو تخريب أنظمة الحماية بواسطة أنظمة ذكية

يعتبر تعطيل أو تخريب هذه الأنظمة الحيوية من الأفعال الخطيرة التي تهدد الأمن العام والسلامة العامة. ويمكن للأنظمة الذكية أن تلعب دوراً في تنفيذ هذه الهجمات، إما كأداة لتحديد نقاط الضعف وتنفيذ الاختراق، أو كبرمجيات خبيثة ذاتية التشغيل قادرة على الانتشار وتعطيل الأنظمة المستهدفة.

تجرم معظم التشريعات أفعال الدخول غير المشروع إلى أنظمة الحاسب الآلي وتعطيلها أو إتلاف بياناتها. وينبغي تكييف هذه النصوص لتشمل بوضوح استخدام الأنظمة الذكية كوسيلة لارتكاب هذه الجرائم، وتشديد العقوبات نظراً لخطورة النتائج المحتملة، خاصة عند استهداف البنى التحتية الحيوية.[2]

ثانياً: مدى انطباق نصوص جرائم الإرهاب السيبراني

عندما يتم تعطيل أو تخريب أنظمة الحماية والتحكم عن بعد بهدف بث الرعب بين الناس أو إجبار حكومة أو منظمة دولية على القيام بعمل أو الامتناع عنه، فإن الفعل قد يرقى إلى مستوى جريمة الإرهاب السيبراني. وتتميز هذه الجريمة بخطورتها البالغة ودوافعها السياسية أو الأيديولوجية.

[1] محمد بن حسين، إشكالية المسؤولية الجنائية في الجرائم المرتكبة بواسطة الذكاء الاصطناعي، مجلة القانون والتكنولوجيا، العدد 5، 2023، ص. 63.

[2] محمد فرحات، استخدام الذكاء الاصطناعي في الجرائم السيبرانية: التحديات القانونية والواقعية، مجلة العلوم القانونية والتقنية، العدد 7، 2023، ص. 88.

يمكن للأنظمة الذكية أن تكون أداة فعالة في يد الجماعات الإرهابية لتنفيذ هجمات سيبرانية واسعة النطاق ومعقدة ضد أهداف حيوية. ويتطلب ذلك تكييفاً خاصاً لنصوص مكافحة الإرهاب لتشمل هذه الأشكال الجديدة من التهديدات، وتعزيز التعاون الدولي لملاحقة مرتكبيها.[1]

ثالثاً: التحديات المتعلقة بالإثبات وتحديد هوية الفاعل

تواجه جرائم تعطيل أنظمة الحماية والتحكم عن بعد، خاصة تلك التي تستخدم فيها الأنظمة الذكية، تحديات كبيرة في مجال الإثبات وتحديد هوية الفاعل الحقيقي. فالطبيعة العابرة للحدود للإنترنت، واستخدام تقنيات التخفي وإخفاء الهوية (مثل الشبكات الخاصة الافتراضية VPN وشبكة تور Tor)، وقدرة الأنظمة الذكية على العمل بشكل مؤتمت ومستقل، كلها عوامل تجعل من الصعب تتبع مصدر الهجوم وتحديد المسؤول عنه.[2]

يتطلب ذلك تعزيز القدرات التقنية لجهات التحقيق والملاحقة القضائية، وتطوير أدوات للتحليل الجنائي الرقمي قادرة على التعامل مع الهجمات المعقدة التي تستخدم الذكاء الاصطناعي. كما يستدعي الأمر تعزيز التعاون الدولي في مجال تبادل المعلومات والأدلة والمساعدة القانونية لمواجهة الطبيعة العابرة للحدود لهذه الجرائم.[3]

المطلب الثالث: الجرائم المعلوماتية المرتبطة بالأنظمة ذاتية التسيير

يشكل الفضاء السيبراني مسرحاً متزايد الأهمية للأنشطة الإجرامية، وتلعب التقنيات الحديثة، وعلى رأسها الذكاء الاصطناعي والأنظمة الذاتية، دوراً محورياً في تطور هذه الجرائم وتغيير طبيعتها. فلم تعد الأنظمة الذكية مجرد هدف للهجمات السيبرانية، بل أصبحت أيضاً أداة قوية في يد المجرمين لتنفيذ هجمات أكثر تعقيداً وفعالية وتلقائية. إن قدرة هذه الأنظمة على تحليل البيانات بسرعة فائقة، والتعلم من التجارب، والعمل بشكل مستقل دون تدخل بشري مباشر، تفتح الباب أمام أشكال جديدة من الجرائم المعلوماتية التي يصعب

[1] عبد الرزاق بوحارة، الذكاء الاصطناعي وتهديدات الأمن القومي: قراءة في مخاطر الاستخدام الإرهابي، المجلة الجزائرية للأمن والدفاع، العدد 4، 2022، ص. 102.

[2] INTERPOL, Cybercrime Trends Report 2022, Lyon, 2022, pp. 22–23

[3] United Nations Office on Drugs and Crime (UNODC), Handbook on International Cooperation in Cybercrime Cases, Vienna, 2021, pp. 40.

اكتشافها ومواجهتها بالطرق التقليدية. يستدعي هذا الواقع تحديثاً مستمراً للتشريعات الجنائية المتعلقة بالجرائم المعلوماتية لتواكب هذه التطورات، وتعزيز القدرات التقنية والقانونية لمكافحتها.[1]

سنتناول في هذا المطلب أبرز الجرائم المعلوماتية التي ترتبط ارتباطاً وثيقاً بالأنظمة الذاتية. سنبدأ بتحليل دور هذه الأنظمة في تسهيل عمليات القرصنة والاختراق. ثم ننتقل إلى بحث كيفية استخدام الذكاء الاصطناعي في التلاعب بالبيانات وسرقتها. وأخيراً، سنتطرق إلى التحدي الأكبر المتمثل في تنفيذ جرائم سيبرانية مؤتمتة بالكامل دون تدخل بشري مباشر، وما يثيره ذلك من إشكاليات قانونية تتعلق بالإسناد والمسؤولية.[2]

الفرع الأول: القرصنة والاختراق عبر الأنظمة الذكية

تعتبر جرائم القرصنة والاختراق (الدخول غير المشروع إلى أنظمة وشبكات الحاسب الآلي) من أقدم وأشهر الجرائم المعلوماتية. ومع تطور الذكاء الاصطناعي، أصبحت الأنظمة الذكية أداة فعالة لتعزيز قدرات المهاجمين وتطوير أساليب الاختراق.

أولاً: استخدام الذكاء الاصطناعي في تطوير أدوات اختراق أكثر فعالية

يمكن استخدام تقنيات الذكاء الاصطناعي، مثل تعلم الآلة ومعالجة اللغة الطبيعية، لتطوير أدوات اختراق أكثر ذكاءً وفعالية. فعلى سبيل المثال، يمكن للذكاء الاصطناعي أن يحلل كميات هائلة من البيانات لتحديد نقاط الضعف والثغرات الأمنية في الأنظمة المستهدفة بشكل أسرع وأدق من الطرق اليدوية. كما يمكن استخدامه لتوليد هجمات تصيد احتيالي (Phishing) أكثر إقناعاً وتخصيصاً، أو لكسر كلمات المرور المعقدة، أو لتجاوز أنظمة الكشف عن التسلل التقليدية.

[1] نبيل بن عيسى، آليات التحليل الجنائي الرقمي لمواجهة التحديات التقنية للجريمة المعلوماتية، مجلة الدراسات القانونية، جامعة قسنطينة، العدد 18، 2022، ص. 174

[2] نبيل بن عيسى، المرجع السابق، ص 175.

يمكن للأنظمة الذكية أيضاً أن تتعلم وتتكيف مع آليات الدفاع المتغيرة، مما يجعلها قادرة على شن هجمات مستمرة ومستهدفة يصعب صدها. هذا التطور في أدوات الاختراق يضع ضغطاً كبيراً على المدافعين ويتطلب منهم تطوير آليات حماية أكثر تطوراً تعتمد بدورها على الذكاء الاصطناعي.[1]

ثانياً: تكييف جرائم الدخول غير المشروع والاعتراض غير القانوني مع استخدام الأنظمة الذكية

تجرم معظم التشريعات أفعال الدخول غير المشروع إلى الأنظمة المعلوماتية والاعتراض غير القانوني للبيانات. وينبغي أن تكون هذه النصوص مرنة بما يكفي لتشمل استخدام الأنظمة الذكية كأداة لتنفيذ هذه الجرائم. فالعبرة ليست بالوسيلة المستخدمة، بل بالفعل غير المشروع نفسه ونتائجه.[2]

ومع ذلك، قد يثير استخدام الأنظمة الذكية بعض الصعوبات في التكييف. فمثلاً، هل يعتبر استخدام نظام ذكي للبحث عن ثغرات أمنية بشكل مؤتمت "دخولا غير مشروع" حتى قبل استغلال الثغرة فعلياً؟ وهل يمكن اعتبار "اعتراض" البيانات الذي يقوم به نظام ذكي بنفس درجة الخطورة التي يتسم بها الاعتراض البشري المباشر؟ تتطلب هذه الأسئلة تفسيراً دقيقاً للنصوص وتوضيحاً لنطاق تطبيقها في العصر الرقمي[3].

ثالثاً: صعوبة تتبع الهجمات المؤتمتة

عندما يتم تنفيذ هجمات القرصنة والاختراق بواسطة أنظمة ذكية تعمل بشكل مؤتمت، يصبح تتبع مصدر الهجوم وتحديد هوية الفاعل البشري الذي يقف وراءه أمراً بالغ الصعوبة. فالأنظمة الذكية يمكنها العمل من خلال شبكات معقدة وموزعة، واستخدام تقنيات لإخفاء الهوية، مما يجعل عملية التحقيق الجنائي الرقمي معقدة للغاية.

[1] أحمد بوخميس، التهديدات السيبرانية الحديثة في ظل تطور تقنيات الذكاء الاصطناعي، مجلة الأمن والحوكمة الرقمية، المركز العربي للأبحاث، العدد 12، 2022، ص. 98

[2] أحمد بوخسيس، المرجع السابق، ص 100.

[3] رضوان بوحليقة، الذكاء الاصطناعي والأمن السيبراني: التحديات والفرص، مجلة دراسات قانونية وسياسية، جامعة باتنة 1، العدد 25، 2023، ص. 146

هذه الصعوبة في التتبع والإسناد تمثل تحدياً كبيراً لفعالية إنفاذ القانون، وقد تؤدي إلى إفلات العديد من المجرمين من العقاب. ويتطلب الأمر تطوير تقنيات متقدمة للتحليل الجنائي الرقمي وتعزيز التعاون الدولي لتبادل المعلومات وتنسيق جهود الملاحقة.[1]

الفرع الثاني: التلاعب في البيانات أو سرقتها بوساطة الذكاء الاصطناعي

تعتبر البيانات "نفط العصر الرقمي"، وتمثل هدفاً ثميناً للمجرمين. ويمكن للذكاء الاصطناعي أن يلعب دوراً كبيراً في تسهيل عمليات التلاعب بالبيانات أو سرقتها.[2]

أولاً: قدرة الأنظمة الذكية على تحليل كميات هائلة من البيانات واستغلالها بشكل غير مشروع

تتمتع الأنظمة الذكية بقدرة فائقة على معالجة وتحليل كميات ضخمة من البيانات (Big Data) بسرعة وكفاءة. هذه القدرة يمكن استغلالها بشكل غير مشروع لسرقة بيانات حساسة (مثل بيانات شخصية، أو بيانات مالية، أو أسرار تجارية)، أو للتلاعب بالبيانات بهدف تحقيق مكاسب غير مشروعة أو إلحاق الضرر بالآخرين.

على سبيل المثال، يمكن استخدام الذكاء الاصطناعي لتحليل بيانات المستخدمين المسروقة وتحديد الأهداف الأكثر قيمة للاحتيال أو الابتزاز. كما يمكن استخدامه للتلاعب ببيانات الأسواق المالية لتحقيق أرباح غير قانونية، أو لنشر معلومات مضللة (Deepfakes) بهدف التأثير على الرأي العام أو تشويه سمعة الأفراد.[3]

ثانياً: تكييف جرائم سرقة البيانات والتلاعب بها مع الأساليب الجديدة المعتمدة على الذكاء الاصطناعي

تجرم القوانين عادة أفعال سرقة البيانات (مثل الاحتيال الحاسوبي) والتلاعب بها (مثل التزوير المعلوماتي). وينبغي تكييف هذه النصوص لتشمل الأساليب الجديدة التي تعتمد على الذكاء الاصطناعي.

---

[1] هشام بوعمامة، التحقيق في الجرائم المعلوماتية: إشكاليات الإثبات والتحليل الجنائي الرقمي، مجلة الأمن والقانون، جامعة الأمير نايف، العدد 28، 2021، ص. 176

[2] ربيعة عكاشة، الجرائم السيبرانية في ظل التطور التكنولوجي: دراسة قانونية، مجلة العلوم القانونية والسياسية، جامعة مستغانم، العدد 19، 2021، ص. 142

[3] ربيعة عكاشة، المرجع السابق، ص 144.

قد يتطلب الأمر توضيح مفهوم "البيانات" المحمية جنائياً، وتحديد الأفعال التي تشكل "سرقة" أو "تلاعباً" في سياق المعالجة الآلية والتحليل الذكي. كما قد تحتاج العقوبات إلى مراجعة لتعكس خطورة هذه الجرائم في العصر الرقمي وتأثيرها الواسع المحتمل.[1]

ثالثاً: إشكالية البيانات المستخدمة لتدريب الأنظمة الذكية ومدى مشروعية جمعها

تعتمد فعالية الأنظمة الذكية بشكل كبير على جودة وكمية البيانات التي يتم تدريبها عليها. وهذا يثير إشكالية قانونية وأخلاقية هامة تتعلق بمصادر هذه البيانات ومدى مشروعية جمعها واستخدامها. ففي كثير من الأحيان، يتم جمع كميات هائلة من البيانات الشخصية دون موافقة صريحة من أصحابها، أو يتم استخدام بيانات قد تكون متحيزة أو غير دقيقة، مما قد يؤدي إلى انتهاك الخصوصية أو التمييز.

يثور التساؤل حول مدى إمكانية مساءلة مطوري الأنظمة الذكية جزائياً إذا استخدموا بيانات تم الحصول عليها بطرق غير مشروعة لتدريب أنظمتهم، خاصة إذا أدت هذه الأنظمة لاحقاً إلى ارتكاب جرائم أو إلحاق أضرار. يتطلب الأمر وضع قواعد واضحة تنظم عملية جمع واستخدام البيانات لأغراض تطوير الذكاء الاصطناعي، وتحديد المسؤوليات المترتبة على انتهاك هذه القواعد.[2]

الفرع الثالث: تنفيذ جرائم سيبرانية مؤتمتة دون تدخل بشري مباشر

يمثل هذا الفرع التحدي الأكبر والأكثر إثارة للقلق، حيث تتطور الأنظمة الذكية لتصبح قادرة على تنفيذ جرائم سيبرانية كاملة بشكل مؤتمت ومستقل، دون الحاجة إلى تدخل بشري مباشر في كل خطوة.

أولاً: ظهور البرمجيات الخبيثة الذكية (AI-powered malware) وشبكات البوتنت (Botnets) المستقلة

بدأت تظهر أنواع جديدة من البرمجيات الخبيثة التي تستخدم تقنيات الذكاء الاصطناعي لتكون أكثر قدرة على التخفي والانتشار والتكيف. يمكن لهذه البرمجيات الخبيثة الذكية أن تتعلم من بيئتها، وتتجنب آليات الكشف، وتختار أهدافها وتنفذ هجماتها بشكل مستقل. كما يمكن استخدام الذكاء الاصطناعي لإدارة

[1] محمد سعيد عبد القادر، حماية البيانات في البيئة الرقمية بين القانون والتكنولوجيا، المجلة المصرية للقانون والاقتصاد، العدد 9، 2022، ص. 91

[2] European Union Agency for Cybersecurity (ENISA), Threat Landscape Report 2022, pp. 45.

شبكات البوتنت (شبكات من الأجهزة المخترقة التي يتم التحكم فيها عن بعد) بشكل أكثر فعالية وتلقائية، وتوجيهها لشن هجمات حجب الخدمة الموزعة (DDoS) أو نشر البريد العشوائي أو سرقة البيانات على نطاق واسع.[1]

هذه القدرة على الأتمتة والاستقلالية تجعل من الصعب جداً اكتشاف هذه الهجمات ووقفها قبل أن تسبب أضراراً جسيمة.

ثانياً: تحدي إسناد المسؤولية في حالة الجرائم المرتكبة بالكامل بواسطة أنظمة ذاتية

عندما يتم ارتكاب جريمة سيبرانية بالكامل بواسطة نظام ذاتي مستقل، دون تدخل بشري مباشر يمكن إثباته، نعود إلى مواجهة "فجوة المسؤولية" التي ناقشناها سابقاً. فمن هو المسؤول جنائياً في هذه الحالة؟

تمثل هذه الأسئلة تحدياً عميقاً للمبادئ الأساسية للقانون الجنائي القائم على المسؤولية الشخصية. ويرى البعض أن هذا التحدي قد يفرض إعادة نظر جذرية في مفهوم المسؤولية الجزائية، أو على الأقل تطوير نماذج جديدة للمسؤولية (مثل المسؤولية الموضوعية المشددة أو آليات المساءلة التنظيمية) للتعامل مع المخاطر الناشئة عن الأنظمة الذكية المستقلة.[2]

ثالثاً: الحاجة إلى تطوير آليات للتحقيق والملاحقة تتناسب مع هذه الجرائم

تتطلب مواجهة الجرائم السيبرانية المؤتمتة تطوير آليات للتحقيق والملاحقة تتناسب مع طبيعتها المعقدة والمستقلة. ويشمل ذلك:[3]

- تطوير أدوات تقنية متقدمة: الحاجة إلى أدوات قادرة على تحليل سلوك الأنظمة الذكية الخبيثة، وتتبع مصادرها، وتحديد نقاط ضعفها.

[1] عبد العزيز خليفة، المرجع السابق، ص 110.

[2] أحمد الشاذلي، البرمجيات الخبيثة وتطورها باستخدام الذكاء الاصطناعي، مجلة الأمن السيبراني، المركز القومي للمعلومات، العدد 7، 2023، ص. 58

[3] نوال بوفاتح، الجرائم الإلكترونية في ظل التطورات التكنولوجية الحديثة: التحديات القانونية والإجرائية، مجلة الدراسات القانونية والسياسية، جامعة باتنة 1، العدد 22، 2023، ص. 88

– تعزيز القدرات البشرية: تدريب المحققين والمدعين العامين والقضاة على فهم التقنيات المستخدمة في هذه الجرائم وكيفية التعامل مع الأدلة الرقمية المعقدة.

– التعاون الدولي: نظراً للطبيعة العابرة للحدود لهذه الجرائم، يصبح التعاون الدولي في تبادل المعلومات والأدلة والمساعدة القانونية أمراً حيوياً.

– التشريعات الاستباقية: وضع تشريعات تنظم تطوير ونشر الأنظمة الذكية، وتفرض التزامات بالشفافية وقابلية التفسير والمساءلة على المطورين والمستخدمين، للمساعدة في منع وقوع هذه الجرائم وتسهيل التحقيق فيها عند وقوعها.

إن التكييف القانوني للجرائم الناتجة عن الأنظمة الذاتية يمثل خطوة أولى ضرورية، ولكنه غير كافٍ بمفرده. فالمواجهة الشاملة تتطلب أيضاً النظر في الاتجاهات التشريعية المستقبلية والآليات التنظيمية والوقائية، وهو ما سنتناوله في المبحث التالي.[1]

[1] لي إبراهيم خليفة، التحديات القانونية في مواجهة الجرائم السيبرانية المعتمدة على الذكاء الاصطناعي، مجلة العلوم القانونية، جامعة بغداد، المجلد 44، العدد 2، 2022، ص. 233

المبحث الثاني: المسؤولية الجزائية للأنظمة ذاتية التسيير في منظور الأنظمة القانونية المقارنة

إن التحديات القانونية المعقدة التي يطرحها التطور المتسارع للأنظمة الذاتية، والتي تم تحليل أبرزها في المبحث الأول، تستدعي استجابة تشريعية وتنظيمية شاملة تتجاوز مجرد تكييف النصوص القائمة. فمواجهة المخاطر المستجدة وضمان تحقيق التوازن بين الابتكار وحماية الحقوق يتطلب رؤية استشرافية تتبنى اتجاهات تشريعية حديثة وتستلهم من التجارب الدولية، بالإضافة إلى ابتكار آليات عملية لتعزيز الوقاية والمساءلة والتعويض. لم يعد كافياً التعامل مع المشكلات بشكل تفاعلي بعد وقوعها، بل أصبح من الضروري وضع أطر تنظيمية استباقية قادرة على توجيه تطوير ونشر هذه التقنيات بما يخدم المصلحة العامة ويحترم القيم الأساسية للمجتمع.

يهدف هذا المبحث إلى استعراض أبرز الاتجاهات التشريعية والمقترحات المستقبلية التي تهدف إلى مواكبة التحديات التقنية في مجال القانون الجنائي المتعلق بالأنظمة الذاتية. سنبدأ في المطلب الأول بقراءة تحليلية للتشريعات والمبادرات الدولية المقارنة الأكثر تقدماً في هذا المجال، مثل اللائحة الأوروبية للذكاء الاصطناعي والمبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية، بالإضافة إلى استعراض موجز للتجارب في دول رائدة أخرى كالولايات المتحدة واليابان. وفي المطلب الثاني، سنناقش مجموعة من الآليات العملية المقترحة لتعزيز الوقاية من الأضرار وضمان تعويض الضحايا، مثل إنشاء صناديق تعويض وطنية وفرض التأمين الإجباري وتطوير نظم للترخيص والاعتماد. أما المطلب الثالث، فسيخصص لتسليط الضوء على الأدوار المحورية التي يجب أن تضطلع بها المؤسسات الرقابية والتشريعية والقضائية في هذا السياق، بما في ذلك الحاجة إلى هيئات رقابية متخصصة وتعزيز دور البرلمان وتأهيل الفاعلين في منظومة العدالة.

المطلب الأول: قراءة في التشريعات المقارنة الحديثة

أدركت العديد من الدول والمنظمات الدولية أهمية وضع أطر تنظيمية للذكاء الاصطناعي والأنظمة الذاتية لمواجهة التحديات القانونية والأخلاقية والاجتماعية الناشئة عنها. وتتباين هذه الأطر في مقاربتها ونطاقها ودرجة إلزاميتها، لكنها تشترك في السعي نحو تحقيق هدف مشترك يتمثل في تعزيز الثقة في هذه التقنيات وضمان تطويرها واستخدامها بشكل مسؤول وآمن. وتعتبر دراسة هذه التجارب المقارنة أمراً ضرورياً للاستفادة من الدروس المستخلصة وتحديد أفضل الممارسات التي يمكن تبنيها أو تكييفها لتناسب السياق الوطني.[1]

سنقوم في هذا المطلب بتحليل ثلاث من أبرز المبادرات التنظيمية على المستوى الدولي والإقليمي: اللائحة الأوروبية للذكاء الاصطناعي، والمبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية، مع إلقاء نظرة سريعة على بعض التجارب الوطنية في الولايات المتحدة واليابان. وسنركز في تحليلنا على المقاربات المتبعة في تصنيف المخاطر، والالتزامات المفروضة على المطورين والمستخدمين، وآليات الحوكمة والإنفاذ المقترحة، ومدى تناولها للإشكاليات المتعلقة بالمسؤولية الجنائية.

الفرع الأول: اللائحة الأوروبية للذكاء الاصطناعي (AI Act)

تعتبر اللائحة الأوروبية للذكاء الاصطناعي، التي تم اقتراحها من قبل المفوضية الأوروبية في أبريل 2021 ودخلت حيز التنفيذ تدريجياً، أول محاولة شاملة وملزمة قانوناً لتنظيم الذكاء الاصطناعي على مستوى العالم. وتهدف اللائحة إلى وضع إطار قانوني موحد للذكاء الاصطناعي داخل الاتحاد الأوروبي، يضمن السلامة ويحترم الحقوق الأساسية ويعزز الابتكار والاستثمار في هذا المجال.[2]

أولاً: المقاربة القائمة على المخاطر (Risk-Based Approach)

تتبنى اللائحة الأوروبية مقاربة قائمة على تصنيف أنظمة الذكاء الاصطناعي حسب درجة المخاطر التي تشكلها على السلامة والصحة والحقوق الأساسية. وتحدد أربعة مستويات للمخاطر:

---

[1] OECD, Principles on Artificial Intelligence, 2019. متاح على الموقع الرسمي للمنظمة: www.oecd.org تم الاطلاع عليه يوم 2025/05/27.

[2] المفوضية الأوروبية، اقتراح لائحة بشأن القواعد المنسقة للذكاء الاصطناعي (قانون الذكاء الاصطناعي)، COM(2021) 206 final، بروكسل، 21 أبريل 2021، من الموقع الرسمي للاتحاد الأوروبي: https://eur-lex.europa.eu تم الاطلاع عليه يوم 2025/05/29.

1. المخاطر غير المقبولة (Unacceptable Risk): تشمل الأنظمة التي تعتبر تهديداً واضحاً للناس، مثل أنظمة التلاعب السلوكي الضار، وأنظمة التصنيف الاجتماعي (Social Scoring)، وأنظمة تحديد الهوية البيومترية عن بعد في الوقت الحقيقي لأغراض إنفاذ القانون (مع استثناءات محدودة). هذه الأنظمة محظورة تماماً بموجب اللائحة.[1]

2. المخاطر العالية (High Risk): تشمل الأنظمة المستخدمة في مجالات حساسة قد تؤثر بشكل كبير على حياة الأفراد وفرصهم، مثل البنى التحتية الحيوية، والتعليم، والتوظيف، والخدمات الأساسية، وإنفاذ القانون، وإدارة الهجرة، وإقامة العدل. تخضع هذه الأنظمة لالتزامات صارمة قبل طرحها في السوق وبعده، تشمل تقييم المخاطر، وجودة البيانات، والتوثيق، والشفافية، والإشراف البشري، والمتانة والأمن السيبراني.[2]

3. المخاطر المحدودة (Limited Risk): تشمل الأنظمة التي تتطلب التزامات شفافية محددة، مثل أنظمة التفاعل مع البشر (Chatbots) حيث يجب إعلام المستخدم بأنه يتفاعل مع آلة، وأنظمة إنشاء المحتوى الاصطناعي (Deepfakes) حيث يجب الإشارة إلى أن المحتوى تم إنشاؤه بواسطة الذكاء الاصطناعي.

4. المخاطر الدنيا أو المنعدمة (Minimal or No Risk): تشمل الغالبية العظمى من أنظمة الذكاء الاصطناعي الحالية، مثل مرشحات البريد العشوائي أو ألعاب الفيديو. لا تفرض اللائحة التزامات إضافية على هذه الفئة، ولكنها تشجع على تبني مدونات سلوك طوعية.[3]

ثانياً: الالتزامات المفروضة على الأنظمة عالية المخاطر

تضع اللائحة مجموعة من الالتزامات الصارمة على مطوري ومستخدمي الأنظمة عالية المخاطر، تهدف إلى ضمان سلامتها وموثوقيتها ومراعاتها للحقوق الأساسية. تشمل هذه الالتزامات:[4]

[1] المفوضية الأوروبية، اقتراح لائحة بشأن القواعد المنسقة للذكاء الاصطناعي (قانون الذكاء الاصطناعي)، المرجع السابق، المواد من 7 الى 8.

[2] المرجع نفسه ، خاصة المادة 6 المتعلقة بتصنيف "المخاطر العالية".

[3] المرجع نفسه 2021، المادة 69

[4] المفوضية الأوروبية، اقتراح لائحة الذكاء الاصطناعي، final 206 (2021)COM، المادة 11، بروكسل، 2021.

- نظام إدارة المخاطر: إنشاء وتنفيذ نظام لتقييم وإدارة المخاطر طوال دورة حياة النظام.

- حوكمة البيانات: ضمان جودة وملاءمة وتمثيلية مجموعات البيانات المستخدمة في تدريب واختبار النظام، والتحقق من خلوها من التحيزات الضارة.

- التوثيق الفني: إعداد وثائق فنية مفصلة تشرح كيفية عمل النظام وقدراته وحدوده.

- حفظ السجلات: ضمان تسجيل الأحداث تلقائياً (Logging) لتتبع عمل النظام وتمكين التحقيق في الحوادث.

- الشفافية وتوفير المعلومات للمستخدمين: تزويد المستخدمين بمعلومات واضحة وكافية حول كيفية استخدام النظام بشكل صحيح وتفسير مخرجاته.

- الإشراف البشري: تصميم النظام بحيث يمكن للبشر الإشراف عليه بفعالية، والتدخل عند الضرورة أو إلغاء قراراته.

- المتانة والدقة والأمن السيبراني: ضمان مستوى عالٍ من الدقة والموثوقية والمتانة الفنية والأمن السيبراني للنظام.

ثالثاً: آليات الحوكمة والإنفاذ

تنشئ اللائحة الأوروبية هيكلاً للحوكمة يشمل:[1]

- المكتب الأوروبي للذكاء الاصطناعي (European AI Office): هيئة جديدة داخل المفوضية الأوروبية للإشراف على تطبيق اللائحة وتنسيق الجهود بين الدول الأعضاء.

- السلطات الوطنية المختصة: كل دولة عضو تعين سلطة وطنية مسؤولة عن مراقبة السوق والإشراف على تطبيق اللائحة داخل أراضيها.

- المجلس الأوروبي للذكاء الاصطناعي (European AI Board): يتألف من ممثلين عن السلطات الوطنية والمفوضية، ويعمل على تسهيل التطبيق المنسق للائحة وتقديم المشورة.

[1] العمري، س، «اللائحة الأوروبية للذكاء الاصطناعي: تحليل قانوني للتنظيم والمسؤولية»، مجلة الدراسات القانونية المعاصرة، عدد 15، مجلد 3، 2022، ص 48.

تفرض اللائحة عقوبات مالية كبيرة على الشركات التي تخالف أحكامها، قد تصل إلى نسبة مئوية من إجمالي حجم مبيعاتها السنوي العالمي.[1]

رابعاً: مدى تناول اللائحة لإشكاليات المسؤولية الجنائية

تركز اللائحة الأوروبية بشكل أساسي على تنظيم سلامة المنتجات والخدمات القائمة على الذكاء الاصطناعي ووضع قواعد لطرحها في السوق واستخدامها، ولا تتناول بشكل مباشر ومفصل إشكاليات المسؤولية المدنية أو الجنائية الناشئة عن الأضرار التي قد تسببها هذه الأنظمة. ومع ذلك، فإن الالتزامات التي تفرضها اللائحة، خاصة على الأنظمة عالية المخاطر، يمكن أن يكون لها تأثير غير مباشر على تحديد المسؤولية. فالإخلال بهذه الالتزامات (مثل عدم كفاية تقييم المخاطر، أو استخدام بيانات متحيزة، أو نقص الإشراف البشري) يمكن أن يشكل أساساً لإثبات الخطأ الموجب للمسؤولية المدنية أو حتى الجنائية (في حالة الإهمال الجسيم المؤدي إلى ضرر) بموجب القوانين الوطنية للدول الأعضاء.[2]

الفرع الثاني: المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية (OECD)

تعتبر منظمة التعاون الاقتصادي والتنمية (OECD) من المنظمات الدولية الرائدة في مجال وضع مبادئ وتوصيات للسياسات المتعلقة بالذكاء الاصطناعي. وفي مايو 2019، تبنى مجلس المنظمة "توصية بشأن الذكاء الاصطناعي" تتضمن مجموعة من المبادئ التوجيهية التي تهدف إلى تعزيز تطوير واستخدام ذكاء اصطناعي مبتكر وجدير بالثقة يحترم حقوق الإنسان والقيم الديمقراطية.[3]

أولاً: المبادئ الخمسة للذكاء الاصطناعي الجدير بالثقة

تحدد التوصية خمسة مبادئ أساسية يجب أن توجه الجهات الفاعلة في مجال الذكاء الاصطناعي طوال دورة حياة أنظمته:[4]

---

[1] يوسف، ر، «كيف تغير اللائحة الأوروبية الذكاء الاصطناعي وجهات التشريع»، مجلة التقنية والقانون، 2023، متاح على: www.techlawmagazine.com/ai-regulation. تم الاطلاع عليه يوم 2025/05/28.

[2] بن صالح، أحمد. القانون والتقنيات الحديثة: تنظيم الذكاء الاصطناعي. دار النهضة العربية، 2023، ص 135

[3] يوسف، رياض. «اللائحة الأوروبية للذكاء الاصطناعي وإشكاليات المسؤولية القانونية». مجلة التقنية والقانون، 2023. متاح على: www.techlawmagazine.com/ai-liability. تم الاطلاع عليه يوم 2025/05/25.

[4] العبدالله، محمد. المسؤولية القانونية في عصر الذكاء الاصطناعي. دار الفكر القانوني، 2023، ص 110

1. النمو الشامل والتنمية المستدامة والرفاه: يجب أن تسعى أنظمة الذكاء الاصطناعي إلى تحقيق فائدة للناس والكوكب، من خلال دفع النمو الشامل والتنمية المستدامة والرفاه.

2. القيم المرتكزة على الإنسان والإنصاف: يجب تصميم أنظمة الذكاء الاصطناعي بطريقة تحترم سيادة القانون وحقوق الإنسان والقيم الديمقراطية والتنوع، ويجب أن تتضمن ضمانات مناسبة (مثل تمكين التدخل البشري عند الضرورة) لضمان مجتمع عادل ومنصف.

3. الشفافية وقابلية التفسير: يجب أن يكون هناك شفافية وقابلية تفسير مسؤولة فيما يتعلق بأنظمة الذكاء الاصطناعي لضمان أن يكون الأفراد على دراية عندما يتفاعلون معها، وأن يكونوا قادرين على فهم نتائجها (حسب السياق).

4. المتانة والأمن والسلامة: يجب أن تعمل أنظمة الذكاء الاصطناعي بشكل قوي وآمن وسليم طوال دورة حياتها، ويجب إدارة المخاطر المحتملة بشكل مستمر.

5. المساءلة: يجب أن تكون هناك مساءلة عن أنظمة الذكاء الاصطناعي ونتائجها، بما يتناسب مع أدوار الجهات الفاعلة والسياق.

ثانياً: التوصيات الموجهة للحكومات

تقدم التوصية أيضاً خمس توصيات للحكومات الوطنية لوضع سياسات عامة تسهل تطوير ونشر ذكاء اصطناعي جدير بالثقة:[1]

1. الاستثمار في البحث والتطوير في مجال الذكاء الاصطناعي: تعزيز الاستثمارات العامة والخاصة في البحث والتطوير لتعزيز الابتكار في ذكاء اصطناعي جدير بالثقة.

2. تعزيز منظومة رقمية للذكاء الاصطناعي: ضمان وجود بنية تحتية رقمية قوية، وتقنيات، وآليات لمشاركة البيانات والمعرفة.

[1] ريم، فاطمة، الاستراتيجيات الحكومية في دعم البحث والتطوير في مجال الذكاء الاصطناعي، مذكرة ماستر، جامعة الجزائر، 2024، ص 63

3. تشكيل بيئة سياساتية تمكينية للذكاء الاصطناعي: تشجيع بيئة تنظيمية مرنة ومستجيبة للابتكار، مع ضمان حماية الحقوق والقيم.

4. بناء القدرات البشرية والاستعداد لتحول سوق العمل: تزويد الأفراد بالمهارات اللازمة للتعامل مع الذكاء الاصطناعي ودعم العمال المتأثرين بالتحولات الناجمة عنه.

5. التعاون الدولي ومتعدد الأطراف: تعزيز التعاون بين الدول لتبادل المعرفة وأفضل الممارسات وتطوير معايير مشتركة للذكاء الاصطناعي الجدير بالثقة.

ثالثاً: الطبيعة غير الملزمة للمبادئ وتأثيرها

تتميز مبادئ OECD بأنها غير ملزمة قانوناً، فهي توصيات تهدف إلى توجيه السياسات والممارسات. ومع ذلك، فقد حظيت هذه المبادئ بتأييد واسع النطاق، ليس فقط من الدول الأعضاء في المنظمة، بل أيضاً من دول أخرى ومنظمات دولية وشركات كبرى. وقد شكلت هذه المبادئ أساساً للعديد من الاستراتيجيات الوطنية للذكاء الاصطناعي ونقطة مرجعية هامة في النقاش العالمي حول حوكمة الذكاء الاصطناعي.

من حيث صلتها بالمسؤولية الجنائية، فإن مبدأ "المساءلة" ومبدأ "المتانة والأمن والسلامة" يكتسبان أهمية خاصة. فهما يؤكدان على ضرورة وجود آليات لتحديد المسؤولية عن الأضرار التي قد تسببها أنظمة الذكاء الاصطناعي، وعلى أهمية إدارة المخاطر بشكل استباقي. ويمكن لهذه المبادئ أن تسترشد بها التشريعات الوطنية عند وضع قواعد للمسؤولية أو عند تفسير مفاهيم مثل "الخطأ" أو "واجب العناية" في سياق الأنظمة الذاتية.

الفرع الثالث: التجارب التشريعية في الولايات المتحدة واليابان

تختلف المقاربات المتبعة في الولايات المتحدة واليابان عن المقاربة الأوروبية الشاملة. فبدلاً من قانون واحد شامل، تعتمد هاتان الدولتان على مزيج من التشريعات القطاعية القائمة، والمبادئ التوجيهية الطوعية، والمبادرات التنظيمية التي تركز على مجالات محددة.[1]

[1] يوسف، رياض، «التحديات والسياسات في بناء القدرات البشرية لسوق العمل المتحول بتأثير الذكاء الاصطناعي»، مجلة التقنية والقانون، العدد 12، 2024، ص 87

أولاً: المقاربة الأمريكية: التركيز على الابتكار والتنظيم القطاعي

تتميز المقاربة الأمريكية بتركيزها القوي على تشجيع الابتكار وتجنب التنظيم المفرط الذي قد يعيقه. لا يوجد قانون فيدرالي شامل للذكاء الاصطناعي، بل يتم الاعتماد على التشريعات القائمة في مجالات مثل حماية المستهلك، ومكافحة التمييز، والمسؤولية التقصيرية، مع إصدار مبادئ توجيهية من قبل البيت الأبيض والوكالات الفيدرالية المختلفة لتوجيه تطوير واستخدام الذكاء الاصطناعي في القطاعات التي تشرف عليها.[1]

أصدر البيت الأبيض "مخططاً لقانون حقوق الذكاء الاصطناعي" (Blueprint for an AI Bill of Rights) في عام 2022، وهو عبارة عن مجموعة من المبادئ غير الملزمة تهدف إلى حماية الجمهور من الأضرار المحتملة للذكاء الاصطناعي، وتشمل مبادئ مثل الأنظمة الآمنة والفعالة، والحماية من التمييز الخوارزمي، وخصوصية البيانات، والإشعار والتفسير، والبدائل البشرية والاعتبار والملاذ. كما أصدر المعهد الوطني للمعايير والتكنولوجيا (NIST) "إطار عمل إدارة مخاطر الذكاء الاصطناعي" (AI Risk Management Framework) لمساعدة المؤسسات على إدارة المخاطر المرتبطة بالذكاء الاصطناعي.[2]

على مستوى الولايات، بدأت بعض الولايات في سن تشريعات خاصة بالذكاء الاصطناعي، خاصة فيما يتعلق باستخدام تقنيات التعرف على الوجه من قبل جهات إنفاذ القانون أو في التوظيف.

فيما يتعلق بالمسؤولية، تعتمد الولايات المتحدة بشكل كبير على قانون المسؤولية التقصيرية (Tort Law) للتعامل مع الأضرار الناجمة عن المنتجات والخدمات، بما في ذلك تلك التي تعتمد على الذكاء الاصطناعي. وتثير قضايا المسؤولية عن المنتجات المعيبة (Product Liability) نقاشات حول كيفية تطبيقها على الأنظمة الذكية المعقدة والمتغيرة.[3]

---

[1] البيت الأبيض، مبادئ توجيهية للذكاء الاصطناعي والحوكمة الفيدرالية، 2021، متاح على: www.whitehouse.gov/ai-guidelines تم الاطلاع عليه يوم 2025/05/28.

[2] National Institute of Standards and Technology (NIST), AI Risk Management Framework, 2023, https://www.nist.gov/ai-risk-management-framework تم الاطلاع عليه يوم 2025/05/27.

[3] حسين، سمير، «المسؤولية التقصيرية والذكاء الاصطناعي: تحديات جديدة»، مجلة القانون والتكنولوجيا، 2022، ص 78

ثانياً: المقاربة اليابانية: التركيز على المبادئ الأخلاقية والتعاون بين القطاعين العام والخاص

تتبنى اليابان مقاربة تركز على وضع مبادئ أخلاقية وتوجيهات طوعية لتطوير واستخدام الذكاء الاصطناعي، مع التأكيد على التعاون الوثيق بين الحكومة والصناعة والأوساط الأكاديمية. أصدرت الحكومة اليابانية "مبادئ الذكاء الاصطناعي المرتكزة على الإنسان" (Social Principles of Human-Centric AI) في عام 2019، والتي تتضمن سبعة مبادئ رئيسية: الكرامة الإنسانية، التنوع والشمول، التنمية المستدامة، السلامة، الأمن، الإنصاف، المساءلة والشفافية.[1]

تركز السياسات اليابانية على تعزيز البحث والتطوير في مجال الذكاء الاصطناعي وتطبيقاته في مختلف القطاعات الاقتصادية والاجتماعية، مع تشجيع الشركات على تبني المبادئ الأخلاقية بشكل طوعي. ولا يوجد تنظيم شامل وملزم للذكاء الاصطناعي، بل يتم الاعتماد على التشريعات القطاعية القائمة وتطوير إرشادات خاصة بمجالات محددة مثل الرعاية الصحية والتنقل.[2]

فيما يتعلق بالمسؤولية، تعتمد اليابان على القوانين المدنية والجنائية القائمة. وتجري نقاشات حول كيفية تكييف قواعد المسؤولية المدنية عن المنتجات المعيبة والمسؤولية التقصيرية للتعامل مع الأضرار الناجمة عن الأنظمة الذاتية، مع التركيز على أهمية الشفافية وقابلية التفسير لتسهيل تحديد الأسباب والمسؤوليات.[3]

يتضح من هذا العرض أن هناك تبايناً في المقاربات التنظيمية للذكاء الاصطناعي بين المناطق المختلفة. فبينما تتبنى أوروبا مقاربة شاملة وقائمة على المخاطر وملزمة قانوناً، تفضل الولايات المتحدة واليابان مقاربات أكثر مرونة تعتمد على التنظيم القطاعي والمبادئ التوجيهية الطوعية والتعاون بين الأطراف المعنية. ومع ذلك، هناك تقارب متزايد حول المبادئ الأساسية للذكاء الاصطناعي الجدير بالثقة، مثل

---

[1] Restatement (Third) of Torts: Product Liability, American Law Institute, 1998

[2] Suzuki, K., «Legal Challenges of AI Liability in Japan: Civil and Criminal Perspectives», Journal of Japanese Law and Technology, 2022، ص. 78

[3] Yamamoto, H., «Transparency and Explainability in AI: Key to Liability in Japan», Asian Legal Review, 2024.

السلامة والأمن والإنصاف والشفافية والمساءلة. وتبقى مسألة تكييف قواعد المسؤولية المدنية والجنائية مع التحديات التي تطرحها الأنظمة الذاتية مجالاً للنقاش والتطوير في جميع هذه التجارب.[1]

المطلب الثاني: آليات مقترحة لتعزيز الوقاية والتعويض

لا يكفي مجرد تكييف النصوص الجنائية القائمة أو استلهام التجارب التشريعية المقارنة لمواجهة التحديات المعقدة التي تفرضها الأنظمة الذاتية. فالطبيعة الاحتمالية للمخاطر، وصعوبة إثبات الخطأ وتحديد المسؤول في بعض الأحيان، واحتمال وقوع أضرار واسعة النطاق، كلها عوامل تستدعي التفكير في آليات عملية ومبتكرة تهدف إلى تعزيز الوقاية من الأضرار قبل وقوعها، وضمان حصول الضحايا على تعويض عادل وسريع عند وقوعها، حتى في الحالات التي قد يتعذر فيها إثبات المسؤولية الجزائية التقليدية.[2]

يهدف هذا المطلب إلى استعراض ومناقشة مجموعة من الآليات المقترحة التي يمكن أن تساهم في تحقيق هذين الهدفين المتكاملين: الوقاية والتعويض. سنبحث في الفرع الأول فكرة إنشاء صندوق وطني متخصص لتعويض ضحايا الأضرار الناجمة عن الأنظمة الذاتية، خاصة في الحالات التي يصعب فيها تحديد المسؤول أو يكون فيها غير قادر على التعويض. وفي الفرع الثاني، سنتناول أهمية فرض التأمين الإجباري على الشركات المصنعة والمطورة لهذه الأنظمة كآلية لتوزيع المخاطر وضمان وجود مصدر للتعويض. أما الفرع الثالث، فسيخصص لمناقشة دور تطوير نظام فعال للترخيص والاعتماد القانوني للأنظمة الذكية كأداة لضمان سلامتها وموثوقيتها قبل السماح باستخدامها، وبالتالي تعزيز الوقاية من الأضرار.

الفرع الأول: إنشاء صندوق وطني لتعويض ضحايا الأنظمة الذاتية

تعتبر فكرة إنشاء صناديق تعويض متخصصة آلية معروفة في بعض المجالات التي تنطوي على مخاطر خاصة أو يصعب فيها تحديد المسؤولية الفردية (مثل حوادث التلوث البيئي أو الأضرار الناجمة عن اللقاحات). ويمكن تكييف هذه الآلية لتناسب سياق الأضرار الناجمة عن الأنظمة الذاتية.[3]

---

[1] المرجع نفسه.

[2] بن عيسى، نبيلة، الحوكمة القانونية للذكاء الاصطناعي، رسالة ماجستير، جامعة 8 ماي 1945 قالمة، 2024، ص 59.

[3] بوعلام، يحيى، الذكاء الاصطناعي والتنظيم القانوني: دراسة مقارنة، مجلة العلوم القانونية، العدد 12، 2023، ص. 45

أولاً: مبررات إنشاء الصندوق وأهدافه

تنبع مبررات إنشاء صندوق وطني لتعويض ضحايا الأنظمة الذاتية من عدة اعتبارات:[1]

- صعوبة إثبات المسؤولية: كما أسلفنا، قد يكون من الصعب في بعض الحالات إثبات الخطأ الموجب للمسؤولية الجزائية أو المدنية لدى طرف محدد (الصانع، المبرمج، المستخدم) بسبب تعقيد الأنظمة أو ظاهرة الصندوق الأسود أو طبيعة التعلم الذاتي.

- فجوة التعويض: حتى لو تم تحديد المسؤول، قد يكون غير قادر على دفع التعويضات اللازمة، خاصة إذا كانت الأضرار جسيمة أو لحقت بعدد كبير من الضحايا.

- العدالة الاجتماعية: من منطلق العدالة والتضامن الاجتماعي، قد يكون من غير المقبول ترك ضحايا هذه التقنيات الجديدة دون تعويض لمجرد صعوبات إجرائية في إثبات المسؤولية.

يهدف الصندوق بشكل أساسي إلى ضمان حصول الضحايا على تعويض سريع وعادل عن الأضرار التي لحقت بهم نتيجة عمل نظام ذاتي، وذلك في الحالات التي يتعذر فيها الحصول على التعويض من المسؤول المباشر أو يكون فيها التعويض غير كافٍ.[2]

ثانياً: آليات تمويل الصندوق وإدارته

تتعدد المصادر المقترحة لتمويل مثل هذا الصندوق، وقد تشمل:[3]

- مساهمات من الشركات المصنعة والمطورة: فرض رسوم أو ضرائب على الشركات التي تنتج أو تسوق الأنظمة الذاتية، خاصة تلك المصنفة عالية المخاطر. يمكن أن تكون هذه المساهمات متناسبة مع حجم مبيعات الشركة أو درجة خطورة منتجاتها.

---

[1] بن عيسى، نبيلة، المرجع السابق، ص 71.

[2] الاتحاد الأوروبي للذكاء الاصطناعي، "اللائحة الأوروبية للذكاء الاصطناعي"، 2024، متاح على: https://digital-strategy.ec.europa.eu/en/policies/european-ai-act تم الاطلاع عليه يوم 2025/05/29.

[3] ديوان، رامي، "آليات التمويل والإدارة في صناديق تعويض الأضرار الناجمة عن الذكاء الاصطناعي"، مجلة القانون والتقنية، العدد 4، 2023، ص. 54

– جزء من أقساط التأمين: تخصيص نسبة معينة من أقساط التأمين الإجباري المفروض على الأنظمة الذاتية (كما سيأتي في الفرع التالي) لتمويل الصندوق.

– مساهمات حكومية: تخصيص جزء من الميزانية العامة للدولة لدعم الصندوق، خاصة في مرحلة التأسيس.

– الغرامات والعقوبات: تحويل جزء من الغرامات المفروضة على الشركات المخالفة لقواعد سلامة الأنظمة الذاتية إلى الصندوق.

أما إدارة الصندوق، فيمكن أن تسند إلى هيئة عامة مستقلة أو جهة حكومية قائمة، وتتولى هذه الجهة وضع معايير واضحة لتحديد الأهلية للحصول على التعويض، وتقييم الأضرار، وتحديد قيمة التعويضات، وإدارة موارد الصندوق واستثمارها.[1]

ثالثاً: التحديات المحتملة (مثل خطر الإفراط في الاعتماد على الصندوق)

رغم المزايا المحتملة، يواجه إنشاء صندوق تعويض وطني بعض التحديات:[2]

– تحديد نطاق الأهلية: وضع معايير دقيقة لتحديد الحالات التي يمكن فيها اللجوء إلى الصندوق، لتجنب تحوله إلى بديل سهل عن ملاحقة المسؤولين الحقيقيين.

– تقدير حجم التمويل المطلوب: صعوبة التنبؤ بحجم الأضرار المستقبلية وبالتالي تقدير حجم التمويل الكافي للصندوق.

– خطر "الخطر الأخلاقي" (Moral Hazard): قد يؤدي وجود الصندوق إلى تقليل حوافز الشركات المصنعة والمستخدمين لاتخاذ أقصى درجات الحيطة والحذر، لاعتمادهم على وجود شبكة أمان للتعويض.

– العبء المالي: قد يشكل تمويل الصندوق عبئاً مالياً كبيراً على الشركات أو الحكومة.

[1] المرجع نفسه، ص 59.

[2] بوعلام، يحيى، المرجع السابق، ص85.

يتطلب تجاوز هذه التحديات تصميماً دقيقاً لآليات عمل الصندوق، بحيث يكمل دور آليات المسؤولية التقليدية ولا يحل محلها، ويركز على الحالات الاستثنائية التي يتعذر فيها التعويض بالطرق العادية، مع وضع ضوابط لمنع إساءة استخدامه.[1]

الفرع الثاني: فرض التأمين الإجباري على الشركات المصنعة والمطورة

يعتبر التأمين آلية تقليدية لإدارة المخاطر وتوزيع عبء الأضرار. ويمكن أن يلعب التأمين الإجباري دوراً هاماً في التعامل مع المخاطر المرتبطة بالأنظمة الذاتية.

أولاً: دور التأمين في توزيع المخاطر وضمان التعويض

يهدف فرض التأمين الإجباري على الشركات المصنعة والمطورة للأنظمة الذاتية، خاصة عالية المخاطر، إلى تحقيق هدفين رئيسيين:[2]

1. توزيع المخاطر: بدلاً من أن تتحمل شركة واحدة كامل عبء التعويض عن حادث جسيم قد يؤدي إلى إفلاسها، يتم توزيع المخاطر على مجموعة أكبر من خلال آلية التأمين.

2. ضمان وجود مصدر للتعويض: يوفر التأمين ضمانة لوجود أموال كافية لتعويض الضحايا عن الأضرار التي لحقت بهم، حتى لو كانت الشركة المسؤولة غير قادرة على الدفع من مواردها الخاصة.

يمكن أن يغطي التأمين المسؤولية المدنية للشركة عن الأضرار التي تسببها منتجاتها، وقد يمتد ليشمل أنواعاً أخرى من التغطيات حسب تصميم النظام التأميني.[3]

---

[1] المفوضية الأوروبية، اقتراح تنظيم الذكاء الاصطناعي، بروكسل، 2021، ص. 47.

[2] العرفاوي، سامي، "دور التأمين في مواجهة مخاطر الذكاء الاصطناعي"، مجلة الدراسات القانونية والاقتصادية، العدد 7، 2023، ص. 45

[3] Jones, M., AI Risk Management and Insurance, Oxford University Press, 2023, pp. 98

ثانياً: تحديد نطاق التأمين الإجباري وحدوده الدنيا

يثير فرض التأمين الإجباري تساؤلات حول نطاقه وحدوده:[1]

- على من يفرض؟ هل يفرض فقط على مصنعي ومطوري الأنظمة عالية المخاطر، أم يشمل فئات أخرى مثل المستخدمين التجاريين؟

- ما هي المخاطر المغطاة؟ هل يقتصر على الأضرار الجسدية والمادية، أم يشمل الأضرار المعنوية أو الاقتصادية؟

- ما هي الحدود الدنيا للتغطية؟ يجب تحديد حدود دنيا لمبالغ التأمين تكون كافية لتغطية الأضرار المحتملة بشكل معقول، مع مراعاة طبيعة المخاطر المرتبطة بكل نوع من الأنظمة.

يتطلب تحديد هذه الجوانب دراسة دقيقة للسوق ولطبيعة المخاطر، وقد تحتاج إلى مراجعة دورية لتواكب التطورات التكنولوجية.[2]

ثالثاً: تأثير التأمين على سلوك الشركات

يمكن أن يكون لنظام التأمين تأثير على سلوك الشركات المصنعة والمطورة:[3]

- الحوافز الإيجابية: قد تقوم شركات التأمين بتقديم أقساط مخفضة للشركات التي تتبنى معايير سلامة أعلى وتستثمر في إدارة المخاطر، مما يشجع على تطوير أنظمة أكثر أماناً.

- المثبطات الخطر الأخلاقي: كما في حالة صندوق التعويض، قد يؤدي وجود التأمين إلى تقليل حذر بعض الشركات، لاعتمادها على أن التأمين سيغطي الأضرار. ولمواجهة ذلك، قد تفرض شركات التأمين شروطاً معينة (مثل نسبة تحمل من المؤمن له) أو تقوم بمراقبة ممارسات السلامة لدى الشركات المؤمنة.

---

[1] العرفاوي، سامي، "دور التأمين في مواجهة مخاطر الذكاء الاصطناعي"، مجلة الدراسات القانونية والاقتصادية، العدد 7، 2023، ص. 52

[2] المرجع نفسه ص، 55.

[3] Smith, J., "Mandatory Insurance for AI Systems: Scope and Limits," Journal of Technology Law, Vol. 15, No. 2, 2024, pp. 121–125.

يعتمد نجاح نظام التأمين الإجباري على تصميمه بشكل يحقق التوازن بين توفير الحماية للضحايا وتشجيع السلوك المسؤول لدى الشركات.[1]

الفرع الثالث: تطوير نظام للترخيص والاعتماد القانوني للأنظمة الذكية

تركز هذه الآلية على جانب الوقاية من الأضرار من خلال ضمان سلامة وموثوقية الأنظمة الذكية قبل السماح بطرحها في السوق أو استخدامها في مجالات حساسة.

أولاً: أهمية الترخيص والاعتماد كآلية وقائية

يهدف نظام الترخيص والاعتماد القانوني إلى وضع معايير ومتطلبات فنية وتنظيمية يجب أن تستوفيها الأنظمة الذكية قبل الحصول على إذن بالتشغيل. ويعتبر هذا النظام آلية وقائية أساسية لعدة أسباب:[2]

- ضمان حد أدنى من السلامة: يضمن أن الأنظمة المطروحة في السوق قد خضعت لاختبارات وتقييمات تثبت استيفاءها لمعايير السلامة والموثوقية المحددة.

- تعزيز الثقة العامة: يساهم وجود نظام ترخيص واعتماد رسمي في بناء ثقة الجمهور والمستخدمين في هذه التقنيات الجديدة.

- تسهيل الرقابة والمساءلة: يوفر إطاراً للسلطات الرقابية لمتابعة أداء الأنظمة المرخصة والتحقيق في الحوادث عند وقوعها.

يمكن أن يكون الترخيص مطلوباً لأنواع معينة من الأنظمة عالية المخاطر (مثل المركبات ذاتية القيادة، أو الأنظمة الطبية الحرجة)، أو للمطورين والمشغلين أنفسهم.[3]

---

[1] الشايب، فؤاد، "التأمين الإجباري ودوره في الحماية القانونية للمتضررين"، مجلة القانون والتشريع، العدد 45، 2021، ص. 112.

[2] European Commission, "Report on AI Liability and Insurance," 2022, available at https://ec.europa.eu/ai/insurance-report

[3] جريدة الحياة الرقمية، مقال بعنوان "كيف يساهم الترخيص في رفع ثقة المستخدمين بالذكاء الاصطناعي"، 15 مارس 2024، ص. 24

ثانياً: تحديد معايير ومتطلبات الترخيص والاعتماد

يجب أن تستند عملية الترخيص والاعتماد إلى معايير ومتطلبات واضحة وموضوعية وقابلة للقياس. وقد تشمل هذه المعايير جوانب مثل:[1]

- السلامة الفنية: متانة النظام، دقته، قدرته على التعامل مع الأعطال والأوضاع غير المتوقعة.
- الأمن السيبراني: حماية النظام من الاختراق والتلاعب.
- جودة البيانات والتحيز: التأكد من جودة البيانات المستخدمة في التدريب وخلوها من التحيزات الضارة.
- الشفافية وقابلية التفسير: قدرة النظام على تفسير قراراته (بدرجات متفاوتة حسب السياق).
- الإشراف البشري: وجود آليات فعالة للإشراف والتدخل البشري.
- الامتثال للقوانين والأخلاقيات: التأكد من أن تصميم النظام وتشغيله يتوافق مع القوانين المعمول بها والمبادئ الأخلاقية.

يتطلب وضع هذه المعايير تعاوناً بين الخبراء الفنيين والقانونيين والأخلاقيين، ويجب أن تكون قابلة للتحديث المستمر لتواكب التطور التكنولوجي.[2]

ثالثاً: الجهات المسؤولة عن منح التراخيص ومراقبة الامتثال

يجب تحديد جهة أو جهات مسؤولة عن عملية منح التراخيص والاعتماد ومراقبة امتثال الأنظمة المرخصة للمعايير والمتطلبات. قد تكون هذه الجهة هيئة تنظيمية قائمة (مثل هيئات تنظيم قطاع النقل أو الصحة) أو هيئة جديدة متخصصة في الذكاء الاصطناعي .[3]

---

[1] الشايب، فؤاد، المرجع السابق، ص 83.

[2] المرجع نفسه، ص، 101.

[3] عبد الرحمن، سامي، "الإشراف البشري والشفافية في تنظيم الذكاء الاصطناعي"، مجلة العلوم القانونية المعاصرة، العدد 13، 2024، ص. 60

يجب أن تتمتع هذه الجهة بالاستقلالية والخبرة الفنية اللازمة للقيام بمهامها بفعالية. وتشمل مهامها مراجعة طلبات الترخيص، وإجراء الاختبارات والتقييمات اللازمة، ومنح التراخيص أو رفضها، ومراقبة أداء الأنظمة المرخصة في السوق، وسحب التراخيص في حالة عدم الامتثال أو ظهور مخاطر غير متوقعة.[1]

إن تطوير نظام فعال للترخيص والاعتماد يمثل استثماراً هاماً في بناء منظومة ذكاء اصطناعي آمنة وجديرة بالثقة، ويساهم بشكل كبير في الوقاية من الأضرار وتقليل الحاجة إلى اللجوء إلى آليات التعويض بعد وقوعها.[2]

المطلب الثالث: أدوار المؤسسات الرقابية والتشريعية

إن مواكبة التشريع الجنائي للتحديات التقنية التي تفرضها الأنظمة الذاتية ليست مجرد عملية صياغة نصوص قانونية جديدة أو تعديل نصوص قائمة، بل هي عملية مستمرة تتطلب تضافر جهود مختلف المؤسسات في الدولة، كل حسب اختصاصه ودوره. فالتشريع وحده لا يكفي إذا لم تكن هناك مؤسسات قادرة على تطبيقه بفعالية، ومراقبته باستمرار، وتطويره بما يتناسب مع المستجدات. كما أن القضاء، الذي يقع على عاتقه تطبيق القانون وتفسيره، يحتاج إلى دعم وتأهيل يمكنه من التعامل مع القضايا المعقدة التي تثيرها هذه التقنيات. لذلك، فإن تحديد وتفعيل أدوار المؤسسات الرقابية والتشريعية والقضائية يعتبر جزءاً لا يتجزأ من استراتيجية المواكبة الشاملة.[3]

سنتناول في هذا المطلب الأدوار المحورية لثلاثة أنواع من المؤسسات في هذا السياق. سنبدأ في الفرع الأول بمناقشة أهمية تأسيس هيئة وطنية متخصصة للرقابة على الذكاء الاصطناعي، تكون بمثابة الجهة المرجعية لتنظيم ومراقبة هذا القطاع الحيوي. وفي الفرع الثاني، سنسلط الضوء على الدور المعزز الذي يجب أن يلعبه البرلمان، ليس فقط في سن التشريعات الأولية، بل أيضاً في المتابعة المستمرة للابتكارات القانونية والتكنولوجية وتقييم أثرها. أما الفرع الثالث، فسيخصص للتأكيد على الحاجة الملحة للتكوين القانوني والتقني

[1] منظمة الأمم المتحدة، "تقرير الحوكمة الأخلاقية والتقنية للذكاء الاصطناعي"، 2023، متاح على: https://un.org/ai-ethics-governance تم الاطلاع عليه يوم، 2025/05/21.

[2] جريدة الحياة الرقمية، المرجع السابق، ص 30.

المستمر للقضاة وأعضاء النيابة العامة لتمكينهم من التعامل بكفاءة وعدالة مع القضايا المتعلقة بالأنظمة الذاتية.

الفرع الأول: تأسيس هيئة وطنية للرقابة على الذكاء الاصطناعي

نظراً للطبيعة المتخصصة والمعقدة لتقنيات الذكاء الاصطناعي وتأثيراتها الواسعة على مختلف جوانب الحياة، تبرز الحاجة إلى إنشاء هيئة وطنية مستقلة ومتخصصة تتولى مهمة تنظيم ومراقبة هذا المجال.

أولاً: مبررات إنشاء هيئة متخصصة ومستقلة

تستند الدعوة إلى إنشاء هيئة وطنية للرقابة على الذكاء الاصطناعي إلى عدة مبررات:[1]

- التخصص والخبرة: تتطلب الرقابة الفعالة على الذكاء الاصطناعي خبرات فنية وتقنية وقانونية وأخلاقية عالية قد لا تتوفر بنفس القدر في الهيئات التنظيمية القائمة ذات الطابع القطاعي العام.

- التنسيق وتوحيد الجهود: يمكن للهيئة المتخصصة أن تلعب دوراً محورياً في تنسيق السياسات والجهود بين مختلف الوزارات والهيئات الحكومية المعنية بالذكاء الاصطناعي، وتوحيد الرؤى والمعايير.

- الاستقلالية والموضوعية: يفضل أن تتمتع الهيئة بدرجة عالية من الاستقلالية عن الحكومة وعن القطاع الخاص لضمان اتخاذ قراراتها بموضوعية وحيادية، بعيداً عن الضغوط السياسية أو التجارية.

- الاستجابة السريعة للتطورات: يمكن للهيئة المتخصصة أن تكون أكثر قدرة على متابعة التطورات التكنولوجية السريعة وتكييف الأطر التنظيمية والرقابية بشكل مرن ومستمر.[2]

ثانياً: المهام والصلاحيات المقترحة للهيئة

يمكن أن تناط بالهيئة الوطنية للرقابة على الذكاء الاصطناعي مجموعة واسعة من المهام والصلاحيات، تشمل على سبيل المثال لا الحصر:

---

[1] لشمري، خالد، "الحاجة إلى مؤسسات رقابية مستقلة في عصر الذكاء الاصطناعي"، المجلة العربية للسياسات العامة، العدد 18، 2024، ص. 39

[2] المرجع نفسه، ص 42.

– وضع السياسات والاستراتيجيات: اقتراح السياسات والاستراتيجيات الوطنية المتعلقة بالذكاء الاصطناعي وتقديم المشورة للحكومة بشأنها.

– إصدار اللوائح والمعايير: وضع وإصدار اللوائح التنفيذية والمعايير الفنية والأخلاقية لتطوير ونشر واستخدام أنظمة الذكاء الاصطناعي، بالتعاون مع الجهات القطاعية المختصة.

– الترخيص والاعتماد: إدارة نظام الترخيص والاعتماد للأنظمة الذكية عالية المخاطر (كما نوقش في المطلب السابق.

– مراقبة السوق والامتثال: مراقبة أنظمة الذكاء الاصطناعي المتداولة في السوق والتحقق من امتثالها للمتطلبات القانونية والتنظيمية.

– التحقيق في الحوادث والشكاوى: التحقيق في الحوادث والأضرار الناجمة عن أنظمة الذكاء الاصطناعي وتلقي ومعالجة شكاوى المتضررين.

– فرض العقوبات: امتلاك صلاحية فرض عقوبات إدارية أو مالية على المخالفين، أو إحالة القضايا إلى الجهات القضائية المختصة.

– التوعية وبناء القدرات: نشر الوعي حول الذكاء الاصطناعي ومخاطره وفرصه، والمساهمة في بناء القدرات الوطنية في هذا المجال.

– التعاون الدولي: تمثيل الدولة في المحافل الدولية المتعلقة بالذكاء الاصطناعي والتنسيق مع الهيئات المماثلة في الدول الأخرى.[1]

ثالثاً: ضمان الموارد والكفاءات اللازمة لعمل الهيئة

لكي تتمكن الهيئة من أداء مهامها بفعالية، يجب ضمان توفير الموارد المالية والبشرية الكافية لها. ويتطلب ذلك:

[1] Future of Life Institute, "AI Governance Recommendations", 2023, accessed May 2025, from https://futureoflife.org/ai-policy. تم الاطلاع عليه يوم 2025/05/30.

- ميزانية كافية: تخصيص ميزانية مستقلة وكافية تمكن الهيئة من استقطاب الكفاءات وتوفير التجهيزات التقنية اللازمة لعملها.

- كفاءات متعددة التخصصات: استقطاب فريق عمل يضم خبراء في مجالات متنوعة تشمل علوم الحاسب، وهندسة الذكاء الاصطناعي، والقانون، والأخلاق، والعلوم الاجتماعية، وإدارة المخاطر.

- التدريب المستمر: توفير برامج تدريب مستمرة لفريق العمل لمواكبة أحدث التطورات التكنولوجية والقانونية.

- آليات عمل فعالة: وضع إجراءات عمل واضحة وفعالة تضمن الشفافية والمساءلة في عمل الهيئة.

الفرع الثاني: تعزيز دور البرلمان في متابعة الابتكارات القانونية

لا يقتصر دور السلطة التشريعية (البرلمان) على مجرد سن القوانين الأولية المتعلقة بالذكاء الاصطناعي، بل يجب أن يمتد ليشمل المتابعة المستمرة والتقييم الدوري لهذه القوانين وتأثيراتها في ظل التطور التكنولوجي المتسارع.[1]

أولاً: دور البرلمان في سن التشريعات الأولية ومراجعتها الدورية

يقع على عاتق البرلمان الدور الأساسي في وضع الإطار التشريعي العام الذي ينظم الذكاء الاصطناعي ويحدد المبادئ الأساسية للمسؤولية والحماية. ويتطلب ذلك نقاشاً مجتمعياً واسعاً واستشارة الخبراء والمتخصصين لضمان أن تكون التشريعات متوازنة وتستجيب للتحديات بشكل فعال.

ولكن نظراً لسرعة التطور التكنولوجي، فإن التشريعات التي تسن اليوم قد تصبح قديمة أو غير كافية غداً. لذلك، يجب أن يتبنى البرلمان آلية للمراجعة الدورية لهذه التشريعات (مثلاً كل بضع سنوات) لتقييم فعاليتها ومدى ملاءمتها للمستجدات، وإدخال التعديلات اللازمة عليها.[2]

[1] بوزيد، سامية، "دور السلطة التشريعية في مواكبة التقدم التكنولوجي: حالة الذكاء الاصطناعي"، مجلة البحوث القانونية والسياسية، جامعة الجزائر 1، العدد 15، 2023، ص. 44

[2] المرجع نفسه ، ص 58.

ثانياً: أهمية اللجان البرلمانية المتخصصة في التكنولوجيا والقانون

يمكن تعزيز قدرة البرلمان على متابعة هذا المجال المعقد من خلال إنشاء أو تفعيل لجان برلمانية متخصصة في قضايا التكنولوجيا والابتكار والقانون الرقمي. يمكن لهذه اللجان أن:[1]

- تتعمق في دراسة القضايا: إجراء دراسات معمقة حول تأثيرات الذكاء الاصطناعي والتحديات القانونية الناشئة عنه.

- تستمع إلى الخبراء: عقد جلسات استماع للخبراء من الأوساط الأكاديمية والصناعية والمجتمع المدني للاستنارة بآرائهم.

- تراقب عمل الحكومة والهيئات الرقابية: متابعة أداء الحكومة والهيئة الوطنية للرقابة على الذكاء الاصطناعي في تطبيق السياسات والتشريعات.

- تقترح التعديلات التشريعية: تقديم مقترحات مدروسة لتعديل القوانين القائمة أو سن قوانين جديدة بناءً على نتائج دراساتها ومتابعاتها.[2]

ثالثاً: استخدام أدوات التقييم التشريعي الاستباقي (Regulatory Impact Assessment)

قبل سن أي تشريع جديد أو تعديل تشريع قائم يتعلق بالذكاء الاصطناعي، من المهم أن يقوم البرلمان أو الحكومة) بإجراء تقييم استباقي لأثر هذا التشريع – Regulatory Impact Assessment RIA. يهدف هذا التقييم إلى تحليل الآثار المحتملة للتشريع المقترح على مختلف الجوانب (الاقتصادية،

[1] بن زكري، فاطمة، التنظيم القانوني للتكنولوجيا الحديثة في التشريع الجزائري، دار الخلدونية، الجزائر، 2021، ص. 213.

[2] عمور، نسرين، "البرلمان وتحديات الثورة الرقمية: قراءة في التشريع المتعلق بالذكاء الاصطناعي"، مجلة القانون والتكنولوجيا، جامعة سطيف 2، العدد 7، 2022، ص. 65.

الاجتماعية، البيئية، الابتكار، الحقوق الأساسية)، وتحديد الفوائد والتكاليف المتوقعة، ومقارنة البدائل المختلفة.[1]

يساعد هذا التقييم على اتخاذ قرارات تشريعية أكثر استنارة وتجنب الآثار السلبية غير المقصودة، ويضمن أن تكون التشريعات فعالة وتحقق الأهداف المرجوة منها بأقل تكلفة ممكنة.

الفرع الثالث: التكوين القانوني والتقني للقضاة وأعضاء النيابة[2]

يمثل القضاء خط الدفاع الأخير عن الحقوق والحريات، وهو الجهة المنوط بها تطبيق القانون وتفسيره في المنازعات الملموسة. ولكي يتمكن القضاة وأعضاء النيابة العامة من التعامل بفعالية وعدالة مع القضايا المعقدة التي تثيرها الأنظمة الذاتية، يجب تزويدهم بالمعرفة والمهارات اللازمة.[3]

أولاً: الحاجة إلى فهم تقني أساسي لعمل الأنظمة الذاتية

لا يمكن للقاضي أو عضو النيابة أن يفصل في قضية تتعلق بنظام ذاتي دون أن يكون لديه فهم أساسي لكيفية عمل هذه الأنظمة، والمفاهيم الأساسية المرتبطة بها (مثل الخوارزميات، تعلم الآلة، البيانات الضخمة، الصندوق الأسود)، والمخاطر المحتملة التي قد تنجم عنها. هذا الفهم التقني ضروري لتقدير الأدلة الرقمية بشكل صحيح، واستجواب الشهود والخبراء بفعالية، وتطبيق القواعد القانونية على الوقائع المعقدة.

لا يعني ذلك أن يصبح القضاة وأعضاء النيابة خبراء في البرمجة، ولكن يجب أن يحصلوا على تكوين يمكنهم من فهم المبادئ الأساسية والمصطلحات الشائعة والتحديات الرئيسية المرتبطة بهذه التقنيات.[4]

ثانياً: تطوير برامج تكوين مستمر تجمع بين القانون والتكنولوجيا

[1] الحسين، عبد الله، مرجع سابق، ص 132.

[2] بن عيسى، نبيل، مرجع سابق، ص 119.

[3] وزارة الرقمنة والإحصائيات، تقرير حول السياسة الوطنية للذكاء الاصطناعي في الجزائر، الجزائر، 2023، ص. 34.

[4] زروقي، نوال، "التكوين القضائي في ظل التطورات التكنولوجية: الذكاء الاصطناعي نموذجاً"، مجلة الدراسات القانونية المعاصرة، جامعة باتنة 1، العدد 10، 2023، ص. 92.

يجب على الجهات المسؤولة عن تكوين القضاة وأعضاء النيابة (مثل المعاهد القضائية) أن تدرج في برامجها وحدات تدريبية متخصصة تجمع بين الجوانب القانونية والتقنية للذكاء الاصطناعي. يمكن أن تشمل هذه البرامج:[1]

- ورش عمل ودورات تدريبية: تغطي المفاهيم التقنية الأساسية، والتحديات القانونية والأخلاقية، والتشريعات المقارنة، ودراسة حالات عملية.
- الاستعانة بالخبراء: دعوة خبراء فنيين وقانونيين لتقديم محاضرات والمشاركة في النقاشات.
- توفير الموارد التعليمية: إتاحة مواد تعليمية محدثة (كتب، مقالات، أدلة إرشادية) حول الذكاء الاصطناعي والقانون.
- التعاون مع الجامعات ومراكز البحث: بناء شراكات لتبادل المعرفة والخبرات.

يجب أن يكون هذا التكوين مستمراً لمواكبة التطورات المتسارعة في هذا المجال[2].

ثالثاً: أهمية الاستعانة بالخبراء الفنيين في المحاكم

حتى مع وجود تكوين أساسي، سيظل القضاة وأعضاء النيابة بحاجة إلى الاستعانة بالخبراء الفنيين المتخصصين في القضايا المعقدة التي تتطلب تحليلاً تقنياً معمقاً (مثل تحليل سبب خلل في نظام ذاتي، أو فحص خوارزمية لتحديد وجود تحيز). يجب أن تتوفر آليات واضحة وفعالة للاستعانة بهؤلاء الخبراء، وضمان استقلاليتهم ونزاهتهم، وتمكين المحكمة من تقييم تقاريرهم وأقوالهم بشكل نقدي.[3]

قد يتطلب الأمر أيضاً إنشاء قوائم معتمدة للخبراء الفنيين في مجال الذكاء الاصطناعي الذين يمكن للمحاكم الاستعانة بهم، ووضع قواعد إجرائية تنظم دورهم في العملية القضائية.

---

[1] خليف، عبد المجيد، القاضي والتحول الرقمي: نحو عدالة مواكبة للعصر، دار هومة، الجزائر، 2022، ص. 107.

[2] مجلس الدولة الجزائري، دليل التكوين المستمر للقضاة، الجزائر، 2023، ص. 54.

[3] عبد الغني، هشام، "العدالة والذكاء الاصطناعي: التحديات والفرص"، المجلة العربية للعلوم القانونية والتقنية، العدد 5، 2022، ص. 39.

خلاصة الفصل:

يمثل التطور المتسارع للأنظمة الذاتية تحدياً وفرصة في آن واحد للقانون الجنائي. فبينما تفتح هذه التقنيات آفاقاً جديدة للابتكار والتقدم، فإنها تثير أيضاً إشكاليات قانونية وأخلاقية معقدة تتعلق بتكييف الجرائم، وتحديد المسؤولية، وحماية الحقوق الأساسية للأفراد والمجتمع. لقد حاولنا في هذا الفصل استكشاف سبل مواكبة التشريع الجنائي لهذه التحديات، بدءاً بتحليل كيفية تكييف نصوص التجريم القائمة لتشمل الأفعال الضارة الناتجة عن الأنظمة الذاتية في مختلف صورها (ضد الأشخاص، ضد الممتلكات، جرائم معلوماتية)، مروراً باستعراض الاتجاهات التشريعية الحديثة والمبادرات الدولية المقارنة التي تسعى لوضع أطر تنظيمية لهذه التقنيات، وصولاً إلى مناقشة الآليات العملية المقترحة لتعزيز الوقاية والتعويض وتحديد الأدوار المنوطة بالمؤسسات المختلفة.

يتضح من خلال هذا التحليل أن المواجهة الفعالة تتطلب مقاربة شاملة ومتعددة الأبعاد، لا تقتصر على التعديلات التشريعية فحسب، بل تشمل أيضاً تطوير آليات تنظيمية ورقابية استباقية (مثل هيئات الرقابة المتخصصة ونظم الترخيص والاعتماد)، وابتكار حلول لضمان تعويض الضحايا (مثل صناديق التعويض والتأمين الإجباري)، وتعزيز قدرات المؤسسات التشريعية والقضائية لمتابعة التطورات وتطبيق القانون بفعالية. إن الهدف هو إيجاد توازن دقيق يحمي المجتمع من المخاطر دون أن يخنق الابتكار، ويضمن المساءلة والعدالة في عصر تتداخل فيه مسؤوليات الإنسان والآلة بشكل متزايد.

الخاتمـــــة

الخاتمة:

في ختام هذه الدراسة التي تناولت إشكالية المسؤولية الجزائية للأنظمة الذاتية وسبل مواكبة التشريع الجنائي للتحديات التقنية، يتضح لنا بجلاء أن التطور المتسارع للذكاء الاصطناعي قد فرض واقعاً جديداً ومعقداً على المنظومة القانونية برمتها، وبشكل خاص على قواعد القانون الجنائي التي ظلت لقرون ترتكز على الفاعل البشري العاقل والمختار. إن قدرة هذه الأنظمة على إحداث أضرار جسيمة بشكل مستقل، تطرح تحديات جوهرية تتطلب تفكيراً قانونياً معمقاً وحلولاً مبتكرة.

لقد حاولنا من خلال الفصل الأول الوقوف على صعوبات تطبيق أركان المسؤولية الجزائية التقليدية، المادية والمعنوية، على الأفعال الصادرة عن كيانات تفتقر للإرادة والتمييز بالمعنى الإنساني، وبحثنا في نماذج إسناد المسؤولية للأطراف البشرية المتعددة التي تقف وراء هذه الأنظمة. وفي الفصل الثاني، انتقلنا إلى تحليل كيفية تكييف الجرائم المختلفة لتشمل الأفعال الضارة لهذه الأنظمة، واستعرضنا الاتجاهات التشريعية الحديثة والآليات المقترحة لمواجهة هذه التحديات على الصعيدين الوقائي والتعويضي، ودور المؤسسات المختلفة في هذا الإطار.

وبناءً على ما تم عرضه وتحليله، يمكن القول إن الإشكالية الرئيسة التي طرحتها الدراسة، والمتمثلة في مدى إمكانية إسناد المسؤولية الجزائية عن الأفعال الضارة الصادرة عن الأنظمة الذاتية في ظل قصور القواعد التقليدية، وسبل مواكبة التشريع الجنائي لهذه التحديات، تجد إجابتها في التأكيد على أن القواعد التقليدية تواجه بالفعل قصوراً حقيقياً، وأن المواكبة تتطلب جهداً تشريعياً وقضائياً وتنظيمياً متكاملاً يتسم بالمرونة والاستشراف.

أما التساؤلات الفرعية التي انطلقت منها الدراسة، فيمكن الإجابة عليها بإيجاز على النحو التالي:

- تطبيق أركان المسؤولية التقليدية يواجه صعوبات جمة، خاصة فيما يتعلق بالركن المعنوي (غياب الإرادة والتمييز) وإثبات العلاقة السببية في ظل تعقيد الأنظمة وتعدد المتدخلين.
- إسناد المسؤولية للأطراف البشرية هو الاتجاه الغالب، لكنه يثير إشكاليات حول تحديد المسؤول بدقة (الصانع، المبرمج، المستخدم) ومعايير الإسناد (الخطأ، الإهمال، المسؤولية الموضوعية)، مع احتمال وجود "فجوة في المسؤولية" في بعض الحالات.
- تكييف الجرائم التقليدية يتطلب تفسيراً موسعاً للنصوص القائمة أو تعديلات تشريعية لاستيعاب الأفعال الضارة للأنظمة الذاتية، سواء كانت جرائم ضد الأشخاص أو الممتلكات أو جرائم معلوماتية.

- الاتجاهات التشريعية المقارنة (كالاتحاد الأوروبي) تتجه نحو تنظيم الذكاء الاصطناعي بشكل شامل، مع التركيز على تصنيف المخاطر وفرض التزامات على المطورين والمستخدمين، وهي تجارب يمكن الاستفادة منها.
- الآليات والمقترحات العملية تشمل تطوير معايير السلامة والشفافية، وإنشاء هيئات رقابية متخصصة، وتفعيل آليات التعويض كالتأمين الإجباري وصناديق التعويض، وتكوين الفاعلين في المنظومة القضائية.

أهم النتائج المتوصل إليها:

1. تُظهر الأنظمة الذاتية قصوراً جوهرياً في استيفاء متطلبات الركن المعنوي للمسؤولية الجزائية التقليدية، مما يجعل مساءلتها المباشرة أمراً مستبعداً في ظل المفاهيم الحالية.
2. تتجه الأنظار نحو مساءلة الأطراف البشرية المتدخلة، لكن تحديد المسؤول بدقة وإثبات الخطأ والعلاقة السببية يمثلان تحدياً كبيراً في ظل تعقد الأنظمة واستقلاليتها المتزايدة.
3. مبدأ الشرعية الجنائية يواجه تحدياً أمام الأفعال الضارة غير المتوقعة أو غير المسبوقة للأنظمة الذاتية، مما يستدعي الحاجة إلى نصوص تجريم أكثر مرونة أو تفسيرات قضائية متطورة.
4. تتطلب الجرائم الناجمة عن الأنظمة الذاتية (ضد الأشخاص، الممتلكات، المعلومات) تكييفاً قانونياً دقيقاً، وقد تحتاج النصوص القائمة إلى تعديل أو استكمال لمواجهة الأشكال الجديدة للإجرام التقني.
5. التشريعات المقارنة الحديثة، مثل اللائحة الأوروبية للذكاء الاصطناعي، تقدم نماذج تنظيمية مهمة ترتكز على تقييم المخاطر وفرض التزامات محددة، ولكنها لا تزال في مراحلها الأولى.
6. مواجهة تحديات الذكاء الاصطناعي في القانون الجنائي تتطلب مقاربة شاملة تجمع بين التعديلات التشريعية، والتنظيم الإداري المسبق، والرقابة الفنية، وآليات التعويض الفعالة، والتكوين المتخصص للقضاة والمحققين.

أهم التوصيات المقترحة:

1. دعوة المشرع إلى مراجعة وتحديث النصوص الجنائية المتعلقة بالمسؤولية عن الخطأ والإهمال لتشمل بشكل صريح وواضح الأضرار الناجمة عن تصميم أو برمجة أو استخدام الأنظمة الذاتية، والنظر في إمكانية إقرار أشكال من المسؤولية الموضوعية في حالات محددة وعالية المخاطر.

2. إنشاء هيئة وطنية متخصصة للرقابة على الذكاء الاصطناعي، تكون مهمتها وضع المعايير الفنية والأخلاقية، ومنح التراخيص للأنظمة عالية المخاطر، ومراقبة الامتثال، والتحقيق في الحوادث.
3. تطوير آليات لتعزيز الشفافية وقابلية التفسير (Explainability) في الأنظمة الذاتية، خاصة تلك المستخدمة في اتخاذ قرارات حساسة، لتسهيل عملية تحديد الأسباب والمسؤوليات عند وقوع الضرر.
4. دراسة إمكانية إنشاء صندوق وطني لتعويض ضحايا الأضرار الناجمة عن الأنظمة الذاتية، خاصة في الحالات التي يصعب فيها تحديد المسؤول أو إثبات الخطأ، أو فرض نظام للتأمين الإجباري على مطوري ومستخدمي الأنظمة عالية المخاطر.
5. تضمين برامج تكوين القضاة وأعضاء النيابة والمحامين ومحققي الضبطية القضائية لمقررات متخصصة حول الجوانب القانونية والتقنية للذكاء الاصطناعي وتحدياته الجنائية.
6. تعزيز التعاون الدولي وتبادل الخبرات والتجارب في مجال تنظيم الذكاء الاصطناعي ومواجهة تحدياته القانونية، والاستفادة من المبادئ التوجيهية والمعايير الدولية.

وفي الختام، نؤكد أن موضوع المسؤولية الجزائية للأنظمة الذاتية سيظل مجالاً خصباً للبحث والنقاش في السنوات القادمة، نظراً للتطور المستمر لهذه التقنيات وتغلغلها المتزايد في حياتنا. ويبقى التحدي الأكبر هو إيجاد التوازن الدقيق بين تشجيع الابتكار الذي يخدم البشرية، وضمان سيادة القانون وحماية الحقوق الأساسية في مواجهة الآلات التي صنعناها بأيدينا وأصبحت تتخذ قرارات تؤثر في مصائرنا.

قائمة المصادر والمراجع

أولًا: المصادر القانونية

أ-القوانين والأوامر

1. القانون الجنائي المصري رقم 58 لسنة 1937، متضمنًا تعديلاته الخاصة بالجرائم التكنولوجية.

ثانيًا: الكتب والمراجع العامة

1. أحمد عبد الكريم سلام، المسؤولية الجنائية عن الجرائم المرتكبة بواسطة الذكاء الاصطناعي، دار الجامعة الجديدة، الإسكندرية، 2021.
2. سامي عبد العال، التقنيات الذكية والتحديات الجنائية المعاصرة، دار الكتب القانونية، القاهرة، 2020.
3. خالد المرزوقي، استقلالية الأنظمة الذاتية ومسؤولية الإنسان: دراسة مقارنة، دار الفكر الحديث، الرياض، 2022.
4. حمد شلبي، المدخل إلى القانون الجنائي، دار النهضة العربية، القاهرة، ط6، 2018.
5. سامي القيسي، مبادئ القانون الجنائي، دار الثقافة القانونية، بغداد، ط1.
6. علي عبد القادر القهوجي، الوجيز في شرح قانون العقوبات – القسم العام، منشورات الحلبي الحقوقية، بيروت، 2012.
7. حسين علي الطباخ، المسؤولية الجنائية في ضوء تطور الذكاء الاصطناعي، دار النهضة العربية، القاهرة، 2020.
8. ناصر عبد القادر، المسؤولية الجنائية في ظل الثورة الرقمية، دار النهضة العربية، 2021.
9. خالد عبد الله، القانون الجنائي في مواجهة التكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2022.
10. سامي جابر، مبدأ الشرعية في القانون الجنائي: من الثبات إلى المرونة، دار النهضة العربية، ط1، 2020.
11. أمي الكيلاني، الأخطاء التقنية كركن في المسؤولية الجزائية: دراسة مقارنة، دار النهضة العربية، 2021.

12. أدية الزهراوي، الإشراف على الأنظمة الذاتية: الأبعاد القانونية والعملية، دار الكتب القانونية، 2021.

13. سامي محمد صالح، المسؤولية الجنائية في الجرائم التكنولوجية، دار الفكر القانوني، عمان، 2019.

14. محمد الكيلاني، القانون الجنائي وتحديات الجرائم المرتبطة بالتكنولوجيا الحديثة، دار النهضة العربية، 2021.

15. عمر الحداد، تأثير الخوارزميات على سلامة الأفراد: دراسة مقارنة، دار الفكر القانوني، القاهرة، 2023.

16. فهد القحطاني، "جريمة الإتلاف وأثرها في ظل التقنيات الذكية"، المؤتمر العربي للقانون والتكنولوجيا، الرياض، 2024.

17. سمير الشريف، "الجرائم الإلكترونية واستخدام الأنظمة الذكية في الاختراق والقرصنة"، مجلة الأمن السيبراني، العدد 8، 2023.

18. أحمد الجابري، "استغلال الحوسبة السحابية والأنظمة الذكية في الجرائم المالية"، المؤتمر الدولي للأمن السيبراني، دبي، 2024.

ثالثا: المقالات العلمية المحكمة

1. كريمة بوشامة، "الإشكالات القانونية للذكاء الاصطناعي في القانون الجنائي"، مجلة دفاتر السياسة والقانون، العدد 28، جامعة خنشلة، 2022.

2. لطفي بوعزة، "الذكاء الاصطناعي والمسؤولية الجنائية: مقاربة قانونية"، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة الجزائر 1، العدد 2، 2021.

3. وسيم حمدي، "إشكالية الركن المادي في الجرائم"، مجلة القانون والتكنولوجيا، العدد 5، 2022.

4. ليلى حمودي، "دور التدخل البشري في المسؤولية عن أفعال الأنظمة الذكية"، مجلة القانون والتكنولوجيا، العدد 12، 2023.

5. فاطمة الزهراء بن عيسى، "إشكاليات الركن المعنوي في الأفعال الصادرة عن الأنظمة الذكية"، مجلة العلوم القانونية والاقتصادية، العدد 18، 2023.

6. فريدة سالم، "تطبيق مفهوم القصد الجنائي في عصر الذكاء الاصطناعي"، مجلة العلوم القانونية الحديثة، العدد 29، 2024.

7. ريم يوسف، "التحديات القانونية للذكاء الاصطناعي في القانون الجنائي"، مجلة القانون والتكنولوجيا، العدد 9، 2023.

8. معاذ سليمان، "الأبعاد التاريخية لتطور نظرية المسؤولية الجزائية وجدلية تطبيقها في عصر الذكاء الاصطناعي"، مجلة كلية القانون الكويتية العالمية، 2021، ص. 99–100.

9. مجلة القانون والسياسة، "الشخصية القانونية للأنظمة الذكية: جدلية ومسارات تطويرية"، العدد 29، 2024.

10. مجلة الحقوق الرقمية، "المسؤولية الجنائية في البرمجيات المعطوبة: تحليل قانوني"، العدد 9، 2022.

11. أحمد زين الدين، "المسؤولية الجنائية عن الأفعال غير العمدية"، مجلة الحقوق المعاصرة، العدد 22، 2022.

12. نور الدين بن حمد، "الإيذاء غير العمدي في القانون الجنائي: دراسة مقارنة"، دار الفكر القانوني، 2021.

13. مصطفى عبد الحميد، "المسؤولية الجنائية عن الأفعال الناتجة عن الأنظمة التقنية"، مجلة القانون والتكنولوجيا، العدد 10، 2023.

14. أحمد صالح، "معايير السلامة في تطوير الأنظمة الذكية: التحديات القانونية والتقنية"، مجلة الدراسات القانونية، العدد 25، 2024.

15. سعاد إبراهيم، "التحيز الخوارزمي وتأثيره على حقوق الإنسان"، مجلة دراسات القانون والتكنولوجيا، العدد 12، 2024.

16. محمد بن حسين، "إشكالية المسؤولية الجنائية في الجرائم المرتكبة بواسطة الذكاء الاصطناعي"، مجلة القانون والتكنولوجيا، العدد 5، 2023.

17. محمد فرحات، "استخدام الذكاء الاصطناعي في الجرائم السيبرانية: التحديات القانونية والواقعية"، مجلة العلوم القانونية والتقنية، العدد 7، 2023.

18. عبد الرزاق بوحارة، "الذكاء الاصطناعي وتهديدات الأمن القومي: قراءة في مخاطر الاستخدام الإرهابي"، المجلة الجزائرية للأمن والدفاع، العدد 4، 2022.

19. أحمد الشاذلي، "البرمجيات الخبيثة وتطورها باستخدام الذكاء الاصطناعي"، مجلة الأمن السيبراني، المركز القومي للمعلومات، العدد 7.

20. نوال بوفاتح، "الجرائم الإلكترونية في ظل التطورات التكنولوجية الحديثة"، مجلة الدراسات القانونية والسياسية، جامعة باتنة 1، العدد 22.

21. ربيعة عكاشة، "الجرائم السيبرانية في ظل التطور التكنولوجي: دراسة قانونية"، مجلة العلوم القانونية والسياسية، جامعة مستغانم، العدد 19.

22. هشام بوعمامة، "التحقيق في الجرائم المعلوماتية: إشكاليات الإثبات والتحليل الجنائي الرقمي"، مجلة الأمن والقانون، جامعة الأمير نايف، العدد 28.

23. مريم العرفاوي، "المسؤولية القانونية عن الأضرار الناجمة عن المركبات ذاتية القيادة"، مجلة القانون والآليات الحديثة، العدد 7، 2023.

24. سامي الحسن، "القرارات الخوارزمية والمسؤولية القانونية: دراسة تحليلية"، مجلة الدراسات القضائية، العدد 8، 2024.

25. لي إبراهيم خليفة، "التحديات القانونية في مواجهة الجرائم السيبرانية المعتمدة على الذكاء الاصطناعي"، مجلة العلوم القانونية، جامعة بغداد، مجلد 44.

رابعا: الرسائل الجامعية

1. عبد الحفيظ بوقرة، المسؤولية الجنائية في ظل الذكاء الاصطناعي: مقاربة تحليلية قانونية، أطروحة دكتوراه، جامعة الجزائر 1، كلية الحقوق، 2023.

2. فوزي بلعياشي، الذكاء الاصطناعي وتحديات الإثبات في القانون الجنائي، أطروحة دكتوراه، جامعة قسنطينة 1، 2024.

3. خديجة بن زيان، المسؤولية الجنائية عن أخطاء الذكاء الاصطناعي: دراسة في القانون الجزائري والمقارن، مذكرة ماستر، جامعة وهران 2، 2022.

4. سميرة دحمان، المسؤولية الجنائية عن الأفعال الناجمة عن الأنظمة الذاتية: دور التدخل البشري، مذكرة ماجستير، جامعة باتنة 2، 2023.

5. هالة بوطرفاية، القصد الجنائي في ظل التطور التكنولوجي: مسؤولية الإنسان والنظام، مذكرة ماجستير، جامعة قسنطينة 2، 2023.

6. أحمد بن عبد الله، التنظيم القانوني للذكاء الاصطناعي ومسؤولية المبرمجين في التشريع الجزائري، رسالة دكتوراه، جامعة الجزائر، 2023.

خامسًا: المواقع الالكترونية

2. الهيئة العامة للاستعلامات، "الذكاء الاصطناعي وتأثيره على الأمن والسلم الدوليين"، متاح على: https://www.sis.gov.eg، تاريخ الاطلاع: 10 جوان 2025.
3. مجلة الجوبة، العدد 85، "الذكاء الاصطناعي والمسؤولية الأخلاقية"، متاح على: http://www.aljoabah.com، تاريخ الاطلاع: 10 جوان 2025.
4. المركز الديمقراطي العربي، "التحديات القانونية للذكاء الاصطناعي"، متاح على: https://democraticac.de، تاريخ الاطلاع: 10 جوان 2025.
5. مجلة أوراق فلسفية جديدة – العراق، "الذكاء الاصطناعي وأخلاقيات المستقبل"، متاح على: https://philospaper.wordpress.com، تاريخ الاطلاع: 10 جوان 2025.
6. المعهد الدولي للعدالة وسيادة القانون(IIJ) ، "الذكاء الاصطناعي والنظم القضائية"، متاح على: https://theiij.org، تاريخ الاطلاع: 10 جوان
7. Brookings Institution2025 ،. "Artificial intelligence and the future of criminal law"، متاح على: https://www.brookings.edu .

فهرس المحتويات

التعيين	الصفحة
	/
البسملة	/
شكر وتقدير	/
مقدمة	أ
الفصل الأول: إسناد المسؤولية الجزائية عن الأنظمة ذاتية التسيير	
المبحث الأول: أركان المسؤولية الجزائية وتحديات الأنظمة ذاتية التسيير	8
المطلب الأول: الركن المادي في جرائم الأنظمة ذاتية التسيير	9
الفرع الأول: السلوك الإجرامي الصادر عن الأنظمة ذاتية التسيير	9
الفرع الثاني: العلاقة السببية بين الفعل والنتيجة	11
الفرع الثالث: طبيعة التدخل البشري في الفعل التقني	13
المطلب الثاني: الركن المعنوي في الجرائم الأنظمة ذاتية التسيير	15
الفرع الأول: غياب الادارة والتمييز في الأنظمة الذاتية	16
الفرع الثاني: عدم ملاءمة القصد الجنائي التقليدي في جرائم الأنظمة ذاتية التسيير	17
الفرع الثالث: الخطأ الغير العمدي كأساس للمسؤولية الجزائية في جرائم الأنظمة ذاتية التسيير	18
المطلب الثالث: نطاق مبدأ الشرعية في جرائم الأنظمة ذاتية التسيير	19
الفرع الأول: مبدأ "لا جريمة ولا عقوبة إلا بنص"	20
الفرع الثاني: صعوبات التكييف في غياب نصوص واضحة	21
الفرع الثالث: الحاجة إلى نصوص مرنة تواكب التطور التكنولوجي	22
المبحث الثاني: نماذج إسناد المسؤولة الجزائية في نطاق جرائم الأنظمة ذاتية التسيير	24
المطلب الأول: إسناد المسؤولية الج ا زئية إلى الصانع والمستخدم	24
الفرع الأول: مسؤولية الصانع والمبرمج عن الأخطاء التقنية والبرمجية	25
الفرع الثاني: مسؤولية المستخدم أو المشغل بسبب الإهمال أو سوء الاستعمال	26
الفرع الثالث: التفاعل بين الصانع والمستخدم وصعوبة تحديد الفاعل الحقيقي	27
المطلب الثاني: المسؤولية المشتركة والتضامنية في نطاق جرائم الأنظمة ذاتية التسيير	28

الفرع الأول: توزيع المسؤولية بين الأط ا رف المتعددة	29
الفرع الثاني: التعاقد والتنازل عن المسؤولية بين الفاعلين	30
الفرع الثالث: التحديات القانونية في إثبات المساهمة الإج ا رمية التقنية	31
المطلب الثالث: إسناد المسؤولية إلى النظام الذاتي ككيان قانوني محتمل	32
الفرع الأول: فكرة الشخصية القانونية للأنظمة الذكية	32
الفرع الثاني: المواقف التشريعية والفقهية الدولية من هذه الفكرة	33
الفرع الثالث: الآثار المترتبة على تبني هذا الاتجاه في القانون الج ا زئي	34
الفصل الثاني: سبل مواكبة التشريع الجنائي للتحديات التقنية	
المبحث الأول: التكييف القانوني للجرائم الناتجة عن الأنظمة الذاتية	39
المطلب الأول: الج ا رئم الواقعة ضد الأشخاص	39
الفرع الأول: القتل غير العمدي بفعل النظام الذاتي	40
الفرع الثاني: الأذى الجسدي الناتج عن خلل تقني	42
الفرع الثالث: المساس بالسلامة الجسدية نتيجة ق ا ر ا رت خوارزمية	44
المطلب الثاني: الجرائم الواقعة ضد الممتلكات	46
الفرع الأول: إتلاف الممتلكات عبر أنظمة ذاتية القيادة	46
الفرع الثاني: الاستخدام غير المشروع لأصول الغير	48
الفرع الثالث: تعطيل نظم الحماية والتحكم عن بعد	50
المطلب الثالث: الج ا رئم المعلوماتية المرتبطة بالأنظمة الذاتية	51
الفرع الأول: القرصنة والاخت ا رق عبر الأنظمة الذكية	52
الفرع الثاني: التلاعب في البيانات أو سرقتها بوساطة الذكاء الاصطناعي	54
الفرع الثالث: تنفيذ جرائم سيبرانية مؤتمتة دون تدخل بشري مباشر	55
المبحث الثاني: الاتجاهات التشريعية والمقترحات المستقبلية	58
المطلب الأول: قراءة في التشريعات المقارنة الحديثة	59
الفرع الأول: اللائحة الأوروبية للذكاء الاصطناعي (AI Act)	59
الفرع الثاني: المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية (OECD)	62

الفرع الثالث: التجارب التشريعية في الولايات المتحدة واليابان	**64**
المطلب الثاني: آليات مقترحة لتعزيز الوقاية والتعويض	**67**
الفرع الأول: إنشاء صندوق وطني لتعويض ضحايا الأنظمة الذاتية	**67**
الفرع الثاني: فرض التأمين الإجباري على الشركات المصنعة والمطورة	**70**
الفرع الثالث: تطوير نظام للترخيص والاعتماد القانوني للأنظمة الذكية	**72**
المطلب الثالث: أدوار المؤسسات الرقابية والتشريعية	**74**
الفرع الأول: تأسيس هيئة وطنية للرقابة على الذكاء الاصطناعي	**75**
الفرع الثاني: تعزيز دور البرلمان في متابعة الابتكا ا رت القانونية	**77**
الخاتمة	**83**
قائمة المراجع	**86**
ملخص	**/**

ملخص:

تتناول هذه المذكرة موضوع المسؤولية الجزائية عن الأنظمة الذاتية التسيير في ظل التحول التكنولوجي المتسارع الذي فرض تحديات قانونية غير مسبوقة، خاصة في مجال العدالة الجزائية. ففي الفصل الأول، يتم التطرق إلى إشكالية إسناد المسؤولية الجزائية لهذه الأنظمة، من خلال دراسة أركان الجريمة ومدى انطباقها على الكيانات غير البشرية. حيث يُعالج الركن المادي عبر تحليل الفعل الجرمي الصادر عن النظام الذاتي والعلاقة السببية، ومدى تدخل العنصر البشري. أما الركن المعنوي، فيُناقش غياب الإرادة والتمييز، وصعوبة إثبات القصد الجنائي، مع إمكانية الاعتداد بالخطأ غير العمدي كأساس بديل. كما يُستعرض مبدأ الشرعية الجنائية والتحديات التي يفرضها التكييف القانوني للجرائم التقنية، والحاجة إلى نصوص مرنة. ويتناول المبحث الثاني نماذج إسناد المسؤولية، سواء للصانع أو المستخدم أو على أساس المسؤولية التضامنية، بل وحتى طرح فكرة منح النظام الذاتي شخصية قانونية.

أما الفصل الثاني فيسلط الضوء على كيفية مواكبة التشريع الجنائي لهذه التطورات، من خلال تكييف الجرائم الواقعة على الأشخاص والممتلكات والمجال المعلوماتي، إضافة إلى استعراض أهم الاتجاهات التشريعية المقارنة، مثل اللائحة الأوروبية والمبادئ التوجيهية الدولية، ليُختتم الفصل باقتراح آليات قانونية وتنظيمية لتعزيز الوقاية، التعويض، والرقابة على الأنظمة الذكية.

الكلمات المفتاحية: المسؤولية الجزائية، الأنظمة الذاتية، الذكاء الاصطناعي، الجرائم التقنية، الركن المادي، الركن المعنوي، العلاقة السببية، القصد الجنائي، مبدأ الشرعية الجنائية، الجرائم الإلكترونية، المسؤولية عن الخطأ، الصانع والمستخدم، الشخصية القانونية للآلات، الجرائم المؤتمتة، اللائحة الأوروبية للذكاء الاصطناعي

Summary:

This dissertation addresses the issue of criminal liability for autonomous systems amid the rapid technological transformation that has imposed unprecedented legal challenges, particularly in the field of criminal justice. In the first chapter, the focus is on the problem of assigning criminal responsibility to such systems by examining the elements of the crime and the extent to which they apply to non-human entities. The material element is addressed through an analysis of the criminal act committed by the autonomous system, the causal link, and the extent of human intervention. As for the mental element, it explores the absence of will and discernment, the difficulty of proving criminal intent, and the possibility of relying on negligence as an alternative basis. The chapter also discusses the principle of legality and the challenges posed by the legal classification of technological crimes, highlighting the need for flexible legal texts. The second chapter examines models of liability attribution, whether to the manufacturer, the user, or through joint liability, even considering granting legal personality to autonomous systems.

The second chapter also sheds light on how criminal legislation is adapting to these developments by classifying crimes committed against individuals, property, and the digital realm. It reviews key comparative legislative trends, such as the European AI Act and international guiding principles. The chapter concludes with proposed legal and regulatory mechanisms to enhance prevention, compensation, and oversight of intelligent systems.

Keywords: Criminal liability, autonomous systems, artificial intelligence, technological crimes, material element, mental element, causality, criminal intent, principle of legality, cybercrime, fault-based liability, manufacturer and user, legal personality of machines, automated crimes, European AI Act.