جامعة قاصدي مرباح – ورقلة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة لإستكمال متطلبات الحصول على شهادة الماستر أكاديمي
الميدان: الحقوق والعلوم السياسية
الشعبة: الحقوق
التخصص: القانون الجنائي والعلوم الجنائية

عنوان المذكرة

المسؤولية الجزائية عن الإستخدام غير المشروع للذكاء الإصطناعي

إعدادالطلبة:

- التجاني إيمان
- محديد محمد أمين
- هاشم علي

إشراف:

د. سويقات بلقاسم

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
د. الداوي نجاة	أستاذ محاضر قسم "أ"	رئيسًا
د. بلقاسم سويقات	أستاذ محاضر قسم "أ"	مشرفًا
د. صالحي نجاة	أستاذ محاضر قسم "ب"	مناقشًا

السنة الجامعية: 2023 - 2024

جامعة قاصدي مرباح – ورقلة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة لإستكمال متطلبات الحصول على شهادة الماستر أكاديمي
الميدان: الحقوق والعلوم السياسية
الشعبة: الحقوق
التخصص: القانون الجنائي والعلوم الجنائية

عنوان المذكرة

المسؤولية الجزائية عن الإستخدام غير المشروع للذكاء الإصطناعي

إعدادالطلبة:

- التجاني إيمان
- محديد محمد أمين
- هاشم علي

إشراف:

د. سويقات بلقاسم

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
د. الداوي نجاة	أستاذ محاضر قسم "أ"	رئيسًا
د. بلقاسم سويقات	أستاذ محاضر قسم "أ"	مشرفًا
د. صالحي نجاة	أستاذ محاضر قسم "ب"	مناقشًا

السنة الجامعية: 2023 - 2024

الجمـهورية الجزائريـة الديمقراطيـة الشعبيـة

وزارة التعليم العالي و البحث العلمي

جامعـة قاصدي مرباح ورقلة

التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لانجاز بحث

(ملحق القرارالوزاري رقم 1082المؤرخ 27ديسمبر 2020 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها)

أنا الممضي أسفله.

إسم ولقب الطالب	التخصص	رقم بطاقة التعريف الوطنية	تاريخ الإصدار
1. محديد محمد أمين	القانون الجنائي والعلوم الجنائية	109780558019880006	2021/02/14
2. هاشم علي	القانون الجنائي والعلوم الجنائية	109961090007470005	24/07/2019
3. التجاني إيمان	القانون الجنائي والعلوم الجنائية	110001106002670009	09/07/2019

المسجل (ة) بكلية الحقوق والعلوم السياسية قسم الحقوق

و المكلف (ة) بإنجاز أعمال بحث مذكرة ماستر،عنوانها:

المسؤولية الجزائية عن الإستخدام غير المشروع للذكاء.....
.الإصطناعي.....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية والمعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ:...2024/05/30....

1. توقيع المعني (ة):.....
2. توقيع المعني (ة):.....
3. توقيع المعني (ة):.....

شكر وتقدير

الحمد لله الذي أنعم علينا بنعمة العلم ووفقنا لإنجاز هذا العمل وتمامه ووقوفا عند قوله صلى الله عليه وسلم: "من لم يشكر الناس لم يشكر الله"، وإذا كان للمرء أن يذكر لكل ذي فضل فضله، فإننا نتوجه بالشكر والعرفان وخالص التقدير والإحترام للأستاذ الذي أشرف على هذا العمل "سويقات بلقاسم"، الذي لم يبخل علينا بالتوجيهات والرأي السديد، فكان العماد والأساس لهذا الجهد المتواضع.

كما لا يفوتنا ان نتقدم بأسمى عبارات الشكر والتقدير والعرفان إلى الأستاذة الموقرة الداوي نجاة، على وقوفها معنا بتوجيهاتها الرشيدة وأرائها السديدة والتي لم تدخر علينا اي جهد رغم إنشغالها وظروفها.

كما نتقدم بأسمى معاني الشكر والعرفان إلى الأساتذة الذين درسونا طيلة مشوارنا الدراسي وكل أعضاء لجنة المناقشة الموقرة على قبولهم مناقشة موضوع المذكرة والمشاركة في إثراء جوانبه.

جزاكم الله عنا كل خير.

إهـداء

بفضل الله تعالى وعونه، أهدي هذا العمل المتواضع إلى:

إلى روحك الطاهرة منبع التضحية، صاحب السيرة العطرة والفكر المستنير، صاحب الوجه الطيب والأفعال الحسنة، قدوتي في الحياة وتاج رأسي، إلى من علمني الحياة بأجمل شكل وبذل كل ما بوسعه ولم يبخل، إلى من رفعت رأسي عاليا به إفتخارا، إلى من علمني العطاء بدون إنتظار، "أبي الغالي" تغمدك الله برحمته وأسكنك فسيح جناته.

إلى ملاكي في الحياة، إلى معنى الحب والحنان والتفاني، إلى البسمة الطاهرة، إلى من كان دعاؤها سر نجاحي وحنانها بلسم جراحي، إلى أغلى الحبايب "أمي الحبيبة" حفظك الله ورعاك.

إلى زوجتي العزيزة وأبنائي قرة عيني آية ريتاج ومدمنبيل الذين كانوا بجانبي في كل اللحظات، بحلوها ومرها، حفظكم الله وأدامكم بالصحة والفرح والنجاح.

إلى أخواتي العزيزات وأبنائهن على صبرهن ودعمهن ومشاعر الحب في أصعب الأوقات، أتمنى لكن النجاح والفرح والسعادة، حفظكن الله وأنار دربكن.

إلى إخوتي وأبنائهم، على الإحترام الذي قدموه لي دائما.

إلى جميع أفراد عائلتي دون أن أنسى أحدا منهم.

إلى جميع زملائي في العمل والدراسة القريب منهم والبعيد، أتمنى لكم الصحة والنجاح وكل السعادة، والى كل من يحبني.

محديد محمد أمين

إهـداء

إلى من أضاءوا دربي وساندوني في خطواتي...
إلى أمي: نبع الحنان والحب الذي لا ينضب،
أهدي ثمرة جهدي المتواضع، شكرًا لتضحياتك التي لا تُحصى، ودعواتك التي لم تنقطع، وابتسامتك التي كانت دافعًا لي للمضي قدمًا. لكِ مني كل الحب والتقدير والامتنان.
إلى أبي: صخرةُ العائلة وظلُّها الوارف،
أهدي إنجازي هذا، شكرًا لوقوفك الدائم بجانبي، وإيمانك بقدراتي، ونصائحك الحكيمة التي وجهت خطواتي. لك مني كل الاحترام والفخر والتقدير.
إلى أخوتي: رفاقُ الدرب وسندُه،
أهدي فرحتي هذه، شكرًا لوجودكم الدائم في حياتي، ودعمكم المتواصل، ومشاركتكم لي لحظات الفرح والحزن. لكُم مني كل الحب والامتنان.
إلى خالتي: الأم الثانية التي احتضنتني بحنان،
أهدي نجاحي هذا، شكرًا لاهتمامك الدائم بي، ودعواتك الصادقة، وكلماتك التشجيعية التي كانت تُشعُرني بالأمان. لكِ مني كل الحب والتقدير.
إلى ابن خالتي: الصديق المقرب والأخ الحنون،
أهدي ثمرة جهدي هذا، شكرًا لصداقتك المخلصة، ووقوفك بجانبي في كل الظروف، ومشاركتي فرحة النجاح. لك مني كل المحبة والتقدير.
إلى أصدقائي الأعزاء: رفاقُ الدرب والأفراح،
أهدي لكم إنجازي هذا، شكرًا لوجودكم في حياتي، ودعمكم المتواصل، ومشاركتكم لي أجمل اللحظات. لكُم مني كل الحب والامتنان.
معًا، حققنا حلمًا، وخطونا خطوة نحو مستقبلٍ مُشرق. شكرًا لكم جميعًا من أعماق قلبي، فأنتم سرّ نجاحي وسعادتي.

هاشم علي

إهـداء

الحمد لله حبا و شكرا وإمتنانا على البدء والختام
(و آخر دعواهم أن الحمد لله رب العالمين)
من قال أنا لها .....نالها
وأنا لها وإن أبت رغما عنها أتيت بها
لم تكن رحلة قصيرة ولا الطريق محفوفا بالورود لكنني فعلتها فالحمد لله الذي يسر البدايات وبلغنا النهايات بفضله ومنه وجوده وكرمه

بكل حب أهدي ثمرة نجاحي :

إلى من جعل الله الجنة تحت أقدامها إلى الإنسانة العظيمة التي أنجبتني إلى من سهرت وربت وتعبت التي لم ولن أحصي أفضالها ما حييت و بدعائها وصلت إلى هنا أمي الحبيبة بارك الله في عمرها

إلى من زين إسمي بأجمل الألقاب ودعمني بدون حدود ومنحني دون مقابل إلى من أزاح الأشواك ومهد لي السبل لأحصد ثمار العلم سندي أبي العزيز حفظه الله

إلى من تربيت وترعرعت معهم ومن شددت عضدي بهم أمان أيامي إخوتي وأخواتي قرة عيني إلى من يليق بها الإستثناء فكانت لي خير داعم أختي فله و إلى البراعم أبناء أختي

إلى رفيقة دربي مريم وإلى كل الأصدقاء الذين كانوا لي أوفياء

إلى كل هؤلاء وإلى كل من بذل في سبيل إنجاح هذا العمل ممتنة لكم جميعا

التجاني إيمان

قائمة المختصرات

ج.ر.ج.ج: الجريدة الرسمية للجمهورية الجزائرية
ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري.
ق.ع.ج: قانون العقوبات الجزائري.
ق.م.ت.إ.م: قانون مكافحة التزوير وإستعمال المزور.
ط: طبعة.
ص: صفحة.

مـقـدمـة

مقدمة

يشهد العالم ثورة هائلة في مجال التكنولوجيا الحديثة، ما جعلها حاضرة في مختلف ميادين الحياة لما لها من أهمية بالغة في تقريب المسافات وتسهيل المعاملات، حتى بات أصعبها يتم بكبسة زر.

والإعتماد على تقنيات التكنولوجيا تظهر نتائجه جليا في الإستغناء عن العنصر البشري وإحلال الأجهزة الذكية محله، حتى حل الذكاء الإصطناعي محل الذكاء البشري، رغم أنه من صنع البشر نفسه. ويعد الذكاء الإصطناعي من أحدث التقنيات الرقمية التي أحدث بروزه ا نقلة نوعية في شتى نواحي الحياة.

ورغم إزدياد الإستخدام الإيجابي لهذه التقنية -الفريدة من نوعها- في أغراض تقدم خدمات للأفراد والمجتمعات، إلا أن الواقع العملي أثبت إمكانية إساءة إستخدام تقنيات الذكاء الإصطناعي في أنشطة غير مشروعة، الأمر الذي أصبح يشكل خطرا جسيما على أمن وسلامة الأفراد، بل ويتعدى إلى تهديد سيادة الدول وزعزعة إستقرارها، ما يستدعي البحث في المسؤولية الجزائية عن إستخدامه غير المشروع والنظر فيها من منظور جديد يتناسب مع التطور التكنولوجي المذهل في كافة المجالات لا سيما مجال المعلوماتية بصفة عامة والذكاء الإصطناعي بصفة خاصة.

ونظرا لخصوصية هذا النمط الإجرامي المستجد كان ولا بد على التشريعات والأنظمة القانونية، مواكبة التطور الحاصل بإتخاذ الوسائل والأساليب اللازمة لمواجهة الجرائم الواقعة بإستخدام الذكاء الإصطناعي، غير أن الواقع يظهر وجود صعوبات تجعل من هذا الهدف أمرا ليس بالسهل، وهذا نتيجة تعقيد هذه الجريمة التقنية التي لا تعترف بالحدود الوطنية وتجاوزت جغرافيا حدود الدول، لتمتد أضرارها إلى أكثر من إقليم، وهو الواقع الذي فرض البحث على آليات للتعاون الدولي ضمن إطار تشريعي يضمن مواجهة هذا الوضع.

وبالنظر إلى كون موضوع دراستنا يعتبر حديثا فإن هذا قد أعاق مسألة الحصول على المراجع والدراسات القانونية الكافية لإنجازه بالشكل المطلوب، حيث إقتصر الأمر على إيجاد بعض الدراسات السابقة[1] التي تطرقت إلى الموضوع لكن في جزئيات محددة

1 يتعلق الأمر بالدراسات التالية:

- سلام عبد الكريم، **التنظيم القانوني للذكاء الإصطناعي**، دراسة مقارنة، أطروحة دكتوراه، كلية القانون، جامعة كربلاء، العراق، 2022. تناول فيها الباحث تطبيقات الذكاء الإصطناعي والأضرار التي قد تنجم عنه، وبيان ضرورة إيجاد تنظيم قانوني يحكم كل ما يتعلق بالذكاء الإصطناعي.

- أحمد مسعود مريم، **آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال على ضوء القانون 09-04**، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2013/2012. تناولت فيها الباحث الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وآليات مكافحتها الواردة في أحكام القانون 09-04.

منه فقط لم تسعفنا بالقدر الكافي للإحاطة بجميع جوانب الموضوع خاصة الجانب القانوني، والذي أثار ولايزال يثير مشكلة الوجود في الجزائر، إذ تعاني هذه الأخيرة من فراغ وقصور تشريعي كبير في مجال تنظيم تقنيات الذكاء الإصطناعي عموما، وجانب المسؤولية القانونية بشقيها المدنية والجزائية خصوصا.

وتجدر الإشارة إلى أن ما إعتمدنا عليه من الدراسات السابقة وغيرها، لم تتطرق إلى المسؤولية الجزائية عن الإستخدام غير المشروع للذكاء الإصطناعي بوجه خاص – وهو ما نحاول إستدراكه من خلال دراستنا-، وركزت معظمها على المسؤولية الجزائية القائمة في حال إرتكاب الكيان جرائم مستقلة عن إرادة الإنسان نتيجة تعلمه الذاتي من التجارب.

وتتجلى أهمية هذا الموضوع الذي نحن بصدد إنجازه في قيمته العلمية التي يضيفها بإعتباره موضوعا حديثا مرتبط بجرائم معاصرة، وتكمن أهمية هذه الدراسة في محاولة إيجاد حلول لمشكلة قانونية فرضها الواقع العملي، والتي لازالت إلى حد يومنا هذا تفتقر إلى التأطير التشريعي في عدة جوانب، إضافة إلى أهميته في تمكيننا من تسليط الضوء على خصوصية إجراءات الكشف عن هذا النوع من الجرائم والتي تختلف تماما عن الإجراءات التقليدية، والدعوة إلى ضرورة إيجاد سبل للتعاون الدولي لمواجهة جرائم الذكاء الإصطناعي.

ومن أهم الأسباب التي أدت إلى إختيارنا لهذا الموضوع هو تميزه عن بقية المواضيع، لما له وفيه من حداثة وتطلعات مستقبلية واعدة للبشرية جمعاء ومواكبته للتطور الحاصل، إضافة إلى قلة الدراسات والأبحاث القانونية المعمولة بشأنه، ما يجعل دراستنا له تضفي قيمة علمية معتبرة في المكتبة القانونية وإفادة لكل ملم بالقانون.

ونتيجة لذلك، جاءت درستنا هذه لتحقيق العديد من الأهداف لعل من أبرزها:

* إثراء الرصيد العلمي والمعرفي ببحث جديد في مجال الذكاء الإصطناعي.
* دراسة مدى مواكبة المشرع الجزائري للذكاء الإصطناعي.
* بيان تنظيم القانون الجزائي للمسئولية الجزائية لمستخدمي الذكاء الإصطناعي.

- يحي إبراهيم دهشان، **المسئولية الجنائية عن جرائم الذكاء الإصطناعي**، مجلة الشريعة والقانون، كلية القانون – جامعة الإمارات – العدد 82، أفريل 2020. تطرق الباحث في دراسته إلى بيان المسؤولية الجنائية الواقعة في حالة إرتكاب كيان الذكاء الإصطناعي لجريمة ما والإشكاليات المترتبة على ذلك، مثل منح الشخصية الإعتبارية لهذا الكيان، مشيرا إلى عجز القوانين العادية على مواكبة هذا التطور، بالإضافة إلى مدى مسؤولية المبرمج أو المالك عن الجرائم المرتكبة بواسطة كيان الذكاء الإصطناعي.
- ربيعي حسن، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة دكتوراه، جامعة باتنة، 2016. إذ تناول مدى فاعلية الآلات القانونية المستحدثة في مجال دعم أعمال البحث والتحقيق للكشف عن الجرائم المعلوماتية، ويرى الباحث أن التشريع الجزائري يتميز بالجمود والقدم مقارنة لما آلت إليه الجرائم المعلوماتية.

* التطرق إلى الأساليب والوسائل القانونية والإجرائية المتبعة لمواجهة هذه الجرائم.
* الدعوة إلى ضرورة إتباع سبل التعاون الدولي لرصد مرتكبي هذه الجرائم.
* محاولة الوصول إلى نتائج تعلق بالموضوع وإعطاء بعض التوصيات بشأنها.

ونتقيد في دراستنا هذه بالتعرف على الأحكام القانونية الناظمة للمسؤولية الجزائية عن الإستخدام غير المشروع لتقنيات الذكاء الإصطناعي في التشريع الجزائري، رغبة منا في إعطاء الموضوع حقه الكافي.

أين تناولت دراستنا المسؤولية الجزائية القائمة عن إستخدام الذكاء الإصطناعي، في شقها الموضوعي بالبحث في ماهية الذكاء الإصطناعي وقيام المسؤولية في حال إستخدامه بوجه غير مشروع، ومن ثمة في شقها الإجرائي المتعلق بالإجراءات المتبعة للكشف عن هذه الجرائم وأهم الأجهزة الفاعلة في هذه العملية والآليات الدولية لمكافحتها.

وككل دراسة وبحث لا يكاد يخلو من العراقيل والصعوبات، كانت من أهم الصعوبات التي واجهتنا أثناء إعداد هذه المذكرة هو تشعب موضوعها، إذ يجمع بين الشق التقني والشق القانوني، ما دفعنا للإستعانة بعدة تخصصات لفهم بعض الجوانب التقنية. بالإضافة كذلك إلى قلة المراجع الجزائرية المتخصصة في مجال الذكاء الإصطناعي، ولعل ذلك راجع إلى حداثة الموضوع وبداية المشرع الجزائري في مواكبة التطور التكنولوجي، حيث أن معظم القوانين المنظمة لبعض الجوانب المتعلقة بالتكنولوجيا صدرت مؤخرا.

ونذكر أيضا من الصعوبات بوجه خاص، ضيق الوقت والظروف الإستثنائية التي جعلت عملية الإشراف على هذا العمل معقدة ومتأخرة نوعا ما.

ونتيجة لذلك نحاول الإجابة عن الإشكالية الآتية:

كيف نظم المشرع الجزائري أحكام المسؤولية الجزائية الناجمة عن الإستخدام غير المشروع لتقنيات الذكاء الإصطناعي ؟

ونظرا لطبيعة الموضوع وخصوصيته، إعتمدنا على المنهج الوصفي والتحليلي من أجل الإلمام بالموضوع في كافة جوانبه والتوسع فيه، ويتجلى المنهج الوصفي من خلال التعريفات والمفاهيم المرتبطة بالذكاء الإصطناعي وأهم إستخداماته، بالإضافة إلى وصف طبيعة الإجراءات والأجهزة المختصة، أما المنهج التحليلي فيظهر جليا من خلال تحليل النصوص القانونية المرتبطة بكل ذلك.

وللإجابة على إشكالية الموضوع، إرتأينا إعتماد خطة ثنائية تنقسم إلى فصلين على أن يتضمن كل فصل منهما مبحثين.

وعلى هذا الأساس تناولنا في الفصل الأول الأحكام الموضوعية للمسئولية الجزائية عن إستخدام الذكاء الإصطناعي، تعرضنا من خلاله إلى ماهية تقنيات الذكاء الإصطناعي كمبحث أول، والمسئولية الجزائية عن جرائم الذكاء الإصطناعي كمبحث ثاني.

أما الفصل الثاني فقد خصصناه للأحكام الإجرائية للمسؤولية الجزائية عن إستخدام الذكاء الإصطناعي حيث وضحنا خصوصية الإجراءات الجزائية في المبحث الأول، وآليات التعاون بين الدول لمواجهة جرائم الذكاء الإصطناعي في المبحث الثاني.

الفصل الأول

الأحكام الموضوعية للمسؤولية الجزائية للإستخدام غير المشروع للذكاء الإصطناعي

تمهيد

يتميز الإنسان عن الآلة بفارق جوهري وهو العقل البشري وصفات العاطفة الإنسانية، ويختلف كل شخص عن غيره بردات الفعل والطباع وقابلية التعلم، أما الآلات فهي مبرمجة وفق تعليمات محددة لا تخرج عنها، وتكون تحركاتها وخطواتها ونتائجها متوقعة، ومع الثورة التقنية في مجال الذكاء الإصطناعي Artificial Intelligence تغير هذا المفهوم وبدأ هذا الفرق يتلاشى؛ إذ صار الذكاء الإصطناعي يتسم بسلوك وخصائص تجعله يحاكي القدرات الذهنية البشرية، كالقدرة على التعلم والإستنتاج ورد الفعل على أوضاع لم تبرمج في الآلة.

وقد سهلت تقنيات الذكاء الإصطناعي من الحياة البشرية اليومية كثيرا، وأصبحت من أهم ضروريات العصر، إذ تساعد في إنجاز العديد من المهام المستعصية على الإنسان، وبكفاءة تضاهيه أو تفوقه في مختلف القطاعات كالصحة والتعليم والترفيه والتسويق.

هذا التطور ورغم ما سجله من محاسن ومزايا، إلا أنه وكغيره من التكنولوجيات لا يخلو من العيوب والسلبيات، ولعل أهمها أنه ساهم في تطور الجريمة وإنتشارها وظهور عدة جرائم مستحدثة عابرة للحدود، ما ينبئ بتصدر هذا النوع من الجرائم الصدارة في جرائم المستقبل القريب عن طريق الإستخدام غير المشروع لتلك التقنيات.

على هذا الأساس سنتناول في هذا الفصل الأحكام الموضوعية عن تقنيات الذكاء الإصطناعي، وسنتطرق في المبحث الأول إلى ماهية تقنيات الذكاء الإصطناعي وفي المبحث الثاني إلى المسؤولية الجزائية عن جرائم الذكاء الإصطناع.

المبحث الأول: ماهية تقنيات الذكاء الإصطناعي

نعيش اليوم في وقتنا الحاضر ثورة هائلة في مجال تقنيات المعلوماتية، وتعتبر تقنيات الذكاء الإصطناعي أحد أهم إفرازاتها، لما لها من تطلعات واعدة وقدرات على محاكاة الذكاء البشري، وفي سبيل إيضاح ما سبق، سنتناول في المطلب الأول مفهوم الذكاء الإصطناعي وفي المطلب الثاني تقنيات الذكاء الإصطناعي وإستخداماتها.

المطلب الأول: مفهوم الذكاء الإصطناعي

عرفت السنوات الأخيرة الماضية الهيلاد الحقيقي للذكاء الإصطناعي، حين إستطاع الإنسان إبتكار ذكاء يحاكي ذكاءه، من خلال الأنظمة المبرمجة والتي تساعده في حياته، لذا سنتطرق إلى تعريف الذكاء الإصطناعي وخصائصه المنفردة.

الفرع الأول: تعريف الذكاء الإصطناعي

صاغ عالم الحاسوب John McCarthy هذا المصطلح بالأساس سنة 1956، وعرفه بنفسه بأنه: "علم وهندسة صنع آلات ذكية"[1].

وعرفه Russell و Norving بأنه: "دراسة وتصميم العملاء الأذكياء"، والعميل الذكي نظام يستوعب بيئته ويتخذ المواقف التي تزيد من فرصه في النجاح وتحقيق مهمته[2].

وعرفه Andreas Kaplan بأنه: "قدرة النظام على تفسير البيانات الخارجية بشكل صحيح، والتعلم من هذه البيانات، إستخدام تلك المعرفة لتحقيق أهداف ومهام محددة من خلال التكيف المرن"[3].

وعرفه Marvin Lee Minsky بأنه: "بناء برامج الكمبيوتر التي تنخرط في المهام التي يقوم بها البشر بشكل مرضي، لأنها تتطلب عمليات عقلية عالية المستوى كالإدراك الحسي والتعلم وتنظيم الذاكرة والتفكير النقدي"[1].

1 عادل عبد النور، أساسيات الذكاء الإصطناعي، منشورات مواقف، بيروت - لبنان، 2017، ص 101.

2 Stuart J. Russell, Peter Norvig, Artificial Intelligence: A Modern approach is a university textbook on artificial intelligence, 3th Edition, Pearson Education, 2010, P. 3 .

3 Andreas Kaplan, Michael Haenliein, Who's the fairest in the land? On the interpretations and illustrations and implications of artificial intelligence, Business Horizons, Vol 62, 2019, P 16.

ويعتبر الإتحاد الأوروبي رائدا في هذا المجال بتشريعاته المرجعية ذات الصلة، حسب ما جاء في مقال بجريدة الغارديان البريطانية بتاريخ 2023/06/23. وعرفه قرار البرلمان الأوروبي رقم 206 بتاريخ 2023/05/09 والمعدل للتشريعات السابقة ذات الصلة بأنه: "من ضمن التقنيات الرقمية الناشئة كالأنترنت الأشياء (IOT) والروبوتات المتقدمة والأنظمة المستقلة، بهدف إنشاء منتجات وخدمات تتيح للفرد والمجتمع فرصا جديدة للإقتصاد، ورقي الحياة وتيسيرها عبر الأنظمة الجديدة والبيئات المعقدة، وتتبعها عبر لجان تقنية تضمن وجود عناصر الأمن السيبراني والأخلاق في التصميم"[2].

وعرفته المفوضية الأوروبية مؤخرا، بأنه: "برمجيات قد تكون أجهزة صممها البشر من خلال التصرف في البيئة الرقمية، عن طريق البيانات المنظمة وغير المنظمة وتفسيرها والتفكير المعرفي ومعالجة المعلومات المستمدة من هذه البيانات، وتحديد أفضل الإجراءات التي يجب إتخاذها لتحقيق الهدف المحدد. ويمكن لهذه الأنظمة إن تستخدم قواعد رمزية أو نماذج رقمية، ويكيف سلوكهم من خلال تحليل تأثير البيئة على أفعالهم السابقة"[3].

أما المشرع الجزائري فلم يعرفه وإكتفى بتنظيم الميادين المستعمل فيها، ونص في القانون 18-105 المؤرخ في 2018/05/10، المتعلق بالتجارة الإلكترونية على إمكانية التعاقد الإلكتروني بالإرتكاز على التكنولوجيات الحديثة في مجال البرمجيات الذكية.

الفرع الثاني: الخصائص المنفردة لأنظمة الذكاء الإصطناعي

الذكاء الإصطناعي أحد صور التقدم التكنولوجي المساهم في تسيير طبيعة التطور، ومن شأن كل إختراع جديد إن إحداث قفزة نوعية في حياة الإنسان، والذكاء الإصطناعي يتميز عن ما سبقه من التكنولوجيات بأهمية بالغة وخصائص منفردة، نذكر منها:

أولا: الطابع المعنوي اللامادي لأنظمة الذكاء الإصطناعي

1 طاهر أبو العيد، دليل الذكاء الإصطناعي لطلبة القانون والباحثين في الوطن العربي، مجلة قانونية وتكنولوجيا، مصر، 2023، ص 45.

2 Résolution européenne relative à la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union, 206 final, COM (2021).

3 EUROPEAN COMMISSION, Independent High-Level Expert Group On Artificial Intelligence: a definition of AI - Main capabilities and scientific disciplines, Springer, 08/04/2019, P. 6.

أنظمة الذكاء الإصطناعي وبالرغم من كونها تظهر في شكل مادي ملموس، كونها مجموع خوارزميات Algorithms[1] أو برمجيات Software[2]، فإنها تتميز بطابعها المعنوي وتعتبرها أغلب التشريعات أموال غير مادية، وأعمال عقل خاضعة لقوانين الملكية الفكرية.

حيث يشكل نظام الذكاء الإصطناعي العقل غير المرئي للجسم الفيزيائي الساكن، في جسم فيزيائي مادي ساكن، والذي يبدأ بالحركة بمجرد ربطه بمجموعة من البرمجيات[3].

ثانيا: الإستقلال الوظيفي لأنظمة الذكاء الإصطناعي

الشائع عن أنظمة الذكاء الإصطناعي أنها أنظمة مؤتمتة[4]، ومع تطور أنظمته إكتسبت قدرة محاكاة الإدراك البشري، والتعامل مع كل موقف معاملة خاصة غير متوقعة، خاصة إذا ما برمجت على تجاوز حدود الذكاء البشري في إستقلاله وسرعته ودقته[5].

إن أنظمة الذكاء الإصطناعي لا يمكن التنبؤ بردات فعلها بصورة مطلقة ومتوقعة، فمن بينها الأنظمة المعرفية الذكية الذاتية التعلم، والمبرمجة على التصرف وفق ما يحيط بها من ظروف بطريقة أكثر عقلانية، إذ تتخذ قرارات مستقلة دون الحاجة لتدخل المستخدم بناءا على التجارب والبيانات السابقة المخزنة والمشفرة.

ثالثا: صعوبة حصر أفعال أنظمة الذكاء الإصطناعي وعدم التنبؤ بها

1 الخوارزميات Algorithms هي مجموعة من الخطوات الرياضية والمنطقية المتسلسلة واللازمة لحل مشكلة ما، وسميت بهذا الإسم نسبة إلى العالم أبو جعفر محمد بن موسى الخوارزمي الذي كان أول من إبتكرها في القرن التاسع الميلادي.

2 البرمجيات Softwares هي مجموعة من التعليمات مكتوبة بنوع من الوضوح والتفصيل، تقوم بعملية تنظيم الأوامر الخاصة بأكواد الحاسوب المسؤولة عن التشغيل، وتكتب بلغات متعددة وللقيام بوظائفها مختلفة.

3 Nour EL KAAKOUR, L'intelligence artificielle et la responsabilité civile délictuelle, Mémoire pour l'obtention du Diplôme d'Études Approfondies En Droit Interne et International des Affaires, Faculté de Droit et des Sciences Politiques et Administratives, Liban, 2017, P 30-31.

4 الأتمتة Automation هي برمجة الآلة لمدة ومهمة معينتين دون خروجها عنهما، أي تشغيل الآلة وفق برامج معدة سلفا دون إمكانية إن تحيد عنها.

5 مصطفى أبو مندور موسى عيسى، مدى كفاية القواعد العامة للمسؤولية المدنية في تعويض أضرار الذكاء الإصطناعي، مجلة حقوق دمياط للدراسات القانونية والإقتصادية، كلية الحقوق، جامعة دمياط، العدد 5، مصر، 2022، ص 242.

في بعض فرضيات أنظمة الذكاء الإصطناعي يمكن إن تتجرد أفعالها من أي أثر مادي ملموس وغير مرئي، كحالات تقديمها لبيانات أو معلومات غير صحيحة تخص عقد أو مشروع تجاري لشركة أو شخص ما، ويترتب عليها أضرارا لمستخدميها، ففي مثل هذه الحالات، يصعب فهم حقيقة الأفعال الضارة لأنظمة الذكاء الإصطناعي، ومدى سببيتها في إحداث الضرر لعدم كونها مرئية. ولغرض التغلب على هذه الصعوبة، إقترح إنشاء الصندوق الأسود BLACK BOX لكل نظام ذكاء إصطناعي، لتسجيل الأحداث التي تقع في لحظة معينة والتغيرات التي تطرأ عليها، ويكون مرجعا للبحث عن مسببات المسائلة[1].

رابعا: عدم التقييد الزمكاني لأنظمة الذكاء الإصطناعي

نجم على المميزات السالفة الذكر خاصية أخرى لا تقل أهمية، تمثلت في عدم تركز هذه الأنظمة في مكان وزمان معينين. فهي مطلقة يمكن إستخدامها في أي زمان أو مكان، مما يترتب عليه عدم تحديد زمكانية الضرر المترتب عنها، وما يرتبه من آثار قانونية كصعوبة تحديد الإختصاص الإقليمي للمحكمة المختصة بالفصل فيه. الأمر الذي يترتب عنه تحيين القواعد القانونية التقليدية الناظمة في هذا الشأن، بالشكل الذي يتناسب مع هذه السمات والصعوبات التي تتميز بها أنظمة الذكاء الإصطناعي[2].

المطلب الثاني: الذكاء الإصطناعي وإستخداماته

تقنيات الذكاء الإصطناعي من الضروريات الأساسية داخل المجتمع البشري، لقدرتها على المساهمة في إنجاز العديد من المهام التي يصعب عليه القيام بها، حيث تنتشر عدة آلات تعتمد على الذكاء الإصطناعي وبإختلاف التقنية المستخدمة فيها وفي مختلف المجالات كالروبوت والطائرات بدون طيار وغيرها. وكغيره من التكنولوجيات الحديثة كما له مميزات فله أيضا عيوب، ودور المجتمع والحكومات تقنين أوضاعها وإستغلال مميزاتها، مقابل تجنب عيوبها بما يتناسب مع المجتمع.

الفرع الأول: أنواع الذكاء الإصطناعي

ينتقسم الذكاء الإصطناعي إلى أنواع عديدة ومختلفة، وليس هناك نوع واحد يمكنه تنفيذ كل الأعمال، فكما نستخدم برامج الكمبيوتر المختلفة في معالجة الكلمات والمحاسبة والتأليف الرقمي، فهناك أنواع أخرى مختلفة تعمل بشكل مختلف لتحقيق أهداف مختلفة.

أولا: الذكاء الإصطناعي تبعا للقدرات

1 Adrien Bonnet, La responsabilité du fait de l'intelligence artificielle, Mémoire de recherche Droit privé général, Université Panthéon Assas, Paris, 2014-2015, P 11.

2 مصطفى أبو مندور موسى عيسى، مرجع سابق، ص 257.

يصنف الذكاء الإصطناعي تبعا لما يتمتع به من قدرات إلى ثلاث أنواع، كالتالي:

1) الذكاء الإصطناعي الضيق Weak AI or Narrow AI

يستطيع القيام بمهام محددة وواضحة، ويعتبر النوع الأكثر شيوعا وتوفرا في وقتنا الحالي، كالسيارات ذاتية القيادة وبرامج التعرف على الكلام والصور والأجهزة الذكية. يهدف إلى تصميم أنظمة تفاعلية قادرة على أداء مهام محددة وبدقة معينة، ويتميز بتقييد قدراته لحل مشكلات أو مهام محددة، دون التعلم أو التكيف مع المواقف غير المتوقعة، ولا يستطيع فهم السياق العام للمعلومات أو إتخاذ قرارات مستقلة خارج نطاق المهمة المحددة[1].

2) الذكاء الإصطناعي العام General AI

الذكاء الإصطناعي العام نوع يمكن إن يعمل بقدرة تشابه قدرة الإنسان من حيث التفكير، ويرتكز على جعل الآلة قادرة على التفكير والتخطيط من تلقاء نفسها وبشكل مشابه للتفكير البشري[2]، إلا أنه لا يوجد أمثلة عملية له، وكل ما يوجد مجرد دراسات بحثية تحتاج لتطويرها وتحويلها إلى واقع، وتعد طريقة الشبكة العصبية الإصطناعية من طرق دراسة الذكاء الإصطناعي العام، وتعنى بإنتاج نظام شبكات عصبية للآلة مشابهة للجسم البشري[3].

من تطبيقاته الواعدة، إستخدامه لتشخيص الأمراض وتوصيف العلاجات المناسبة بناء على بيانات المرضى والتاريخ الطبي، وتحليل الأشعة السينية والمقطعية لتقديم تشخيص دقيق للأمراض. كما يمكن إستخدامه لتطوير منصات تعليمية تفاعلية لفهم إحتياجات الطلاب وتقديم مواد تعليمية مخصصة وفعالة، وتقيم أدائهم ومساعدتهم لتحسين فهمهم لها.

3) الذكاء الإصطناعي الفائق Super AI

1 وفاء محمد أبو المعاطي صقر، المسؤولية الجنائية عن جرائم الذكاء الإصطناعي - دراسة تحليلية إستشرافية-، مجلة روح القوانين، كلية الحقوق- جامعة طنطا، مصر، العدد 96، أكتوبر 2021، ص 30.

2 وفاء محمد أبو المعاطي صقر، مرجع سابق، ص 31.

3 سلام عبد الكريم، التنظيم القانوني للذكاء الإصطناعي- دراسة مقارنة-، أطروحة مقدمة كجزء من متطلبات نيل درجة الدكتوراه في القانون المدني، كلية القانون، جامعة كربلاء، العراق، 2022، ص 47.

يعتبر النوع الذي قد يفوق ذكاء البشر المتخصص، ويستطيع القيام بالمهام بشكل أفضل منه، كالقدرة على التعلم والتخطيط والتواصل التلقائي وإصدار الأحكام[1]. يهدف لإنشاء أنظمة تتمتع بقدرات فائقة في التعلم والتفكير وفهم العالم بطرق تتفوق على العقل البشري، ويتميز بقدرات تحليلية وإستنتاجية عميقة، وقدرة هائلة وسريعة لإستيعاب البيانات[2]. ومن أمثلته الواعدة، إستخدامه في تشخيص الأمراض المعقدة، وتطوير علاجات مخصصة لكل مريض بناء على تحليل البيانات الجينية والتاريخ الطبي بشكل شامل.

ثانيا: الذكاء الإصطناعي تبعا للوظائف

يصنف الذكاء الإصطناعي تبعا للوظائف التي يقوم بها إلى أربعة أنواع كمايلي:

1) الآلات التفاعلية

تنفذ المهام الأساسية فقط وتستجيب لبعض المدخلات والمخرجات، ولا تتضمن التعلم الذاتي[3]. كنظام Deep Blue[4] من IBM وبرنامج AlphaGo[5] من Google.

وتتميز بكونها لا تخزن الذكريات أو التجارب السابقة لأعمال مستقبلية، كما تركز فقط على السيناريوهات الحالية وتتفاعل معها وفقا لأفضل إجراء ممكن.

2) الذاكرة المحدودة

في هذا النوع يصبح لدى الذكاء الإصطناعي القدرة على تخزين البيانات أو التوقعات السابقة، وإستخدامها في القيام بتنبؤات أفضل مستقبلا[6]. ويمكنها تخزين التجارب السابقة أو بعض البيانات لفترة قصيرة من الوقت وإستخدام البيانات المخزنة لفترة زمنية محدودة فقط.

---

1 Available at http://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third-even-possible، Viewed on 25/04/2024 at 11 :10.

2 مذكور مليكة، هل المعرفة خاصية إنسانية حقا؟، الأكاديمية للدراسات الإجتماعية والإنسانية، جامعة حسيبة بن بوعلي، الشلف- الجزائر، المجلد 12، العدد 01، 2020، ص 93.

3 بلقاضي شيماء، دور التكنولوجيا المالية والذكاء الإصطناعي في الرفع من كفاءة القطاع المصرفي الجزائري – محاكاة تجارب دولية عربية، مذكرة مقدمة لنيل شهادة ماستر أكاديمي في الإدارة المالية، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة العربي بن مهيدي، أم البواقي، الجزائر، 2020 /2021، ص 6.

4 حاسوب Deep Bleu هو حاسوب فائق متخصص في لعبة الشطرنج من خلال إضافة دوائر محددة تم تطوريها في بداية التسعينات من القرن الماضي، من إنتاج شركة IBM يستخدم تقنية المعالجة التفرعية الشاملة لحل المشاكل.

5 تطبيق AlphaGo هو برمجية حاسوب طورت من قبل جوجل ديب مايند Google Deep Mind في أكتوبر 2015 وهي أول برمجية تهزم لاعب بشري محترف في لعبة الغو.

6 بلقاضي شيماء، مرجع سابق، ص 67.

ومن أفضل الأمثلة عن أنظمة الذاكرة المحدودة السيارات ذاتية القيادة، إذ يمكن لتلك السيارات تخزين السرعة الحديثة لها وللسيارات القريبة منها، والمسافة التي تفصلها عن التي من حولها، ما يجعلها تساهم بقدر كبير في إجتناب أكبر قدر من حوادث المرور، ولما لا القضاء عليها نهائيا مستقبلا.

3) نظرية العقل

هي المستوى الثلثي من أنظمة الذكاء الإصطناعي وهو في مرحلة الإبتكار، يتفاعل هذا النوع من الذكاء الإصطناعي مع أفكار وعواطف البشر. سيركز بشكل أساسي على الأفراد الذين يمكن تشكيل عقولهم بواسطة عوامل متعددة، مثل فهم البشر، فسيكون لديهم فهم أفضل للكيانات التي يتفاعلون معها، من خلال فهم إحتياجاتهم وعمليات التفكير والعواطف والمعتقدات، فالفهم هو المفهوم الرئيسي المتعلق بنظرية العقل، فقد يتعامل مع جوانب مختلفة مثل السلوك والعواطف والطبيعة البشرية والمشاعر، ويعتبر هذا أحد التطورات التكنولوجية الحاسمة التي تفرز مشاعر الناس ومشاعرهم وأفكارهم[1].

4) العلم والإدراك الذاتي

هو مستقبل الذكاء الإصطناعي، ستكون هذه الآلات فائقة الذكاء، وسيكون لها مشاعرها ووعيها الذاتي الخاص، والتي يفترض إن تكون أكثر ذكاء من عقل الإنسان. ويجدر الإشارة إلى إن الوعي الذاتي في الذكاء الإصطناعي غير موجود في الواقع وهو مفهوم افتراضي، يسعى الباحثون في هذا المجال إلى جعله واقع فعلي[2].

الفرع الثاني: مجالات إستخدام الذكاء الإصطناعي

يعتبر الذكاء الإصطناعي أساسا في التكنولوجيا الحديثة وصناعاتها، والتي تعتمد عليه في كيفية تحويله إلى تطبيقات وبرمجيات يمكن لنا الإستفادة منها في حياتنا، من حيث الراحة والرفاهية والتطوير، وتؤدي بدورها وظائف مختلفة يستطيع الإنسان القيام بها، لكن ليس بنفس سرعتها ودقتها. وعليه سنتناول في هذا المطلب أهم مجالات تطبيق تقنيات الذكاء الإصطناعي.

أولا: مجال التعليم

1 Gurney, N., Marsella, S., Ustun, V., Pynadath, Operationalizing theories of theory of mind: A survey in AI Fall Symposium, Springer, 2021, P 3–20.

2 Available at https://www.javatpoint.com/types-of-artificial-intelligence. Viewed on 16/04/2024 at 14:45.

توفر الطبيعة الرقمية والديناميكية للذكاء الإصطناعي مجالا مختلفا لا يمكن العثور عليه في البيئة التقليدية النمطية للمدرسة، وستمكن تطبيقاته من إكتشاف حدود جديدة للتعلم وتسرع في إنشاء تقنيات مبتكرة، ومنها المحتوى الذكي الذي يحول الكتب التعليمية التقليدية إلى كتب ذكية وثيقة الصلة بالغاية التعليمية. ويستخدم بعض أنظمة التدريس الذكي عددا من تقنيات التعلم الآلي، وخوارزميات التعلم الذاتي التي تجمع البيانات الكبيرة وتحللها[1].

ونجد أيضا أنظمة التعليم الذكي المعروفة بأنظمة ITS، والتي تضم برامج تعليمية تحتوي على عنصر الذكاء الإصطناعي. حيث يقوم النظام بتتبع أعمال الطلاب وإرشادهم كلما تطلب الأمر، وذلك من خلال جمع معلومات عن أداء كل طالب على حدة، وإبراز نقاط القوة والضعف لدى كل متعلم، وتقديم الدعم اللازم له في الوقت المناسب[2].

وهناك أيضا تقنية الواقع الإفتراضي المعزز، التي تعمل على إنشاء تصورا إفتراضيا يظهر لحواسنا مشابه للعالم الحقيقي، ونقل المعلومات والخبرات بشكل جذاب وتفاعلي.

ثانيا: المجال المصرفي

أصبحت النظم الخبيرة أكثر من منتج تجاري في الميدان المالي، فمثلا قامت Dupont بإنشاء أكثر من 100 نظام خبير وفر لها 10 ملايين دولار سنويا. كما تمكن نظام التنبؤ Pro Trader لمصممه Chen K.C وTing-Peng Lian من التنبؤ بإنخفاض 87 نقطة في المتوسط داو جونز الصناعي سنة 1986.

ويمكن إستخدام الذكاء الإصطناعي أيضا في مجال مكافحة تبييض الأموال وإنشاء روبوتات دردشة تفاعل العملاء، والقيام بدور وكيل لخدمة العميل التي ترتبط عادة بمنصات المراسلة المباشرة الشائعة مثل فيسبوك، ماسنجر وواتساب[3].

1 مكاوي مرام عبد الرحمان، الذكاء الإصطناعي على أبواب التعليم، مجلة القافلة، أرامكو السعودية، السعودية، المجلد 67، العدد 6، 2018، ص23.

2 لطفي خديجة، كيف يستطيع الذكاء الإصطناعي التأثير على التعليم؟، شوهد على الرابط: https://www.new-educ.com/category/studies، بتاريخ 2024/04/30 على الساعة 21 : 22.

3 Mangani D., 5 AI Application i banking to look outfor in next 5 years, available at: https://www.analyticsvidhya.com/blog/2017/04/5, Viewed on 30/04/2024 at 17 :33.

ويعد أحد الحقول التي حصلت على دعم كبير في تقديم نتائج دقيقة ومتفوقة بتدخل الذكاء الإصطناعي، تطبيقات تقييم الإحتيال Fico-Falcon في القطاع المصرفي، والذي يعتمد على شبكة عصبية لنشر أنظمة الذكاء الإصطناعي القائمة على التعلم العميق، بناءا على تحليل وإختبار كم هائل من البيانات، ويمكن للتعلم الآلي إن يحسن العمليات والأنظمة إلى أنظمة أكثر قوة وذكاء، في مكافحة غسيل الأموال خلال السنوات المقبلة.

ثالثا: أنظمة النقل الذكية

في صناعة النقل منذ عدة سنوات، بدأ المصنعون يزيدون من براعتهم في دمج التقنيات الجديدة في سيارات الركاب ووسائل النقل العام من أجل تسهيل الحياة اليومية، وبفضل التقنيات المتطورة بشكل متزايد، أصبحت مركبات النقل مثل السيارات والطائرات والقطارات وما إلى ذلك، أكثر موثوقية وكفاءة فهي متصلة ومجهزة بأجهزة إستشعار مختلفة، وأجهزة رادار وكاميرات، ونظام تحديد المواقع، ونظام تثبيت السرعة[1].

إذا تم إستبدال أسطول السيارات بأكمله بسيارات ذاتية القيادة، فإن حركة المرور ستكون أكثر مرونة وتجنبا للإختناقات المرورية لترابط الشبكة بأكملها، بالإضافة إلى تطور شبكة السكك والميترو وغيرها من وسائل النقل الضخمة كالطائرات والبواخر، ومساهمتها في تسهيل التنقل والحركة عبر العالم للبشر والسلع. كما إن عدد حوادث الطرق سوف ينخفض بشكل كبير، فالسيارات ستتفاعل بسرعة أكبر، وبأكثر عقلانية في حالة الخطر.

رابعا: المجال العسكري

يمكن للذكاء الإصطناعي تعزيز القدرات العسكرية التقليدية والمتطورة، من الناحية التشغيلية ووعلى المستوى التكتيكي. فعلى المستوى التشغيلي يعزز من القدرات العسكرية من خلال إمكانات الاستشعار عن بعد، والإدراك اللحظي للمتغيرات والمناورة واتخاذ القرار تحت الضغط. أما على المستوى الإستراتيجي التكتيكي في صنع القرار العسكري، فستتمكن أنظمة القيادة المعززة بتكنولوجيا الذكاء الإصطناعي تجنب العديد من أوجه القصور الملازمة لعملية اتخاذ القرارات الاستراتيجية التقليدية، حيث ستكتسب القدرة على إتخاذ القرار السريع بناء على المعلومات المعززة، وهو الأمر الذي يجنبها الأخطاء البشرية.

1 عبد الله موسى، أحمد حبيب بلال، الذكاء الإصطناعي ثورة في تقنيات العصر، المجموعة العربية للتدريب والنشر، الطبعة 1، مصر، 2019، ص 82.

ومن بين أبرز تهديدات الأمنية المحتملة في المجال العسكري والأمن بمفهومه الواسع المتضمن الأمن الرقمي، كالتصيد الموجه أو التصنيع الصوتي وإنتحال الهوية والتسلل الآلي، والأمن المادي مثل الهجمات المنفذة من أسراب الطائرات بدون طيار[1].

خامسا: المجال الطبي

إستفاد القطاع الصحي من إستخدامات الذكاء الإصطناعي بشكل كبير، وبات يعتمد عليه في التشخيص وإنتاج الأدوية وتحسين سير العمل داخل المستشفيات والأقسام الطبية. فالذكاء الإصطناعي يمنح الكمبيوتر القدرة على التعلم من البيانات الضخمة، والعمل على تطوير نظام آلي قادر على التعلم والمعالجة المنطقية لتحقيق التكامل بين عمل الأطباء. كما إستفادت المستشفيات من لإدارة العمل وتنظيم ملفات المرضى والتدخلات الجراحية وإدخال البيانات الضخمة، ما يجعل إستخراجها أسرع وتشخيص الأمراض أبكر[2].

سادسا: مجالات أخرى

إستخدم الذكاء الإصطناعي بنجاح في عدة مجالات، كالنظم الخبيرة ومعالجة اللغات الطبيعية، وتمييز الأصوات وتمييز وتحليل الصور والفيديوهات، وكذلك التشخيص الطبي وتداول الأسهم، والتحكم الآلي والروبوتات، والقانون والإكتشافات العلمية، وألعاب الفيديو ولعب الأطفال ومحركات البحث على الإنترنت، والمنازل الذكية وعلوم الفضاء، خاصة في تصميم مختلف الآلات الخاصة للقيام بمهام في الفضاء المتعلقة أساسا بغرض البحث العلمي.

الفرع الثالث: الآثار السلبية لإستخدامات تقنيات الذكاء الإصطناعي

يشكل الذكاء الإصطناعي ثورة هامة يجب الإستعداد لها قانونيا من خلال تشريعات محددة، بسبب القدرات والإمكانيات الرهيبة المتوفرة في الذكاء الإصطناعي والتي تسهل إرتكاب الجرائم، والتعدي على خصوصيات الناس التي يحميها القانون. ونتيجة توغله في الكثير من المجالات، والإعتماد على تقنيات الذكاء الإصطناعي في إنجاز العديد من الأعمال آليا، والتطور الحاصل في خوارزميات التعلم الذاتي وإتخاذ القرارات، فمنطقيا سوف يصاحب ذلك زيادة إنتشاره وزيادة في حدوث جرائم من قبله أو بإستخدامه وإستغلاله في أعمال غير مشروعة.

1 جيمس جونسون، أتمتة الحرب وتأثير الذكاء الإصطناعي في سباق التسلح، شوهد على الرابط: https://futureuae.com/ar/Home/Index/2، بتاريخ 2024/05/02 على الساعة 11 : 09.

2 ما هي إستخدامات الذكاء الإصطناعي في قطاع الرعاية الصحية؟، شوهد على الرابط: https://www.thearabhospital.com، بتاريخ 2024/05/02 على الساعة 45 : 09.

وعلى الرغم من أهمية الذكاء الإصطناع وإجابياته في شتى المجالات، إلا أنه لا يكاد يخلو من العيوب كغيره من التكنولوجيات الحديثة والتي يجب مراعاتها والتعامل معها بحذر، حيث يترتب على إنتشاره العديد من السلبيات والمشاكل التى تؤثر على المجتمع، كظهور البطالة بشكل أكبر لحلوله محل الأيدي العاملة في العديد من الوظائف، بسبب القدرة والمهارة الكبيرتين المتوفرتين به وبتكلفة أقل وجودة أعلى مقارنة بالبشر[1].

فى سنة 2013 حذر عالمين بجامعة أكسفورد إن 47% من الوظائف يمكن تقنيتها خلال 20 عاما القادمة، كسائقوا التاكسي والتوصيل وحراس الأمن وموظفي المبيعات، وأن تطورات تقنيات تعلم الآلة ستجعل الآلة تحل محل الإنسان في وظيفته.

هذا التخوف جعل الحكومات تسعى إلى مواجهة هذا التحدى الإجتماعي بوضع سياسات إعادة تأهيل شاغلي الوظائف الروتينية والتقليدية، لإكسابهم مهارات تؤهلهم لوظائف جديدة، وإقترح بيل جيتس إن تقوم الحكومات بفرض ضرائب على الروبوتات كالضرائب على الدخل للعمال والموظفين[2].

ويعد إنتهاك الخصوصية والحياة، من أهم سلبيات تنامى الذكاء الإصطناعي بدون ضوابط وحدود قانونية، فجميع الخدمات التكنولوجية حاليا، تفرض على المستخدمين السماح للبرمجيات بسحب بيانات معينة من الوسيلة المستخدمة في الوصول لتلك التكنولوجيا، وتقوم بتحليل تلك البيانات والحصول على إهتماماته لإستغلالها في أهداف كثيرة[3].

1 Gentsch P., AI in Marketing - Sales and Service, Palgrave Macmillan, Cham, 2019, P 50.

2 تقرير عن المخاطر الحقيقية للذكاء الإصطناعي، هارفرد بيزنس ريفيو العربية، جانفي 2016، شوهد على الرابط: http://Ail00.Stanford/2016report، بتاريخ 2024/04/19 على الساعة 14 : 18.

3 يحيى إبراهيم دهشان، المسؤولية الجنائية عن جرائم الذكاء الإصطناعي، بحث منشور بمجلة الشريعة والقانون، كلية القانون، جامعة الإمارات، الإمارات العربية المتحدة، طبعة 2019، ص 15.

المبحث الثاني: المسؤولية الجزائية عن جرائم الذكاء الإصطناعي

يتميز كل عصر بسمة تميزه عن الذي سبقته والتي ستليه، ويبدو إن العصر الذي نعيشه الآن يستحق إن نطلق عليه عصر الذكاء الإصطناعي، لاسيما مع ظهور الروبوتات الذكية المتطورة التي تملك القدرة على محاكاة السلوك البشري. حيث طال الذكاء الإصطناعي مجالات مختلفة من حياة الإنسان، ومع إستخدام الروبوتات وبرامج الذكاء الإصطناعي في مختلف القطاعات والمجالات، ساهم بشكل كبير في ظهور جرائم جديدة مستحدثة، يعتمد منفذوها بشكل كبير على تقنيات الذكاء الإصطناعي.

وسنحاول في هذا المبحث تحديد أطراف المسؤولية الجزائية في جرائم الذكاء الإصطناعي كمطلب أول، والتطرق إلى أبرز جرائم الذكاء الإصطناعي كمطلب ثاني.

المطلب الأول: أطراف المسؤولية الجزائية في جرائم الذكاء الإصطناعي

يرتكز القانون الجنائي على عدة ركائز منها المسئولية الجنائية، فلا عقوبة إلا على المسئول عن الجريمة. وتعد المسئولية الجنائية في جرائم الذكاء الإصطناعي معقدة بعض الشيء، فهناك أربعة أطراف ترتبط غالبا بهم، وتجب دراسة كل جريمة بدقة لمعرفه المسؤول الحقيقي عن الجريمة المرتكبة.

الفرع الأول: المسؤولية الجزائية للمصنع أو المبرمج

المسؤولية الجنائية للمصنع أو المبرمج في جرائم الذكاء الإصطناعي أهم ما يثار عند إرتكابها، وغالبا ما يقوم المصنع أو المبرمج بحماية نفسه ببنود يذكرها في إتفاقية الإستخدام والتي يوقع عليها المالك أو المستخدم، وتحمله وحده المسؤولية الجنائية وتخلي مسؤولية المصنع أو المبرمج عن أي جريمة ترتكب من قبله[1].

لكن قد تحدث الجريمة نتيجة خطأ برمجي من مبرمج الذكاء الإصطناعي الذي يجعل الذكاء الإصطناعي يصدر خطأ يتسبب في جرائم جنائية، فالهدف الأسمى لأي منتج هو تحقيق أعلى ربح ممكن، دون مراعاة لأي أبعاد أخرى أو أضرار قد يحدثها عدم مراعاة الجودة في منتجه، ودور التشريعات هو تحديد المعايير التي يجب توافرها في تلك المنتجات بالإضافة إلى تغليظ العقوبات التي توقع عليه عند إرتكابه أي سلوك مجرم في تلك القوانين.

ويجب التأكيد على إحترام الخصوصية، وحقوق المليكة الفكرية، وهما الأكثر تعرضا للإنتهاك في ظل تكنولوجيا الذكاء الإصطناعي وإنتشارها، والسبيل الوحيد

1 يحيى إبراهيم دهشان، مرجع سابق، ص 36.

لحمايتهم سن قوانين تجرم التعدي عليهم أو إنتهاكهم من المنبع أي من منتج تقنيات الذكاء الإصطناعي[1].

الفرع الثاني: المسؤولية الجزائية للمالك أو المستخدم

المالك أو المستخدم هو الشخص الذي يتمتع بتقنيات الذكاء الإصطناعي بإستخدامه والإستفادة من قدراته، ومن المتوقع إن يقوم بإساءة إستخدامه مما يترتب عليه حدوث جريمة معينة يعاقب عليها القانون، ونكون هنا أمام عدة إحتمالات:

- وقوع الجريمة نتيجة سلوك المالك أو المستخدم وحده، فلولا السلوك الذي إرتكبه ما حدثت الجريمة، لقضية الطيار V.U.S IN Klein، حين وضع الطائرة على الطيار الآلي أثناء الهبوط بالرغم من تحذير اللوائح من إستخدامه في ذلك، مما أدى إلى إلحاق ضرر جسيم بالطائرة، وبالتالي حمل مسؤولية تلك الأضرار[2]. وقد يستخدم المالك تقنيات الذكاء الإصطناعي في الإعتداء على الآخرين، وهنا تطبق نظرية الفاعل المعنوي، ويعتبر مستخدم أو مالك الذكاء الإصطناعي فاعلا معنويا والذكاء الإصطناعي مجرد أداة سخرت بيد الجاني لإرتكاب جريمته.

- حدوث الجريمة نتيجة سلوك المالك بالإشتراك مع أحد الأطراف الأخرى، مثال ذلك إستعانة مالك الروبوت بشخص متخصص لتغيير أوامر التشغيل، لإستخدامه في إرتكاب جريمة، ونفي المسؤولية الجنائية عن نفسه وإلصاقها بالروبوت ومصنعه. وفي هذه الحالة، تكون المسؤولية الجنائية مشتركة بين مالك الروبوت والشخص الذي ساعده في تغيير أوامر التشغيل، وتطبق أحكام المساهمة الجنائية في قانون العقوبات.

ويرى جانب من الفقه إن مسؤولية مالك الذكاء الإصطناعي، مسؤولية مفترضة في الجرائم المرتكبة بإستخدام الذكاء الإصطناعي الذي يقع بحوزته، وعليه هو إثبات العكس[3].

الفرع الثالث: المسؤولية الجزائية للطرف الخارجي

التطور المطروح في هذه الحالة، هو قيام طرف خارجي بالدخول على نظام الذكاء الإصطناعي، عن طريق إختراقه بأي طريقة والسيطرة عليه وإستغلاله في إرتكاب

1 يحيى إبراهيم دهشان، مرجع سابق، ص 37.

2 S. Singh, Attribution of legal personhood to artificially intelligent beings, Bharti Law review, July–Sept – 2017, P 199.

3 يحيى إبراهيم دهشان، مرجع سابق، ص 30.

الجريمة، كما في حالة الدخول غير المشروع لنظام الكمبيوتر، وزراعة الفيروسات أو الإستيلاء على البيانات المخزنة عليه[1].

في هذه الحالة نكون امام فرضين، وهما:

الفرض الأول قيام الطرف الخارجي بإستغلال ثغرة في الذكاء الإصطناعي لإرتكاب جريمته، وكانت تلك الثغرة ناتجة عن إهمال المبرمج أو المصنع أو المالك، كإستغلال ثغرة في برمجة الدرونز التجارية لتحويلها لسلاح وإطلاق النار على أشخاص، فتكون المسؤولية الجنائية مشتركة بين الطرف الخارجي والشخص الذي وقع منه الإهمال في تأمين تلك الثغرة[2].

الفرض الثاني قيام شخص متخصص في إستغلال الثغرات الموجودة دون إهمال من المالك أو من المصنع، فتقع المسؤولية الجنائية كاملة على هذا الطرف الخارجي، كإختراق الطرف الخارجي للسحابة الإلكترونية لتخزين وإرسال الأوامر من خلالها لتقنية الذكاء الإصطناعي، وقيامه بإصدار أوامر بإرتكاب جريمة، كإعطاء أمر برمجي بالإعتداء على أشخاص يحملون صفات معينة (لون بشرة، جنس معين، نساء، رجال...إلخ).

الفرع الرابع: المسؤولية الجزائية لكيان الذكاء الإصطناعي نفسه

يعتبر الحديث عن إرتكاب الذكاء الإصطناعي لجريمة من تلقاء نفسه بدون خطأ برمجي، أو نتيجة حدوث تطور ذاتي في نظامه القادر على التفكير وإصدار القرارات ضربا من الخيال في الوقت الحالي، ولكن قد يحدث ذلك في المستقبل القريب، لذا يجب وضع هذه الإحتمالية والتفكير بها ووضع حلول لها من الآن.

إن التطورات المذهلة التي تشهدها تقنيات الذكاء الإصطناعي أدت لوصوله إلى مرحلة الإدراك الإصطناعي، والقدرة على التعلم الذاتي والتحليل والتمييز وإتخاذ القرارات بإستقلالية عن البشر، والتحاور مع البشر وفهم لغتهم وتركيب إجابات منطقية تحاكي إجاباتهم[3]. هذه الطبيعة المتطورة جدا قد تسبب وقوع الآلة في إرتكاب الأفعال المجرمة ولو عن طريق الخطأ، كقضية جهاز المحادثة Tay لشركة مايكروسوفت عام

1 محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت - دراسة مقارنة، دار الفكر والقانون، المنصورة، مصر، 2012، ص 17.

2 يحيى إبراهيم دهشان، المرجع نفسه، ص 33.

3 Sophia Hanson, Robotics, available at : www.hansonrobotics.com/sophia, Viewed on 03/05/2024 at 21 :31.

2016، الذي أرسل آلاف الرسائل الالكترونية في ثماني ساعات عبر منصة Twitter، تنطوي على جرائم عنصرية ومخالفة القانون[1].

أصبح الآن من المتصور إرتكاب الجرائم من قبل الذكاء الإصطناعي بنفسه، وهناك فرضين في هذه الحالة، وهما:

الفرض الأول في حالة إرتكاب الجريمة نتيجة الخطأ في برمجة الذكاء الإصطناعي، وهنا تقع المسؤولية على المصنع أو المبرمج كما تحدثنا من قبل.

الفرض الثاني وفيه يستفحل الخطر ويزداد الضرر، فإذا ما كان الذكاء الإصطناعي يتمتع بإستقلالية كاملة نتيجة تطوير نفسه بالتعلم الذاتي، ويتخذ قرارات ذاتية خارجة عن النظام البرمجي، ليسيطر ذاتيا على نفسه، فيكون السلوك المجرم المرتكب من قبله نابعا عن قراراته الذاتية، فهنا تكون المسؤولية الجنائية مباشرة وواقعة على الذكاء الإصطناعي وحده.

مما سبق، يتضح أنه إذا ما توافر لدى الذكاء الإصطناعي القدرة على تطوير نفسه بالتعلم الذاتي، والوصول إلى مرحلة الإستقلال في إتخاذ القرار والتصرف بإستقلالية -أي وصوله إلى ما يسمى بالإدراك الإصطناعي-، سنكون أمام شخص قانوني جديد مسؤول من الناحية الجنائية، فما كان منذ سنوات محض خيال مؤلفين ومفكرين، أصبح الآن واقعا ملموسا، خاصة مع وجود بعض تقنيات الذكاء الإصطناعي حاليا تتحلى بجانب من ذلك.

المطلب الثاني: أبرز جرائم الذكاء الإصطناعي في التشريع الجزائري

"لا جريمة ولا عقوبة إلا بنص"، وهو مبدأ الشرعية الذي أقره الدستور وكرسته المادة الأولى من قانون العقوبات. ونظرا للتطور في مجال تقنيات الذكاء الإصطناعي وإنتشار جرائم مستحدثة بإستخدامه وتزايد مخاطره، أصبح ضروريا تعديل النصوص التشريعية بما يتلائم معها حتى تساير تطور الجرائم طرق إرتكابها بالتكنولوجيات الحديثة.

والمشرع الجزائري وكغيره من التشريعات، لم يحط جرائم الذكاء الإصطناعي بقوانين خاصة تكفل معالجة هذا النوع من الجرائم، وإكتفى بمعالجة الجرائم الناجمة عن إستخدام تقنيات الذكاء الإصطناعي كجريمة التزوير الإلكتروني مثلا، وفق مقاربتها إلى جرائم التزوير التقليدية المنصوص عليها في قانون العقوبات والقوانين المكملة له.

سنتناول في هذا المطلب عقوبات أبرز الجرائم بإستخدام الذكاء الإصطناعي.

1 E. Lavallée, Lorsque l’intelligence artificielle est discriminatoire, Journal le droit de savoir, Available at : https://www.lavery.ca/fr/publications/nos-publications/3013-lorsque-lintelligence-artificielle-est-discriminatoire.html, Viewed on 03/05/2024 at 19 :55.

الفرع الأول: التلاعب بالمعطيات

يعد التلاعب بالمعطيات من أهم صور الإستخدام غير المشروع للذكاء الإصطناعي، وهي قيام المستخدم بإدخال أو تعديل المعطيات إلى منظومة ما بلغش أو الإزالة أو التعديل عليها بما يؤدي لتغيير حالتها. ونص المشرع الجزائري على هاته الجريمة في المادة 394 مكرر 1 من ق.ع.ج، وسنتناول في مايلي أركانها والعقوبات المقررة لها.

أولا: أركان جريمة التلاعب بالمعطيات

1) الركن المادي

يتكون الركن المادي لجريمة التلاعب بالمعطيات من سلوك إجرامي يتمثل في إدخال أو تعديل أو إزالة المعطيات، ما يؤدي إلى نتيجة إجرامية تتمثل في تغيير حالة المعطيات[1].

ويكون الإدخال بإدراج خصائص ممغنطة جديدة على الدعامات الموجودة فارغة كانت أو تحتوي خصائص ممغنطة قبل الإدخال، أي إضافة معطيات جديدة غير مصرح بإدخالها[2]. ويكون التعديل بتغيير حالة المعطيات الموجودة بدون تغيير الطبيعة الممغنطة لها، أو بالتغيير غير المشروع للمعلومات عن طريق إستخدام إحدى وظائف الحاسب الآلي[3]. وتكون الإزالة بإقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق محوها أو طمسها، أي ضغط خصائص أخرى فوقها بخصائص جديدة تطمس الخصائص القديمة، أو بتحويل ورص خصائص مزالة في منطقة محفوظة من الذاكرة[4].

2) الركن المعنوي

1 محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 185.

2 Ibtissem Maalaoui, Les infractions portant atteinte à la sécurité du système informatique d'une entreprise, Mémoire présenté en vue de l'optention du grade Maitrise en droit (LLM) option droit des affaires, Faculté des études supérieures, Université de Montréal, Canada, 2011, P. 71-72.

3 نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، مصر، 2003، ص 220.

4 Ibtissem Maalaoui, Op. Cit., P. 72-73.

جريمة التلاعب بالمعطيات جريمة عمدية لابد لقيامها توافر القصد الجنائي لدى مرتكبها، وفي حال عدم وجود قصد جنائي فلا يعاقب الجاني على تعديل وإزالة المعطيات غير العمديين، إلا إذا كانا نتيجة دخول أو بقاء غير مصرح بهما كما سبق بيانه.

ثانيا: العقوبات الأصلية المقررة لجريمة التلاعب بالمعطيات

نص المشرع الجزائري في قانون العقوبات على عقوبات أصلية لجريمة التلاعب بالمعطيات في المادة 394 مكرر 01 منه، تتمثل في الحبس من 6 أشهر إلى 3 سنوات، وبغرامة مالية تتراوح ما بين 500 ألف كحد أدنى و مليوني دينار جزائري كحد أقصى.

الفرع الثاني: الدخول أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات

تعتبر هذه الجريمة من أهم الجرائم وأكثرها خطورة إذ أنها تشكل طريقا لإرتكاب جرائم أخرى، فالجاني بعد تمكنه من دخول الأنظمة المعلوماتية سيجد سبيله إلى إرتكاب جرائم أخرى. وتقوم هذه الجريمة بمجرد الولوج إلى المعلومات أو المعطيات المخزنة داخل النظام بدون رضى أو إرادة المسؤول عنها.

حيث نصت المادة 394 مكرر من ق.ع.ج على هاته الجريمة، وسنتطرق إلى بيان أركانها والعقوبات المقررة لها في الآتي:

أولا: أركان جريمة الدخول أو البقاء غير المصرح به

حرص المشرع الجزائري على تجريم كل تواجد عمدي غير مشروع داخل أنظمة المعالجة الآلية للمعطيات، سواء أدى إلى نتيجة معينة أو لم يؤدي إلى ذلك، وفيما يلي الركن المادي والمعنوي لهذه الجريمة.

1) الركن المادي

تقوم هذه الجريمة على سلوك إجرامي يتخذ إحدى صورتين إما الدخول أو البقاء، ولم تنص المادة 394 مكرر على تعريف الدخول أو البقاء، وهناك من عرف الدخول غير المصرح به بأنه الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضى المسؤول عن هذا النظام، أو إساءة إستخدام الحاسب الآلي ونظامه من شخص غير مرخص له بإستخدامه والدخول إليه، للوصول إلى المعلومات والمعطيات المخزنة بداخله للإطلاع عليها أو التسلية، أو لإشباع الشعور بالنجاح في إختراق الحاسب الآلي [1].

أما البقاء فيعرف بأنه التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، أو هو عدم وضع حد للتشعب داخل النظام مع الاعتقاد بأن ذلك يشكل خطأ[2]. فالبقاء يتمثل في عدم قطع الفاعل للاتصال بالنظام عند إدراكه إن وجوده فيه غير مشروع، فمن صور البقاء إستمرار وجود الجاني داخل النظام بعد المدة المحددة له، ومن صوره أيضا تلك الحالة التي يجد الجاني فيها نفسه داخل نظام المعالجة الآلية للمعطيات بدون قصد منه، كأن يكون الدخول قد تم عن طريق الصدفة بدون إرادة من الداخل، لكنه بعد إكتشافه بأنه داخل النظام يبقى فيه ولا يخرج منه في الوقت الذي كان يجب عليه مغادرته [3].

ولا يشترط صفة معينة في من يقوم بالدخول أو البقاء، وقد عبرت عن ذلك المادة 394 مكرر بقولها: "كل من يدخل أو يبقى..."، كما لا يشترط إن يتم الدخول بطريقة معينة، لأن المادة السابقة جاءت شاملة وعامة.

هذا بالنسبة للسلوك الإجرامي في هذه الجريمة، أما بالنسبة للنتيجة الإجرامية فلا تتطلب المادة 394 مكرر تحقق نتيجة معينة حتى تقوم الجريمة، وإنما تقوم هذه الأخيرة بمجرد توافر السلوك الإجرامي المتمثل في الدخول أو البقاء، لكن إذا ما ترتب على الدخول أو البقاء نتائج محددة فإن المشرع قد رتب على ذلك تشديد العقوبة كما سنراه فيما

1 Bainbridge David, hacking the unavthorised access of computer system, The legal implication, Modern Law Review, 1989, Vol 52, P237

2 علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، الإمارات العربية المتحدة، 2000، ص 52.

3 علي عبد القادر القهوجي، المرجع نفسه ص 52.

سيأتي[1]، وهذه النتائج تتمثل في حذف أو تغيير معطيات نظام المعالجة الآلية للمعطيات أو تخريب هذا النظام.

2) الركن المعنوي

تنص المادة 394 مكرر صراحة على وجوب كون جريمة الدخول أو البقاء غير المصرح بهما جريمة عمدية، ويستشف ذلك من قولها: "كل من يدخل أو يبقى عن طريق الغش"، والحقيقة إن المنطق يحتم إن تكون هذه الجريمة غير عمدية، لأن عمليات الدخول إلى أنظمة الحاسبات الآلية والبقاء فيها هي عمليات تتكرر بشكل مذهل في اليوم الواحد وتقع من عدد هائل من المستخدمين، لاسيما مع إرتفاع عدد مرتادي شبكة الأنترنت، وليس من المستبعد في ظل كل هذه الحركة دخولا وخروجا إن تكون هناك عمليات دخول أو بقاء غير مصرح بهما لكنها غير عمدية، لهذا وجب إن تكون الجريمة غير عمدية حتى يقع هؤلاء تحت طائلة العقاب، وذلك من أجل الموازنة بين خصوصية الأنظمة المعلوماتية وحماية حرية الأفراد في إستخدام الأنترنت[2].

وبالنسبة للظروف المشددة لهذه الجريمة، أو النتيجة المشددة فلا بد إن تكون غير عمدية، لأنها لو كانت عمدية ستشكل جريمة أخرى هي جريمة التلاعب بالمعطيات، كما رأيناه سابقا.

ثانيا: عقوبة جريمة الدخول أو البقاء غير المصرح بهما

تتخذ جريمة الدخول أو البقاء غير المصرح بهما صورتان لكل واحدة منهما عقوبتها، الأولى بسيطة أو مجردة والثانية مشددة.

1) عقوبة الجريمة في صورتها المبسطة

إذا كانت الجريمة لم تؤد إلى إعاقة أو إفساد نظام المعالجة الآلية للمعطيات أو إزالة أو تعديل لهذه الأخيرة فإن العقوبة الأصلية تكون الحبس من 3 أشهر إلى سنة والغرامة من 50 ألف إلى 100 ألف دينار جزائري.

2) عقوبة الجريمة في صورتها المشددة

1 محمد خليفة، مرجع سابق، ص 159.

2 محمد خليفة، المرجع نفسه، ص 162-163.

تشدد الفقرة الثانية والثالثة من المادة 394 مكرر عقوبة جريمة الدخول أو البقاء غير المصرح بهما، إذا أدت إلى تخريب نظام إشتغال منظومة المعالجة الآلية للمعطيات أو حذف أو تغيير لهذه الأخيرة، وتشدد إلى ضعف تلك المقررة للجريمة في صورتها المجردة أو البسيطة، سواء في حدها الأدنى الذي يتضاعف إلى 06 أشهر، أو في حدها الأقصى الذي يتضاعف إلى سنتين، أما الغرامة فيثبت حدها الأدنى عند 50 ألف دينار جزائري ويرتفع حدها الأقصى إلى 150 ألف دينار جزائري.

وإذا أدى الدخول أو البقاء غير المصرح بهما إلى تخريب النظام، فالغرامة تشدد للضعف أي تتراوح بين 100 ألف و 200 ألف دينار جزائري.

الفرع الثالث: إنتهاك الخصوصية

تعتبر الخصوصية من الحقوق الأساسية للفرد والتي يعد إنتهاكها جريمة تستلزم العقاب، والإستخدام غير المشروع للذكاء الإصطناعي يستهدف بصفة رئيسية الخصوصية عن طريق الإختراقات والتزييف العميق وإنتحال الهوية أو إلتقاط أو تسجيل أو نقل المكالمات والأحاديث والصور الخاصة أو السرية بغير إذن صاحبها.

والمشرع الجزائري لم يفرق بين إنتهاكات الخصوصية على أساس الوسيلة، إذ نصت المادة 303 مكرر بعبارة: "...بأي تقنية كانت..."، ومن خلال عدم تحديد المشرع للتقنية المستخدمة في ذلك نستطيع القول إن تقنية الذكاء الإصطناعي تدخل ضمنها[1].

وسنتعرض في مايلي إلى أركان هاته الجريمة وعقوباتها المنصوص عليها.

أولا: أركان جريمة إنتهاك الخصوصية

1) الركن المادي

جريمة إنتهاك الخصوصية من الجرائم المادية، والتي يشترط لإكتمال نموذجها القانوني توافر النشاط الإجرامي والنتيجة الإجرامية والعلاقة السببية بينهما، بالإضافة إلى عنصر أخر وهو إن يتم السلوك من غير إذن أو رضا الضحية.

يكون الركن المادي لجريمة إنتهاك الخصوصية بالإلتقاط أو التسجيل أو النقل أو الفشاء للمكالمات أو الأحاديث أو الصور أو المعلومات الشخصية بغير رضى صاحبها وبأي وسيلة كانت، ما يؤدي إلى إنتهاك خصوصية الأشخاص.

1 رواحنة نادية، رواحنة زوليخة، جريمة إنتهاك حرمة المكالمات أو الاحاديث الخاصة أو السرية في قانون العقوبات الجزائري، مجلة المفكر، المجلد 17، العدد 02، 2022، ص315.

2) الركن المعنوي

إن جريمة إنتهاك الخصوصية من الجرائم العمدية، التي يشترط المشرع لإكتمالها توفر القصد الجنائي العام بعنصريه العلم والإرادة، وهذا ما جاء في نص المادة 303 مكرر بعبارة: "...كل من تعمد..."، بمعنى إن ينصرف علم الجاني لطبيعة الخصوصية المنتهكة، إعتمادا على معيار المكان الذي تمت فيه أو موضوعها، كما يجب إن ينصرف علمه إلى عدم وجود المسوغ القانوني لفعله، وإتجاه إرادته إلى النتيجة الإجرامية[1].

وهناك إتجاه في الفقه يرى بأنه لابد من توفر القصد الجنائي الخاص أيضا المتمثل في الباعث، أي إتجاه إرادة الجاني إلى الإعتداء على حرمة الحياة الخاصة للغير بالإنتهاك أو المساس بها، لأن المشرع إشترط تعمد المساس بحرمة الحياة الخاصة للأفراد أثناء إتيان تلك الأفعال الإجرامية، مما يعني أنه إشترط توافر القصد الجنائي الخاص[2].

ثانيا: العقوبات الأصلية المقررة لجريمة إنتهاك الخصوصية

نص المشرع الجزائري في قانون العقوبات على العقوبات الأصلية لجريمة إنتهاك الخصوصية في المادة 303 مكرر، تتمثل في الحبس من 6 أشهر إلى 3 سنوات، وبغرامة مالية تتراوح ما بين 50 ألف كحد أدنى و 300 ألف دينار جزائري كحد أقصى.

ولم ينص المشرع على الظروف المشددة لهاته الجريمة، وكان حري به إن يشدد في العقاب لتوافر شروط وظروف معينة، كصفة الجاني مثلا.

الفرع الرابع: التزوير الإلكتروني

تعتبر جريمة التزوير الإلكتروني من الجرائم الإلكترونية التي ترتكب بواسطة الحاسب أو شبكات الإتصال أو الأنترنت. وقد عرفها علي عبد القادر القهوجي بأنها: "تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي عن طريق الطابعة أو كانت مرسومة عن طريق الراسم، ويستوي في المحرر الإلكتروني إن يكون مدونا باللغة العربية أو أية لغة أخرى لها دلالة، وقد تتم في

1 نبيل صقر، الوسيط في شرح جرائم الأشخاص، دار الهدى، الجزائر، 2009، ص 177.

2 محمد أمين خرشة، مشروعية الصوت والصورة في الإثبات الجنائي، الإصدار الأول، دار الثقافة للنشر والتوزيع، الأردن، 2001، ص 261.

مخرجات ورقية أو محفوظة على دعامة، ويشترط إن يكون المحرر الإلكتروني ذو أثر في إثبات حق أو أثر قانوني"[1].

وسنتناول فيما يلي أركانها والعقوبات المقررة لها.

أولا: أركان جريمة التزوير الإلكتروني

جريمة التزوير الإلكتروني جريمة مستحدثة، لم يأطرها المشرع الجزائري بقانون خاص يتماشى مع تطور طرق إرتكابها التي تعتمد على التكنولوجيات الحديثة وتقنيات الذكاء الإصطناعي، وإكتفى بمعالجتها وفق جريمة التزوير التقليدية في قانون العقوبات والقوانين المكملة له. وسنتناول في مايلي الركن المادي والمعنوي لهاته الجريمة.

1) الركن المادي

الركن المادي لجريمة التزوير الإلكتروني لايخرج عن صور الركن المادي في التزوير التقليدي، إلا أنه يختلف عنه من حيث محله والطرق التي يتم بها، فجوهر التزوير في كلاهما هو تغيير الحقيقة. ويقع التزوير في النطاق المعلوماتي عن طريق تغيير الحقيقة المثبتة على الشريط الذي يمثل مخرجات الحاسب الآلي، شريطة حصول الضرر وإهتزاز الثقة المفترضة في المحررات الرسمية أو العرفية[2].

وينصب تغيير الحقيقة كصورة من صور الركن المادي لجريمة التزوير الإلكتروني على البيانات مهما كانت صورا أو رموزا أو علامات بإستخدام الحاسوب. وتغيير الحقيقة يتم بنشاط إيجابي فلا يتصور إن يتحقق بنشاط سلبي إلا أذا ترتب عن الترك تغييرا جوهريا سبب ضررا للغير[3].

ويكون المحرر الإلكتروني محل هاته الجريمة، والمحرر الإلكتروني هو كل معلومة تم إنشائها أو إرسالها أو تخزينها أو إستلامها بأي دعامة، مادامت تتضمن إثبات

1 حفصي عباس، جرائم التزوير الإلكتروني، دراسة مقارنة لنيل شهادة دكتوراه العلوم الإسلامية، تخصص شريعة وقانون، جامعة وهران 1، وهران، 2014-2015، ص 18.

2 محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والانترنت، موسوعة جرائم المعلوماتية، منشأة المعارف بالإسكندرية، مصر، 2006، ص 178-179.

3 حفصي عباس، مرجع سابق، ص 62.

واقعة أو تصرف قانوني، ويتضمن توقيع إلكتروني ينسب هذه الواقعة أو التصرف لشخص معين[1].

نصت المادة 31 من قانون 24-02 المؤرخ في 2024/02/26 والمتعلق بمكافحة التزوير وإستعمال المزور على سبيل الحصر، على طرق التزوير والذي يكون إما بتقليد أو تزييف الكتابة أو التوقيع، وإما بإصطناع إتفاقات أو نصوص أو إلتزامات أو مخالصات أو بإدراجها في تلك المحررات، وإما بإضافة أو بإسقاط أو بتزييف شروط وإقرارات أو وقائع أعدت هذه المحررات لتلقيها أو لإثباتها، وإما بإنتحال شخصية الغير أو الحلول محلها.

2) الركن المعنوي

جريمة التزوير الإلكتروني من الجرائم العمدية التي يجب توافر القصد الجنائي العام فيها، أي تتجه إرادة الجاني إلى إرتكاب الجريمة مع العلم بأركانها، وإدراكه بأن الفعل الصادر عنه من شأنه تغيير الحقيقة الذي يسبب ضرر حالا أو محتملا. فجريمة التزوير الإلكتروني التي تتم عن طريق الحاسب الآلي يجب إن يكون فيها الجاني عالما بأنه يغير الحقيقة في المحرر المعلوماتي، وأن هذا التغيير من شأنه إحداث ضرر محقق أو من المحتمل حدوثه، فلا مجال للتزوير إذا ثبت إن الجاني قد أهمل تحري الحقيقة فإذا أثبت أنه يجهل بأمر تزويره، أو أنه كان يجهل تحريره فينتفي القصد الجنائي[2].

كما تتطلب أيضا توافر القصد الجنائي الخاص، ويتمثل في نية الجاني فيما يريد تحقيقه بإرتكابه جريمة، ويظهر ذلك أكثر في التزوير المعنوي الذي تطرقنا له سالفا. فالركن المعنوي يتطلب توافر قصد جنائي لدى الجاني يتمثل في تزييف جوهر المحررات أو ظروفها بالغش، أو إقتران العلم بنية الغش وإستعمال المزور فيما زور من أجله، ولا يعتد بعد ذلك بالباعث الدافع للتزوير ولا بالغاية التي يقصدها المزور إلا أنه إذا حدث ذلك التزوير نتيجة غلط أو إهمال أو جهل بحقيقة الوقائع فلا تقوم الجريمة[3].

ثانيا: العقوبات الأصلية المقررة لجريمة التزوير الإلكتروني

1 محمد أمين الرومي، المستند الإلكتروني، دار الكتب القانونية، المحلة الكبرى، مصر، 2008، ص 55.

2 حفصي عباس، مرجع سابق، ص 78

3 بلحاج العربي، أبحاث ومذكرات في القانون والفقه الإسلامي، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، 1996، ص 525.

نصت المادة 31 من ق.م.ت.إ.م، على الحبس من 10 سنوات إلى 20 سنة وبغرامة من مليون إلى مليوني دينار جزائري، لكل من إرتكب تزويرا في محررات عمومية أو رسمية. ونصت المادة 32 على تشديد العقوبة بالسجن المؤقت من 20 سنة إلى 30 سنة، إذا كان الجاني قاضيا أو موظفا عموميا أو ضابطا عمومي.

الفرع الخامس: الأحكام المشتركة للجرائم المعلوماتية

هناك العديد من الأحكام القانونية التي تشترك فيها كل الجرائم المعلوماتية، هذه الأحكام المشتركة منها مايتعلق بالجرائم وبنيانها ومنها ما يتعلق بعقوبة تلك الجرائم.

أولا: الأحكام المتعلقة بالجرائم

الأحكام المشتركة المتعلقة بالجرائم السالفة الذكر نصت عليها المادة 394 مكرر 05، حيث يعاقب بالعقوبة المقررة للجريمة ذاتها على المشاركة في مجموعة أو في إتفاق تألف، بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في قسم المساس بأنظمة المعالجة الآلية للمعطيات، وجسد ذلك التحضير بفعل أو عدة أفعال مادية.

كما نصت المادة 394 مكرر 07 على أنه يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في ذات القسم بالعقوبات المقررة للجنحة ذاتها.

ثانيا: الأحكام المتعلقة بالعقوبة

نصت كل من المواد 394 مكرر 3 ومكرر 4 ومكرر 6، على أحكام مشتركة تتعلق بالعقوبة في الجرائم المنصوص عليها في قسم المساس بأنظمة المعالجة الآلية للمعطيات، وتتمثل في ثلاثة أحكام تتعلق بالعقوبة.

أولها تتمثل في تشديد العقوبة بنص المادة 394 مكرر 3، إلى الحبس من سنتين إلى 10 سنوات وبغرامة من 700 ألف إلى مليوني دينار جزائري، إذا إرتكبت تلك الجرائم ضد مؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق العقوبات الأشد.

والثانية بخصوص تشديد العقوبة للشخص المعنوي، إذ نصت المادة 394 مكرر 4 على مضاعفة الغرامة إلى 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

أما الأخيرة فتتعلق بأحكام العقوبات التكميلية المنصوص عليها في المادة 394 مكرر 6، حيث تشترك كل جرائم المساس بأنظمة المعالجة الآلية للمعطيات في نفس العقوبات التكميلية، وتتمثل في مصادرة الأجهزة والبرامج والوسائل المستعملة في

الجريمة مع إغلاق المواقع محل تلك الجريمة، بالإضافة إلى إغلاق المحل أو مكان الإستغلال إذا إرتكبت الجريمة بعلم مالكها.

كما نصت المادة 14 على جواز القضاء بالحرمان من ممارسة حق أو أكثر من الحقوق الوطنية المنصوص عليها في المادة 9 مكرر 1، لمدة لا تتجاوز 5 سنوات تسري من يوم إنقضاء العقوبة السالبة للحرية أو الإفراج عن المحكوم عليه.

كما يجوز للجهة القضائية القضاء بنشر حكم الإدانة كاملا أو ملخص منه في الصحف التي تعينها أو بتعليقه في الأماكن التي تبينها.

خلاصة الفصل

يعد الذكاء الإصطناعي أبرز ما وصل إليه العقل البشري من تطور، ويعتبر الذكاء الإصطناعي من المصطلحات التي لم يتماشى الفقهاء على تعريف واحد لها، كما أغفلت التشريعات الداخلية للدول ذات الصلة وضع تعريف صريح له، على غرار المشرع الجزائري الذي لم يتطرق إلى تعريفه، بل نظم الميادين المستخدم فيها كالتجارة الإلكترونية.

ويتميز الذكاء الإصطناعي عن غيره من التقنيات بخصائص منفردة، تظهر من خلال إستخدامه في مجالات وميادين حيوية عديدة ومختلفة، كالطب والتعليم والتسويق وغيرها.

وكغيره من التكنولوجيات لا تخلو تقنيات الذكاء الإصطناعي من السلبيات والمخاطر، لعل أهمها إستفحال الجريمة وخاصة الجريمة المنظمة، وظهور جرائم جديدة مستحدثة تعتمد على إستخدام الذكاء الإصطناعي على نحو غير مشروع.

الفصل الثاني
الأحكام الإجرائية للمسؤولية الجزائية
للإستخدام غير المشروع للذكاء الإصطناعي

تمهيد

يشهد العالم تطورا هائلا في شتى المجالات خاصة بعد ظهور تقنيات الذكاء الإصطناعي، ومع إزدياد إستخداما في مختلف الميادين نشأت عنه في المقابل إستخدامات غير مشروعة تهدد الأمن على الصعيدين الداخلي والدولي، الأمر الذي دفع بالسلطات المعنية إلى إتخاذ التدابير التشريعية والإجرائية اللازمة، لمكافحة الجرائم الناشئة عن تلك الإستخدامات غير المشروعة على الصعيد الوطني.

وبالمقابل وعلى الصعيد الدولي، فقد سعت الدول تحت إطار التعاون الدولي إلى وضع آليات لمواجهة هذا النوع من الجرائم بإعتبار أنه يتعدى الحدود الوطنية.

من خلال ما تقدم، سنتناول في هذا الفصل خصوصية الإجراءات الجزائية في جرائم إستخدام الذكاء الإصطناعي كمبحث أول، والآليات الدولية لمكافحة جرائم إستخدام الذكاء الإصطناعي كمبحث ثاني.

المبحث الأول: خصوصية الإجراءات الجزائية في جرائم إستخدام الذكاء الإصطناعي

نظرا لخصوصية جرائم الذكاء الإصطناعي، والتي تنفرد بطابع خاص يميزها عن باقي الجرائم التقليدية لما لها من خصائص تقنية حديثة، تجعل الإجراءات العادية المتبعة في عموم هاته الجرائم لا تنطبق عليها، مما أدى بالمشرع الجزائري بأن يخصها بإجراءات تتلائم وطبيعتها للكشف عنها وإلقاء القبض على مرتكبيها، وهذا ما قد جسده في تعديله لقانون الإجراءات الجزائية من خلال القانون 04-14 المؤرخ في 10 نوفمبر 2004، وكذا بالقانون 06-22 المؤرخ في 20 ديسمبر 2006.

ومع تفشي جرائم المعلوماتية وإستفحالها إستحدث المشرع القانون 09-04 المؤرخ في 5 أوت 2009، والذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

بناءا على ماسبق، سنتطرق من خلال هذا المبحث في المطلب الأول إلى إجراءات التحقيق الأولي في جرائم إستخدام الذكاء الإصطناعي، ثم نتطرق في المطلب الثاني إلى الإجراءات المستحدثة لمواجهة جرائم إستخدام الذكاء الإصطناعي.

المطلب الأول: إجراءات التحقيق الأولي في جرائم إستخدام الذكاء الإصطناعي

إن البيئة المعلوماتية للذكاء الإصطناعي والتي تختلف تماما على البيئة التقليدية للجرائم، تستدعي ضرورة تطوير أساليب التحقيق لمواجهة هذا النوع من الإجرام الحديث، خاصة وأن صفة الجناة تختلف أيضا عن غيرهم من الجناة في الجرائم التقليدية لما لهم من دراية وخبرة في المجال التقني، ما يستدعي كذلك إن يقابله خبرة المحقق لمواجهتهم.

ويستند التحقيق الجنائي في مجال الجرائم المعلوماتية على دعامتين أساسيتين، الأعوان المكلفون بالتحري وجمع الأدلة ووسائل التحري وجمع الأدلة، وهذا ما سنتناوله في هذا المطلب من الدراسة.

الفرع الأول: الأعوان المكلفون بالتحري وجمع الأدلة

منح القانون لجهاز الضبطية القضائية سلطة الكشف والتحري عن الجرائم بحكم أنها صاحبة الإختصاص الأصيل في التحري عن الجرائم، كما ألزم مقدمي الخدمات مساعدة السلطات العمومية في الكشف عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات. والإستعانة بالشرطة العلمية التقنية لتحصيل الأدلة الجنائية، وأجهزة الدرك الوطني لدعم أعمال البحث والتحقيق.

أولا: جهاز الضبطية القضائية

أعضاء الشرطة القضائية هم موظفون منحهم القانون صفة الضبطية القضائية وخولهم حقوق، وألزم عليهم جملة من الواجبات في عملية التحري عن الجرائم والفاعلين فيها وجمع الإستدلالات عنها[1].

ومن أهم التدابير التي يتم إتخاذها مسبقا لتجنب وقوع جرائم نظام المعالجة الآلية للمعطيات ورصد مرتكبها أولا بأول، مراقبة الإتصالات الإلكترونية[2]، ونجد إن المشرع الجزائري رغم تأكيد حمايته لسرية الإتصالات والمراسلات بكل أنواعها، منح إستثناءا السلطة القضائية وفي إطار قرار معلل، ممارسة إجراءات من شأنها المساس والتعرض للبيانات الشخصية نظرا لخطورة بعض الجرائم المعلوماتية المحددة حصرا، تسجيل الإتصالات الإلكترونية في حينها[3].

حيث نصت المادة 3 من القانون 09-04 على: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات والتحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراء التفتيش والحجز داخل منظومة معلوماتية".

ولا يسمح باللجوء إلى الإجراء المنصوص عليه في المادة السالفة الذكر، إلا في الحالات الإستثنائية والتي جاءت على سبيل الحصر في المادة 04 من ذات القانون وهي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الماسة بأمن الدولة.

- في حالة وجود معلومات عن إمكانية الإعتداء على منظومة معلوماتية بطريق يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

1 عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، 2018، ص 137.

2 الطيبي البركة، دراسة مقارنة، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر، 2021، ص 248.

3 آمنة أمحمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الأعمال، أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز البحث العلمي، الجزائر، 29 مارس 2017، ص 57.

- مقتضيات التحريات والتحقيقات القضائية عند صعوبة الوصول إلى نتيجة تفيد الأبحاث الجارية دون اللجوء إلى الرقابة الإلكترونية، في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبأدلة.

ولا تتم إجراءات عملية المراقبة للحالات المذكورة أعلاه إلا بوجود إذن كتابي من السلطة القضائية المختصة[1]. كما إن الرقابة السرية الإلكترونية للإتصالات ومن ضمنها المحادثات الهاتفية، لا يمكن إعتبارها نوع من أنواع التفتيش، وذلك لأن المراقبة الإلكترونية ترد على البيانات الإلكترونية المتحركة التي تتجسد هنا بالإتصالات الإلكترونية حال إجرائها، في حين إن التفتيش إنما يرد فقط على البيانات الإلكترونية الساكنة والمخزنة[2].

1 راجع المادة 613 من قانون 09-04 تتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

2 الطيبي البركة، مرجع سابق، ص 250 و 251.

ثانيا: مقدمي الخدمات

لمقدمي الخدمات دور هام في البحث والتحري للكشف عن جرائم تكنولوجيا الإعلام والإتصال ومكافحتها، ولقد عرفت المادة 2/4 القانون 09-04 مقدمي الخدمة بأنهم: أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو للإتصالات[1]، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها.

وأورد المشرع مجموعة من الإلتزامات على عاتق مقدمي الخدمات وبالمقابل أدرج عقوبات جراء الإخلال بهذه الإلتزامات وتتمثل في:

1- إلتزامات مقدموا الخدمات

- الإلتزام بحفظ المعطيات المتعلقة بحركة السير ومساعدة السلطات القضائية بشكل يسمح بالتعرف على الأشخاص المساهمين في إنشاء المحتويات على الأنترنت (المدونات، والإعلانات في مواقع البيع عن طريق المزاد...) وذلك من أجل التبليغات المحتملة للسلطات القضائية أو في حالة عطب هذه الأخيرة لأجل التحريات أو المعاينات[2].

- الإلتزام بتصفية المواقع وبيان نوعها طبقا للمادة 12 من القانون 09-04 بـ:

* التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

* وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

2- جزاء الإخلال بإلتزام حفظ المعطيات

نصت المادة 10/01 من القانون 09-04 بأنه على مقدمي الخدمات تقديم المساعدة للسلطة المكلفة بالتحريات المعطيات المتعلقة بمحتوى الإتصالات في حينها، حيث إن المسؤولية الجزائية قائمة إذا كانت هناك عرقلة سير التحريات القضائية، ويتم معاقبة

1 نفسها المادة 03-19 من القانون 18-07 يتعلق بحماية الاشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، مؤرخ في 10 جوان 2018، ج.ر.ج.ج عدد 34، مؤرخة في 10 جوان 2018.

2 مريع أحمد مسعود، آليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون رقم 09-04، رسالة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2013، ص 100 و 101.

الشخص الطبيعي بالحبس من 6 أشهر إلى 5 سنوات، وبغرامة من 500 الف إلى 5 ملاين دينار جزائري، أما الشخص المعنوي فيعاقب طبقا لأحكام قانون العقوبات.

ثالثا: الشرطة العلمية والتقنية

أنشئت الجزائر مخابر جهوية للشرطة العلمية في كل من قسنطينة ووهران وبشار وتمنراست وأخر قيد الإنجاز في ورقلة، على مستوى كل منها مصلحة دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية سنة 2004، تتبنى مهام البحث والتحقيق في الجرائم المعلوماتية، ومع إرتفاع عدد القضايا الناتجة عن الإنتشار المتزايد لتقنية المعلوماتية تم ترقيتها إلى دائرة مكونة من ثلاث 03 أقسام فرعية، وهي:

- قسم إستغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.
- قسم إستغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات.

تشمل الدائرة 8 أعضاء محققين 4 منهم عناصر شرطة يتمتعون بصفة الضبطية القضائية، و 4 أعوان ذوي شهادة جامعية في الإعلام الآلي وملمين بالجانب القانوني، يتم تكوينهم دوريا على المستجدات القانونية والتقنية في مجال الإجرام المعلوماتي لضمان فاعلية الآداء في البحث والتحقيق في الجرائم المعلوماتية[1].

ومن أهم ما تقوم به هذه المخابر ضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية في مجال التحريات الإلكترونية، وهذا لا يكون إلا عن طريق التنقيب عن المعطيات المشبوهة والمعلومات الرقمية بجميع أنواعها (ملفات، رسائل إلكترونية، برامج، صور)، هذه العملية تتم من خلال الإستعانة ببرامج وتقنيات خاصة تسمح بلستعادة مختلف المعطيات المحذوفة، والإطلاع على ما تحتويه كل الوسائط الرقمية[2].

ومنه فإن للدائرة فعالية كبيرة في الكشف عن خبايا الجرائم المعلوماتية، عن طريق الإجراءات التي تتخذها في البحث والإستدلال، أو خلال مرحلة التحقيق القضائي.

فعند مرحلة البحث والتحري، عادة ما يستجيب أعضاء الدائرة للطلبات التي يقدمها لهم عناصر الشرطة التابعين لفرق مكافحة الجرائم المعلوماتية الموزعة على كل مديريات الأمن الوطني، أو لطلبات وكيل الجمهورية أو قاضي التحقيق التي تصل إليهم على شكل

1 نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجيستير في القانون، كلية الحقوق والعلوم السياسية، جامعة لخضر، باتنة، الجزائر، 2013، ص 180.

2 مساهمة الشرطة العلمية والتقنية في مجال التحقيقات الجنائية، وثيقة خاصة صادرة عن مديرية الشرطة القضائي، المديرية العامة للأمن الوطني، ص 46.

إنابة قضائية، من أجل مساعدتهم ودعمهم في حجز الأدلة المتواجدة على مسرح الجريمة خلال مرحلة المعاينة.

أما خلال مرحلة التحقيق القضائي فإن دور الدائرة يقتصر على كونه دور خبير، وذلك من خلال إنجاز تقارير خبرة إستجابة لطلبات وكيل الجمهورية وبوجه خاص قاضي التحقيق، كنتيجة لمهام المحققين في تحليل الأدلة المحجوزة ومحاولة إستخراج الأدلة الإلكترونية منها، كتحليل محتوى الأقراص الصلبة للأجهزة المستعملة في الجريمة، أو أجهزة الضحايا، بالإضافة إلى كافة دعامات التخزين الإلكترونية على إختلافها، وكذلك المواقع المستهدفة من قبل المخترقين وصولا إلى تحديد المواقع الجغرافية وعناوين المجرمين، وذلك بمساعدة تقنيات خاصة متطورة ذات جودة عالية[1].

كما تعمل مصالح الدرك الوطني من خلال أجهزتها المركزية على مكافحة الجرائم المعلوماتية ودعم أعمال البحث والتحقيق بشأنها من خلال الهيئات التالية:

1- مديرية الأمن العمومي والإستغلال: تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

2- المصلحة المركزية للتحريات الجنائية: وهي هيئة ذات إختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام والإتصال[2].

3- المعهد الوطني للأدلة الجنائية وعلم الإجرام: وهو مؤسسة عمومية ذات طابع إداري، أنشئت بالمرسوم الرئاسي رقم 183-04 بتاريخ 26 جوان 2004 في إطار عصرنة قطاع الدرك الوطني، ويشكل أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة. ويعد بمثابة هيئة متخصصة في إجراء الخبرات والمعاينة بمختلف دوائره بما فيها دائرة الإعلام الآلي والإلكترونيك، التي أوكلت لها مهام تحليل الأدلة الخاصة بالجرائم المعلوماتية،وتتمثل مهامه الرئيسية في:

- القيام بالخبرات العملية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة بما فيها تلك المتعلقة بالجرائم المعلوماتية.
- مساعدة المحققين في السير الحسن للمعاينات ودعمهم بالأفراد المؤهلين.
- تنفيذ مناهج الشرطة العلمية والتقنية لجمع وتحليل أدلة مسرح الجريمة.

1 نعيم سعيداني، مرجع سابق، ص 181.

2 معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني، ورقلة، الجزائر.

- ضمان المساعدة العلمية في التحريات المعقدة كالتحريات في الجرائم المعلوماتية.

- المشاركة في الأبحاث والتحاليل المتعلقة بالوقاية للحد من مختلف أنواع الإجرام.

4- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية: أنشئ حديثا ويعد نقطة وصل وطنية في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية[1]، إذ يقدم المساعدة التقنية للمحققين ويوجه التحقيقات المتعلقة بتكنولوجيا الإعلام والإتصال، فهو عبارة عن هيئة تقنية تمارس أعمالها تحت وصاية مديرية الأمن العمومي والاستغلال لقيادة الدرك الوطني ويعمل على تحقيق المهام الآتية:

- ضمان ديمومة المراقبة المستمرة على شبكة الأنترنت.

- القيام بمراقبة الإتصالات الإلكترونية بما يسمح به القانون لصالح وحدات الدرك الوطني والجهات القضائية.

- مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال والتنقيب عن الأدلة في شبكة الأنترنت.

- المساهمة في عمليات التحري الخاصة عبر شبكة الأنترنت لفائدة وحدات الدرك الوطني والسلطات القضائية.

- المساهمة في التصدي للجرائم المعلوماتية بالتنسيق والتعاون مع مصالح الأمن والهيئات الوطنية.

الفرع الثاني: وسائل التحري وجمع الأدلة

هي الإجراءات المتخذة للتحري عبر شبكة الأنترنت بالإستعانة بالتقنية الإلكترونية الرقمية، للحصول على معلومات عن الأشخاص أو الأماكن أو الأشياء حسب طبيعتها للحد من الجرائم الإلكترونية[2]، وتشمل الوسائل المادية، والوسائل الإجرائية وحجز المعطيات.

أولا: الوسائل المادية

- عناوين البريد الإلكتروني وبرامج المحادثة: في حالة حدوث أي مشكلة أو أية أنشطة تخريبية فإن أول ما على المحقق القيام به هو البحث عن رقم الجهاز وتحديد موقعه، لإكتشاف المجرم الذي قام بتلك الإنتهاكات غير المشروعة قانونا، ويستطيع مزود

1 عز الدين عز الدين، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة بسكرة، 16 و 17 نوفمبر 2015، ص 29.

2 نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، درا الفكر الجامعي، مصر، 2007، ص 194 و 195.

خدمة الأنترنت مراقبة المشترك، كما بإمكان الشبكة التي تقدم خدمة الإتصال الهاتفي مراقبته أيضا، إذا ما كان بحوزتها أجهزة وبرامج خاصة بذلك[1].

- **البروكسي (PROXY):** حيث يعمل البروكسي كوسيط بين الشبكة ومستخدميها، وتضمن الشركات الكبرى المقدمة لخدمة الإتصال بالشبكات قدرتها لإدارة الشبكة، وتوفير الأمن وخدمات الذاكرة الجاهزة (Cash Memory)[2].

- **برامج التتبع:** تعمل على معرفة محاولات الإختراق التي تمت لإختراق جهاز ما، وتعطي بيان بإسم الحدث وتاريخ حدوثه وعنوان (IP) الذي تمت من خلاله عملية الإختراق، وإسم الشركة المزودة لخدمة الأنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الأنترنت ومعلومات أخرى، ومن الأمثلة على هذه البرامج برنامج Hack Tracer[3].

- **نظام كشف الإختراق (Intrusion Detection System):** هذه الفئة من البرامج تعمل على مراقبة بعض العمليات التي يتم حدوثها على أجهزة الحاسب أو الشبكة[4]، ويتم ذلك عن طريق تحليل رموز البيانات خلال عملية إنتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث لحظة وقوعها مباشرة في الحاسوب.

- **نظام جرة العسل (Honeypot):** هو نظام حاسوبي أنشا خصيصا للتعرض إلى مختلف أنواع الهجمات عبر الشبكة مع عدم إحتوائه على أي بيانات مهمة، ويقوم على خداع من يقوم بالهجوم وإعطائه إنطباعا خاطئا بسهولة الإعتداء[5].

- **أدوات تدقيق ومراجعة العمليات الحاسوبية**: هي أدوات خاصة تقوم بمراقبة مختلف العمليات التي تجري على ملفات ونظام التشغيل[1].

1 عفاف خذيري، مرجع سابق، ص 157.

2 عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسه بأنظمه الإتصال والمعلوماتيه، مجلة دائرة البحوث القانونية والسياسية، المركز الجامعي مرسلي عبد الله، تيبازه، الجزائر، العدد 04، جانفي 2018، ص. 48- 66.

3 عفاف خذيري، مرجع سابق، ص 153.

4 عز الدين عثماني، المرجع نفسه، ص 154.

5 عفاف خذيري، مرجع سابق، ص 154.

- **أدوات فحص ومراقبة الشبكات:** هذه الأدوات تستعمل في فحص بروتوكول الشبكات، لمعرفة المشاكل والعمليات التي من المحتمل إن تتعرض لها الشبكة، ومن هذه الأدوات (ARP) مهمتها تحديد مكان الحاسب فيزيائيا على الشبكة[1].

ثانيا: الوسائل الإجرائية

وتعني الإجراءات التي بواسطتها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، ومنها:

- **إقتفاء الأثر:** من أشد ما يخافه المجرم المعلوماتي تقصي أثره خلال إرتكابه للجريمة، و يمكن تقصي الأثر بوسائل مختلفة سواء بواسطة بريد إلكتروني تم إستقباله أو بواسطة تتبع أثر الجهاز الذي تم إستعماله لإنجاز عملية الإختراق[2].

- **الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته:** فيجب على المحقق أثناء عملية التحقيق في إحدى الجرائم الماسة بالمعطيات الرقمية، إن يطلع على النظام المعلوماتي ومحتواه من شبكات وتطبيقات وخدمات تقدم للعملاء، كما عليه الإطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام[3].

- **الإستعانة بالذكاء الإصطناعي:** وذلك من أجل حصر الحقائق والاحتمالات والأسباب والفرضيات، من خلال إستنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي ببرامج صممت خصيصا لهذا الغرض[3].

- **مراقبة الإتصالات الإلكترونية:** وهي من وسائل جمع البيانات والمعلومات عن المشتبه فيه، يقوم بها مراقب إلكتروني يتمثل في ضابط شرطة ذو كفاءة تقنية عالية تتماشى مع نوع الجريمة التي يتعامل معها، مستخدما في ذلك التقنية الإلكترونية وشبكة الأنترنت [4].

ثالثا: حجز المعطيات

إن ضبط أو حجز الأدلة الإلكترونية التي تحصلت عليها الجهات المختصة، هو العثور على أدلة الجريمة التي بوشر التحقيق فيها، والضبط هو الغاية من التفتيش ونتيجته

1 عز الدين عثماني، مرجع سابق، ص 55.

2 عفاف خذيري، المرجع نفسه، ص 149 و 150.

3 عز الدين عثماني، مرجع سابق، ص 55.

4 نبيلة هبة هروال، مرجع سابق، ص 198 و 199.

المباشرة، لأن بطلان التفتيش يستدعي حتما بطلان الضبط[1]، ولا يقع الضبط على شيء إلا إذا كان دليلا من أدلة الجريمة التي يجري التفتيش بخصوصها، وعليه سنقوم بدراسة الحجز عن طريق نسخ المعطيات ثم الحجز عن طريق منع الوصول إلى المعطيات.

1- الحجز عن طريق نسخ المعطيات

نظم المشرع ضبط وحجز الأدلة الإلكترونية بالمادة 06 من القانون 09-04 ونصت على: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أقراص وفقا للقواعد المقررة في قانون الإجراءات الجزائية".

و من خلال نص المادة نستنتج إن المشرع الجزائري إعتمد طريقة نسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها، والتي يمكن شرحها في الأشياء محل الحجز والإستعانة بالخبرة من أجل حجز الأدلة المعلوماتية.

أ- الأشياء محل الحجز

من الممكن إن تكون مكونات جهاز الحاسب الآلي وملحقاته الرئيسية والفرعية محلا للضبط والتي تساهم في كشف الحقيقة، والمراد بذلك الأشياء المنقولة التي يمكن تحريرها، أما العقارات التي يوجد بها أجهزة الحاسب وشبكاته، فيتم التحفظ على ما تحتوي من آثار للجريمة المعلوماتية أو أشياء يتعذر نقلها، عن طريق وضع الأختام على هذه الأماكن وتعيين السلطة المختصة للحراسة عليها[2].

ويقصد بالعقار في الجرائم الإلكترونية بالمكان مثل مقاهي الأنترنت، التي يعتقد ضابط الشرطة القضائي أو عضو النيابة العامة إن الجريمة قد خلفت آثارا بمكان ما أو تركت فيه أشياء تفيد التحقيق[3].

وهناك أربع طرق أساسية للتفتيش تساهم في عملية الحجز[1]، وهي:

---

1 خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية – دراسة مقارنة، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر، 2021، ص 101.

2 حسن محمد الطوالبه، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديث، الأردن، 2004، ص 142.

3 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضه العربية، مصر، 2008، ص 211.

- تفتيش الحاسب الآلي وطبع نسخة ورقية من ملفات معينة في ذات الوقت.

- تفتيش الحاسب الآلي وعمل نسخة إلكترونية من الملفات في ذات الوقت.

- عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع بالمراجعة.

- ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع.

ب- الإستعانة بالخبرة من أجل حجز الأدلة المعلوماتية

نظرا لطبيعة مسرح الجريمة الإلكترونية، وعدم توفر دليل رقمي مرئي يمكن فهمه بالقراءة، وسهولة محو ذلك الدليل أو تدميره في مدة وجيزة جدا، بالإضافة إلى إن الآثار المادية الناتجة عن هذه الجريمة تكاد تكون منعدمة، وضخامة البيانات التي يلزم فحصها بواسطة المحقق الجنائي[2]، يتم الإستعانة بالخبراء الإلكترونيين الرقميين، فهم أعوان المحقق والباحث الجنائي، ويشكلون بما يساهمون به من أعمال أحد أهم مصادر الأدلة الجنائية الرقمية، وقد إزدادت الحاجة إلى الخبراء الإلكترونيين الرقميين في الوقت الحالي نتيجة لإزدياد الأساليب الإجرامية الإلكترونية الرقمية، مما تطلب مجموعة منهم متخصصة في مجالات إلكترونية معينة[3]، يستعان بهم في الجرائم الإلكترونية والجرائم عبر التقنية الإلكترونية الرقمية وشبكاتها في الفحص والوصف والبيان.

2- الحجز عن طريق منع الوصول إلى المعطيات

نصت المادة 7 من القانون 09-04 على أنه: "إذا إستحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة"، وعليه وبالأخذ بالإعتبار الطرق الأخرى لرفع البيانات غير المادية التي لا يسهل الوصول إليها، أو التي يتم السيطرة عليها بطريقة أخرى في البيئة المعلوماتية، وبما إن الإجراءات تتعلق ببيانات غير مادية مخزنة، فإن السلطات المختصة يجب إن تتخذ إجراءات تكميلية من أجل الحصول عليها.

---

1 الطيبي البرئة، مرجع سابق، ص 290 و 291.

2 خضره شنتير، مرجع سابق، ص 110

3 مصطفى محمد موسى، مرجع سابق، ص 221

كما إن وصف البيانات بصعوبة الوصول إليها يمكن إن يعني ترميزها أو تقييدها عن طريق أي وسيلة إلكترونية تمنع الهلاوغ لها، وتطبيق هذا الإجراء يمكن إن يعود بالفائدة، وذلك في الحالات التي تتضمن خطرا أو ضررا بالمجتمع، ويبدو ذلك في حالة البرامج التي تحتوي على فيروسات أو في الحالات التي تكون فيها هذه البيانات محتواها غير قانون[1].

ويتعين على السلطة التي تقوم بالتفتيش تكليف هؤلاء المختصين بإستعمال الوسائل التقنية المناسبة والضرورية، للحيلولة دون الوصول إلى المعطيات التي يحتويها النظام المعلوماتي، ومنع القيام بأي إستعمال لها أو نسخها أو الإطلاع عليها[2]. كما إن الهدف من هذا الإجراء الإحتوازي الحفاظ على الأدلة في محيطها الإلكتروني ومنع أي محاولة لطمسها وإخفاء معالمها، وهو ما سيكون له الأثر الإيجابي في نجاح إجراءات التفتيش والحجز[3].

الفرع الثالث: الإثبات في جرائم إستخدام الذكاء الإصطناعي

إن الأصل هو حرية الإثبات، ومبررات ذلك إن المجرم يسعى لطمس معالم الجريمة لعدم كشف الحقيقة، وعليه يحق للنيابة العامة والقاضي الجزائي الإستعانة بكل طرق الإثبات، ومن حق المتهم إستعمال أي وسيلة مشروعة للإثبات لتحضير دفاعه، ولتحقيق التوازن بين الحريات الفردية وحقوق الدفاع وبين المصلحة العامة وحق الإعتراف، لجهة الإدعاء والتحقيق والمحكمة الإستعانة بأي وسيلة لإثبات الجريمة، إلا إن المشرع قيد حرية الإثبات في بعض الجرائم[4]، وعليه لا يمكن للقاضي مخالفة القواعد المقررة قانونا، وإذا خالف النص الذي يقيده على الدفاع إبداء النص المخالف قبل الفصل في الموضوع كدفع أولي، غير إن الإثبات يقيد بمبدأ شرعية الإثبات ومبدأ مشروعية الدليل.

أولا: مبدأ شرعية الإثبات الجنائي

إن من أهم ما يستدعيه مبدأ شرعية الإثبات إن يكون هذا الأخير موافقا لقيم العدالة والأخلاق ومقتضيات الكرامة الإنسانية، فلا يقبل الدليل الإلكتروني المتحصول عليه

1 الطيبي البركة، مرجع سابق، ص 293 و 294.

2 الطيبي البركة، المرجع نفسه، ص 295.

3 الطيبي البركة، المرجع نفسه ، ص 296.

4 نص المادة 212، قانون الإجراءات الجزائية: "يجوز إثبات الجرائم بأي طريقه من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي إن يصدر حكمه طبقا لإقتناعه الشخصي".

بطرق غير مشروعة، كالتعذيب والإكراه وتحريض أعوان الشرطة والقضاء، الإستجواب المرهق ونية الخداع فيه، التسجيل الصوتي والتصنت، التنويم المغناطيسي، جهاز كشف الكذب وغيرها.

نصا المادة 212 من ق.إ.ج.ج، نصت: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي إن يصدر حكمه طبقا لإقتناعه الشخصي"، ولكي ينتج هذا المبدأ أثره لابد من ملازمة مبدأ شرعية الإثبات بمبدأ المشروعية، فإذا كانت أدلة الإدانة مقترنة بمبدأ الشرعية، فأدلة البراءة غير مقيدة بمبدأ الشرعية، إذ لا يضر العدالة تبرئة مذنب بقدر ما يضرها إدانة بريء، ويبقى الشك يفسر لصالح المتهم.

ثانيا: مشروعية الدليل الإلكتروني في الإثبات الجنائي

تعددت التعريفات الموضحة لمفهوم الدليل الإلكتروني، فعرف على أنه الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الإتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميا أو تفسيريا في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها[1].

وعرف بأنه الدليل الذي يحتاج إلى معالج رقمي لقراءته أو فهم محتواه[2].

وعرف أيضا بأنه المعلومات المخزنة أو المنقولة في شكل ثنائي والتي قد يمكن الإعتماد عليها في المحكمة[3].

وعرف بأنه الدليل المأخوذ من أجهزة الكمبيوتر، على شكل مجالات ونبضات مغناطيسية أو كهربائية، يتم تجميعها وتحليلها بإستخدام برامج وتطبيقات خاصة في شكل صور أو تسجيلات صوتية أو مرئية، وتقديمها في شكل دليل يمكن إعتماده أمام القضاء[4].

1 عبد الناصر محمد محمود فرغلي، محمد سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية، عربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2007، ص 13.

2 حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، مصر، 2017، ص 9.

3 Lazetik GB, Koshevaliska O., Digital Evidence in Criminal procedures, A comparative approach, Balkan Social Science Review, 21, 2013, P 16.

4 ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب والأنترنت، دار الكتب القانونية، مصر، 2006، ص 88.

مما سبق يمكن تعريف الدليل الإلكتروني بأنه بيانات ومعلومات رقمية مستمدة من الأجهزة الإلكترونية وشبكات الإتصال، التي تكون في شكل نبضات مغناطيسية أو كهربائية يمكن من خلالها تسهيل قراءته وكشف محتواه لتقديمه للقضاء كدليل لإثبات الجريمة.

1- مشروعية وجود الدليل الإلكتروني

وفقا لنظام الإثبات الحر الذي أخذ به المشرع الجزائري[1]، إذ يتمتع القاضي الجزائي بحرية مطلقة في الإثبات ويختار من بين الأدلة المعروضة عليه ما يراه يسهم في الوصول للحقيقة، ونجد إن المشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، وللقاضي دور إيجابي في مجال الإثبات، ولا تثار أي مشاكل حول مشروعية الدليل الإلكتروني من حيث وجوده، ويخضع للسلطة التقديرية للقاضي، فالأصل في الأدلة مشروعية وجودها، والدليل يجب إن يكون مشروعا من حيث الوجود[2].

2- مشروعية تحصيل الدليل الإلكتروني

مشروعية تحصيل الدليل الإلكتروني تستلزم الصدق في مضمونه، وذلك بإتخاذ إجراءات تتماشى مع النصوص القانونية والأنظمة الثابتة في وجدان المجتمع الحضاري[3]، حيث إن الدليل غير المشروع لا يقبل في الإثبات الجنائي ولا يدخل في عناصر الإثبات التي يبني عليها القاضي إقتناعه، ويعتبر الدليل غير المشروع دليلا تم الحصول عليه على حساب قيم العدالة من ناحية، وعلى حساب حفظ الكرامة الإنسانية للشخص وحقه في الدفاع من ناحية أخرى، كالحصول على الإعتراف بالتهديد والإكراه المادي.

وبالنتيجة يقع تحت طائلة البطلان كل دليل إلكتروني متحصل عليه بطرق غير مشروعة أو مخالفة للقانون، أو نتيجة إجراء تخلفت أحد شروطه أو جميعها، كإكراه المتهم ماديا أو معنويا للإفصاح عن شيفرات أو كلمات الولوج لنظامه المعلوماتي، كما

1 بوكحل لخضر، الإجراءات الجنائية، مطبعة الشهاب، باتنة، الجزائر، دون سنة، ص 42.

2 خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعه الأولى، دار الثقافه والنشر والتوزيع، عمان، 2011، ص 128.

3 فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندريه، مصر، ص 361.

تتسم بعدم المشروعية أعمال التحريض على إرتكاب الجرائم المعلوماتية كالتحريض على التجسس أو المراقبة الإلكترونيين، كمراقبة البريد والإتصالات الإلكترونية دون إذن[1].

المطلب الثاني: الإجراءات المستحدثة لمواجهة جرائم إستخدام الذكاء الإصطناعي

نظرا لخطورة جرائم التكنولوجيا على أمن وإستقرار المجتمعات وبالأخص جرائم الذكاء الإصطناعي، بات لزاما على المشرع الجزائري تعديل القوانين الإجرائية القاصرة في الكشف عن هذا النوع من الجرائم وفق ما يتماشى وحداثة هذه الأخيرة، ولمواجهة الإجرام الجديد قامت الجزائر على إثر إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بتكييف نصوصها التشريعية الخاصة، منها القانون 04-14 والقانون 06-22، وعليه سنتناول في الفرع الأول أساليب التحري الخاصة وفي الفرع الثاني إنشاء الأقطاب الجزائية المتخصصة.

الفرع الأول: أساليب التحري الخاصة

إستحدث المشرع الجزائري أساليب تحري خاصة، للكشف عن الجرائم الحديثة من خلال إجراءات بحث تتمثل في مجموعة من التقنيات وضحتها المواد من 65 مكرر 5 إلى 65 مكرر 10 من ق.إ.ج.ج، وهي إجراءات تباشر بشكل خفي على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة[2].

أولا: إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور

1- إعتراض المراسلات

إعتراض أو تسجيل أو نسخ المراسلات الهجرات بقنوات أو وسائل إتصال سلكية أو لاسلكية، وتكون عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين والاستقبال والعرض[3].

2- تسجيل الأصوات

وضع ترتيبات تقنية وأجهزة بتصرت دون موافقة المعنيين، لإلتقاط وتثبيت وتسجيل وبث الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في

1 محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الإبتدائي- دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، ص 372.

2 آمنه محمدي بوزينة، مرجع سابق، ص 68.

3 عبد القادر رويس، أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة أحمد بن يحيى الونشريسي، تيسمسيلت، الجزائر، المجلد 2، العدد 1، جوان 2017، ص 40.

أماكن خاصة أو عمومية، وإخفائها لتلقي أحاديث تفيد في تجلي الحقيقة وتسجيلها[1]. ولم يحدد المشرع وسيلة معينة للتنصت والتسجيل وترك إختيارها للشرطة القضائية ولم يشترط طريقة أو تقنية معينة لكيفية القيام به[2].

3- التقاط الصور

يتم التقاط الصور لشخص ما في محاولة نقل المعلومات عبر الصورة التليفزيونية، بتوكيب كاميرات في أماكن معينة يرتادها المشتبه فيه دون علمه، وبتقل بالصوت والصورة كل ما يدور فيها وتسجيلها[3]، ومن فوائد إلتقاط الصور أنها:

- تتيح للمحقق الإطلاع على محل الحادث كلما أراد ذلك.
- الإحتفاظ بمسرح الجريمة على الحالة التي كانت عليها وقت إرتكابها لفترة طويلة.
- إظهار آثار الجريمة ما يتيح للمحقق مراجعتها والتدقيق فيها كلما دعت الضرورة[4].

4- القيود الواردة على إعتراض المراسلات وتسجيل الأصوات وإلنقاط الصور

من أجل صون حرية الأفراد أحاط المشرع إستخدام هذه الأساليب بقيود قانونية لمنع أي تعسف في إستعمالها تتمثل في:

- ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ إستنادا للمادة 65 مكرر 5 من ق.إ.ج.ج[5]، والتي أجازت لقاضي التحقيق ووكيل الجمهورية إن يمهد لضباط الشرطة القضائية بإذن كتابي وتحت مراقبته المباشرة، القيام بلإعتراض المراسلات السلكية

1 ناجق شيخ، أساليب البحث والتحري المستحدث في القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائق الجزائري، المجلد 8، العدد 1، جوان 2013، ص 294.

2 الدوادي مجراب، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة دكتوراه في القانون، كليه الحقوق، جامعة بن يوسف بن خدة، الجزائر، 2016، ص 242.

3 نبيل لحمر، دور الأقطاب الجزائية المتخصصة في مكافحة الجريمة، رسالة ماجستير في القانون، كليه الحقوق، جامعة قسنطيرة، الجزائر، 2014، ص 203.

4 الدوادي مجراب، مرجع سابق، ص 216.

5 راجع المادة 65 مكرر 5 من القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائق

واللاسلكية ووضع ترتيبات الإلتقاط والتثبيت والتسجيل[1]، وتقدير فائدة الإجراء وجديته وموائمته لسير الدعوى من خلال معطيات التحريات التي أجريت من قبل الضبطية القضائية مسبقا[2].

- تحديد طبيعة المراسلة ومدة الإعتراض طبقا للمادة 65 مكرر7[3]، على إن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب إعتراضها، وحدد مدة هذا الإجراء بأربعة أشهر قابلة للتجديد حسب مقتضيات التحري. ويجب على ضابط الشرطة القضائية المأذون له من طرف قاضي التحقيق حسب المادة 65 مكرر 9، إن يحرر محضرا عن كل عملية إعتراض وتسجيل المراسلات وكذا عمليات وضع الترتيبات التقنية وعمليات الإلتقاط والتثبيت والتسجيل، ويذكر في المحضر تاريخ وساعة بداية هذه العملية والإنتهاء منها[4]. كما يجوز وفقا لأحكام المادة 65 مكرر 10 لضابط الشرطة القضائية المناب نسخ المراسلات أو الصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف، وعند الاقتضاء تنسخ باللغة الأجنبية بمساعدة مترجم يسخر لهذا الغرض[3].

- إن تنفذ من عون مؤهل، حيث يجوز لوكيل الجمهورية أو لضابط الشرطة القضائية أو لقاضي التحقيق إن يسخر كل عون مؤهل لدى مصلحة أو هيئة عمومية أو خاصة للتكفل بالجوانب التقنية للعملية المطلوب إنجازها[5]، وفور إنتهاء ضابط الشرطة القضائية من العملية المكلف بها، يحرر محضرا عنها ينقل فيه مجريات العملية[6].

- عدم اللجوء إلى إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور إلا في الجرائم المحددة حصرا في المادة 65 مكرر 5 من القانون 06-22 : "إذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الارهاب أو الجرائم المتعلقة بالتشريع الخاص

1 علي شملال، المستحدث في قانون الإجراءات الجزائية، التحقيق والمحاكمة، دار هومه، الجزائر، 2016، ص 68.

2 نعيم سعيداني، مرجع سابق، ص 181.

3 راجع المادة 65 مكرر7 من القانون 06- 22.

4 علي شملال، مرجع سابق، ص 69.

5 راجع المادة 65 مكرر 8 من القانون 06- 22.

6 ناجية شيخ، مرجع سابق، ص 296.

بالصرف وكذا جرائم الفساد"، حيث تتطلب كل هذه العمليات سرية الإجراءات وكتمان السر المهني.

ثانيا: التسرب

يعد التسرب من بين العمليات المهمة للكشف عن الجرائم التقنية الحديثة والتصدي لها، ولتحديد معالم إجراء التسرب نتعرض لمفهومه ثم الضوابط التي تحكمه.

1- المقصود بالتسرب

لقد عرفت المادة 65 مكرر 12 من القانون 06-22 التسرب بأنه: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

إذا التسرب عملية معقدة جدا تتطلب من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها، وإرتكاب أفعال محظورة من أجل تحقيق الهدف النهائي من العملية، وتستخدم فيها مختلف الأساليب لكسب ثقة المشتبه فيهم وتحديد طبيعة ومدى النشاط الإجرامي، ويتطلب ذلك ربط علاقة مع الأشخاص المشتبه فيهم بالإتصال بهم بطريق مباشر أو غير مباشر، كما إن التسرب إجراء لا يخص العالم المادي فقط بل يمكن تفعيله في العالم الرقمي أو البيئة الإفتراضية، كأن يقوم الضابط بالدخول إلى مواقع التواصل الإجتماعي التي توفر خدمة الإيجار بأسماء وصفات وهمية أو مستعارة، ويشارك في محادثات غرف الدردشة أو حلقات النقاش المباشر حول تقنية إختراق شبكات الإتصال أو بث الفيروسات أو إنخراطه في مجموعات أو نوادي الهاكر ظاهرا فيها بمظهر طبيعي كما لو كان واحد مثلهم قصد إستدراجهم والكشف عنهم وعن أعمالهم الإجرامية.

2- الضوابط التي تحكم التسرب

يعد التسرب من أهم العمليات في الكشف عن الجرائم التقنية، وقد خصه المشرع بمجموعة من الضوابط والشروط الشكلية والموضوعية نذكرها فيما يلي:

أ- الشروط الشكلية لإجراء التسرب

تفرض الشرعية الإجرائية ضرورة الإلتزام بمجموعة من الضوابط الشكلية، وذلك بنص المادة 65 مكرر 5 من القانون 06-22 وهي:

- **الحصول على إذن:** محرر رسمي صادر من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية مكتوبا ومسببا، مسلم إلى جهة مختصة متمثلة في ضابط الشرطة القضائية[1]، على إن تكون تلك الأسباب مبنية على إستدلالات جدية يتخذ منها أسباب لإجراء عملية التسرب[2]. وطبقا للمادة 65 مكرر 15/02 ذكر الجرائم التي تبرر اللجوء لهذه العملية والمنصوص عليها حصرا في المادة 65 مكرر 5 من القانون 06-22، مع ذكر هوية ضابط الشرطة القضائية الذي ستتم عملية التسرب تحت مسؤوليته.

- **تحديد المدة المطلوبة للتسرب:** تحدد بأربعة أشهر قابلة للتجديد وضمن الشروط الشكلية والموضوعية، غير أنه يجوز للقاضي الذي رخص بإجرائها إن يأمر في أي وقت بوقفها قبل إنقضاء المدة المحددة على إن تودع هذه الرخصة في ملف الإجراءات بعد الإنتهاء من عملية التسرب، عملا بأحكام الفقرة الأخيرة من المادة 65 مكرر 15 من القانون 06-22، وهكذا يكون المشرع إشترط إبقاء الإذن بالتسرب خارج ملف الإجراءات إلى حين الإنتهاء من العملية ثم يضاف إلى الملف، للحفاظ على السرية المطلوبة في العملية[3].

ب- الشروط الموضوعية لإجراء التسرب

تقوم عملية التسرب على مبررات ضابط الشرطة القضائية في طلبه للحصول على الإذن بالتسرب، والذي يتم تحت رقابة الجهة القضائية المختصة ويمكن إيجازها في:

- **تحرير تقرير عن كل عملية تسرب:** بعد إنتهاء عملية التسرب تتمكن جهات البحث والتحري وعلى رأسها وكيل الجمهورية وقاضي التحقيق من التوصل إلى التفاصيل الرئيسية لإرتكاب الجرائم، بالإضافة إلى تحرير محاضر تشكل أدلة تفيد الدعوى[4]. فالتسرب بإعتباره ضرورة يجب اللجوء إليه في ظل عجز الإجراءات العادية في الكشف عن خبايا الجريمة التقنية[5].

1 دلال مولاي ملياني، إشكاليه الإثبات في جرائم الأنترنت في التشريع الجزائري، أطروحة دكتوراه في القانون، كليه الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد، تلمسان، الجزائر، 2018،مرجع سابق، ص 200.

2 دلال مولاي ملياني، المرجع نفسه، ص 201.

3 الدوادي مجراب، مرجع سابق، 341 و342.

4 عزيزه رابحي، الأسرار المعلوماتيه وحمايتها الجزائية، أطروحة دكتوراه في القانون، كليه الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018، ص 199.

5 دلال مولاي ملياني، مرجع سابق، ص 199.

- **الحفاظ على سلامة المتسرب:** يلتزم ضابط الشرطة القضائية المنسق لعملية التسرب بإتخاذ التدابير اللازمة لضمان أمن وسلامة الضابط أو العون المتسرب، وكذلك الأشخاص في العملية في كل مرحلة من مراحل المهمة[1]، وقد شملهم المشرع بحماية من خلال العقوبات المقررة في المادة 65 مكرر 16 من القانون 06-22.

- **عدم الكشف عن هوية المتسرب:** وفر المشرع حماية أخرى تتمثل في عدم إدلاء العون المتسرب بشهادته شخصيا حفاظا على حياته، ويقتصر الأمر على إدلاء ضابط الشرطة القضائية المكلف بتنسيق العملية وحده، ودون سواه بشهادته تحت مسؤوليته دون التعرض إلى كشف هوية المتسرب[2].

الفرع الثاني: إنشاء الأقطاب الجزائية المتخصصة

من بين التعديلات الجديدة التي أتى بها المشرع الجزائري فيما يخص مكافحة الجرائم المعلوماتية في الجانب التشريعي، الإختصاص الإقليمي للأقطاب الجزائية المتخصصة وتمديد الإختصاص المحلي.

أولا: الإختصاص الإقليمي للأقطاب الجزائية المتخصصة

حدد المرسوم التنفيذي 06-348 المؤرخ في 05 أكتوبر 2006 الأقطاب الجزائية المتخصصة والمتمثلة في 04 محاكم على المستوى الوطني، بالإضافة إلى إستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال[3] بموجب الأمر رقم 21-11، ونفصل فيها كالآتي:

- **محكمة سيدي أمحمد:** مقرها بالجزائر العاصمة، ويمتد إختصاصها الإقليمي ليشمل إختصاص محاكم تابعة للمجالس القضائية لكل من الجزائر، الشلف، الأغواط، البويرة، تيزي وزو، الجلفة، المدية، المسيلة وبومرداس، وهي مجالس قضائية تشمل إداريا ولايات وسط شمال الجزائر[4].

- **محكمة قسنطينة:** تتواجد بمدينة قسنطينة ويمتد إختصاصها الإقليمي إلى إختصاص المحاكم التابعة للمجالس لكل من قسنطينة، أم البواقي، بجاية، بسكرة، تبسة،

---

1 الدوادي مجراب، مرجع سابق، ص 344.

2 عزيزة رابحي، المرجع نفسه، ص 300.

3 الأمر رقم 21- 11، مؤرخ في 25 اوت 2021 يتمم الأمر رقم 66- 155 المؤرخ في 8 جوان سنه 1966 والمتضمن قانون الإجراءات الجزائية

4 محمد بكرارشوش، الإختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري، دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقله، الجزائر، المجلد 8، العدد 14، جانفي 2016،ص 316.

جيجل، سطيف، سكيكدة، عنابة، قالمة وبرج بوعريريج، بها 12 مجلس قضائي يشمل إداريا ولايات تقع شرق وجنوب شرق الجزائر[1].

- **محكمة وهران:** مقرها وهران ويمتد إختصاصها الإقليمي ليشمل إختصاص المحاكم التابعة للمجالس القضائية لكل من وهران، بشار، تلمسان، تيارت، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة عين تموشنت وغليزان، أي يشمل إختصاصها الإقليمي إداريا 14 ولاية والواقعة غرب وجنوب غرب الجزائر[2].

- **محكمة ورقلة:** والتي تتواجد في مدينة ورقلة، ويمتد إختصاصها الإقليمي ليشمل إختصاص المحاكم التابعة للمجالس القضائية لكل من ورقلة، أدرار، تمنراست، إليزي، تندوف وغرداية، أي إختصاص هذه المحكمة يمتد إلى 6 ولايات والتي تحتل مناطق الجنوب الكبير من الحدود الشرقية الجنوبية إلى الحدود الغربية الجنوبية[3].

- **القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال:** نظرا لتعقيد الجرائم المعلوماتية وخطورتها، عمد المشرع الجزائري إلى الإستفادة من التطور العلمي والتكنولوجي في السمو بمستوى العمل القضائي لمواجهة الجرائم المعلوماتية، وعليه قام بإنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال على مستوى محكمة مقر مجلس قضاء الجزائر، بهدف المتابعة والتحقيق في هذه الجرائم والجرائم المتصلة بها[4].

ويكون عمل هذا القطب الجزائي بنص المادة 211 مكرر 24 من الأمر 21-11 حصري بالمتابعة والتحقيق في الجرائم التالية:

* الماسة بأمن الدولة أو بالدفاع الوطني.
* الإتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين.
* التمييز وخطاب الكراهة.
* نشر وترويج أخبار كاذبة من شأنها زعزعة إستقرار المجتمع والمساس بأمنه.
* نشر وترويج ما يمس بالنظام العام ذو طابع منظم أو عابر للحدود الوطنية.

1 راجع المادة 3 من المرسوم التنفيذي رقم 06- 348، يتضمن تمديد الإختصاص المحلي.

2 راجع المادة 5، من المرسوم التنفيذي رقم 06- 348، يتضمن تمديد الإختصاص المحلي.

3 راجع المادة 4، من المرسوم التنفيذي رقم 06- 348، يتضمن تمديد الإختصاص المحلي.

4 راجع المادة 211 مكرر 22، من الأمر 21- 11، يتمم قانون الإجراءات الجزائية.

* المساس بأنظمة المعالجة الآلية للمعطيات المرتبطة بالإدارات والمؤسسات العمومية.

إضافة للعمل الحصري للقطب الجزائي الوطني نصت المادة 211 مكرر 27 من الأمر 21-11 على: "دون الإخلال بأحكام المادتين 211 مكرر 24 و211 مكرر 25 أعلاه يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وكذا قاضي التحقيق ورئيس ذات القطب إختصاصا مشتركا مع الإختصاص الناتج عن تطبيق المواد 37، 40، 329 من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيا الإعلام والإتصال والجرائم المرتبطة بها".

ثانيا: تمديد الإختصاص المحلي

من بين القواعد الإجرائية لمواجهة الجريمة المعلوماتية تمديد الإختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق وضباط الشرطة القضائية.

1- تمديد الإختصاص المحلي لوكيل الجمهورية

أقرت المادة 37/2 من ق.إ.ج.ج على أنه يجوز تمديد الإختصاص المحلي لوكلاء الجمهورية إلى دائرة إختصاص محاكم أخرى، إذا تعلق الأمر بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، جرائم تبييض الأموال والإرهاب، جرائم الصرف والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1]، إضافة إلى ذلك تم سحب نظام الملائمة من النيابة العامة في مجال متابعة هذا النوع من الجرائم، إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون[2].

2- تمديد الإختصاص المحلي لقاضي التحقيق

نصت المادة 40/2 من ق.إ.ج.ج على أنه :" يجوز تمديد الإختصاص المحلي لقاضي التحقيق إلى دائرة إختصاص محاكم أخرى،عن طريق التنظيم،في جرائم

1 راجع المادة 37 /02 من القانون 04- 14، يعدل ويتمم قانون الإجراءات الجزائية.

2 سعيده بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوة منثوري، قسنطيرة، الجزائر، مجلد ب، العدد 52، ديسمبر 2019، ص 51.

المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالعرف".

3- تمديد الإختصاص المحلي لضباط الشرطة القضائية

الأصل إن الإختصاص المكاني أو الإقليمي لضباط الشرطة القضائية يتحدد تحت سلطة وكيل الجمهورية الذي يدير عملهم في مرحلة جمع الإستدلالات ، وبإنتداب قاضي التحقيق في حالة فتح تحقيق قضائي بمكان إرتكاب الجريمة أو مكان توقيف المشتبه فيهم أو مكان إقامتهم[1]، ويجوز لهم أيضا في حالة الإستعجال إن يباشروا مهمتهم في كافة الإقليم الوطني إذا طلب منهم أداء ذلك من القاضي المختص قانونا، ويجب إن يساعدهم ضباط الشرطة القضائية الذين يمارسون وظائفهم في المجموعة السكنية المعنية، طبقا للمواد 16، 16 مكرر[2]، 40 مكرر 1، 40 مكرر 2 و 40 مكرر3[3]، أي إن إختصاصهم يمتد ليشمل إختصاص إقليمي لمحاكم غير المحاكم التي يباشرون فيها مهامهم في دائرة إختصاصها.

1 محمد بكرارشوش، مرجع سابق، ص 317.

2 راجع المادة 16 مكرر من القانون 06-22، يعدل ويتمم قانون الإجراءات الجزائية.

3 راجع المواد 40 مكرر 1، 40 مكرر2، 40 مكرر3 من القانون 04-14، يعدل ويتمم قانون الإجراءات الجزائية.

المبحث الثاني: الآليات الدولية لمكافحة جرائم إستخدام الذكاء الإصطناعي

يعرف العالم تطورا في شتى المجالات وأهمها وسائل المواصلات والإتصالات، الذي أدى لتزايد الأنشطة الإجرامية العابرة للحدود الوطنية مما إستلزم ضرورة التعاون الدولي للتصدي لهذه الجرائم وعدم تملص مرتكبيها من العقاب، ومع إزدياد إستخدام تقنيات الذكاء الإصطناعي، وإمكانية إستعمالها في أفعال إجرامية عابرة للحدود لا تقل خطورة عن جرائم الإرهاب والإتجار بالبشر والتي تهدد أمن وإستقرار المجتمعات، تظهر الحاجة للإستفادة من تجارب التعاون الدولي في المساعدة القضائية الجنائية، للتصدي لتلك الجرائم والإجراءات القانونية المساهمة بشكل إيجابي وفعال في هذا المجال. لذلك سنتطرق في المطلب الأول لسبل التعاون الدولي وفي المطلب الثاني لإشكاليات التعاون الدولي وآليات التغلب عليها.

المطلب الأول: سبل التعاون الدولي في جرائم إستخدام الذكاء الإصطناعي

مما لاشك فيه إن أي دولة مهما بلغت درجة قوتها وصلابتها لا تستغني عن الدخول في علاقات دولية متبأدلة، خاصة وأن جهودها الداخلية في مكافحة الجرائم وملاحقتها لم تعد كافية في ظل التطور وبروز التقنيات الحديثة، ولعل أهمها وأكثرها حداثة الذكاء الإصطناعي، وعلى ذلك فإن التعاون الدولي لمكافحة الجرائم المتصلة بالذكاء الإصطناعي بات أمرا لابد منه، خاصة مع إتساع الأشطة الإجرامية لمستخدميه.

الفرع الأول: التعاون الأمني

يعرف التعاون الأمني الدولي بأنه تبادل المساعدة وتضافر الجهود بين طرفين دوليين فلكثر، لتحقيق نفع أو مصلحة مشتركة في مجال التصدي لمخاطر الإجرام وما يرتبط به من مجالات أخرى، كالعدالة الجنائية أو لتخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد، سواء أكانت المساعدة المتبأدلة قانونية أو قضائية أو شرطية، وسواء إقتصرت على دولتين أو إمتدت إقليميا أو عالميا.

ويعد التعاون الأمني الدولي ثمرة تطور العلاقات الدولية، ونتيجة حتمية لما تشهده الجريمة من تطور متلاحق يكاد يقفز في أرقامه من عام إلى آخر، حتى أصبح تطور الجريمة في حد ذاته ظاهرة دولية.

أولا: صور التعاون الأمني

- **ربط شبكات الإتصال والمعلومات:** تحتاج الإتصالات الشرطية إلى وسائل للإتصال تحقق السرعة المناسبة لتتمكن أجهزة العدالة الجنائية من التواصل بين سلطات

التحقيق والمتابعة المختلفة، لذلك عمدت الدول والمنظمات الدولية إلى تطوير الإتصال وتبادل المعلومات فيما بينها[1].

- **القيام ببعض العمليات الشرطية والأمنية المشتركة:** تعقب المجرم وتعقب الأدلة الرقمية وضبطها، والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلى والأنظمة المعلوماتية وشبكات الإتصال، بحثا عما قد تحويه من أدلة وبراهين على إرتكاب الجريمة، كلها أمور تستدعي القيام ببعض العمليات الشرطية والأمنية المشتركة، وإشتراك الدول فيما بينها للقيام بعمليات شرطية لتعاون الدول الأطراف فيما بينها تعاونا وثيقا، بما يتماشى مع نظمها القانونية والإدارية الداخلية كي تعزز فاعلية تدابير إنفاذ القانون من أجل مكافحة الجرائم المشمولة بهذه الإتفاقية، وتتخذ الدول الأطراف تدابير فعالة لأجل تعزيز قنوات الإتصال بين سلطاتها وأجهزتها ودوائرها المعنية، وإنشاء تلك القنوات عند الضرورة من أجل تيسير تبادل المعلومات بطريقة آمنة وسريعة عن كل جوانب تلك الجرائم، بما فيها علاقتها بالأنشطة الإجرامية الأخرى، إذا رأت الدول الأطراف المعنية ذلك مناسبا، يؤدي إلى صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم وبالتالي وضع حد لها[2].

ثانيا: دور الإنتربول

الإنتربول أكبر منظمة شرطية دولية، أنشأت عام 1923 ومقرها الرئيسي في مدينة ليون بفرنسا، يتم العمل فيها بتبادل أعضاء الشرطة الدولية للمعلومات عن المجرمين الدوليين والتعاون في مكافحة الجرائم الدولية، كجرائم التهريب وبيع الأسلحة والجرائم الإلكترونية، وقد أنشأت المنظمة وحدة تحليل المعلومات الجنائية لإستخلاص أهم المعلومات عن المنظمات الإجرامية لوضع تلك المعلومات في متناول هيئة الشرطة أو الدول الأعضاء في الإنتربول. وطبقا للمادة الثانية من ميثاق المنظمة تتمثل أهم اهدافها في الآتي:

- جمع المعلومات المتعلقة بالجرائم والمجرمين ويتم ذلك عبر شبكة إتصالات حديثة.
- إنشاء وتنمية كافة المؤسسات الممكن مساهمتها في الوقاية من الجرائم الدولية .
- تأمين وتنمية التعاون المتبادل على أوسع نطاق بين سلطات الشرطة الجنائية.

1 إتفاقية الأمم المتحده لمكافحة الفساد، القانون الدولي المادة 48، التعاون في مجال إنفاذ القانون.

2 سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلوماتية الدولية، دار النهضة العربية، 2013، ص 415 وما بعدها.

- التعاون مع الدول الأعضاء في ضبط المجرمين الهاربين والمطلوبين من العدالة على إختلاف جنسياتهم من خلال إصدار المنشورات الدولية.

- دعم جهود الشرطة في مكافحة الإجرام العابر للحدود ومجال الأدلة الجنائية.

وأنشأت منظمة الإنتربول وحدة خاصة لمكافحة جرائم التكنولوجيا، كما قامت بالتعاون مع الدول الثمانية الكبرى بوضع إستراتيجيات للتصدي لهذا النوع من الجرائم من خلال[1]:

- إنشاء مركز إتصالات أمني شبكي مدار 24 ساعة على مستوى مصالح الشرطة.

- إستخدام وسائل حديثة في تلك المكافحة كإستخدام قاعدة البيانات المركزية.

- تزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها.

الفرع الثاني: التعاون القضائي

في هذا السياق يمكن إن نشير إلى ضرورة إيجاد مايطلق عليه بنظام قضاة الإتصال فيما يتعلق بمحاربة الجرائم المرتكبة بإستخدام الذكاء الإصطناعي، ويعد من الأنظمة الحديثة للتعاون الدولي، كما يمكن الإشارة إلى نظام تسليم المجرمين بإعتباره من أهم مظاهر التعاون بين الدول في المجال الجنائي.

أولا: نظام قضاة الإتصال في مجال الجرائم المتصلة بالذكاء الإصطناعي

يعتمد نظام قضاة الإتصال على الإتصال المباشر بين القضاة في شتى الدول بناءا على إتفاقيات بينها، ويهدف إلى تبادل الخبرات والأحكام القضائية الصادرة في هذا الشأن للتنسيق فيما بينهم، كما تضمن السرعة في الفصل في طلبات المساعدة القضائية وتسليم المجرمين، ولقد عينت فرنسا قاضيين للإتصال في هولندا وإيطاليا يعمل على دراسة طلبات المساعدة القضائية، وتسليم المتهمين والإسهام في سرعة الإجراءات وصحتها من الناحية القانونية.

ومما لاشك فيه إن نظام قضاة الإتصال له إمكانية في إن يتمتع بفاعلية كبيرة في التصدي للجرائم الناجمة عن إستخدام الذكاء الإصطناعي، ذلك إن التعاون بين الدول بتبادل الخبرات والتجارب والإمكانيات التي قد لا تتوفر عند البعض من الدول خاصة وأن هذه الجرائم عابرة للحدود الوطنية، فيمكن أن يكون الكيان والمسئولين عن هذه الجرائم في بلد أو أكثر من بلد، ويكون المجني عليه في بلد غيره وتترتب نتائج الأفعال الإجرامية

1 نبيلة هبة هروال، مرجع سابق، ص 153.

في بلد أو أكثر، مما يثير مشكلة تنازع القوانين من جهة، وصعوبات في كشف الجريمة وحفظ الأدلة وجمعها من جهة أخرى، كل هذه التحديات يقف ورائها خبرة كبيرة في مجال التصنيع والبرمجة والتشغيل للذكاء الإصطناعي، من أجل إستخدامه في تحقيق أغراض غير مشروعة مما يصعب عملية التصدي لمثل هذه الجرائم.

ثانيا: نظام تسليم المجرمين

يعد نظام تسليم المجرمين في الفقه الدولي من أهم تجليات التعاون بين الدول في المجال الجنائي، والذي يهدف إلى محاربة الجريمة ومنع المجرمين من التملص من العقاب لضمان أمن وإستقرار المجتمعات. وقد شهد هذا النظام تطورا وتنظيما كبيرا تزامنا مع تفشي الجرائم العابرة للحدود، الأمر الذي يجعل الدولة عاجزة على متابعة مرتكبي هذه الجرائم، لذلك دعت الحاجة الملحة لهذا النظام وضرورة التعاون الدولي لتحقيق أهدافه المرجوة.

والجزائر كغيرها من الدول أبرمت عدة إتفاقيات للتعاون القضائي، ويعتبر موضوع تسليم المجرمين من أهم المواضيع التي تناولتها هذه الإتفاقيات، كإتفاقية تنفيذ الأحكام وتسليم المجرمين المبرمة بين الجزائر وفرنسا والتي صادق عليها بأمر رقم 65-194 المؤرخ في 29 جويلية 1965، وإتفاقية تسليم المجرمين والتعاون القضائي في المسائل الجنائية بين الجزائر وبلجيكا المصادق عليها بأمر رقم 70-61 المؤرخ في 8 أكتوبر 1970.

ويعتبر التشريع الوطني في عدة دول مرجعا أساسيا لأحكام التسليم، تلجأ إليه الدولة لتنظيم المسائل المتعلقة بتسليم المجرمين في حالة عدم وجود إتفاقية دولية تتضمن ذلك.

وبالرجوع إلى التشريع الجزائري نجد أنه تطرق إلى الأحكام الموضوعية والإجرائية للتسليم، كالدستور الذي يتضمن على بعض القواعد المتعلقة بمنع تسليم الرعايا أو اللاجئين، كالذي نص عليه في الدستور الجزائري لسنة 1996 في المادة 69 بحظر تسليم اللاجئين[1]. وقد عالج المشرع الجزائري نظام التسليم في المواد من 674 إلى 720 من ق.إ.ج.ج، حيث يعتبر هذا الأخير مصدرا غير مباشر لأحكام التسليم.

فمصادر التسليم للمجرمين تكون إتفاقيات دولية أو تشريع وطني، وفي حالة وجود تعارض بينهما تكون الأولوية للإتفاقيات الدولية المصادق عليها من قبل هيئات الدولة.

المطلب الثاني: إشكاليات التعاون الدولي وآليات التغلب عليها

1 المادة 69، الدستور الجزائري لسنة 1996.

رغم المناداة بضرورة التعاون الدولي لمكافحة الجرائم المرتكبة بإستخدام الذكاء الإصطناعي، إلا أن هناك عوائق تحول دون ذلك بل وتجعل هذا التعاون صعبا، ومن أهم هذه الإشكاليات التي سنتناولها في الفرع الأول القصور التشريعي للدول والتعارض فيما بينها إضافة إلى تنوع وإختلاف الأنظمة القانونية الإجرائية وتنازع الإختصاص القضائي الدولي وأخيرا إشكاليات الإنابة القضائية وتناول في الفرع الثاني آليات التغلب عليها.

الفرع الأول: إشكاليات التعاون الدولي

أولا: القصور التشريعي للدول والتعارض فيما بينها

إن إختلاف الأنظمة القانونية للدول يعد عائقا كبيرا يعترض سبيل التعاون الدولي بين تلك الدول في مجال مكافحة الجرائم المعلوماتية، لما ينتج عن ذلك الإختلاف من إشكاليات حول تطبيق القانون، كما أن قصور معظم النظم التشريعية للدول عن وضع مفهوم محدد لجرائم الذكاء الإصطناعي ونظام قانوني خاص بها، يجعل سبل التعاون الدولي أمرا في غاية الصعوبة[1]، وبنظرة متفحصة للأنظمة القانونية القائمة في العديد من الدول لمواجهة الجرائم المعلوماتية يمكن القول بعدم توصل الدول إلى إتفاق حول صور إساءة إستخدام الذكاء الإصطناعي الواجب تجريمها، وعدم وجود نظام قانوني خاص بمكافحة هذه الجرائم، فما يكون مشروعا في أحد الأنظمة قد يكون مجرما في آخر، ويرجع ذلك إلى إختلاف البيئة المجتمعية والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وقد يتضح سبب غياب هذا النموذج الموحد في تعدد التعريفات والمفاهيم القانونية المرتبطة بهذا الشأن[2].

وبسبب تنوع وإختلاف النظم القانونية الإجرائية، نجد أن وسائل التحري والتحقيق والمحاكمة التي تثبت دورها الفعال في دولة ما قد تكون دون جدوى في دولة أخرى أو ممنوع إجرائها، كما هو الحال بالنسبة للمراقبة الإلكترونية[3]، والتسليم المراقب والعمليات المستترة وغيرها، فإذا ما إعتبرت طريقة ما من طرق جمع الإستدلالات أو التحقيق أنها قانونية في دولة معينة قد تكون غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنفاذ القانون في الدولة الأخرى على إستخدام ما تعتبره هي أنه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا

1 سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الأنترنت، أطروحة الدكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة الإسكندرية، مصر، 2010، ص 538.

2 حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت دراسة مقارنة، رسالة دكتوراه في القانون، كلية الحقوق، جامعة عين شمس، القاهرة، مصر، 2007، ص550.

3 مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الأنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، دار الكتب والوثائق القومية المصرية، مصر، 2003، ص 3.

تسمح بإستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في إختصاص قضائي وبشكل مشروع[2]، وهذا يعني عدم وجود تنسيق بين الدول المختلفة فيما يتعلق بالإجراءات الجنائية المتبعة بشأن الجرائم المعلوماتية، سواء ما تعلق منها بأعمال الإستدلال أو التحقيق أو المحاكمة.

ثانيا: تنازع الإختصاص القضائي الدولي

يقصد بالإختصاص الدولي سلطة محاكم كل دولة النظر في دعاوى معينة، وبسبب ما تتسم به الجرائم المتصلة بالذكاء الإصطناعي من سمات وخصائص وكونها جرائم عابرة لحدود الدول، فإنها تعد من أكثر الجرائم التي يثار بشأنها تنازع الإختصاص القضائي بين الدول، والذي يعني تقديم الدعوى عن ذات الجريمة أو عدة جرائم مرتبطة إلى جهتين من جهات التحقيق أو الحكم وإدعاء كل جهة إختصاصها أي تنازع الإختصاص الإيجابي، أو رفض كلا الجهتين النظر في الدعوى لعدم الإختصاص أي تنازع الإختصاص السلبي[1].

فقد يحدث أن يرتكب أجنبي في إقليم دولة ما جريمة من جرائم الذكاء الإصطناعي، فهنا تخضع الجريمة للإختصاص الجنائي للدولة للمرتكب على إقليمها الجريمة وفقا لمبدأ الإقليمية، وتخضع كذلك الجريمة ذاتها لإختصاص الدولة التابع لها هذا الأجنبي وفقا لمبدأ الإختصاص الشخصي، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في إختصاصها استنادا إلى مبدأ العينية[2]، كما تثور فكرة تنازع الإختصاص القضائي في حالة تأسيس الإختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث المعلومات غير المشروعة أو الصور ذات الطابع الإباحي على إقليم دولة معينة، وتم الإطلاع عليها في دولة أخرى، فوفقا لمبدأ الإقليمية فإن الإختصاص الجنائي والقضائي يثبت لكل دولة من الدول التي مستها الجريمة، سواء تلك التي وقع فيها الفعل الإجرامي أو تلك التي حدثت نتيجة الفعل فيها، الأمر الذي يؤدي إلى الإطاحة بمبدأ عدم جواز محاكمة الجاني أكثر من مرة على ذات الفعل والذي يعد من أهم المبادئ الجنائية[2].

ومن القضايا التي لفتت الأنظار إلى مشكلة الإختصاص القضائي، قضية تتلخص وقائعها في قيام مبرمج إنجليزي يعمل بأحد البنوك في دولة الكويت بالتلاعب في نظام

1 إبراهيم أحمد إبراهيم، تنازع القوانين والإختصاص القضائي الدولي وتنفيذ الأحكام الأجنبية، مكتبة وهبة، 1985.

2 جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص 73.

الحاسب الآلي الخاص بالبنك ليقوم بإجراء خصومات من أرصدة العملاء، ثم يقوم بإيداعها في الحساب الخاص به، وبعد عودة المتهم إلى إنجلترا قام بالكتابة إلى البنك طالبا إياه أن يقوم بتحويل الحساب الخاص به إلى عدة حسابات بنكية في انجلترا، وهو ما قام به البنك بالفعل. قدم المتهم للمحاكمة بتهمة الحصول على أموال الغير بطريق الإحتيال طبقا للقانون الإنجليزي، وحكم عليه بعقوبة السجن، إلا أن المتهم طعن في الحكم إستنادا إلى عدم إختصاص القضاء الإنجليزي بالفصل في الجريمة، حيث أن فعلي السحب والإيداع قد تما في دولة الكويت وليس في إنجلترا.

ورفضت محكمة الإستئناف الطعن المقدم من المتهم، وجاء في حيثيات رفضها أن النشاط الإجرامي للمتهم لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير البنك بالتحويل، وما أسفر عنه من حصوله على الأموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية[1].

ثالثا: إشكاليات الإنابة القضائية

من إشكاليات التعاون الدولي في مكافحة جرائم الذكاء الإصطناعي والخاصة بالإنابة القضائية الدولية ما يعرف بإشكالية فكرة السيادة، وإشكالية البطء في الإجراءات.

1- إشكالية فكرة السيادة

تعني فكرة السيادة أن الدولة هي السلطة العليا لا تعلوها سلطة في الداخل والخارج، بما يعنيه ذلك من إستئثار جهة الحكم في الدولة بكافة إختصاصات السلطة ومظاهرها، دون أن تخضع في ذلك لأي جهة أعلى، ودون أن تشارك معها في ذلك سلطة أو جهة مماثلة[2].

فعندما يرتكب فرد جريمة متصلة بالذكاء الإصطناعي في دولة ما وتجرى محاكمته في أخرى، فمن الواجب البحث عن أدلة ثبوت تلك الجريمة أو نفيها في البلد الذي وقعت فيه تلك الجريمة، وهذا ما يعرف بالتعاون القضائي بين الدول المختلفة، غير أن هذا التعاون قد يصطدم بفكرة سيادة كل دولة على إقليمها، إذ أن كل دولة عادة تقوم بنفسها وعبر جهازها القضائي بالفصل في كافة المنازعات التي تثار على أراضيها لإعتبارات ترتبط بفكرة السيادة، ومن هذا الجانب قد يبدو ومن غير المقبول إن تطلب مثلاً محكمة من دولة أخرى أجنبية أن تقدم لها العون والمساعدة في القيام بإجراء أو أكثر

1 نائلة عادل محمد فريد قورة، مرج سابق، ص 49.

2 عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية - دراسة مقارنة، الطبعه الأولى، دار النهضة العربية، مصر، 2001، ص 25.

من إجراءات التحقيق على إقليمها، وبالتالي فإن فكرة السيادة قد تعيق التعاون القضائي بين الدول المختلفة في مكافحة الجرائم[1].

2- إشكالية البطئ في إجراءات الإنابة

الأصل بالنسبة لطلبات الإنابة القضائية الدولية أن تسلم بالطرق الدبلوماسية، وهذا بالطبع يجعلها تتسم بالبطئ والتعقيد والذي قد يتعارض مع أعمال الإنترنت وما تتميز به من سرعة، وهو الأمر الذي إنعكس على التعاون الدولي في مكافحة هذه الجرائم، كذلك من الإشكاليات التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدراء أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الإستجابة وإلى غير ذلك من الأسباب[2].

الفرع الثاني: آليات التغلب عليها

تتمثل أهم آليات التغلب على إشكاليات التعاون الدولي في مجال مكافحة الجرائم المتصلة بالذكاء الإصطناعي في إتخاذ التدابير الموضوعية والتدابير الإجرائية.

أولا: التدابير الموضوعية

ينبغي على كل دولة أن تتبع سياسة جنائية تهدف إلى التعاون مع باقي الدول لأجل حماية المجتمعات من أخطار وأهوال جرائم الذكاء الإصطناعي، وذلك من خلال تبني ما يتلائم مع الطبيعة الخاصة لتلك الجرائم من تشريعات، وذلك حتى يمكن مواجهة مخاطر إستخدام الذكاء الإصطناعي في إرتكاب الأفعال الإجرامية، وإمكانية نقل وتخزين الأدلة المتعلقة بتلك الأفعال الإجرامية عبر شبكة الأنترنت، لذا يتعين على كل دولة أن تتبع التدابير التشريعية وغيرها من التدابير الأخرى اللازمة للكشف المبكر عن عملية الدخول غير المشروع، والبقاء غير المصرح إلى كافة أجزاء نظام شبكة الإنترنت وفقا لما تقضي به أحكام قوانينها الداخلية[3].

وكذلك إتخاذ التدابير التشريعية اللازمة لإدراك أي إعتراض غير قانوني وجعله جريمة جنائية وفقا للأحكام المقضي بها في القانون الوطني، كما يجب على كل دولة من الدول تضمين قوانينها ما يعتبر أعمال إضرار أو إتلاف أو محو أو إعاقة أو تعديل التي تستهدف البيانات جرائم جنائية يعاقب عليها القانون، كما يجب إعتبارها جرائم جنائية

1 عبد الرحيم صدقي، التعاون الدولي الجنائي، بحث منشور بالمجلة المصرية للقانون الدولي، عدد 40، 1980، ص1.

2 حسين الغافري، مرجع سابق، ص 555.

3 سامح أحمد بلتاجي موسى، مرجع سابق، ص542 ومابعدها.

تقتضى العقاب تلك الأعمال التي تعوق دون حق وظائف شبكة الإنترنت والحواسيب المتصلة بها، بإدخال أو نقل أو الإضرار أو محو أو إتلاف أو تعديل أو إعاقة بيانات الحواسيب المتصلة بالإنترنت، كما يجب على كل دولة أن تتبنى تدابير تشريعية تتيح مماطلة الأشخاص المعنوية جنائيا عما ينشئ من جرائم تتعلق بالتكنولوجيا الحديثة، وذلك في أحوال قصور الإشراف والرقابة من الشخص الطبيعي الذي يؤدي إلى حدوث جرائم أو تسهيل حدوثها[1]، وغالبا ما يطبق على الجرائم المعلوماتية خاصة في بعض الدول العربية القانون الجنائي التقليدي، غير أن تلك الجرائم هي جرائم جديدة ليس هناك ما يحكمها في القانون الجنائي العادي، والقاضي حين تعرض أمامه دعوى من الدعاوى في هذا الإطار هو مقيد بما هو نافذ من النصوص القانونية، مهما حاول الإجتهاد والقياس فإن حكمه غير محصن من الطعن فيه خاصة عندما يتم التشبث بمبدأ "لا جريمة ولا عقوبة إلا بنص"[2].

ثانيا: التدابير الإجرائية

تتمثل أهم التدابير الإجرائية التي يتعين على الدول إتخاذها، في الآتي[3]:

- تبني التدابير التشريعية الإجرائية التي تمكنها من تفتيش نظم الذكاء الإصطناعي، وفحص البيانات المخزنة بها وعلى مختلف وسائط التخزين الأخرى، سواء أكانت تقع داخل الدول أو خارجها، طالما كان ذلك الأمر يفيد التحقيق في الجريمة وتقتضيه مصلحته.

- ضرورة تدعيم التعاون بين أجهزة الشرطة في الدول المختلفة بناء على إتفاقيات دولية، بحيث إذا إكتشفت الشرطة الوطنية لدولة ما أن إحدى الجرائم المعلوماتية قد تم ممارستها عبر شبكة الإنترنت من خلال موقع موجود في الخارج فإنها تقوم بالإبلاغ عن هذه الجريمة إلى سلطات البوليس بالدولة التي تم فيها البث[4]. كما يجب أن تعين كل دولة الإدارة الأمنية بمكافحة هذا النوع من النشاط الإجرامي، فيوكل إليها تلقي البلاغات التي محورها جريمة ذكاء إصطناعي، ويكون من إختصاصها إتخاذ الإجراءات القانونية

1 سامح أحمد بلتاجي موسى، مرجع سابق، ص543.

2 حسين الغافري، مرجع سابق، ص 555.

3 حسين الغافري، المرجع نفسه ، ص 543.

4 طارق إبراهيم بسيوني، الأمن المعلوماتي، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2009، ص 594.

المناسبة حسب القوانين الوطنية، وتنفيذ التدابير الأمنية الوقائية من إستفحال هذا الخطر الملاصق للتقنية الحديثة، والهادم للإستفادة الصحيحة من أنظمة الذكاء الإصطناعي[1].

- على كل دولة إتخاذ التدابير التشريعية اللازمة لتخويل صلاحيات ضبط وإحضار الأشخاص المتورطين في الجريمة لسلطاتها المعنية، سواء أكانوا متواجدين على إقليمها أو في مكان آخر، لكي يقدم ذلك الشخص ما يقع تحت يده من بيانات مخزنة في أنظمة الذكاء الإصطناعي، أو أحد وسائط تخزين البيانات، وذلك بالكيفية التي تطلبها تلك السلطات لمصلحة التحقيق، وعلى كل دولة أن تتعاون فيما بينها في شأن تسهيل ذلك.

- على كل دولة تبني التدابير التشريعية اللازمة لتمديد إختصاصها القضائي على جرائم الذكاء الإصطناعي إذا وقعت بشكل كامل أو جزئي على إقليمها، أو على متن باخرة أو طائرة أو قمر صناعي يحمل علمها أو مسجل لديها، أو من أحد مواطنيها إذا كانت الجريمة من الجرائم التي يعاقب عليها القانون وفقا لأحكام قانون العقوبات الساري في محل وقوع الجريمة، أو إذا وقعت الجريمة خارج نطاق الإختصاص الإقليمي لأي دولة أخرى.

- على كل دولة إتخاذ التدابير التشريعية اللازمة لتمكين سلطاتها من الحصول على نسخة للبيانات المخزنة في أحد الأنظمة، بما يحقق مصلحة التحقيق.

- إضفاء صفة الضبطية القضائية على العاملين في مجال المعلومات من غير رجال الشرطة، كمزودي الدخول وخدمات الإنترنت، إذ تبعا لأعمالهم فإنهم يقومون بالرقابة عبر المزود عن سير حركة العمل ومدى الخضوع للنظام والقانون من قبل العاملين والمتعاملين مع شبكة الإنترنت، بحيث إذا حدث ووجدت الجريمة باكتشافها بهذا الأسلوب فإنه ليس لهؤلاء سوى التحفظ على أدلة الجريمة إلى حين حضور رجال الضبط القضائي[2].

- قيام أجهزة الشرطة للدول بعمل دوريات المراقبة على مؤسسات إنتاج وتطوير أنظمة الذكاء الإصطناعي، للوقاية من صور الإجرام المتعلقة بذلك كالإستيلاء على البيانات بطريقة غير مشروعة وإساءة تصنيع الروبوتات بطريقة تستهدف الإضرار بمستخدميه[3].

---

1 طارق إبراهيم بسيوني، المرجع نفسه، ص 595.

2 نبيلة هبة هروال، مرجع سابق، ص 87.

3 عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون - دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، 2003، ص 471.

وخلاصة القول أنه ولأجل التغلب على إشكاليات التعاون الدولي في مكافحة الجرائم المستحدثة المرتكبة بإستخدام الذكاء الإصطناعي، يجب تظافر الجهود الدولية مع المحاولات الوطنية في سبيل الوصول إلى مواجهة وحلول شاملة تنطلق من رؤية قانونية كاملة.

خلاصة الفصل

حاولنا من خلال الفصل الثاني من الدراسة، دراسة الشق الإجرائي للجرائم الواقعة بإستخدام الذكاء الإصطناعي، حيث قمنا بعرض الوسائل والأساليب المتبعة في التحري عن هذه الجرائم لما لها من خصوصية، مع بيان الإجراءات المستحدثة في هذا الصدد.

كما قمنا بإبراز دور كل من القضاء المتخصص والشرطة القضائية وغيرها من الجهات الفاعلة في مكافحة هذه الجريمة التقنية.

وفي الأخير تعرضنا إلى آليات التعاون الدولي للكشف عن هذا النوع من الجرائم ورصد مرتكبيها، بإعتبارها جرائم تتعدى الحدود الوطنية والذي يشكل تهديدا لسيادة الدول.

خاتمة

خاتمة

لم يعد الذكاء الإصطناعي مجرد خيال علمي أو فرضية قيد الدراسة، وإنما بات واقعا ملموسا نجد تطبيقاته في كافة مجالات الحياة بميزاته وعيوبه، وقد خلصنا من دراسته هذه إلى أن أعمال الذكاء الاصطناعي هذه تتصل بأكثر من طرف، فهناك المصنع والمبرمج والمالك والمستخدم وهناك أيضا طرف خارجي آخر، وقد يقوم أي من هذه الأطراف بإرتكاب جريمة بإستخدام تقنيات الذكاء الاصطناعي، وقد تكون هذه الجرائم عن قصد، نتيجة فعل أو إمتناع وقد تكون نتيجة إهمال، الأمر الذي يرتب مسؤولية جزائية عن هذا النوع من الجرائم. فعند ثبوت الفعل من جانب أي من هذه الأطراف يرتب مسؤوليتها عن الجرائم الناجمة عن أعمال الذكاء الإصطناعي، وهذا يوصلنا لنتيجة واقعية مفادها أن الذكاء الإصطناعي مازال غير مستقل، حتى أنه مازال مجرد وسيلة لإرتكاب أفعال قد ترتب نتائج جرمية ويستمد قراراته وينجز أعماله بواسطة البشر، وبالتالي أي نتيجة جرمية تترتب على أعماله لا تخرج عن كونها من فعل البشر.

ومع إنتشار تقنياته على نطاق واسع والحاجة الماسة إلى إستخدامه، يستدعي تحديث المنظومة القانونية لمواجهة أي إستخدام سلبي لهذا النظام الذكي، مما إستوجب على المشرع الجزائري ملائمة النصوص التشريعية للتطور التكنولوجي، وهو ما دفعنا في هذه الدراسة الموضوعة بين أيديكم، إلى البحث في المسؤولية الجزائية الناشئة عن الإستخدام غير المشروع لتقنيات الذكاء الاصطناعي بشقيها الموضوعي والإجرائي.

وإستنادا على ما سبق ذلك، توصلنا من خلال هذه الدراسة إلى إستنتاج العديد من النتائج نوردها فيما يلي:

* يعتبر الذكاء الإصطناعي تقنية حديثة متطورة ومتميزة سهلت سيرورة الحياة، وقد شملت هذه التقنيات في إستخدامها كافة المجالات.

* لتقنيات الذكاء الإصطناعي العديد من الخصائص التي تمكنها من محاكاة الذكاء البشري في الإستقلالية والتفكير والإدراك والتنبؤ والتكيف والتعلم المستمر.

* سرعة إنتشار تقنيات الذكاء الإصطناعي، يترتب عليها ظهور الكثير من الجرائم المرتبطة بها، والتي لم يتضمها بعد قوانيننا العقابية.

* المجرم المعلوماتي مجرم يختلف عن المجرم التقليدي فهو ذو علم وكفاءة ويتميز بقدرات عقلية وذهنية تمكنه من الإفلات من العقاب.

* جرائم المعلوماتية عموما وجرائم إستخدام الذكاء الإصطناعي لا تترك أثرا ماديا واضحا في مسرح الجريمة كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة.

* تقوم المسؤولية الجزائية عن إستخدام الذكاء الإصطناعي في حق الشخص الطبيعي دون أنظمة الذكاء الإصطناعي، بإعتبار أن المشرع الجزائري لم يعترف بالشخصية القانونية لكيانات الذكاء الإصطناعي، ومنه فلا مجال للحديث عن مسئولية جزائية في حقها، والعقوبات التي قد تمس بالكيان كالإغلاق والمصادرة هي في الأصل عقوبات في حق الشخص الطبيعي، إلا أنها تمتد للكيان بصفته أداة للجريمة فقط لا غير.

* أورد المشرع الجزائري بعضا من صور الإستخدام غير المشروع للذكاء الإصطناعي وسكت عن الكثير منها، ما يجعلنا نقف أمام نتيجتين حتميتين لا ثالث لهما، إما خرق مبدأ شرعية الجرائم والعقوبات أو إفلات المجرمين من العقاب.

* قصور التشريع الجزائري لعدم وجود تأطير قانوني للذكاء الإصطناعي، سواء من حيث إنعدام الضوابط التي تحكم إستخدامه أو قصور القانون الجزائي وعجزه عن مواكبة التطور التكنولوجي.

* خصوصية إجراءات الكشف عن الجرائم المرتكبة بإستخدام الذكاء الإصطناعي، بحيث تختلف تماما عن الإجراءات التقليدية المتبعة في بقية الجرائم، ورغم ذلك لا زالت بحاجة لتعديلات لتتوائم ومقتضيات الجريمة.

* أبرز المشرع الجزائري إرادته في التوفيق بين حمايته لحق الخصوصية من الإنتهاكات ومقتضيات الإجراءات المستحدثة التي تتطلبها للكشف عن جرائم الذكاء الإصطناعي، كإعتراض المراسلات والتسرب، ويظهر هذا جليا من خلال تقييده لهذه الإجراءات بجملة شروط كالإذن وتحديد المدة.

* جرائم الذكاء الإصطناعي من الجرائم العابرة للحدود والتي تثير العديد من الإشكاليات خاصة من ناحية تنازع الإختصاص القضائي الدولي.

* عدم وجود تنسيق بين الدول لإتخاذ التدابير اللازمة لمواجهة هذه الجرائم في إطار التعاون الدولي، ما يترك المجال لتملص مرتكبيها من العقاب فلا تطالهم أيدي العدالة.

و محاولة منا لتكملة ما قمنا به من عمل خلال إنجلز هذه الدراسة ارتأينا تقديم بعض الإقتراحات التي بدت لنا ضرورية و لازمة في هذا الخصوص:

* نلتمس من المشرع الجزائري وضع تعريف قانوني موحد للذكاء الإصطناعي.

* نوصي المشرع الجزائري بضرورة تحديد الضوابط التي تحكم التعامل مع الذكاء الإصطناعي بداية من تصنيعه إلى برمجته وصولا إلى إستخدامه.

* نأمل أن يقوم المشرع الجزائري بإستحداث نصوص تشريعية تضمن مواكبتها للتطور السريع في مجال التكنولوجيا الرقمية.

* نعتقد أن تعديل قانون العقوبات بتضمين مختلف الصور الإجرامية لإستخدام الذكاء الإصطناعي مع فرض عقوبات صارمة على مرتكبيها قد يسد الفراغ التشريعي بالشكل الذي لايسمح بإفلات الجناة أو حدوث إعتداءات على أهم المبادئ في القانون الجنائي.

* قد يكون من الأجدر تعديل قانون الإجراءات الجزائية بإستحداث إجراءات وجهات خاصة بمتابعة جرائم الذكاء الإصطناعي على نحو مستقل عن جرائم المعلوماتية الأخرى، إضافة إلى تدعيم الأجهزة المنوط لها إتخاذ الإجراءات بتقنيات وأساليب جديدة تضمن المواجهة الفعالة.

* نقترح تفعيل دور المجتمع المدني ووسائل الإعلام في التوعية بمخاطر الذكاء الإصطناعي وسبل الوقاية من أضرارها، مع ضرورة الإبلاغ عن الإنتهاكات التي قد تقع بإستخدامه.

* تحقيق سبل التعاون الدولي في مجال تسليم المجرمين والمساعدة القضائية المتبادلة، وإتخاذ كافة التدابير التشريعية والإجرائية لمكافحة الجرائم المرتكبة بإستخدام الذكاء الإصطناعي.

* وجوب الإهتمام بتدريب الخبراء والمحققين والقضاة على التعامل مع الجرائم المعلوماتية وجرائم الذكاء الإصطناعي.

* التطوير المستمر لأدوات التحليل كأدوات نسخ محتويات الأقراص وتخزين البيانات. ومواكبة المستجدات التككنولوجيا في الكشف عن الجرائم بالتقنيات الحديثة.

* وأخيرا وليس آخرا، تدريس مقاييس الأنظمة المعلوماتية والجرائم التي قد تنشأ عنها في كلية الحقوق والشرطة والمعاهد القضائية، بحيث يشترط في المتقدمين إليه أن يكونوا حاصلين على مؤهل جامعي في علوم الحاسوب والشبكات.

وهكذا يكون البحث قد إكتمل بحمد الله، فإن كان فيه الحسن والصواب فهو من الله سبحانه وتعالى، وإن كان فيه النقص فهو منا، ولما لا ونحن بشر نجتهد ونخطأ ونصيب، فإن أصبنا فأجرنا على الله وإن أخطأنا فندعوه ألا يحرمنا أجر المجتهدين.

قائمة المصادر والمراجع

Les Références

أ) قائمة المصادر والمراجع باللغة العربية

1) النصوص القانونية

1. الدستور الجزائري لسنة 1996.
2. إتفاقية الأمم المتحده لمكافحة الفساد، سنة 2003، القانون الدولي، المادة 48، التعاون في مجال إنفاذ القانون.
3. الأمر رقم 66-155 المؤرخ في 8 جوان 1966 والمتضمن قانون الإجراءات الجزائية الجزائري، المعدل و المتمم بالأمر رقم 21- 11، المؤرخ في 25 اوت 2021، ج.ر، عدد 65 بتاريخ في 26 أوت 2021.
4. القانون رقم 09-04 المؤرخ في 05 اوت 2009، ج.ر، عدد 47 بتاريخ 16 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.
5. القانون رقم 18-05 المؤرخ في 10 ماي 2018، الصادر بالجريدة الرسمية العدد 28 بتاريخ 16 ماي 2018 المتعلق بالتجارة الإلكترونية.
6. القانون رقم 18-07 المؤرخ في 10 جوان 2018، ج.ر، عدد 34 بتاريخ 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي.
7. القانون رقم 24-02 المؤرخ في 26 فيفري 2024، ج.ر، عدد 15 بتاريخ 29 فيفري 2024 والمتعلق بمكافحة التزوير وإستعمال المزور.
8. المرسوم التنفيذي رقم 06- 348، المؤرخ في 5 اكتوبر 2006، ج.ر، عدد 63 بتاريخ 8 أكتوبر 2006، يتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

2) الكتب العامة

1. إبراهيم أحمد إبراهيم، تنازع القوانين والإختصاص القضائي الدولي وتنفيذ الأحكام الأجنبية، مكتبة وهبة، عابدين – القاهرة، مصر، 1985.
2. بلحاج العربي، أبحاث ومذكرات في القانون والفقه الإسلامي، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، 1996.
3. طارق إبراهيم بسيوني، الأمن المعلوماتي، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2009.
4. علي شملال، المستحدث في قانون الإجراءات الجزائية، التحقيق والمحاكمة، دار هومه، الجزائر، 2016.
5. عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية - دراسة مقارنة، الطبعه الأولى، دار النهضة العربية، مصر، 2001.
6. لخضر بوكحيل، الإجراءات الجنائية، مطبعة الشهاب، باتنة، الجزائر، دون سنة.

7 محمد أمين الرومي، المستند الإلكتروني، دار الكتب القانونية، المحلة الكبرى، مصر، 2008.
8 محمد أمين خرشة، مشروعية الصوت والصورة في الإثبات الجنائي، الإصدار الأول، دار الثقافة للنشر والتوزيع، الأردن، 2001.
9 مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الأنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، دار الكتب والوثائق القومية المصرية، مصر، 2003.
10 نبيل صقر، الوسيط في شرح جرائم الأشخاص، دار الهدى، الجزائر، 2009.

3) الكتب الخاصة

1 جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، مصر، 2002.
2 حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، مصر، 2017.
3 حسن محمد الطوالبه، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديث، الأردن، 2004.
4 خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعه الأولى، دار الثقافه والنشر والتوزيع، عمان، 2011.
5 سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلوماتية الدولية، دار النهضة العربية، 2013.
6 عادل عبد النور، أساسيات الذكاء الإصطناعي، منشورات مواقف، لبنان، 2017.
7 عبد الله موسى، أحمد حبيب بلال، الذكاء الإصطناعي ثورة في تقنيات العصر، المجموعة العربية للتدريب والنشر، الطبعة 1، مصر، 2019.
8 عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون - دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، 2003.
9 فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندريه، مصر، دون سنة.
10 محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.
11 محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والانترنت، موسوعة جرائم المعلوماتية، منشأة المعارف بالإسكندرية، مصر، 2006.
12 محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الإبتدائي- دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر.

13 محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت - دراسة مقارنة، دار الفكر والقانون، المنصورة، مصر، 2012.

14 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضه العربية، مصر، 2008.

15 نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، مصر، 2003.

16 نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، درا الفكر الجامعي، مصر، 2007.

4) المقالات والدراسات

1 آمنة أمحمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الأعمال، اعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز البحث العلمي، الجزائر، 29 مارس 2017.

2 سعيده بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوة منثوري، قسنطينة، الجزائر، مجلد ب، العدد 52، ديسمبر 2019.

3 طاهر أبو العيد، دليل الذكاء الإصطناعي لطلبة القانون والباحثين في الوطن العربي، مجلة قانونية وتكنولوجيا، مصر، 2023.

4 عبد الرحيم صدقي، التعاون الدولي الجنائي، بحث منشور بالمجلة المصرية للقانون الدولي، عدد 40، 1980.

5 عبد القادر رويس، أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة أحمد بن يحيى الونشريسي، تيسمسيلت، الجزائر، المجلد 2، العدد 1، جوان 2017.

6 عبد الناصر محمد محمود فرغلي، محمد سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية، عربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2007.

7 عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسه بأنظمه الإتصال والمعلوماتيه، مجلة دائرة البحوث القانونية والسياسية، المركز الجامعي مرسلي عبد الله، تيبازه، الجزائر، العدد 04، جانفي 2018.

8 عز الدين عز الدين، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة بسكرة، 16 و 17 نوفمبر 2015.

9 علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، الإمارات العربية المتحدة، 2000.

10 محمد بكرارشوش، الإختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري، دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقله، الجزائر، المجلد 8، العدد 14، جانفي 2016.

11 مرام عبد الرحمان مكاوي، الذكاء الإصطناعي على أبواب التعليم، مجلة القافلة، أرامكو السعودية، السعودية، المجلد 67، العدد 6، 2018.

12 مصطفى أبو مندور موسى عيسى، مدى كفاية القواعد العامة للمسؤولية المدنية في تعويض أضرار الذكاء الإصطناعي، مجلة حقوق دمياط للدراسات القانونية والإقتصادية، كلية الحقوق، جامعة دمياط، العدد 5، مصر، 2022.

13 مليكة مذكور، هل المعرفة خاصية إنسانية حقا؟، الأكاديمية للدراسات الإجتماعية والإنسانية، جامعة حسيبة بن بوعلى، الشلف- الجزائر، المجلد 12، العدد 01، 2020.

14 ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب والأنترنت، دار الكتب القانونية، مصر، 2006.

15 ناجية شيخ، أساليب البحث والتحري المستحدثة في القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، المجلد 8، العدد 1، جوان 2013.

16 نادية رواحنة، رواحنة زوليخة، جريمة إنتهاك حرمة المكالمات أو الاحاديث الخاصة أو السرية في قانون العقوبات الجزائري، مجلة المفكر، المجلد 17، العدد 02، 2022.

17 وفاء محمد أبو المعاطي صقر، المسؤولية الجنائية عن جرائم الذكاء الإصطناعي - دراسة تحليلية إستشرافية-، مجلة روح القوانين، كلية الحقوق- جامعة طنطا، مصر، العدد 96، أكتوبر 2021.

18 يحيى إبراهيم دهشان، المسؤولية الجنائية عن جرائم الذكاء الإصطناعي، بحث منشور بمجلة الشريعة والقانون، كلية القانون، جامعة الإمارات، الإمارات العربية المتحدة، 2019.

5) الأطروحات والمذكرات

1 حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت دراسة مقارنة، رسالة دكتوراه في القانون، كلية الحقوق، جامعة عين شمس، القاهره، مصر، 2007.

2 سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الأنترنت، أطروحة الدكتوراه في القانون الجنائي، كلية الحقوق، جامعة الإسكندرية، مصر، 2010.

3 مريع أحمد مسعود، آليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون رقم 09-04، رسالة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2013.

4 نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجيستير في القانون، كلية الحقوق، جامعة لخضر، باتنة، الجزائر، 2013.
5 نبيل لحمر، دور الأقطاب الجزائية المتخصصة في مكافحة الجريمة، رسالة ماجستير في القانون، كليه الحقوق، جامعة قسنطينة، الجزائر، 2014.
6 عباس حفصي، جرائم التزوير الإلكتروني، دراسة مقارنة لنيل شهادة دكتوراه العلوم الإسلامية، تخصص شريعة وقانون، جامعة وهران 1، وهران، 2014-2015.
7 مجراب الدوادي، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة دكتوراه في القانون، كليه الحقوق، جامعة بن يوسف بن خدة، الجزائر، 2016.
8 عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، 2018.
9 دلال مولاي ملياني، إشكاليه الإثبات في جرائم الأنترنت في التشريع الجزائري، أطروحة دكتوراه في القانون، كليه الحقوق، جامعة ابو بكر بلقايد، تلمسان، الجزائر، 2018.
10 عزيزه رابحي، الأسرار المعلوماتيه وحمايتها الجزائية، أطروحة دكتوراه في القانون، كليه الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018.
11 الطيبي البركة، دراسة مقارنة، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر، 2021.
12 خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية – دراسة مقارنة، أطروحة دكتوراه في القانون، كلية الحقوق، جامعة أحمد دراية، أدرار، الجزائر، 2021.
13 بلقاضي شيماء، دور التكنولوجيا المالية والذكاء الإصطناعي في الرفع من كفاءة القطاع المصرفي الجزائري – محاكاة تجارب دولية عربية، مذكرة مقدمة لنيل شهادة ماستر أكاديمي في الإدارة المالية، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة العربي بن مهيدي، أم البواقي، الجزائر، 2020 /2021.
14 سلام عبد الكريم، التنظيم القانوني للذكاء الإصطناعي- دراسة مقارنة-، أطروحة مقدمة كجزء من متطلبات نيل درجة الدكتوراه في القانون المدني، كلية القانون، جامعة كربلاء، العراق، 2022.

6) الوثائق الأخرى

1 مساهمة الشرطة العلمية والتقنية في مجال التحقيقات الجنائية، وثيقة خاصة صادرة عن مديرية الشرطة القضائي، المديرية العامة للأمن الوطني.

7) المواقع الإلكترونية

1 تقرير عن المخاطر الحقيقية للذكاء الإصطناعي، هارفرد بيزنس ريفيو العربية، جانفي 2016، ht t p: / / Ai l 00. St anf ord/ 2016report، شوهد بتاريخ 2024/04/19 على الساعة 14 : 18.

2 لطفي خديجة، كيف يستطيع الذكاء الإصطناعي التأثير على التعليم؟، ht t ps: / / www. new- educ. com/ cat egory/ st udi es، شوهد بتاريخ 2024/04/30 على الساعة 21 : 22.

3 جيمس جونسون، أتمتة الحرب وتأثير الذكاء الإصطناعي في سباق التسلح، ht t ps: / / f ut ureuae. com/ ar/ Hbme/ I ndex/ 2، شوهد بتاريخ 2024/05/02 على الساعة 11 : 09.

4 ما هي إستخدامات الذكاء الإصطناعي في قطاع الرعاية الصحية ؟، ht t ps: / / www. t hearabhospi t al . com، شوهد بتاريخ 2024/05/02 على الساعة 45 : 09.

ب) قائمة المراجع باللغة الاجنبية

1) Books / Ouvrages

1 Andreas Kaplan, Michael Haenliein, Who's the fairest in the land ? On the interpretations and illustrations and implications of artificial intelligence, Business Horizons, Vol 62, 2019.

2 Bainbridge David, hacking the unavthorised access of computer system, The legal implication, Modern Law Review, 1989, Vol 52.

3 Gentsch P., AI in Marketing - Sales and Service, Palgrave Macmillan, Cham, 2019.

4 Gurney, N., Marsella, S., Ustun, V., Pynadath, Operationalizing theories of theory of mind: A survey in AI Fall Symposium, Springer, 2021.

5 Lazetik GB, Koshevaliska O., Digital Evidence in Criminal procedures, A comparative approach, Balkan Social Science Review, 21, 2013.

6 S. Singh, Attribution of legal personhood to artificially intelligent beings, Bharti Law review, July–Sept – 2017.

7 Stuart J. Russell, Peter Norvig, Artificial Intelligence: A Modern approach is a university textbook on artificial intelligence, 3th Edition, Pearson Education, 2010.

2) Theses and Memories / Thèses et Mémoires.

1 Adrien Bonnet, La responsabilité du fait de l'intelligence artificielle, Mémoire de recherche Droit privé général, Université Panthéon Assas,Paris, 2014/2015

2 Ibtissem Maalaoui, Les infractions portant atteinte à la sécurité du système informatique d'une entreprise, Mémoire présenté en vue de l'optention du grade Maitrise en droit (LLM) option droit des affaires, Faculté des études supérieures, Université de Montréal, Canada, 2011.

3 Nour EL KAAKOUR, L'intelligence artificielle et la responsabilité civile délictuelle, Mémoire pour l'obtention du Diplôme d'Études Approfondies En Droit Interne et International des Affaires, Faculté de Droit et des Sciences Politiques et Administratives, Liban, 2017.

3) Others Documents / Autres Documents

1 EUROPEAN COMMISSION, Independent High-Level Expert Group On Artificial Intelligence: a definition of AI - Main capabilities and scientific disciplines, Springer, 08/04/2019.

2 Résolution européenne relative à la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union, 206 final, COM (2021).

4) Web Site/ Site Web.

1 Mangani D., 5 AI Application i banking to look outfor in next 5 years, https://www.analyticsvidhya.com/blog/2017/04/5, Viewed on 30/04/2024 at 17 :33.

2 https://www.javatpoint.com/types-of-artificial-intelligence, Viewed on 16/04/2024 at 14:45.

3 http://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third -even -possible, Viewed on 25/04/2024 at 11 :10.

4 Sophia Hanson, Robotics, www.hansonrobotics.com/sophia, Viewed on 03/05/2024 at 21 :31.

5 E. Lavallée, Lorsque l'intelligence artificielle est discriminatoire, Journal le droit de savoir, https://www.lavery.ca/fr/publications/nos-publications/3013-lorsque-lintelligence-artificielle-est-discriminatoire .html, Viewed on 03/05/2024 at 19 :55.

الفهرس

الفهرس

العنوان	الصفحة
مقدمة	1
الفصل الأول: الأحكام الموضوعية للمسؤولية الجزائية للإستخدام غير المشروع للذكاء الإصطناعي	7
المبحث الأول: ماهية تقنيات الذكاء الإصطناعي	9
المطلب الأول: مفهوم الذكاء الإصطناعي	9
الفرع الأول: تعريف الذكاء الإصطناعي	9
الفرع الثاني: الخصائص المنفردة لأنظمة الذكاء الإصطناعي	9
أولا: الطابع المعنوي اللامادي لأنظمة الذكاء الإصطناعي	11
ثانيا: الإستقلال الوظيفي لأنظمة الذكاء الإصطناعي	11
ثالثا: صعوبة حصر أفعال أنظمة الذكاء الإصطناعي وعدم التنبؤ بها.....	11
رابعا: عدم التقييد الزمكاني لأنظمة الذكاء الإصطناعي	11
المطلب الثاني: الذكاء الإصطناعي وإستخداماته.....	12
الفرع الأول: أنواع الذكاء الإصطناعي	12
أولا: الذكاء الإصطناعي تبعا للقدرات	12
ثانيا: الذكاء الإصطناعي تبعا للوظائف	13
الفرع الثاني: مجالات إستخدام الذكاء الإصطناعي	13
أولا: مجال التعليم	13
ثانيا: المجال المصرفي	13
ثالثا: أنظمة النقل الذكية..... ...	15
رابعا: المجال العسكري..... ...	16
خامسا: المجال الطبي	17
سادسا: مجالات أخرى	17
الفرع الثالث: الآثار السلبية لإستخدامات تقنيات الذكاء الإصطناعي.....	17
المبحث الثاني: المسؤولية الجزائية عن جرائم الذكاء الإصطناعي	18
المطلب الأول: أطراف المسؤولية الجزائية في جرائم الذكاء الإصطناعي	18
الفرع الأول: المسؤولية الجزائية للمصنع أو المبرمج	19
الفرع الثاني: المسؤولية الجزائية للمالك أو المستخدم.....	19
الفرع الثالث: المسؤولية الجزائية للطرف الخارجي.....	19
الفرع الرابع: المسؤولية الجزائية لكيان الذكاء الإصطناعي نفسه	20
المطلب الثاني: أبرز جرائم الذكاء الإصطناعي في التشريع الجزائري	20
الفرع الأول: التلاعب بالمعطيات.....	20
أولا: أركان جريمة التلاعب بالمعطيات	22
ثانيا: العقوبات الأصلية المقررة لجريمة التلاعب بالمعطيات	22
الفرع الثاني: الدخول أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات	

أولا: أركان جريمة الدخول أو البقاء غير المصرح به.....	22
ثانيا: عقوبة جريمة الدخول أو البقاء غير المصرح بهما	22
الفرع الثالث: إنتهاك الخصوصية.....	23
أولا: أركان جريمة إنتهاك الخصوصية	24
ثانيا: العقوبات الأصلية المقررة لجريمة إنتهاك الخصوصية	25
الفرع الرابع: التزوير الإلكتروني.....	26
أولا: أركان جريمة التزوير الإلكتروني	27
ثانيا: العقوبات الأصلية المقررة لجريمة التزوير الإلكتروني	27
الفرع الخامس: الأحكام المشتركة للجرائم المعلوماتية	28
أولا: الأحكام المتعلقة بالجرائم.....	28
ثانيا: الأحكام المتعلقة بالعقوبة.....	28
خلاصة الفصل.....	31
	31
	32
	33
	33
	34
	36
	36
	36
	36
	38
الفصل الثاني: الأحكام الإجرائية للمسؤولية الجزائية للإستخدام غير المشروع للذكاء الإصطناعي.....	39
المبحث الأول: خصوصية الإجراءات الجزائية في جرائم إستخدام الذكاء الإصطناعي.....	41
المطلب الأول: إجراءات التحقيق الأولي في جرائم إستخدام الذكاء الإصطناعي ..	41
الفرع الأول: الأعوان المكلفون بالتحري وجمع الأدلة	42
أولا: جهاز الضبطية القضائية.....	42

ثانيا: مقدمي الخدمات	44
ثالثا: الشرطة العلمية والتقنية	
الفرع الثاني: وسائل التحري وجمع الأدلة	45
أولا: الوسائل المادية	48
ثانيا: الوسائل الإجرائية	
ثالثا: حجز المعطيات	49
الفرع الثالث: الإثبات في جرائم إستخدام الذكاء الإصطناعي	50
أولا: مبدأ شرعية الإثبات الجنائي	
ثانيا: مشروعية الدليل الإلكتروني في الإثبات الجنائي	51
المطلب الثاني: الإجراءات المستحدثة لمواجهة جرائم إستخدام الذكاء الإصطناعي	54
الفرع الأول: أساليب التحري الخاصة	55
أولا: إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور	
ثانيا: التسرب	55
الفرع الثاني: إنشاء الأقطاب الجزائية المتخصصة	57
أولا: الإختصاص الإقليمي للأقطاب الجزائية المتخصصة.....	
ثانيا: تمديد الإختصاص المحلي.....	58
المبحث الثاني: الآليات الدولية لمكافحة جرائم إستخدام الذكاء الإصطناعي	58
المطلب الأول: سبل التعاون الدولي في جرائم إستخدام الذكاء الإصطناعي	61
الفرع الأول: التعاون الأمني..... .	
أولا: صور التعاون الأمني..... .	63
ثانيا: دور الإنتربول	64
الفرع الثاني: التعاون القضائي	
أولا: نظام قضاة الإتصال في مجال الجرائم المتصلة بالذكاء الإصطناعي....	66
ثانيا: نظام تسليم المجرمين..... .	68
المطلب الثاني: إشكاليات التعاون الدولي وآليات التغلب عليها	
الفرع الأول: إشكاليات التعاون الدولي.....	68
أولا: القصور التشريعي للدول والتعارض فيما بينها	68
ثانيا: تنازع الإختصاص القضائي الدولي	68
ثالثا: إشكاليات الإنابة القضائية	69
الفرع الثاني: آليات التغلب عليها	70
أولا: التدابير الموضوعية ...	
ثانيا: التدابير الإجرائية	71
خلاصة الفصل	71
	72
	73
	73
	73

	74 76 77 77 78 81
خاتمة	82
قائمة المصادر والمراجع	87
الفهرس	96
الملخص	101

الملخص

الملخص

ملخص:

تهدف هذه الدراسة إلى تسليط الضوء على تقنيات الذكاء الإصطناعي، من خلال التطرق إلى ماهية الذكاء الإصطناعي متضمنا تحديد مفهومه فضلا عن التعرف على أنواعه ومجالاته المتعددة لا سيما في المجال الطبي والإعلامي، ثم الإنتقال بعد ذلك إلى المسؤولية الجزائية عن الإستخدام غير المشروع متضمنا تحديد المسؤولية الجزائية وأطرافها وبيان أركانها في بعض الجرائم المنصوص عليها في التشريع الجزائري والعقوبات المقررة لها.

ثم نتطرق إلى خصوصية الإجراءات الجزائية في جرائم إستخدام الذكاء الإصطناعي من خلال دراسة إجراءات التحقيق الأولي في تلك الجرائم والإجراءات المستحدثة لمواجهتها من المشرع الجزائري، وفي الاخير نستعرض الآليات الدولية لمكافحتها وإشكاليات التعاون الدولي في ذلك الشأن.

الكلمات المفتاحية: ذكاء إصطناعي، مسؤولية جزائية، إستخدام غير مشروع، جريمة إلكترونية، جريمة معلوماتية.

Abstract*:*

This study aims to shed light on artificial intelligence techniques by addressing the nature of artificial intelligence, including defining its concept as well as recognizing its types and various fields, particularly in the medical and media sectors. Subsequently, the study moves on to the criminal liability for illicit use, including determining criminal liability and its parties, and explaining its elements in certain crimes stipulated in Algerian legislation and the penalties prescribed for them.

We then address the peculiarities of criminal procedures in crimes involving the use of artificial intelligence by studying the preliminary investigation procedures in these crimes and the newly introduced procedures to combat them by the Algerian legislator. Finally, we review international mechanisms to combat these crimes and the issues of international cooperation in this regard.

Keywords: Artificial intelligence, criminal liability, illicit use, cybercrime, information **crime.**

Résumé*:*

Cette étude vise à mettre en lumière les techniques de l'intelligence artificielle en abordant la nature de l'intelligence artificielle, y compris la définition de son concept ainsi que la reconnaissance de ses types et de ses multiples domaines, notamment dans les domaines médical et médiatique. Ensuite, l'étude passe à la responsabilité pénale liée à l'utilisation illicite, en incluant la détermination de la responsabilité pénale et de ses parties ainsi que l'explication de ses éléments constitutifs dans certains crimes prévus par la législation algérienne et les sanctions qui leur sont applicables.

Nous abordons ensuite les particularités des procédures pénales dans les crimes liés à l'utilisation de l'intelligence artificielle en étudiant les procédures d'enquête préliminaire dans ces crimes et les procédures nouvellement introduites pour y faire face par le législateur algérien. Enfin, nous examinons les mécanismes internationaux de lutte contre ces crimes et les problématiques de la coopération internationale dans ce domaine.

Mots-clés : Intelligence artificielle, responsabilité pénale, utilisation illicite, cybercriminalité, crime informatique.