

جامعة الشاذلي بن جديد –
الطارف
كلية الحقوق والعلوم
السياسية



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

الرقم التسلسلي:.....

مذكرة بعنوان

التحريرات الالكترونية في مواجهة الجريمة المعلوماتية

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون جنائي وعلوم جنائية

إشراف الأستاذة
د. مقدم رشا

إعداد الطالبتين
-مويسي بسمة
-زياني نور الهدى

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
د. بوكوبة مريم	أستاذ محاضر-ب	الشاذلي بن جديد -الطارف	رئيسا
د. مقدم رشا	أستاذ محاضر-أ	الشاذلي بن جديد -الطارف	مشرفاً ومقرراً
د. مدار توفيق	أستاذ محاضر-ب	الشاذلي بن جديد -الطارف	ممتحنا

السنة الجامعية: 2025/ 2026

شكر

يقول الحبيب المصطفى ﷺ: 'مَنْ لَمْ يَشْكُرِ النَّاسَ لَمْ يَشْكُرِ اللَّهَ'

أولاً وقبل كل شيء ..نحمد الله العلي القدير، حمد الشاكرين الذاكرين، الذي أمدنا بالصحة والعافية، وأسبغ علينا من كرمه وتوفيقه ما جعلنا نتمم هذا العمل الأكاديمي، فلك الحمد يا ربي حتى ترضى، ولك الحمد إذا رضيت، ولك الحمد بعد الرضا.

إلى منارة البحث وعماد هذا العمل.. الأستاذة المشرفة الفاضلة ..نتقدم بخالص شكرنا وعظيم امتناننا لسيادتها، لما حَبَّتْنا به من سعة صدر، ونُصَحِ أبوي، وتوجيهاتٍ علمية سديدة كانت بمثابة البوصلة التي أنارت لنا عتمة الصعاب وذللت أمامنا عقبات البحث. لقد كانت رعاية جنابها العلمية نعم العون ونعم السند، فجزاها الله عنا خير الجزاء.

إلى القامات العلمية السامقة.. رئيس وأعضاء لجنة المناقشة الموقرة ..نرفع أسمى عبارات التقدير والاحترام لقبولكم تشريف هذا العمل بالتقييم والمناقشة. إن وقوفنا اليوم أمام قاماتكم العلمية هو فخرٌ لنا، وثقتنا كاملة في أن نصائحكم المصوبة وتقويمكم السديد سيكون التاج الذي يكتمل به بهاء هذه المذكرة.

إلى الأساتذة الأفاضل في كلية الحقوق. كل الشكر والامتنان إلى كل أستاذ ومعلم نهلنا من بحر علمه طيلة مسيرتنا الجامعية، وإلى كل من قدم لنا يد العون، وتسهيلات البحث، أو منحنا معلومة أثرت هذا العمل المتواضع من قريب أو من بعيد.

ختاماً ..نسأل الله عز وجل أن يتقبل منا هذا العمل، وأن يجعله نافعا ولبنة طيبة في صرح العلم والقانون، وأن يوفقنا جميعا لما يحبه ويرضاه.

إهداء

"حين تشرق شمس الوصول، تلتفت الروح ممتنة لكل يد حانية مسحت عنها عناء السير،
ولكل قلب آمن بها وبدد عنها غمام الحيرة. اليوم، وأنا على عتبة هذا القطاف المبارك، أنسج
من خيوط العرفان والوفاء إهدائي هذا"

ومصادقاً لقوله سبحانه وتعالى: ﴿إِنَّ الَّذِينَ آمَنُوا وَعَمِلُوا الصَّالِحَاتِ إِنَّا لَا نُضِيعُ أَجْرَ مَنْ
أَحْسَنَ عَمَلًا﴾ سورة الكهف الآية 30

أهدي هذا الإنجاز لروحي التواقة للتميز، والتي آمنت بأن الأهداف النبيلة تستحق الصبر
والمقاومة. شكراً لنفسي التي لم تخذل طموحي، وحافظت على إشراقها وتفاؤلها في كل عثرة

إلى فخري الشامخ، وقدوتي الأبدية، ومنبع قناعاتي، أبي الغالي

تجسيدا لقول الشاعر "أبي يا منبع الآمال يا سندي، ويا ثوراً أضيء به ظلام غدي". إليك يا
مَنْ رأيتُ في كفاحه معنى الإرادة، وَمَنْ كان اسمي مقترناً باسمه مبعث اعتزازي الأكبر،
أهدي إليك ثمرة جهد كنت أنت ملهمه ووقوده.

إلى مرافئ الحنان العذب، أمي الحبيبة

إلى التي غمرتني بنقاء الحب، واحتوت قلقي بفيض دعائها الصامت خلف السجود؛ نجاحي
هذا هو غرس يديك الكريمتين وطهر رضاك.

إلى زهرات حياتي وسر بهجتي، أختي الحبيبتين

يا رفيقات العُمر وملاذ الروح الحنون، مَنْ كانت كلماتهما بلسماً يطرد التعب، ونبضهما يملأ
قلبي بالأمل والتفاؤل في كل خطوة.

إلى درعي الحصين وسندي المتين، أخوي الغاليين

عضدي الذي لا يلين، وجدار أمانني في مواجهة الأيام؛ شكراً لأنكما كنتما دائماً السند الذي
أرتكز عليه بثقة وفخر، واليد التي تدفعني نحو المعالي

إلى رفيقة الدرب وصديقتي الغالية

وكما قال الأديب جبران خليل جبران "الصديق هو حاجة الروح مُشبعة". إلى مَنْ جاورتني
في رحلة البحث، وتقاسمت معي ثقل المسؤولية ومخاض الأفكار، وكانت بكلماتها الصادقة
ودعمها الجميل خير معين لي، ومعك احتفل اليوم بجمال الوصول وبلذة النجاح المشترك.

{فلكم جميعاً أهدي ثمرة هذا الجهد راجية أن يكون بداية لمستقبل أكثر إشراقاً ونجاحاً}

بسمه مويسي

بسم الله الذي بنعمته تتم الصالحات، ومنه العون والمدد، والذي أنار بصيرتي وأمدني بالقوة والصبر لأخطأ أولى خطواتي في محراب العلم.

{إلى نفسي..}

ومصادقاً لقوله سبحانه: ﴿يُرِيدُونَ أَن يُطْفِئُوا نُورَ اللَّهِ بِأَفْوَاهِهِمْ وَيَأْبَى اللَّهُ إِلَّا أَن يُتِمَّ نُورَهُ﴾. الآية 32 من سورة التوبة أهدي هذا التميز لنفسي التي واجهت الصعاب بابتسامة، وجعلت من التحديات سلماً للصعود، شكراً لروحي الشغوفة التي لم تهدأ وكانت كلما تعثرت، استمدت من اسمها {نور} ضياء يضيء لها ممرات هذا البحث.

إلى ملاذي الآمن وسرّ وجودي، أمي الحبيبة.

إلى مَنْ دعاؤها سياجي، ورضاها غايتي، مَنْ صاغت من الصبر ثوباً لتلبسني تاج التميز، إليك يا نبض الفؤاد ويا أجمل النعم.

إلى سندي الشامخ وعزّي، أبي الغالي.

إلى مَنْ علمني أن القمم لا تُنال إلا بالمشابرة، مَنْ لم يبخل يوماً بعباءٍ أو توجيه، وكان طيف فخره بي هو الدافع الأكبر لأتجاوز كل الصعاب.

إلى أختي الكبرى

التي كانت وما زالت كالغيمة الماطرة بالحب والدعم في كل مراحل مسيرتي.

إلى أخي الأكبر

عضدي الذي أستند إليه، واليد التي تدفعني دائماً نحو الأمام بثقة وقوة.

إلى أخي الأصغر، والداعم الأكبر والأنقى

بلسم الروح، ومأمن الأسرار، إلى مَنْ رافق قلقي خطوة بخطوة، وكان المؤمن الأول بقدراتي، مَنْ منحني طاقة الاستمرار في لحظات التعب، وكان سنداً بحجم الكون ليصنع معي هذا النجاح.

إلى رفيقة الدرب وصديقتي الوفية

"إن الصداقة الحقيقية هي روح واحدة تسكن في جسدين"، مَنْ شاركتني عناء السهر ومخاض الأفكار، وكانت كتفاً ثابتاً لا يميل كلما ثقلت عليّ مشاق البحث.

إلى الأحباب وكل مَنْ ساندني

..وكما قيل في الأثر: "الناس للناس مدام الوفاء بهم". إلى تلك القلوب النقية التي آمنت بي، وإلى كل مَنْ مدّ لي يد العون، أو غمرني بصدق دعائه، أو ترك في مسيرتي أثراً طيباً دفعني نحو الأمام ولو بكلمة عابرة، إن حضوركم في حياتي هو الذي جعل لهذا الإنجاز معنى.

{أهديكم جميعاً ثمرة جهدي ومذكرتي هذه}

نور الهدى زياني

مقدمة

مقدمة

شهد العالم مع مطلع الألفية الثالثة طفرة تكنولوجية غير مسبوقة، نقلت المجتمعات الإنسانية من عالمها المادي الملموس إلى فضاء افتراضي لا تحده جغرافيا ولا تقيده حدود. وإذا كانت هذه الثورة الرقمية قد ذلت العقبات وسهلت سبل التواصل والتبادل المعرفي والاقتصادي، فإنها في الوقت ذاته أفرزت وجها مظلما تمثل في ولادة نمط إجرامي مستحدث يُعرف بـ "الجريمة المعلوماتية". هذا الإجرام المعاصر لا يُشبه الجريمة التقليدية في شيء، فهو يتميز بكونه عابرا للحدود، غير مرئي، وينفذ جناة يتمتعون بمهارات فنية عالية وذكاء تقني حاد، يعتمدون فيه على الخداع وتشفير البيانات وتمويه الهويات، مستغلين الفضاء السيبراني كملجأ آمن للإفلات من العقاب.

أمام هذا التحول النوعي في السلوك الإجرامي، تلقت القواعد الكلاسيكية للقانون الجنائي صدمة عنيفة، تجلت في ظهور ما يُعرف بـ "أزمة القانون الجنائي"، إذ وقفت التشريعات الجنائية ومصالح الضبطية القضائية عاجزة -في البداية- بآلياتها التقليدية عن مواجهة جريمة تولد وتنفذ وتُمحى آثارها بضغطة زر واحدة في بيئة افتراضية خفية. فالدليل في هذه الجرائم ليس له أثرا ماديا يُرى بالعين المجردة، بل هو "أثر رقمي" سريع التلاشي وسهل التدمير والتحويل، مما جعل حتمية التطوير الإجرائي أمرا لا مناص منه.

من رحم هذه الحاجة الملحة، انبعثت "التحريات الإلكترونية" كآلية إجرائية مستحدثة ومنظومة متكاملة من أدوات البحث والتحقيق الرقمي. وقد سعى المشرع الجزائري من خلالها إلى تسليح القضاء الجنائي بالوسائل التقنية اللازمة لاقتفاء الأثر الرقمي واختراق النظم المعلوماتية لضبط الأدلة الرقمية وضمان مشروعيتها أمام المحاكم. إلا أن هذا التطور المتسارع لم يتوقف عند عتبة البرمجيات التقليدية، بل قفز قفزة نوعية مع ولوج العالم عصر "الذكاء الاصطناعي"، حيث بدأت الأنظمة الخوارزمية الذكية، والتحليلات التنبؤية، وتقنيات التعرف الآلي تتغلغل في صلب منظومة البحث الجنائي، لتتحول التحريات الإلكترونية من مجرد رد فعل لاحق على وقوع الجريمة المعلوماتية، إلى آلية استباقية قادرة على التنبؤ بالسلوك الجرمي الشاذ وقمع الجريمة قبل استفحال أثرها.

أولا: أهداف الدراسة

- تسعى هذه الدراسة من خلال الإحاطة بأبعاد الموضوع إلى تحقيق جملة من الأهداف الرئيسية:
- **تأصيل الإطار القانوني:** تبين ماهية التحريات الإلكترونية وتمييزها عن التحريات التقليدية، وتحديد الأساس القانوني لإجراءات المراقبة الرقمية وتتبع الاتصالات.
 - **تقييم الفعالية الإجرائية:** قياس مدى نجاعة الوسائل التقنية وتطبيقات الذكاء الاصطناعي في الكشف عن الجريمة المعلوماتية وملاحقة مرتكبيها ميدانيا.

- إبراز المعادلة الحقوقية: البحث في كيفية إيجاد توازن حقيقي وحماية دستورية للحق في الخصوصية الرقمية وحرمة الحياة الخاصة في مواجهة التغول التقني لآليات التحري المستحدثة

ثانياً: دوافع اختياره (أسباب الاختيار)

تتضافر جملة من الأسباب والدوافع الذاتية والموضوعية التي جعلت من هذا الحقل المعرفي حيويًا وجديرًا بالبحث:

- **الأسباب الموضوعية:** تتمثل في التطور المتسارع للظاهرة الإجرامية المعلوماتية وعجز الآليات التقليدية عن مواجهتها، مما جعل من دراسة التحريات الإلكترونية ضرورة حتمية للوقوف على مدى مواكبة الترسانة القانونية للتحديات التقنية الحديثة، لاسيما مع إقحام تقنيات الذكاء الاصطناعي في منظومة العدالة الجنائية.
- **الأسباب الذاتية:** تنبع من الرغبة الشخصية والتخصص الأكاديمي في تعميق البحث في فقه القانون الجنائي وتكنولوجيا المعلومات، ومحاولة تقديم إسهام علمي متواضع يحل الثغرات الإجرائية ويقترح حلولاً قانونية تخدم الباحثين ومرفق القضاء على حد سواء.

ثالثاً: صعوبات البحث

لم تكن الدراسة في هذا الحقل المعرفي خالية من العقبات، بل واجهتنا جملة من الصعوبات أبرزها:

- **التطور التقني المتسارع:** الذي يجعل بعض الآليات أو القوانين عرضة للتقادم السريع أمام الطفرات التكنولوجية المتجددة يومياً.
- **ندرة المراجع المتخصصة:** لاسيما تلك التي تربط بصفة مباشرة ودقيقة بين الإجراءات الجنائية وتطبيقات الذكاء الاصطناعي في البيئة التشريعية المحلية، مما تطلب جهداً مضاعفاً في تجميع المادة العلمية وتحليلها.
- **طبيعة الموضوع الهجينة:** التي تجمع بين شق قانوني جاف وشق تقني تكنولوجي معقد، مما تطلب تدليل المفاهيم الهندسية والمعلوماتية وصياغتها في قالب قانوني رصين ومبسط.

رابعاً: إشكالية الدراسة

تكمن النقطة الجوهرية في هذا الموضوع في كونه يقع عند أدق نقطة تماس بين التطور التكنولوجي المتسارع والضمانات الحقوقية؛ إذ يثير إشكالية بالغة الحساسية تتمثل في كيفية الموازنة بين "مقتضيات الفعالية الإجرائية" في ملاحقة الجريمة المعلوماتية باستخدام أحدث

تقنيات التحري والذكاء الاصطناعي، وبين "اعتبارات حماية حقوق الإنسان وحرمة الحياة الخاصة" الرقمية للمواطنين.

وبناءً على هذا التسلسل المفاهيمي، تتبلور الإشكالية المحورية لهذه الدراسة في التساؤل التالي:

"إلى أي مدى توفق التشريعات الحديثة بين الفعالية التقنية للتحريات الإلكترونية والضمانات الدستورية لحماية الحياة الخاصة؟"

خامساً: المنهج المتبع

تحقيقاً لأهداف الدراسة وللإجابة على الإشكالية المطروحة، اعتمدنا على **المنهج الوصفي التحليلي، والمقارن** وذلك من خلال وصف طبيعة الجريمة المعلوماتية وآليات التحري الإلكتروني، ثم تحليل النصوص القانونية المنظمة لهذه الإجراءات في قانون الإجراءات الجزائية والقوانين المكملة له للوقوف على مدى كفايتها ومواطن القصور فيها. كما أخذنا بدراسة **استشرافية** من أجل عرض ومناقشة مساهمة تكنولوجيا الذكاء الاصطناعي ومستقبل البحث الجنائي في الفضاء الافتراضي.

سادساً: خطة الدراسة

وللإحاطة بجميع جوانب الإشكالية المطروحة، وتفكيك أبعادها الموضوعية والإجرائية، اعتمدنا خطة دراسة ثنائية متكاملة، ومقسمة على النحو الآتي:

. الفصل الأول: الإطار المفاهيمي والقانوني للتحريات الإلكترونية في مواجهة الجريمة المعلوماتية، قسمناه إلى مبحثين:

-المبحث الأول: ماهية الجريمة المعلوماتية والتحريات الإلكترونية

- المبحث الثاني: الأساس القانوني والمؤسسي للتحريات الإلكترونية

• الفصل الثاني: آليات التحريات الإلكترونية ودورها في مواجهة الجريمة المعلوماتية في ظل الذكاء الاصطناعي، قسمناه إلى مبحثين:

-المبحث الأول: وسائل وأساليب التحريات الإلكترونية

-المبحث الثاني: التحديات القانونية والعملية للتحريات الإلكترونية

الفصل الأول

الإطار المفاهيمي والقانوني
للتحرّيات الإلكترونية في مواجهة
الجريمة المعلوماتية

تمهيد

شهد العالم مع مطلع القرن الحادي والعشرين ثورة تكنولوجية ورقمية أحدثت تحولا جذريا في بنية الجريمة المعاصرة . فلم تعد الجرائم مقتصرة على الواقع المادي الملموس، بل انتقلت إلى ما يُعرف بـ" الفضاء السيبراني"، حيث أصبحت التقنيات الحديثة أداة وهدفا للجريمة في آن واحد. وقد أدى هذا التحول إلى ظهور ظاهرة جديدة تُعرف بـ "الجريمة المعلوماتية"، وهي ظاهرة عابرة للحدود تتسم بالغموض، السرعة، والقدرة الفائقة على محو الآثار الرقمية.

إن التعقيد التقني الذي تحمله هذه الجرائم الافتراضية أدى إلى عجز النصوص القانونية التقليدية والقواعد الإجرائية الكلاسيكية عن استيعابها أو ملاحقة مرتكبيها بشكل فعال . ونتيجة لذلك، برزت ضرورة صياغة مقاربات مفاهيمية دقيقة لتعريف هذه الجرائم وتطوير آليات مبتكرة لمكافحتها، وأبرز تلك الآليات "التحريات الإلكترونية".

تُعد التحريات الإلكترونية محورا رئيسيا في السياسة الجنائية المعاصرة، حيث تزود سلطات التحقيق بصلاحيات تقنية تمكنها من التصدي لهذه الجرائم المستحدثة. بناءً على ذلك، يُخصص هذا الفصل لتناول الظاهرة من جانبيها المفاهيمي والقانوني.

- المبحث الأول: ماهية الجريمة المعلوماتية والتحريات الإلكترونية

-المبحث الثاني: الأساس القانوني للتحريات الإلكترونية

المبحث الأول: ماهية الجريمة المعلوماتية والتحريات الإلكترونية

تُعتبر المعلوماتية علماً يركز على جمع البيانات، معالجتها، وتخزينها بطريقة فعالة، مما ساهم في تشكيل أساس قوي للتطورات التكنولوجية الحديثة. ومع توسع استخدام التقنيات الرقمية، برزت أنواع جديدة من الجرائم المرتبطة بالفضاء الرقمي، الأمر الذي استلزم تطوير آليات مبتكرة للتحقيق تعتمد على الإلكترونيات انطلاقاً من هذه الحاجة، اكتسبت التحريات الإلكترونية أهمية متزايدة كوسيلة حديثة في مجال البحث والتحري. هذا المبحث يهدف إلى دراسة مفهوم المعلوماتية عبر تقديم تعريفها، بيان خصائصها الأساسية، ومن ثم الانتقال لنتناول موضوع التحريات الإلكترونية باعتبارها أداة فاعلة لمواجهة التحديات المرتبطة بالجرائم الرقمية.

المطلب الأول: مفهوم الجريمة المعلوماتية

تعددت التعريفات المرتبطة بالمعلوماتية واختلفت في مضمونها، مما أدى إلى صعوبة الوصول إلى فهم موحد لهذه الظاهرة المعروفة بالجريمة المعلوماتية. سنحاول من خلال هذا المطلب تقديم تعريف واضح، لننتقل بعد ذلك إلى تسليط الضوء على خصائصه.

الفرع الأول: تعريف المعلوماتية

يستلزم ضبط النظام الإجرائي للتحريات الإلكترونية تحديد الإطار المفاهيمي للمحيط الرقمي الذي تُستمد منه الأدلة الجنائية. وتأتي 'المعلوماتية' كركيزة أساسية لهذه البيئة الافتراضية، مما دفع المشرع والفقيه الجزائي لتأطيرها حمايةً لمنظومة المعالجة الآلية للمعطيات. وتأسيساً على ذلك، نخصص هذا الفرع لبيان المفهوم القانوني والتشريعي للمعلوماتية

أولاً: التعريف اللغوي للمعلوماتية: يعود أصل ومفهوم كلمة المعلوماتية في اللغة إلى كونها مصطلحاً حديث العهد باللسان العربي التقليدي، حيث تمت إضافتها لتغطية مجال علمي وتقني جديد نشأ بظهور الحوسبة وتكنولوجيا المعلومات.

تعتبر كلمة معلوماتية مشتقة من الجذر الثلاثي (ع-ل-م)، الذي يرتبط بمعاني الإدراك والمعرفة، ويشير إلى استيعاب الحقائق والمعلومات. فحسب المعاجم العربية، تعني "المعلومة" ما يتم معرفته أو إدراكه من حقيقة أو خبر، وقد تم اعتماد هذا المفهوم اللغوي لتطوير مصطلح "المعلوماتية"

كما ظهر مصطلح المعلوماتية "Informatique" باللغة الفرنسية لأول مرة في أوائل ستينيات القرن العشرين في فرنسا، ليعبر عن المجال العلمي والهندسي الذي يختص بالمعالجة الآلية للمعلومات باستخدام الحواسيب. تم صياغة هذا المصطلح من مزج كلمتين فرنسيتين: "Information" بمعنى المعلومات، و "Automatique" بمعنى الآلية، ليعكس الهدف الأساسي للمجال المتمثل في التحكم الآلي بالبيانات وتحويلها إلى معلومات يمكن معالجتها والاستفادة

منها. بعد إطلاقه في فرنسا، بدأ المصطلح بالانتشار تدريجياً في العالم الغربي مواكبا التطور السريع في تقنيات الحوسبة والبرمجيات.

مع منتصف القرن العشرين، دخل المصطلح إلى اللغة العربية نتيجة جهود التعريب. في بداياته، كان يُستخدم للإشارة إلى معالجة المعلومات بواسطة الحاسوب وأنظمة البرمجيات فقط، إلا أن معناه توسع ليشمل مجالات أوسع مثل: نظم المعلومات الرقمية، قواعد البيانات، الشبكات والاتصالات الرقمية، إدارة المعلومات في المؤسسات العلمية والإدارية...، ثم أصبح مفهوم المعلوماتية يتجاوز مجرد ترجمة لكلمة "معلومات"، فهو يعبر عن نظام متكامل يشمل جمع ومعالجة وتخزين وتحليل ونقل المعلومات بطرق آلية باستخدام التقنيات الحديثة. هذا الشمول جعله حجر الزاوية في فهم البيئة الرقمية التي تنشأ فيها وتدار الجرائم المعلوماتية.

ثانياً: التعريف الاصطلاحي للمعلوماتية: المصطلح نفسه فهو ترجمة للكلمة الفرنسية "Informatique"، التي ظهرت في أوائل الستينيات لتعبر عن معالجة المعلومات بأسلوب آلي عبر الحاسوب¹.

كما يتكون المصطلح الفرنسي من المزج بين كلمتين هما Information: (معلومات) و Automatique (آلي). وبالتالي، يشير إلى عملية تحويل البيانات إلى صيغة يمكن التعامل معها بواسطة الوسائل التقنية. في السياق العربي، تجاوزت كلمة "المعلوماتية" حدود المعنى اللغوي لكلمة "المعلومة" لتصبح مفهوماً علمياً وتقنياً قائماً بذاته. فهي تدل اليوم على العلم أو النظام المخصص لدراسة وتنظيم ومعالجة البيانات بصورة آلية عبر استخدام التقنيات الحديثة كالحواسيب والتقنيات الرقمية².

ثالثاً: التعريف التشريعي للجريمة المعلوماتية

أ- تعريف التشريع الفرنسي للمعلوماتية: لا يتضمن قانون العقوبات الفرنسي تعريفاً عاماً وشاملاً للجريمة المعلوماتية، إلا أن النصوص الجنائية تحدد الأفعال المخالفة المتعلقة بالمجال المعلوماتي على أنها مجموعة من التصرفات المجرمة التي تتم باستخدام الوسائل التقنية أو تؤثر في سلامة البيانات. ومن بين تلك الأفعال:

-الدخول غير المصرح به إلى نظام معالجة البيانات الآلي.

-التلاعب بالبيانات أو إتلافها.

-تعطيل أنظمة الكمبيوتر³.

1- زكريا فؤاد، المعجم الفلسفي للمصطلحات التقنية، دار العلم للملايين، القاهرة-مصر، 2007، ص 112.

2- نبيل الزهيري، مصطلحات معلوماتية عربي-إنجليزي، دار الفكر، عمان، 2012، ص 45.

-أنظر أيضاً، رشيد عادل، علم المعلومات والمكتبات، دار الفكر العربي، بيروت، 2010، ص 78.

3- عبد السلام مسدور، الجريمة المعلوماتية: دراسة مقارنة بين التشريع الجزائري والفرنسي، دار النهضة العربية، الجزائر، 2015، ص

من ذلك نستنتج تعريفا تشريعيا فرنسيا يستخلص من نصوص العقوبات الفرنسية: "الجريمة المعلوماتية في التشريع الفرنسي هي كل فعل وقع في بيئة تقنية باستخدام الحاسوب أو الشبكات، ويؤدي إلى الإضرار بسلامة النظام أو البيانات، والتي نص القانون على تجريمها في المواد المتعلقة بنظم المعالجة الآلية للبيانات".

ب-تعريف التشريع المصري للمعلوماتية: يتناول القانون المصري قضايا الجرائم المعلوماتية في إطار قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، حيث تم تجريم مجموعة من الأفعال المرتبطة باستخدام التقنية. إلا أن القانون لم يقدم تعريفا اصطلاحيا دقيقا لتلك الجرائم ضمن نصوصه، وإنما اكتفى بتحديد بعض الصور المجرمة مثل:

-الدخول غير المصرّح إلى البيانات

-تعطيل أو تقييد نظم المعالجة الآلية.

-الاحتياز الإلكتروني .

فالجريمة المعلوماتية في التشريع المصري هي كل فعل مجرم يقع باستخدام أو عبر الوسائل التقنية المتقدمة مثل الحاسوب والاتصالات، ويستهدف سلامة البيانات أو نظم الاتصالات أو يؤثر على الأمن السيبراني⁴.

ج-تعريف التشريع الأمريكي للمعلوماتية: تتميز الولايات المتحدة بوجود نظام شامل يهدف إلى حماية البيانات والتصدي للجرائم المعلوماتية. يعد قانون الاحتياز وسوء الاستخدام الحاسوبي، حيث تُوضح رؤية التشريع الأمريكي للجرائم المعلوماتية بأنها تشمل جميع الأفعال المرتكبة باستخدام الحواسيب أو الشبكات الرقمية والتي تُلحق أضرارا مادية أو معنوية على المصالح القانونية. وتشمل هذه الجرائم اختراق الأنظمة بشكل غير مشروع، الاحتياز عبر الشبكات الرقمية، وسرقة البيانات⁵.

د-تعريف المعلوماتية حسب اتفاقية بودابست: وفقا لما ورد في اتفاقية بودابست لعام 2001 بشأن الجريمة المعلوماتية، لم يتم تقديم تعريف اصطلاحى مباشر لهذا النوع من الجرائم ضمن نص الاتفاقية. إلا أنها تتضمن إطارا يحدد مجموعة من الأعمال الإلكترونية التي تصنف كجرائم عند ارتكابها عبر أنظمة معالجة البيانات الآلية. فقد أشارت إلى أبرز الأفعال التي تدرج ضمن هذا السياق، منها :

-الوصول غير المصرّح به إلى أنظمة المعالجة الآلية للبيانات.

-التدخل غير القانوني في البيانات.

4 - أحمد حسين الهضيبي، قانون مكافحة جرائم تقنية المعلومات المصري: دراسة تحليلية مقارنة، دار الفكر العربي، القاهرة، 2020، ص 24-22.

5 - سامي فؤاد، الجرائم المعلوماتية في القانون المقارن، دار الثقافة القانونية، القاهرة-مصر، 2018، ص 73-81.

-تخريب أو إتلاف أنظمة الكمبيوتر أو البيانات المعالجة.

يتضح مما سبق ذكره، أن اتفاقية بودابست تركز على مقارنة معيارية تحدد الأفعال الإجرامية ضمن الفضاء الرقمي، مما يوفر أدوات قانونية لمعالجة الجرائم المعلوماتية عبر إطار دولي موحد.

ه-تعريف المشرع الجزائري للمعلوماتية:

بناءً على التوجه التشريعي الجزائري، نجد أن المشرع قد ابتعد عن وضع تعريف فقهي مجرد للمعلوماتية، واعتمد بدلاً من ذلك مقارنة إجرائية وعملية ركزت على تحديد ماهية "المنظومة المعلوماتية" لتستوعب الأبعاد التقنية للجريمة المعاصرة. وقد تجسد هذا المفهوم صراحة في المادة الثانية (الفقرة ب) من القانون رقم 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث عرّفها بأنها "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين".

ويُستشف من هذا التعريف المتأثر بالاتفاقيات الدولية—لا سيما اتفاقية بودابست—أنه يكمل ويلتقي مع المفهوم الذي تبناه المشرع سابقاً في القانون رقم 15-04 المعدل لقانون العقوبات تحت مسمى "نظام المعالجة الآلية للمعطيات"؛ إذ يقوم المفهوم بمجمله على ثلاثة عناصر أساسية: عنصر هيكلي يشمل الأجهزة المنفصلة أو الشبكات المتصلة كالحواسيب والخوادم، وعنصر وظيفي يتمثل في عمليات المعالجة الآلية التي تخرج النظم التقليدية من هذا النطاق، وأخيراً عنصر توجيهي يرتبط بالبرمجيات والأوامر الرقمية التي تقود النظام، مما يمنح النص القانوني المرونة الكافية لمواكبة التطورات المتسارعة في عالم الجريمة الرقمية.

رابعاً: تعريف الجريمة المعلوماتية في الفقه: لم تحظ الجريمة المعلوماتية بتعريف موحد في الفقه الجنائي نظراً لحدثة الظاهرة وسرعة تطورها التقني، إضافة إلى تنوع أشكالها واختلاف المصالح التي تمسها. هذه العوامل دفعت الفقه الجنائي نحو تبني اتجاهات متنوعة لتحديد طبيعتها وحدودها بالاستناد إلى آراء العلماء والفقهاء في المجال.

عرفت الجريمة المعلوماتية، بأنها: "كل سلوك إجرامي يتم عبر الحاسب الآلي أو شبكات الاتصال، أو يستهدف نظم المعلومات الخاصة بالآخرين، ما يؤدي إلى انتهاك سرية أو سلامة البيانات أو تعطيل عملها". يبرز هذا التعريف عنصرين أساسيين: الوسيلة التقنية المستخدمة في الجريمة والمصلحة المعلوماتية المعتدى عليها، مما يعكس الطابع المزدوج للجريمة المعلوماتية بين التقنية والمصالح القانونية⁶.

6 - غنام محمد غنام، "الدليل المستمد من الحاسب الآلي ومدى حجتيته في الإثبات الجنائي"، مجلة الحقوق، جامعة الكويت، المجلد 26، العدد 1، 2002، ص 17

كما عرفت الجريمة المعلوماتية، على أنها لا تقتصر على توظيف الوسائل التقنية في الجرائم التقليدية فحسب، بل تشمل أيضا أفعالا خاصة بالمجال الرقمي مثل الدخول غير المشروع إلى الأنظمة أو العبث بالبيانات، ما يميز هذه الجرائم عن غيرها من حيث طبيعتها الفعلية ومنطلقها المعلوماتي⁷.

بناءً على هذه التعاريف، يتضح أن الفقه قد أخذ بعين الاعتبار عدة عناصر جوهرية عند تعريف الجريمة المعلوماتية، أهمها:

- اعتماد الوسائل التقنية مثل الحاسب الآلي وشبكات الاتصال.

- محل الاعتداء، كالبيانات والأنظمة المعلوماتية.

- الطبيعة الخاصة للبيئة الرقمية.

- الخصائص الإجرائية المستحدثة لهذه الجرائم.

وعليه يمكننا تعريف الجريمة المعلوماتية، بأنها: "سلوك إجرامي غير مشروع يرتبط باستخدام الوسائل المعلوماتية أو يستهدف نظم البيانات، مما يؤدي إلى انتهاك السرية أو المساس بسلامة أو حسن سير النظام المعلوماتي متى توافرت أركان المسؤولية الجنائية.

الفرع الثاني: خصائص الجريمة المعلوماتية

يعتبر موضوع أو محل الجريمة الالكترونية أهم خاصية تتمثل بها هذه الجريمة باعتبارها جريمة مستحدثة عن غيرها من الجرائم التقليدية. بحيث تكون المعلومات والبرامج هي محل الاعتداء، وعليه نكون أمام ظاهرة إجرامية مستحدثة ذات طبيعة خاصة، مما تمنحها لونا وطابعا قانونيا خاصا ويميزها بمجموعة من الخصائص المختلفة عن الجرائم التقليدية، منها ما هو مرتبط بالجريمة، ومنها ما هو مرتبط بالمجرم⁸.

أولاً: صعوبة اكتشاف الجريمة الالكترونية: تعد الجرائم الإلكترونية التي تحدث ضمن الفضاء المعلوماتي تحديا كبيرا بسبب صعوبة اكتشافها وسرعة تنفيذها. هذه الجرائم غالبا ما ترتكب بسرية تامة، حيث يتم تبادل المعلومات والبيانات ونقلها على شكل نبضات إلكترونية مغناطيسية عبر شبكة الإنترنت، وتكون في معظم الأحيان منظمة وعابرة للحدود، مما يؤدي إلى تأثيرها على أراضي عدة دول نتيجة الاستخدام المتزايد والواسع للإمكانات التي توفرها شبكة الإنترنت.

تكمن صعوبة الكشف عن الجرائم الإلكترونية في عدم ظهور أي أثر مرئي لها، فهي ترتكب في فضاء غير مادي وغير ملموس، فضلا عن قدرة الجناة على تدمير الأدلة خلال لحظات

7 - عمر أبو الفتوح حمامي، "الحماية الإجرائية للمعلوماتية وأثرها في الإثبات الجنائي: دراسة مقارنة"، مجلة الفكر القانوني والاقتصادي، جامعة بنها، يناير 2017، ص 35

8 - غنية باطلي، الجريمة الإلكترونية: دراسة مقارنة، ط1، الدار الجزائرية، الجزائر، 2016، ص 33.

وجيزة، مما يزيد من تعقيد العملية. ذلك يبرز الطبيعة الخفية لهذه الجرائم، والتي يصعب على الضحايا ملاحظتها بسبب إمكانية التلاعب غير المرئي بالبصمات أو الذبذبات الإلكترونية داخل الشبكات التي تسجل البيانات.

والجدير بالذكر، أن هذا النوع من الجرائم أصبح أكثر انتشارا بسبب توافر خبرة ومعرفة عميقة لدى مرتكبيها في مجالات الحوسبة وتقنيات الإنترنت، مما يسهل عليهم إخفاء آثارهم وتجنب الملاحقة القانوني. بالإضافة إلى ذلك انعدام ثقافة التبليغ لدى المجني عليهم عن هذه الجرائم، وهذا راجع إلى خوفهم من تجنب الاساءة وإلى السمعة وهز الثقة فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية، ومن بين الأسباب التي تؤدي إلى صعوبة اكتشاف الجريمة الإلكترونية تعود إلى الجاني، وأخرى على المجني عليه⁹.

ثانيا: صعوبة إثبات الجريمة الإلكترونية: إن اكتشاف الجريمة الإلكترونية ليس أمرا سهلا، وفي حال اكتشافها والابلاغ عنها فإن إثباتها والتحقيق فيها أمر صعب، وهذا ما يميزها عن غيرها من الجرائم الأخرى، وهي صعوبة الإثبات الجنائي فيها حيث يكون من الصعب إثبات أركانها لأنها لا تترك آثار مادية¹⁰. وتتمثل صعوبة الإثبات في الجريمة الإلكترونية، فيما يلي:

أ. فضاء الجريمة: أي أن الجريمة ترتكب في فضاء تكنولوجي غير ملموس وغير مادي، فلا تترك أي أثر خارجي بعد ارتكابها لانعدام الدليل المرئي الملموس.

ب. صعوبة الاحتفاظ بآثار الجريمة: أي أن الأدلة فيها غير مرئية فهي عبارة عن نبضات الكترونية تنساب إلى غير الحاسوب والشبكة المعلومات¹¹

ثالثا: الجريمة الإلكترونية عابرة للحدود الوطنية: تُعرف الجريمة الإلكترونية، بأنها ذات بعد عالمي وعابر للحدود، إلا أنه يجب التنويه إلى أنها ليست جريمة دولية بالمعنى القانوني المتعارف عليه. فالجريمة الدولية تُعرف بشكل حصري وفق نظام روما الأساسي، وتشمل جرائم مثل الحرب، العدوان، والإبادة الجماعية. لذلك، من الضروري التمييز بين الجرائم المعلوماتية، التي تصنف ضمن نطاق القانون الجنائي الدولي، وبين الجرائم الدولية التي تندرج تحت مظلة القانون الدولي الجنائي.

أما الحديث عن الطابع العالمي للجريمة المعلوماتية فيمكن في ارتباطها بالتقنيات الحديثة وما أفرزته من تطور هائل في مجال الاتصال. هذه التطورات أدت إلى تحييد الحدود الجغرافية بين الدول، ما يسمح للجريمة الإلكترونية بتجاوز حدود الدولة التي ترتكب فيها لتصل آثارها إلى

¹⁰ -المرجع نفسه، ص 43.

¹¹ - بجاد عبد الرؤوف بوديسة، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص: قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي -برج بوعريريج، الجزائر، 2021، ص

مستويات عالمية، حيث أتاحت التقنيات المتصلة عالميا لهذه الجرائم أن تصبح عابرة للحدود الوطنية .

وعليه فإن الطبيعة العالمية تمكن الجاني من ارتكاب جريمة إلكترونية في أي دولة ما، ومنه تعتبر الجريمة المعلوماتية شكلا جديدا من الجرائم العابرة للحدود الوطنية والقارية والدولية¹².

المطلب الثاني: صور وأشكال الجريمة المعلوماتية

تنطوي صور وأشكال الجريمة المعلوماتية على تنوع كبير ولا تقتصر على نمط واحد، فهي تشمل مجموعة واسعة من الأفعال غير القانونية التي يتم تنفيذها عبر الوسائل التقنية أو تستهدف الأنظمة الرقمية. وقد عمل العديد من الباحثين والخبراء القانونيين على تصنيف هذه الجرائم وفقا لطبيعة الأفعال المرتكبة ومدى ارتباطها بالبيئة الرقمية وتأثيراتها القانونية. فيما يلي نستعرض أبرز تلك الأشكال كما أوردتها الدراسات والكتابات المتخصصة:

الفرع الأول: صور الجريمة المعلوماتية

لا تقتصر الجريمة المعلوماتية على نمط سلوكي محدد، بل تتنوع صورها وأشكالها تبعاً لتعدد الوسائل التقنية المستخدمة في تنفيذها والأهداف الحمائية التي تُستهدف من خلالها. وبناءً على ذلك، سنخصص هذا الفرع لتسليط الضوء على أبرز أشكال الجرائم المعلوماتية وتصنيفها وفقاً لطبيعة السلوك الإجرامي المرتكب في البيئة الرقمية.

أولاً: الاختراق غير المشروع للأنظمة المعلوماتية: يُعد هذا النوع من الجرائم واحداً من أكثر الأنواع شيوعاً وأقدمها، ويشمل دخول شخص غير مخول إلى نظام معالجة البيانات أو الشبكات الرقمية دون تصريح. يهدف الجاني في الغالب إلى الاطلاع على البيانات المخزنة أو التلاعب بها، مما يشكل اعتداء صريحاً على الخصوصية وأمن المعلومات¹³.

ثانياً: التلاعب بالبيانات أو التعديل غير القانوني: يتضمن هذا النوع من الأنشطة حذف البيانات، تعديلها، إدراجها، أو تشويهها ضمن الأنظمة الرقمية بغير تفويض قانوني، مما يؤدي إلى تأثير سلبي على سلامة البيانات ودقتها وموثوقيتها¹⁴.

ثالثاً: تعطيل أو إفساد نظم المعلومات: يشير هذا النوع إلى التسبب في تعطيل كامل أو جزئي لوظائف النظام المعلوماتي، مما يؤدي إلى عدم القدرة على استخدامه أو جعله غير ملائم للعمل بشكل طبيعي¹⁵.

12 - يعيش تمام شوقي، الجريمة المعلوماتية-دراسة تأصيلية مقارنة، مطبعة الرمال، ط1، الوادي، الجزائر، 2019، ص29.

13- داود حسن طاهر، جرائم نظم المعلومات، دار الفكر العربي، الرياض-المملكة العربية السعودية، 2000، ص ص: 35-42.

14- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، دار النهضة العربية، عمان، 2009، ص ص: 48-55.

15- محمود مرسى، الجريمة المعلوماتية: دراسة جنائية مقارنة، دار النهضة، القاهرة-مصر، 2012، ص ص: 79-85.

رابعاً: جرائم التشهير الإلكتروني ونشر المحتوى غير القانوني: تتضمن بث أو نشر مواد ذات طبيعة مسيئة أو تشهيرية أو مخالفة للأنظمة القانونية، سواء عبر المنتديات الإلكترونية أو منصات التواصل الاجتماعي¹⁶.

الفرع الثاني: أشكال الجريمة المعلوماتية

تتنوع الجريمة المعلوماتية في شكلها الخارجي وفقاً لطبيعة الهدف الذي تتعرض له، مما يؤدي إلى ظهور أنماط جديدة من الجرائم التي تستلزم اتباع آليات خاصة للتحري عنها. بناءً على ذلك، سنتناول في هذا الفرع تصنيف أبرز أشكال الجرائم المعلوماتية، مع تبيان الفارق بين الجرائم التي تستهدف الأنظمة الرقمية بشكل مباشر وتلك التي تُستخدم فيها التكنولوجيا كأداة لتنفيذ جرائم تقليدية.

أولاً: الاحتيال الإلكتروني: يشير إلى استخدام الوسائل التقنية بشكل غير قانوني بهدف خداع الأفراد أو المؤسسات لتحقيق مكاسب غير مشروعة. ويتضمن ذلك، على سبيل المثال، استغلال بطاقات الائتمان أو تنفيذ عمليات سحب غير قانونية عبر الإنترنت¹⁷.

ثانياً: الجرائم المرتبطة بالملكية الفكرية الرقمية: تشمل التعدي على حقوق الملكية من خلال تداول البرامج المقرصنة أو استخدام نسخ غير مرخصة من المواد المحمية بحقوق التأليف والنشر¹⁸.

ثالثاً: الاحتيال عبر البريد الإلكتروني (Phishing): يعد هذا النوع من الجرائم وسيلة لانتحال شخصية إلكترونية بهدف خداع الضحايا، مما يسمح بسرقة بياناتهم أو الحصول على معلومات حساسة بشكل غير مشروع¹⁹.

رابعاً: انتهاك سرية البيانات: يعني هذا المفهوم الوصول غير المصرح به إلى البيانات الشخصية أو الخاصة دون الحصول على إذن مسبق من مالكها، وهو ما يُعد خرقاً لخصوصية الأفراد²⁰.

المطلب الثالث: مفهوم التحريات الإلكترونية وتمييزها عن التحريات التقليدية

أدى التطور التكنولوجي والتقني الذي أثر على المنظومة المعلوماتية، بالإضافة إلى الطبيعة الخاصة للدليل الإلكتروني، إلى تغييرات جذرية في المفاهيم التقليدية المتعلقة بطرق وإجراءات

¹⁶ - نهلا عبد القادر المومني، الجرائم المعلوماتية، دار النهضة العربية، عمان، 2008، ص ص: 80-88.

¹⁷ - سامي فؤاد، الجرائم المعلوماتية في القانون المقارن، دار الثقافة القانونية، القاهرة-مصر، 2018، ص ص: 120-130.

¹⁸ - محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت: الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2007، ص ص: 98-105.

¹⁹ - أحمد حسين الهضيبي، المرجع السابق، ص ص: 67-73.

²⁰ - غانم المرضي الشمري، الجرائم المعلوماتية: ماهيتها، خصائصها وكيفية التصدي لها قانونياً، الدار العلمية الدولية، الأردن، 2016، ص ص: 102-110.

جمع الأدلة. ونتيجة لذلك، أصبح من الضروري إعادة تقييم منهجيات بعض الإجراءات التقليدية المستخدمة في التحقيق بالجرائم، خاصة الجرائم المرتبطة بالمعلوماتية.

الفرع الأول: مفهوم التحريات الإلكترونية والتحريات التقليدية

تقتضي مواجهة الإجرام المعلوماتي المعاصر تجاوز الأنماط التقليدية في البحث والتحري، نظراً لطبيعة البيئة الافتراضية التي تقع فيها هذه الجرائم وتخفي معالمها. وإذا كانت التحريات التقليدية تركز على محددات مادية ملموسة كالزمن والمكان والمعاينة العينية، فإن التحريات الإلكترونية تنبثق كآلية إجرائية مستحدثة تعتمد على وسائل تقنية ورقمية تهدف إلى اقتفاء الأثر الرقمي وضبط الأدلة الافتراضية. وتأسيساً على هذا التمايز الإجرائي، نخصص هذا الفرع لإجراء مقارنة تأصيلية بين مفهومي التحريات الإلكترونية والتقليدية

أولاً: تعريف التحريات الإلكترونية: تعرف التحريات الإلكترونية، على أنها إجراء قانوني منظم يستند إلى تقنيات رقمية متقدمة تُستخدم لجمع وتحليل الأدلة المستمدة من الأنظمة الإلكترونية. يهدف هذا النوع من التحريات إلى كشف الجرائم أو التحقق من الوقائع، مع الالتزام بضمان سلامة الأدلة وصلاحياتها للاعتماد ضمن الإجراءات القضائية.

يكمن الفرق بين التحري بصفة عامة والتحري في الجرائم المعلوماتية في أن التحري بصفة عامة هو عمل أمني أساسي وقانوني على درجة عالية من السرية يقوم بها المتحري مستخدماً حواسه الخمس سواء بالوسائل أو دونها للحصول على بيانات تعريفية أو توضيحية عن الأشخاص والأماكن والأشياء حسب طبيعتها للحد من الجريمة أو ضبطها لتحقيق الأمن أو أي غرض آخر. أما التحري في الجرائم المعلوماتية هو عمل أمني وقانوني متخصص يقوم به المتحري مستخدماً بالإضافة إلى حواسه الخمس التقنيات الإلكترونية الرقمية من الحسابات وشبكاتها وخدماتها للحصول على بيانات ومعلومات تعريفية أو توضيحية للحد من هذه الجرائم أو ضبطها لتحقيق الأمن أو أي غرض آخر.

ثانياً: تعريف التحريات في شكلها التقليدي: التحريات التقليدية هي مجموعة من الإجراءات والوسائل التي تعتمد أساساً على الجهد البشري والخبرة الميدانية في جمع المعلومات وتحليلها، بهدف كشف الحقائق والوصول إلى أدلة تساعد في حل القضايا. وتتركز هذه التحريات على الملاحظة الدقيقة، والقدرة على الربط بين المعطيات المختلفة، بعيداً عن الاعتماد الكلي على الوسائل التكنولوجية الحديثة.

تنقسم مصادر التحريات في شكلها التقليدي، إلى مصادر شخصية وأخرى رقابية ومسجلة. فالمصادر الشخصية تعتمد على الأفراد، مثل المرشد والمخبر اللذين يزودان المحقق بمعلومات مهمة قد تسهم في توجيه مسار التحقيق، كما يشمل ذلك الجمهور الذي قد يقدم بلاغات أو شهادات مفيدة، ووسائل الإعلام التي قد تحتوي على معطيات أو مؤشرات ذات صلة، بالإضافة إلى أسلوب التنكر الذي يمكن من الحصول على معلومات بشكل غير مباشر. أما المصادر

الرقابية والسجلات، فتشمل المراقبة التي تهدف إلى تتبع الأنشطة أو الأشخاص لفهم سلوكهم، إلى جانب السجلات الرسمية التي توفر معلومات موثقة ودقيقة، والسجلات غير الرسمية التي تستخدم كمصادر مساندة تدعم التحقيق وتكمل الصورة العامة.

بناءً على ما تقدم نرى أنه لا يوجد فرق جوهري بين تعريف التحري بشكل عام وفقاً للشرح القانون الجنائي وتعريف التحريات في الجرائم الإلكترونية، باستثناء الجانب الفني المتعلق بالأدوات والأساليب المستخدمة لإجراء التحريات. وكما توجد تحريات وقائية وأخرى قمعية في الجرائم التقليدية، فإن الأمر ذاته ينطبق على التحريات في الجرائم الإلكترونية. ومن الخصائص البارزة التي تتميز بها إجراءات التحري مقارنة بغيرها من الإجراءات أنها تنفذ بسرية تامة ودون علم الشخص المستهدف، مع الالتزام بعدم المساس بحريته أو كرامته أو حرمة مسكنه.

الفرع الثاني: التمييز بين التحريات الإلكترونية والتحريات التقليدية

أشرنا في الفرع السابق لتعريف التحريات الإلكترونية بالمفهوم العام والتحريات التقليدية في الجرائم المعلوماتية، بيد أن السؤال الذي يفرض نفسه هل التحقيق في الجرائم الإلكترونية يتميز عن التحقيق في الجرائم التقليدية؟ هناك إجماع حول المنظور العالمي للجريمة المعلوماتية من حيث طبيعتها ونطاقها وارتباطها بشبكات دولية، مما أثر على الاقتصاد العالمي والتنمية وقابليتها للانتشار السريع، مما جعل التحقيق في الجرائم الإلكترونية يتميز عن التحقيق الجنائي في الجرائم التقليدية²¹. ويمكن بيان أهمها في الآتي:

أولاً: يتميز التحقيق في الجرائم الإلكترونية بتطور المفاهيم المستخدمة فيه، فأصبح هنالك مصطلحات جديدة تعد أكثر قرباً وملائمة للبيئة الافتراضية والتقنية التي تباشر فيها إجراءات التحقيق، فمثلاً: استخدام مصطلح "الولوج" بدلاً من مصطلح "التفتيش"، واستخدام مصطلح "النسخ" بدلاً من مصطلح "الضبط"، وهذه المصطلحات تتلاءم مع البيئة الافتراضية أكثر منها في الجريمة التقليدية²².

ثانياً: يعد التحقيق في الجرائم الإلكترونية ذو ذاتية خاصة ومستقلة مستمدة من الطبيعة الخاصة والمميزة للجريمة الإلكترونية عن الجريمة التقليدية، فالتحقيق بها لا يعد استثناءً عن التحقيق في العالم المادي، فأكثر المساحات الافتراضية التي تنمو فيها الجريمة الإلكترونية هي بيئة شبكات الإنترنت وقواعد البيانات والبريد الإلكتروني والنقود الإلكترونية والتجارة

21 - محمد الأمين البشري، "الأساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية"، محاضرة مقدمة في الحلقة العلمية رقم 13: تحليل الجرائم المستحدثة والسلوك الإجرامي، مقر جامعة نايف العربية للعلوم الأمنية، المنعقدة في الفترة من 17-19 جانفي 2011، ص 12.

22 - عمر محمد أبو بكر بن يونس، "الجرائم الناشئة عن استخدام الإنترنت"، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2004، ص 885.

الإلكترونية والأسهم والسندات والأنظمة الأمنية الحساسة ونشر الفيروسات والإرهاب الإلكتروني²³.

ثالثاً: غالباً ما يتخذ الدليل في الجرائم الإلكترونية شكلاً مغايراً للشكل التقليدي للدليل، فالجريمة التي ترتكب بواسطة الكمبيوتر تنشأ في الخفاء، وينصب الاعتداء فيها على معطيات الكمبيوتر، فالتعامل مع مسرح الجريمة الإلكترونية والتحفظ على الدليل يجعلها تتميز في التحقيق عنها في الجرائم التقليدية²⁴، وبالتالي يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية وما تخلفه من آثار غير مرئية.

رابعاً: التحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم التقليدية، إذ يصعب توضيحها لهيئة المحكمة ويسهل زرع الشك في وجدانها، ويرجع ذلك إلى صعوبة إدراك المفاهيم التي يشملها موضوع التحقيق والبحث محل الادعاء، لاسيما مع عدم وجود سلطات تحقيق ومحاكمة متخصصة للتحقيق والفصل في الجريمة الإلكترونية. فإذا كان التحقيق يعتمد على ذكاء المحقق وفننته وقوة ملاحظته ومحاولته بكل جهد ممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث عنها وصولاً للكشف عن الحقيقة، فإنه يتطلب تطوير أساليبه من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في البيئة الافتراضية²⁵.

خامساً: إن التحقيق في الجرائم الإلكترونية أمام متهم من نوع خاص يتميز بنسبة عالية من الذكاء والخداع، فضلاً عن قدرات فنية ومعرفة بجهاز الكمبيوتر وتقنياته، ما يتطلب إمكانيات مادية وتشريعات وإجراءات تختلف عن التحقيق في الجرائم التقليدية، مما أدى إلى ظهور ما يسمى بأزمة القانون الجنائي، خاصة من حيث طبيعة السلوك الإجرامي الإلكتروني، فإن القانون لا يستطيع تجريم أفعال لم ينص عليها المشرع حتى لو كانت هذه الأفعال مستهجنة، لما هو مقيد به من مبدأ الشرعية الجنائية. فغياب الإمكانيات المادية لمواجهة التقنيات الفنية العالية، والنقص بالتشريعات المتعلقة بالتحقيق، يقود إلى أدنى مستوى أداء لجهات التحقيق في الجرائم الإلكترونية، لاسيما أن بعض إجراءات التحقيق والإجراءات المتبعة في التفتيش والضبط وتكوين فرق العمل لها سمات خاصة وتحتاج إمكانيات مادية باهظة للكشف عن الجريمة الإلكترونية²⁶.

سادساً: إن التحقيق في الجريمة الإلكترونية يختلف عنه في التحقيق في الجريمة التقليدية، حيث يعاني المجتمع في كثير من الدول من عدم منح الجرائم المرتكبة بواسطة جهاز الكمبيوتر

23 - محمد الأمين البشري، المرجع السابق، ص 11.

24 - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان -الأردن، 2011، ص 143 وما بعدها.

25 -أحمد عبد الإله المرافي، "الجريمة الإلكترونية ودور القانون الجنائي في الحد منها -دراسة تحليلية تأصيلية مقارنة"، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص75.

26 - طارق إبراهيم الدسوقي، أمن المعلومات والبحث الجنائي في جرائم الإنترنت، دار الجامعة الجديدة، الإسكندرية، مصر، 2011، ص

وتقنيات الاتصال الاهتمام التشريعي والقضائي اللازمين، لاسيما مع غياب الإطار التشريعي الموحد بين الدول وضعف التعاون الأمني بينهما، وهذا الأمر ترك المجال مفتوحا لتنفيذ العديد من جرائم الكمبيوتر الدولية مثل تبييض الأموال والاتجار بالمخدرات والاعتداء على قواعد البيانات. إلى جانب ذلك، فإنه يقصد العمليات الجرمية الإلكترونية التي تتجاوز في العادة الحدود الجغرافية للبلدان، حيث جعلت من مرتكبي الجرائم الإلكترونية يتحدون جهات التحقيق التقليدية للدول ذات السيادة، فبتنظيمهم هجوما منظما من أي جهاز كمبيوتر في أي مكان في العالم ثم تمرير الهجوم عبر الحدود الوطنية المختلفة، مما أتاح الفضاء الإلكتروني لمرتكبي هذه الجرائم مجالا لإخفاء هوياتهم أو تمويهها، وبات الأمر بالقبض على مجرمي هذا النوع من الجرائم بالنسبة لجهات التحقيق محفوفاً بالخطر والعقبات التقنية على جهات التحقيق²⁷.

بناءً على ما سبق ذكره، ونظرا للاختلاف الجوهرى بين التحقيق الجنائي في الجرائم الإلكترونية مقارنة بالجرائم التقليدية، تبرز الحاجة إلى إجراء تعديلات جوهرية ووضع تشريعات خاصة تتوافق مع طبيعة وإجراءات التحقيق الحديث. هذه التشريعات يجب أن تواكب تطور الجريمة وأساليبها المتجددة، خاصة وأن النصوص العامة الواردة في قوانين العقوبات الحالية قد لا تكون كافية لتحقيق العدالة في هذا المجال. إذ يمكن أن يؤدي التعقيد والطبيعة الخاصة لهذه الجرائم إلى صعوبة معاقبة مرتكبيها، مما قد يتركهم دون محاسبة قانونية.

وفي هذا الجانب يُحمد المشرع الجزائري على سن تشريع القانون رقم 09-04 المؤرخ في 5 أوت 2009، ويتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي يهدف إلى حماية البيانات والمعلومات الحكومية والأنظمة والشبكات المعلوماتية الخاصة بالدولة أو أحد الأشخاص الاعتبارية العامة من الاعتراض أو الاختراق أو العبث بها أو إتلافها أو تعطيلها بأي صورة كانت، ففي هذا القانون كان هناك تنظيم إجرائي دقيق ينظم إجراءات الضبط والتحقيق والمحاكمة المتعلقة بالجرائم، بالإضافة إلى حالات الدفاع وإجراءاته، وتنظيم عمل الخبراء المتخصصين في مجال جرائم مكافحة تقنية المعلومات، والقرارات والأوامر الجنائية المتعلقة بتنفيذ القانون

المبحث الثاني: الأساس القانوني للتحريات الإلكترونية

كفل الدستور الجزائري حماية الأفراد أثناء معالجة البيانات ذات الطابع الشخصي، معتبرا ذلك حقاً أساسيا، كما عزز أهمية ذلك من خلال معاقبة كل من يتعدى على هذه الحقوق²⁸. وبالنظر لذلك، أصدر المشرع نصوصاً تشريعية مختلفة تهدف إلى تنظيم عمليات معالجة البيانات وحمايتها لتتماشى والتطور السريع في تقنيات الإعلام والاتصال وظهور أنماط جديدة من الجرائم عبر الفضاء الرقمي، من أجل مواجهة التحديات الناشئة.

27 - جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة- مصر، 2008، ص 67.
28 - نص الدستور الجزائري لسنة 2020، من خلال نص المادة 27 منه، على أنه: "...حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.
يعاقب القانون على كل إنتهاك لهذه الحقوق"، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 82، 2020.

إن المشرّع الجزائري واستجابة منه لهذه الحاجة، عمل على وضع نصوص قانونية تهدف إلى الكشف عن هذه الجرائم ومكافحتها بفعالية. إذ يُعد القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، واحدًا من أبرز الأطر التشريعية في هذا المجال، حيث وضع قواعد تُمكن السلطات المختصة من استخدام تقنيات حديثة، مثل المراقبة الإلكترونية، تفتيش الأنظمة المعلوماتية وحجز البيانات الرقمية.

وقد عزز هذا الإطار القانوني بتعديلات مست قانون الإجراءات الجزائية الجزائري المقنن بالأمر رقم 66-155 المؤرخ في 8 جوان 1966²⁹، حيث ألغي واستحدث بالقانون رقم 25-14 المؤرخ 3 أوت 2025³⁰، مما أتاح استخدام وسائل تحرٍ خاصة لمواجهة الجرائم الخطيرة، بما فيها الجرائم الإلكترونية. ولضمان حماية الحقوق والحريات الفردية، تم إخضاع تلك الإجراءات لرقابة القضاء. بناءً على ذلك، تعتمد التحريات الإلكترونية في التشريع الجزائري على نظام قانوني متكامل يسعى إلى تحقيق توازن بين فعالية التحقيقات وضمان صون الحقوق الأساسية للمواطنين.

المطلب الأول: الإطار القانوني للتحريات الإلكترونية في الجزائر

أولى المشرّع الجزائري اهتمامًا كبيرًا بمكافحة الجرائم المعلوماتية ومواكبة التطورات التكنولوجية، من خلال صياغة إطار قانوني يتيح استخدام التحريات الإلكترونية للكشف عن هذا النوع من الجرائم. وبرز هذا الاهتمام بشكل أساسي في القانون رقم 04-09 الصادر بتاريخ 5 أوت 2009، الذي يتناول القواعد الخاصة بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها. وقد نص القانون على مجموعة إجراءات محددة للتحري في البيئة الرقمية، مثل تفتيش الأنظمة المعلوماتية، حجز البيانات الرقمية، واعتراض الاتصالات الإلكترونية، مع التأكيد على أهمية خضوع هذه الإجراءات لرقابة السلطة القضائية. بالإضافة إلى ذلك، عزز المشرّع هذا الإطار من خلال إدخال تعديلات على قانون الإجراءات الجزائية، مما أتاح اعتماد أساليب تحرٍ خاصة للتصدي للجرائم الخطيرة، بما في ذلك الجرائم المعلوماتية، والهدف منه تحقيق التوازن بين ضمان فعالية التحقيق وحماية الحقوق والحريات الفردية.

وقد تطرق المشرّع الجزائري لموضوع التحريات الإلكترونية والجريمة المعلوماتية في عدة نصوص قانونية، وليس في قانون واحد فقط. أهمها ثلاثة نصوص أساسية يمكننا التطرق إليها فيما يلي:

الفرع الأول: القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال

²⁹ - الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم 48، الصادر بتاريخ 10 يونيو 1966.

³⁰ - القانون رقم 25-14 المؤرخ في 3 أوت 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 54، 2025.

يُمثل القانون رقم 04-09 الصادر في 5 أوت 2009 الإطار القانوني المخصص للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها³¹. ويهدف إلى وضع قواعد واضحة للتحري والتحقق في الجرائم المعلوماتية، من خلال تبني أدوات تقنية متطورة تشمل مراقبة الاتصالات الإلكترونية، تفتيش الأنظمة المعلوماتية، وحجز البيانات الرقمية، وكل ذلك يتم تحت إشراف الجهات القضائية المختصة.

يحتوي القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، على ستة (6) فصول تناولت على التوالي: أحكام عامة، مراقبة الاتصالات الإلكترونية، القواعد الإجرائية، التزامات مقدمي الخدمات، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، التعاون والمساعدة القضائية الدولية. وبذلك يكون القانون رقم 04-09 السالف الذكر، قد تضمن مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف، مصالح معينة لتفادي وقوع الجرائم الإلكترونية أو الكشف عنها وعن مرتكبيها في وقت مبكر³². ويمكن تلخيص أهم هذه التدابير كما يلي:

أولاً: مراقبة الاتصالات الإلكترونية: حدد نص المادة 04 من القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية، وهي:

- أ- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- ج- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

غير أن المشرع الجزائري ومن خلال نفس النص القانوني أكد على أنه لا يجوز إجراء عمليات المراقبة في الحالات السابقة المذكورة إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة.

ثانياً: القواعد الإجرائية: تضمنت المواد من 5 إلى 9 من القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجموعة من القواعد الإجرائية التي تهدف إلى الوقاية من الجرائم الإلكترونية ومكافحتها، وتتمثل هذه الإجراءات في:

³¹ قانون رقم 04-09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 47، الصادرة بتاريخ 16 أوت 2009.

³² - أسهمان بوضياف، "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري في ظل القانون 04-09"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف-المسيلة، الجزائر، المجلد 15، العدد 01، 2022، ص 36.

أ- **تفتيش المنظومات المعلوماتية:** نصت عليها المادة 05 من القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال³³، حيث يجوز للسلطات القضائية في إطار قانون الإجراءات الجزائية وفي الحالات التي تسمح ئءؤرلابالجوء إلى المراقبة الإلكترونية - التي سبق وأشرنا إليها- الدخول بغرض التفتيش ولو عن بعد إلى منظومة تخزين أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، وإذا تبين أن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة ووفقاً لمبدأ المعاملة بالمثل، كما يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

ب- **حجز المعطيات المعلوماتية:** عندما يتم إجراء التفتيش قد تكتشف السلطة التي تباشر في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم ومرتكبيها، فيتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار وفقاً للقواعد المقررة في نصوص القانون الإجراءات الجزائية رقم 14-25 المؤرخ في 1 أوت 2025³⁴. أما إذا استحال إجراء الحجز لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال الإجراءات اللازمة، والتقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة. وفي إطار ممارسة سلطة التفتيش يمكن للسلطة التي تباشر هذه الإجراءات أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، وتستعين في ذلك بالأشخاص المؤهلين لاستعمال الوسائل التقنية المناسبة لذلك³⁵.

هذا، وقد فرض القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، على مقدمي الخدمات مجموعة من الالتزامات التي تساهم بدورها في الوقاية من الجرائم الإلكترونية ومكافحتها. حيث ألزمهم بتقديم المساعدة للسلطات، إذ يجب على مقدمي الخدمات تقديم المساعدة اللازمة للسلطات المكلفة وذلك من أجل حفظ المعطيات ووضعها تحت تصرف السلطات المكلفة بالتحريات القضائية، كما يتعين على مقدمي الخدمات في إطار هذه المساعدة كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق³⁶.

33- أنظر نص المادة 5 من القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

34- تنص المادة 6 من القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، على أنه: "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 أحرار وفقاً للقواعد المقرر في قانون الإجراءات الجزائية".

35- أنظر نصي المادتين 7 و8 من القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

36- أنظر نص المادة 10 من القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

كما أقر المشرع الجزائري من خلال نص المادة 11 من القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ضرورة حفظ المعطيات المتعلقة بحركة السير، حيث يلتزم مقدمو الخدمات بحفظ ما يلي:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات المستعملة للاتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم بالاتصال وكذا عناوين المواقع المطلع عليه.

ج-التعاون والمساعدة القضائية الدولية: أقر المشرع الجزائري من خلال نصوص القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أن المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

كما أقر إمكانية تبادل المساعدة القضائية الدولية في إطار التحريات أو التحقيقات القضائية الجارية لمعينة الجرائم الإلكترونية وكشف مرتكبيها، وذلك من أجل جمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، بشرط ألا يكون في إجراء هذه المساعدة القضائية الدولية مساس بالسيادة الوطنية أو النظام العام، كما يشترط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب³⁷.

الفرع الثاني: التحريات الالكترونية في ظل قانون الإجراءات الجزائية

نظم المشرع الجزائري التحريات الالكترونية ضمن أحكام قانون الإجراءات الجزائية من خلال مواد عديدة، نوجزها فيما يلي:

-اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، والتي نص عليها ضمن النصوص القانونية من 114- 119 من قانون الإجراءات الجزائية.

-في إجراءات التسرب، والتي نص عليها ضمن نصوص المواد من 120 إلى 127 من قانون الإجراءات الجزائية.

- استحدث أيضا القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، ضمن نصوص المواد من 335 إلى 342 من قانون الإجراءات الجزائية.

³⁷ - أنظر نصوص المواد من 15-19 من القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

الفرع الثالث: القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المعدل والمتمم

يُعتبر القانون رقم 07-18 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المعدل والمتمم³⁸، بمثابة مرجع أخلاقي لتعاملات معالجة البيانات ذات الطابع الشخصي، حيث يُولي أهمية قصوى لعدم انتهاك حقوق الإنسان أو المساس بالحريات العامة والحياة الخاص. وقد سن القانون العديد من التدابير لضمان حماية البيانات الشخصية، منها شرط الحصول على الموافقة المسبقة للشخص المعني بمعالجة بياناته، وإذا كان الشخص قاصرًا أو فاقداً للأهلية القانونية، فإن الموافقة تعتمد على ممثله القانوني أو الشرعي، وفق أحكام قانون الأسرة. مع ذلك، استثنى القانون بعض الحالات التي لا تتطلب موافقة مسبقة، مثل الحالات المرتبطة بالجرائم والعقوبات أو تلك التي تتناول تدابير أمنية خاضعة لسلطات قضائية أو إدارية محددة.

إن الهدف من سن هذا القانون هو الحد من الانتهاكات غير القانونية المتعلقة بحقوق الأفراد من خلال اشتراط التصريح المسبق للقيام بعمليات معالجة البيانات الشخصية، إذ لا تتأتى عملية التصريح إلا من خلال السلطة الوطنية لحماية البيانات ذات الطابع الشخصي، التي تقدّم التراخيص بعد دراسة الطلبات في إطار احترام الحريات والحقوق الأساسية. وقد تم تنظيم هذه الإجراءات بشكل تفصيلي في نصوص المواد من 7 إلى 21 من القانون السالف الذكر.

لدى تنفيذ هذا القانون ومراقبة الامتثال له، أنشأ المشرع الجزائري السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، حيث تعدّ هذه السلطة هيئة إدارية مستقلة تعمل تحت وصاية رئيس الجمهورية مع تمتّعها بالشخصية المعنوية والاستقلال المالي والإداري، ويحدد مقرّها بالجزائر العاصمة، في حين تم تحديد تشكيلتها ونظام عملها ضمن نصوص المواد من 22 إلى 31 من القانون السالف الذكر.

من حقوق الأفراد التي كفلها القانون هو الحق في الإعلام قبل الحصول على المعلومات، أي قبل الشروع في أي عملية لمعالجة معلوماتهم الشخصية، فلا يجوز معالجة بيانات أي شخص دون إعلامه مسبقًا والحصول على موافقته. كما يحق للشخص الوصول إلى بياناته الخاصة للتأكد من صحتها، بالإضافة إلى حقه في طلب تصحيح أو تحديث أو حذف بياناته إذا كانت معالجة المعطيات تخالف أحكام القانون، كما أتاح القانون للأفراد الحق في الاعتراض على استخدام بياناتهم لأغراض دعائية.

³⁸ - قانون رقم 07-18 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 34، 2018، المعدل والمتمم بالقانون رقم 11-25 المؤرخ في 24 جويلية 2025، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 48، الصادرة بتاريخ 24 جويلية 2025.

غير أنه، وبخصوص هذا الإجراء المذكور أعلاه –الحق في الإعلام والحصول على الموافقة–، نجد المشرع الجزائري من خلال تعديل القانون رقم 07-18 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، بموجب القانون رقم 25-11 المؤرخ في 24 جويلية 2025، قد استحدث الباب الخامس مكرر "معالجة المعطيات ذات الطابع الشخصي لأغراض الوقاية من الجرائم والكشف عنها وإجراء التحريات والتحقيقات والمتابعات الجزائية وتنفيذ العقوبات وتطبيقها"، حيث نصت المادة 45 مكرر في فقرتها 7، على أنه: "... بغض النظر عن أحكام المادتين 7 و8 من هذا القانون، لا تشترط الموافقة المسبقة للشخص المعني لمعالجة المعطيات ذات الطابع الشخصي المذكور في هذا الباب.

لا يجوز معالجة المعطيات ذات الطابع الشخصي التي تجمعها السلطات المختصة بموجب هذا الباب إلا لأغراض الوقاية من الجرائم والكشف عنها وإجراء التحريات والتحقيقات والمتابعة الجزائية وتنفيذ العقوبات وتطبيقها، وفي حالة معالجتها لأغراض أخرى، تطبق الأحكام التشريعية ذات الصلة المنصوص عليها في هذا القانون وفي التشريع الساري المفعول".

في مقابل هذه الحقوق، فرض القانون التزامات على المسؤولين عن معالجة البيانات، ومن بينها ضمان سلامة وأمان البيانات الشخصية من التلف أو الضياع أو النشر أو الوصول غير المصرح به. كما أوجب اتخاذ تدابير تقنية وتنظيمية لمنع أي اختراق لهذه البيانات.

إضافةً إلى ذلك، ألزم القانون مزودي الخدمات، وخاصة في المجال الإلكتروني، بإبلاغ السلطة الوطنية لحماية المعطيات عن أي ضياع أو إفشاء أو وصول غير مصرح به للبيانات أثناء عمليات المعالجة، خصوصًا إذا كان ذلك يمس الحياة الخاصة للأشخاص.

كما وسّع المشرع من مجال الحماية ليشمل البعد الدولي لمعالجة المعطيات، ولذا تم حظر نقل البيانات الشخصية إلى دول أجنبية إلا بعد الحصول على ترخيص مسبق من السلطة الوطنية ووفقًا لأحكام محددة وردت في نصي المادتين 44 و45 من القانون رقم 07-18 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المعدل والمتمم.

الفرع الرابع: قانون العقوبات الجزائري المعدل والمتمم

نظم المشرع الجزائري لأول مرة تجريم الأفعال التي تمس بأنظمة الحاسب الآلي تأثرًا بظهور أشكال جديدة من الجرائم التي أفرزتها الثورة المعلوماتية، والتي لم تكن معروفة سابقًا. وفي هذا الإطار، دفع التطور التكنولوجي المشرع إلى تعديل نصوص قانون العقوبات بموجب القانون رقم 04-15³⁹، حيث أضيف قسم جديد تحت عنوان القسم السابع مكرر "المساس بأنظمة

³⁹ قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 71، الصادرة بتاريخ 10 نوفمبر 2004.

المعالجة الآلية للمعطيات"، حيث يحتوي هذا القسم على تسعة (9) مواد من المادة 394 مكرر إلى المادة 394 مكرر 8 -التي عرفت عدة تعديلات-⁴⁰، وقد تناول فيها تجريم مجموعة من الأفعال التي تُعد انتهاكاً لأنظمة المعالجة الآلية للبيانات، مع تحديد العقوبات المناسبة لكل جريمة وفقاً للنصوص القانونية الواردة.

أولاً: جريمة الدخول أو البقاء عن طريق الغش إلى نظام معالجة البيانات: تتمثل هذه الجريمة، في فعل الدخول الإلكتروني أو التقني إلى النظام المعلوماتي باستخدام وسائل فنية دون وجه حق أو إذن مسبق. هذا الفعل يُعتبر غير مشروع بحد ذاته⁴¹. حيث تنص المادة 394 مكرر من القانون رقم 06-24 المؤرخ في 28 أبريل 2024، المتضمن تعديل قانون العقوبات، على أنه: "يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك جذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال للمنظومة، تكون العقوبة الحبس من سنة (1) إلى (3) سنوات والغرامة من 100.000 دج إلى 300.000 دج".

أما بالنسبة لفعل البقاء غير المشروع داخل النظام، فيُقصد به استمرار التواجد غير المصرح به من قبل صاحب النظام أو المسؤول عنه، حتى بعد الدخول غير المقصود أو العارض للنظام، مع العلم بأن البقاء داخل النظام يشكل خرقاً للموافقة⁴².

فبمفهوم نص المادة 394 مكرر السالفة الذكر، فإن المشرع الجزائري أورد ظرفين يمكن أن يؤديا إلى تشديد العقوبة على الجاني في هذه الجرائم، حيث يتحقق الظرف الأول إذا أدى الدخول أو البقاء إلى محو أو تعديل البيانات داخل النظام. أما الظرف الثاني فيتحقق إذا تسببت هذه الأفعال بضرر للنظام أو تعطيل وظيفته.

وعليه، فإن المشرع الجزائري سعى لتوفير حماية قانونية صارمة للأنظمة المعلوماتية، نظراً لحساسيتها وأهميتها في العصر الحالي.

ثانياً: جرائم الاعتداء على المعطيات الموجودة داخل نظم المعلوماتية: تعتبر من الجرائم الحديثة التي أولاها المشرع الجزائري أهمية خاصة نظراً لتزايد الاعتماد على التقنيات الحديثة

⁴⁰ -القانون رقم 06-24 المؤرخ في 28 أبريل 2024، المتضمن تعديل قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 30، الصادرة بتاريخ 30 أبريل 2024، المعدل والمتمم بالأمر رقم 02-16 المؤرخ في 19 جوان 2016، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 37، الصادرة بتاريخ 22 جوان 2016.

⁴¹ - أمال قارة، الجريمة المعلوماتية، رسالة ماجستير، القانون الجنائي والعلوم الجنائية، جامعة الجزائر 1، الجزائر، 2002. ص44.

⁴² - حنان مهداوي، "التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري"، مجلة الفكر القانوني والسياسي، جامعة محمد لمين دباغين سطيف 2، المجلد، العدد 2، 2022، ص 1064.

في الحياة اليومية. وقد نصت المواد 394 مكرر 1 و 394 مكرر 2 من قانون العقوبات المعدل والمتمم، على تجريم هذا النوع من الأفعال وتحديد العقوبات الرادعة للمسؤولين عنها.

نصت المادة 394 مكرر 1 من قانون العقوبات، على أنه: "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

كما نصت المادة 394 مكرر 2 من قانون العقوبات، على أنه: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش، بما يأتي:

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

يتبين من خلال هذين النصين، أن جرائم الاعتداء على نظم المعلوماتية تتخذ شكلين رئيسيين:
أ-الشكل الأول: هو جريمة التلاعب بالمعطيات، التي تتحقق إذا قام الفاعل بأي من الأفعال التالية:

- إدخال معطيات بالنظام المعلوماتي عن طريق الغش.

- إزالة معطيات موجودة بالنظام المعلوماتي عن طريق الغش.

- تعديل معطيات داخل النظام المعلوماتي بطرق غير مشروعة.

ب-الشكل الثاني: هو جريمة التعامل غير المشروع في هذه المعطيات، فتتحقق كما جاء في نص المادة 394 مكرر 2، عبر التعامل في معطيات صالحة لارتكاب جريمة، ويتضمن ذلك أي سلوك يُبرز وجود علاقة بين شخص ومعطيات غير قانونية، ويشمل تصميمها، جمعها، توفيرها للآخرين، أو نشرها بهدف تسهيل ارتكاب الجرائم. كما قد يتضمن التعامل في معطيات متحصّل عليها من جريمة، حيث يشمل هذا السلوك المحظور حيازة أو إفشاء أو نشر أو استخدام المعلومات المستخرجة من جرائم مثل الدخول غير المشروع إلى النظم المعلوماتية أو التلاعب بمعطياتها.

وعليه، توضح هذه المواد أن الهدف من هذه العقوبات هو حماية نظم المعلوماتية والبيانات التي تتضمنها، والتي أصبحت من أصول العصر الحديث التي يجب الحفاظ عليها لضمان سلامة المجتمعات الرقمية وأمنها⁴³.

المطلب الثاني: الإطار القانوني الدولي والإقليمي للتحريات الإلكترونية

يشهد العالم تطوراً تكنولوجياً متسارعاً أدى إلى انتشار الجريمة المعلوماتية، التي تتميز بطابعها العابر للحدود وصعوبة كشفها بالوسائل التقليدية. لذلك، أصبح من الضروري وضع إطار قانوني دولي ينظم التحريات الإلكترونية ويعزز التعاون بين الدول. وتُعد اتفاقية بودابست من أبرز هذه الجهود، إلى جانب دور الإنترنت والأمن المتحدة، حيث تهدف هذه الجهود إلى تحقيق التوازن بين مكافحة الجريمة المعلوماتية وحماية الحقوق والحريات.

الفرع الأول: اتفاقية بودابست لمكافحة الجريمة المعلوماتية

تعدّ اتفاقية بودابست لمكافحة الجريمة المعلوماتية لعام 2001، خطوة مفصلية في مجال القانون الدولي، حيث وضعت إطاراً شاملاً للإجراءات القانونية الحديثة لمواجهة الجرائم الإلكترونية، إذ قامت الاتفاقية على مبدأ أساسي يتمثل في إلزام الدول الأعضاء بمواءمة تشريعاتها الداخلية ونظمها القضائية مع الإجراءات المنصوص عليها فيها، وهذا يعكس إدراك المجتمع الدولي للطبيعة العابرة للحدود للجرائم المعلوماتية، والتي لا يمكن التصدي لها بفعالية إلا من خلال التنسيق والتوحيد بين الدول في الأسس القانونية والإجرائية⁴⁴. من بين أبرز هذه الإجراءات:

أولاً: المحافظة المؤقتة على البيانات المخزنة: إن الهدف من ذلك، هو ضمان الاحتفاظ بالمعلومات الرقمية وحمايتها من الضياع أو التلف، نظراً لأهمية تلك البيانات كأدلة رئيسية في التحقيقات الجنائية. وقد تم تصنيف هذا الإجراء كأحد أصعب الإجراءات العملية بسبب الطبيعة المؤقتة للأدلة الرقمية وسرعة ضياعها أو حذفها. لذلك، أجازت المادة 16 من الاتفاقية للسلطات الوطنية إصدار أوامر قضائية عاجلة لحفظ البيانات الفوري ولضمان عدم فقدانها، ما يُبرز أهمية تحقيق التوازن بين فعالية التحقيق وحماية حقوق الأفراد وخصوصيتهم الرقمية⁴⁵.

ثانياً: آليات جمع المعلومات الخاصة بالمشتبه بهم: تناولت الاتفاقية هذه الآليات، والتي قد تتمثل في أرقام الهواتف وعناوين البريد الإلكتروني وعناوين المواقع الإلكترونية. وهذه الإجراءات تعتبر أدوات أساسية لتحديد هوية مرتكبي الجرائم الإلكترونية. ورغم ذلك، تُظهر

⁴³ - عائشة بوخيزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، رسالة تخرج لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2013/2012، ص 82.

⁴⁴ - أيوب بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية: دراسة مقارنة، مشورات الحلبي القانونية، لبنان، 2009، ص 45.

⁴⁵ - الحلو أحمد، وآخرون، الأدلة الإلكترونية (الجوانب القانونية والتقنية)، معهد القانون، جامعة بيرزيت، فلسطين، 2015، ص 35.

هذه الممارسات تحدياً قانونياً يتمثل في حماية الخصوصية الفردية، إذ ينبغي جمع هذه المعلومات من خلال إجراءات قانونية رسمية وتحت إشراف قضائي لضمان احترام الحقوق المدنية أثناء التحقيقات.

ثالثاً: إجراءات التفتيش الرقمي: نصّت الاتفاقية على هذه الإجراءات، والتي يجب أن تتم بموجب إذن رسمي من أجل الوصول إلى البيانات المخزنة في مواقع محددة، بهدف جمع الأدلة مع مراعاة عدم المساس بحقوق الأفراد الأساسية. كما تطرقت الاتفاقية إلى استخدام التنصت كإجراء جديد لمكافحة الجرائم المعلوماتية. ويتضمن ذلك مراقبة المراسلات، تسجيل المكالمات، أو استخراج الصور مع ضرورة الحصول على موافقة قضائية مسبقة لضمان استخدام هذه الوسائل بطرق قانونية ومحدودة. تُظهر هذه التطورات كيفية موازنة القوانين مع التقنيات المتقدمة لضبط الجرائم الرقمية دون تجاوز الحقوق القانونية.

هذا، وقد أكدت الاتفاقية (وخاصة في المادة 23 وما يليها) على أهمية التعاون الدولي كركيزة أساسية لتفعيل الإجراءات السابقة. ويتضمن ذلك تبادل المعلومات والأدلة بسرعة وفعالية، وتطوير آليات تسليم المجرمين ووضع أحكام خاصة بالجرائم المعلوماتية العابرة للحدود. هذا البند يعكس إدراك المجتمع الدولي لحقيقة أن المجرمين الإلكترونيين غالباً ما ينفذون جرائمهم من خارج حدود دول الضحايا، مما يجعل التعاون بين الدول عاملاً حيوياً لنجاح التحقيقات وتقديم المتهمين للعدالة.

ونشير أيضاً، إلى أن اتفاقية بودابست لمكافحة الجريمة المعلوماتية، قد ركزت على تحديث الأسس القانونية التقليدية، مثل إجراءات التفتيش الرقمي، والحفظ المؤقت للبيانات، والتنصت الرقمي بما يتماشى مع التطورات التكنولوجية المستمرة. ومن خلال توحيد الإجراءات القضائية بين الدول الأعضاء وتعزيز الشراكة الدولية، ساهمت الاتفاقية في تحسين فعالية مكافحة الجرائم الإلكترونية وتعزيز الأمن الرقمي على المستوى العالمي.

وعليه، تُعدّ اتفاقية بودابست رؤية قانونية دولية متكاملة في مجال مكافحة الجرائم المعلوماتية. فقد وفّرت إطاراً تشريعياً وإجرائياً شاملاً يعزز التعاون الدولي ويطور الأدوات القانونية والتقنية الحديثة لضمان الكشف عن الجرائم الرقمية ومعاينة مرتكبيها بفعالية، مع الحفاظ على حقوق الأفراد وخصوصيتهم⁴⁶.

الفرع الثاني: دور المنظمات الدولية في مكافحة الجريمة المعلوماتية

أولاً: الإنترنت ومكافحة الجريمة المعلوماتية: تدير منظمة الإنترنت شبكة اتصالات سلكية محمية تغطي مناطق واسعة من العالم، حيث تربط بين الدول الأعضاء عبر مكاتبها الوطنية الرئيسية وبين الأمانة العامة للإنترنت في مدينة ليون بفرنسا. حيث تتيح هذه الشبكة نقلاً سريعاً

⁴⁶ -موسى مصطفى محمد، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، مصر، 2005، ص 23.

وآمنا للرسائل الإلكترونية التي قد تشمل نصوصا مكتوبة، صورا فوتوغرافية، بصمات الأصابع وغيرها من البيانات.

تسعى منظمة الإنتربول إلى تعزيز عملية تبادل المعلومات عبر شبكة دولية تعمل على دعم جهود مكافحة الجريمة. يتم هذا التبادل بين الهيئات الدولية والجهات المختصة الأخرى، مع التركيز على مجموعة متنوعة من الجرائم، مثل الاتجار بالبشر، جرائم التهريب الضريبي، وجرائم الفساد. يعتبر ضباط الشرطة القضائية الجهة المسؤولة عن تجميع وتقديم المعلومات للمنظمات الدولية، ومنها منظمة الإنتربول. التي تعتمد عدة طرق في عملية تبادل المعلومات، نوضحها فيما يلي:

أ- الوصول المباشر إلى المعلومات: بموجب المادة 54 من نظام الإنتربول لمعالجة البيانات، يُسمح للمكاتب المركزية الوطنية والكيانات الدولية بالوصول المباشر إلى قاعدة البيانات الشرطية تحت شروط وقواعد تضمن السرية وحماية البيانات⁴⁷.

ب- الربط الإلكتروني: يُعد الربط الإلكتروني أحد أدوات التبادل المعلوماتي، ولكنه يتطلب تحقيق عدة شروط أساسية منها، أن تكون أهداف الربط واضحة ومتناسبة مع أنشطة المنظمة، وأن يعزز التعاون الشرطي الدولي ويحقق مستوى مناسباً من السرية⁴⁸.

ج- تنزيل البيانات: يُستخدم هذا النوع من التبادل في حالات التعاون الشرطي لمكافحة الجريمة عندما تكون آلية الربط الإلكتروني غير مناسبة بسبب التكلفة أو المتطلبات الفنية. لتحقيق ذلك، يجب أن يكون الغرض من التنزيل محدداً⁴⁹.

تُساهم منظمة الإنتربول في تعزيز كفاءة التعاون الدولي من خلال تطوير وسائل وآليات التبادل، وذلك من أجل مواجهة التحديات الأمنية المختلفة برؤية تركز على الشفافية وحماية البيانات ضمن الإطار القانوني المحدد، حيث يتم تبادل المعلومات من خلال منظومة الإنتربول للمعلومات باستخدام وسائل متعددة يمكن تلخيصها فيما يلي:

1- الاتصال بواسطة جهاز X400: تُعد هذه الوسيلة إحدى الركائز الأساسية لتبادل المعلومات بين الأمانة العامة والمكاتب المركزية الوطنية، أو بين المكاتب المركزية الوطنية المختلفة. يتم ربط الشبكات عبر نظام الاتصالات الهاتفية الدولية التابع للدولة الحاضنة للمكتب المركزي الوطني، أو عبر شبكات الاتصالات الدولية لفرنسا، أو بين دولتين تربطهما شبكة اتصال مباشرة. تتميز هذه الوسيلة بكونها أكثر اقتصادية مقارنة بالمكالمات الهاتفية التقليدية، إذ يمكن أن تصل تكلفة المكالمات الهاتفية الدولية إلى ستة أضعاف تكلفة الاتصالات عبر شبكة المعلومات، ومع ذلك، يتطلب تشغيل الأجهزة المستخدمة خبرات فنية متقدمة من المشغل

47 - مروة بومعزة، الأنتربول وآليات عمله في إطار مكافحة الجريمة، مجلة البيان للدراسات القانونية والسياسية، جامعة البشير الإبراهيمي- برج بوعريش-الجزائر، المجلد 5، العدد 2، 2020، ص 248.

48 - المرجع نفسه، ص 249.

49 - المرجع نفسه، ص 250.

المختص، والذي يخضع عادة لفترة تدريب في مقر المنظمة الدولية لاكتساب المهارات اللازمة لإدارة أجهزة الاتصال هذه. كما تتولى الأمانة العامة عملية تركيب الجهاز بالمكاتب الوطنية المركزية، وتحمل الدولة المضيفة تكلفة الجهاز، مع إمكانية تقديم الدعم من قبل الأمانة العامة في حالات محددة لتغطية تكاليف الجهاز والتركيب والتشغيل⁵⁰.

2-الاتصال عبر الهاتف الدولي وأجهزة الفاكس: بجانب استخدام شبكة X400، تُسهل الاتصالات الدولية الهاتفية التواصل المباشر بين رؤساء المكاتب المركزية الوطنية والأمانة العامة. ومع أن تكلفة هذه الوسيلة تقع على عاتق الجهة المتصلة، فإنها تسهم بشكل كبير في تيسير القنوات الدبلوماسية والتنسيقية بين الأطراف المعنية. بالإضافة إلى ذلك، تُستخدم أجهزة الفاكس لتبادل الرسائل الرسمية بشكل سريع، حيث تُنقل الرسائل مباشرةً ويتم التأكيد على استلامها فوراً. ومن بين أبرز مزايا هذه الوسيلة السرعة والكفاءة في إيصال الرسائل، إلا أنها مصحوبة بتكاليف مالية مرتفعة بالمقارنة مع الخيارات الأخرى⁵¹.

ثانياً: الأمم المتحدة ومكافحة الجريمة المعلوماتية: بذلت هيئة الأمم المتحدة جهوداً كبيرة لمواجهة تحديات الجرائم السيبرانية، مع التركيز على التعاون الدولي وتعزيز العمل المشترك بهدف الحد من انتشار هذا النوع من الجرائم، ويأتي ذلك انطلاقاً من الاعتقاد بأن مكافحة هذه الجرائم تتطلب وعياً بخطورتها وأبعادها على المستوى العالمي. في هذا السياق، نظّمت الأمم المتحدة عدة مؤتمرات ألقت الضوء على هذه القضية وقدمت نماذج وإرشادات للعمل الفعال. فيما يلي نوضح أبرز هذه المؤتمرات:

أ-المؤتمر السابع للأمم المتحدة لمنع الجريمة ومعاملة المجرمين، الذي انعقد في مدينة ميلانو بإيطاليا في الفترة الممتدة بين 21 أوت و30 سبتمبر⁵² 1985، حيث ناقش المؤتمر دور حماية النظم التقنية وتقديم التوصيات اللازمة للحد من الجرائم السيبرانية.

ب-المؤتمر الثامن للأمم المتحدة الذي عُقد في هافانا، كوبا، بين 27 أوت و7 سبتمبر 1990. وقد أبرز هذا المؤتمر الحاجة إلى نماذج تسليم المجرمين وتعزيز التعاون في القضايا الجنائية، بما في ذلك مراقبة المتورطين في الجرائم الإلكترونية وملاحقتهم قانونياً. إن إحدى أبرز القضايا التي ناقشها المجتمعون كانت مقاييس وضع سياسات جنائية شاملة وتعديلات قانونية مناسبة لتجريم أشكال السلوك السيبراني غير المشروع والتعامل معه بجدية. كما شمل ذلك مصادرة عائدات الأنشطة غير القانونية واعتماد آليات وقائية لحماية الأفراد واحترام حقوق الإنسان⁵³. ألم وقد تمثلت التوصيات والمحاور الرئيسية، فيما يلي:

50 - سراج الدين الرويب، آلية الإنتربول في التعاون الدولي الشرطي، ط1، الدار المصرية اللبنانية، مصر، 2001، ص737.

51 - المرجع نفسه، ص ص: 173-175.

52 - سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر-باتنة، الجزائر، 2012-2013، ص83.

53 - مكتب الأمم المتحدة المعني بالمخدرات والجريمة، تاريخ الاطلاع: 28 مارس 2026، على الساعة 22:28، على رابط الآتي:

<http://www.cdonu.org>

1-تحديث القوانين الجنائية لتحسين تطبيقها بما يواكب التطورات التقنية.

2-مصادرة الأموال والعوائد الناتجة عن الأنشطة غير المشروعة.

3-تعزيز توعية الموظفين المختصين، القضاة، وجهات التحقيق بقضايا الجرائم السيبرانية وأهمية التعامل معها بفعالية من خلال تدريبهم على إجراءات التحقيق والمتابعة.

4-التعاون مع المنظمات الدولية لضمان حماية مصالح الضحايا.

ج-المؤتمر التاسع للأمم المتحدة، الذي انعقد بالقاهرة بين 29 أبريل و8 ماي 1995، ناقش حماية خصوصية الأفراد وبياناتهم الشخصية من تهديدات تكنولوجيا المعلومات وتعزيز التنسيق والتعاون بين الدول لمكافحة الجرائم السيبرانية بفعالية⁵⁴.

د-المؤتمر الثاني عشر للأمم المتحدة حول الجريمة والعدالة الجنائية، المنعقد في سلفادور، البرازيل، خلال الفترة الممتدة من 12 إلى 19 أبريل 2010، حيث ناقش التحولات التكنولوجية وتأثيرها على مكافحة الجريمة، وشدد على الدور الريادي للأمم المتحدة في تحديد القواعد الإجرائية لمواجهة الجرائم الإلكترونية. ودعى المؤتمر إلى تعزيز القدرات الوطنية لملاحقة الجرائم الإلكترونية والتحقيق فيها بكافة أشكالها.

هـ-المؤتمر الثالث عشر للأمم المتحدة حول الجريمة والعدالة الجنائية، الذي انعقد في الدوحة، قطر، خلال الفترة بين 12 و19 أبريل 2015. أقر مجموعة من التوصيات لمواجهة الجرائم السيبرانية، تضمنت ما يلي:

-ضرورة استحداث وسائل وبرامج جديدة لتسهيل مكافحة الجرائم الإلكترونية.

-بناء قدرات أفراد أجهزة إنفاذ القانون والعدالة الجنائية للتحري عن هذه الجرائم ومعالجتها، بما يشمل الأدلة الرقمية وآليات التعامل مع الأدلة الإلكترونية.

-إمكانية إنشاء أطر دولية للتعاون المتعدد الأطراف، وفي هذا السياق أوصى الاتحاد الإفريقي بوضع اتفاقية تتعلق بالجرائم السيبرانية.

-التنبيه بالصعوبات التي تواجه أجهزة إنفاذ القانون في الوصول إلى البيانات الضرورية أثناء التحقيقات. مع التأكيد على ضمان حقوق الإنسان وسيادة القانون وصون الخصوصية، بحيث يكون الوصول إلى هذه المعلومات محكومًا بمبادئ قانونية ورقابية شفافة.

-إشراك القطاع الخاص بشكل فعال في جهود مكافحة الجرائم السيبرانية، بما يضمن تبادل المعلومات وتعزيز التعاون الدولي .

و-انعقد المؤتمر الخامس عشر للقانون الجنائي في ريو دي جانيرو بالبرازيل عام 2017، حيث ناقش مجموعة متنوعة من القضايا المتعلقة بالجرائم السيبرانية، منها:

-الاحتيال الإلكتروني، مثل التسلل أو الإضرار بالبيانات الرقمية بهدف تحقيق مكاسب اقتصادية.

-اختراق الأنظمة المعلوماتية، بما في ذلك التلاعب أو تشويه أو تخريب البيانات وبرمجيات الكمبيوتر.

-تخريب الشبكات والاتصالات الإلكترونية، بهدف تعطيل أداء الأنظمة أو التسبب بخسائر اقتصادية أو انتهاك الخصوصية.

وقد توصل الأعضاء المجتمعون في ختام هذا المؤتمر إلى مجموعة من التوصيات الإجرائية للحد من الجرائم السيبرانية، نوجزها فيما يلي:

- تعزيز الأدوات القانونية لتنظيم إجراءات التحقيق والرقابة وفقاً للمعايير الدولية.
- وضع قيود صارمة على السلطات الرسمية لتجنب أي انتهاك لحقوق الإنسان والخصوصية.
- التأكيد على أهمية صياغة قواعد واضحة لمراقبة واستخدام الأدلة الإلكترونية ضمن المعايير القضائية.

-تطوير تشريعات توفر المرونة اللازمة للتعامل مع تحديات البيئة الرقمية المعاصرة .

وعليه مما سبق ذكره، فإنه بالإجمال قد أسفرت هذه المؤتمرات عن إرادة جماعية لتعزيز التنسيق بين الدول والمنظمات الدولية والقطاعات الخاصة لتطوير أدوات فعالة لمكافحة الجريمة بكافة أشكالها، مع مراعاة حقوق الإنسان والحفاظ على الخصوصية وسياق السيادة القانوني.

الفرع الثالث: الإطار القانوني الإقليمي للتحريات الإلكترونية

يُعد الإطار القانوني الإقليمي للتحريات الإلكترونية مكماً للجهود الوطنية والدولية في مواجهة الجرائم المعلوماتية، خاصة لطابعها العابر للحدود. ويهدف إلى توحيد التشريعات وتعزيز التعاون بين الدول داخل نفس الإقليم. وقد ساهمت منظمات مثل جامعة الدول العربية والاتحاد الإفريقي في وضع اتفاقيات تنظم التحريات الإلكترونية وتسهّل تبادل المعلومات والأدلة الرقمية، بما يحقق التوازن بين مكافحة الجريمة واحترام سيادة الدول.

أولاً: الإطار القانوني للتحريات الإلكترونية في الدول العربية: حددت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية، من خلال المواد 3، 4 و 5

الإطار القانوني الذي ينظم مكافحة جرائم تقنية المعلومات، حيث يمكن استخلاص مجموعة من المبادئ الأساسية التي تستند إليها⁵⁵، نوجزها فيما يلي:

أ- نطاق تطبيق الاتفاقية، الذي يتناوله نص المادة 3، حيث تشير إلى أن أحكام الاتفاقية تطبق على الجرائم ذات الطابع العابر للحدود، سواء كانت تلك الجرائم قد ارتُكبت في أكثر من دولة، أو تمت عملية التخطيط لها أو إدارتها من خارج الدولة، أو تضمنت مشاركة جماعات إجرامية منظمة، أو أدت إلى آثار تتجاوز حدود الدولة الواحدة.

ب- مبدأ السيادة المرسخ، والذي تضمنه نص المادة 4، إذ تلتزم الدول بتنفيذ أحكام الاتفاقية بما يتماشى مع نظمها القانونية الوطنية، مع ضرورة احترام مبدأ عدم التدخل في الشؤون الداخلية وعدم ممارسة أي صلاحيات خارج أراضيها.

ج- عنصر التجريم، الذي يناقشه نص المادة 5، حيث تفرض الاتفاقية على الدول الأطراف إدراج الأفعال المتعلقة بجرائم تقنية المعلومات ضمن قوانينها الوطنية.

من خلال هذه المبادئ المذكورة أعلاه، يمكن استنتاج أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية، تهدف إلى تحقيق توازن بين تعزيز التعاون الدولي في مجال مكافحة الجرائم المرتبطة بالتكنولوجيا الحديثة، وبين حماية سيادة الدول وضمان ملائمة الإجراءات مع تشريعاتها الداخلية.

كما تضمنت الاتفاقية الصادرة عن جامعة الدول العربية، ولا سيما المواد من 6 إلى 21، إطاراً قانونياً شاملاً يهدف إلى تجريم مجموعة واسعة من الجرائم المعلوماتية، في مسعى يعكس الفهم العميق للتطور المتسارع لهذه الجرائم وأخطارها. استُهلّت هذه المواد بتركيز على الجرائم التي تمس أمن وسلامة الأنظمة المعلوماتية، مثل الدخول غير المشروع، الاعتراض غير القانوني، والاعتداء على سلامة البيانات، وهي أفعال تهدد بشكل مباشر البنية التحتية الرقمية وتهدد سرية المعلومات وسلامتها. كما شملت الاتفاقية تجريم الأدوات والوسائل المستخدمة في ارتكاب هذه الأفعال، بما في ذلك إنتاج وحياسة وتوزيع البرامج والتقنيات وكلمات المرور المستخدمة لأغراض غير قانونية، مما يعكس توجهاً استباقياً يستهدف منع وقوع الجرائم قبل حدوثها.

امتد نطاق الاتفاقية ليشمل الجرائم ذات الطابع المالي والأخلاقي أيضاً، حيث تم النص على تجريم التزوير والاحتيال الإلكتروني لما لهما من انعكاسات سلبية على الثقة والمعاملات

⁵⁵ - الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، اطلع عليها بتاريخ 28 مارس 2026، على الساعة 20:33، عبر الرابط الآتي:

الاقتصادية في الفضاء الرقمي. هذا، وقد أولت الاتفاقية اهتمامًا خاصًا للجرائم المتعلقة بالإباحية، خصوصًا تلك الموجهة ضد الأطفال، فضلاً عن الأفعال التي تعد انتهاكًا لخصوصية الأفراد. وركزت الاتفاقية أيضًا على مكافحة الجرائم الخطيرة المنفذة عبر الوسائل الإلكترونية، مثل الإرهاب وجرائم الجريمة المنظمة، بما في ذلك غسل الأموال والاتجار بالبشر والمخدرات، ما يشير إلى وعي المشرع العربي بتوظيف التكنولوجيا لتعزيز نطاق وخطورة هذه الجرائم.

وفي السياق نفسه، أكدت الاتفاقية على حماية الحقوق القانونية المرتبطة بالبيئة الرقمية، مع التركيز على صون حقوق المؤلف والحقوق المجاورة. كما جرّمت الأفعال المتعلقة بسوء استخدام أدوات الدفع الإلكتروني، بهدف تعزيز أمان المعاملات المالية الإلكترونية. واختتمت المواد بأحكام عامة تتناول الشروع في ارتكاب الجرائم والمساهمة فيها، مع الإشارة إلى تحميل المسؤولية الجنائية للأفراد والمؤسسات على حد سواء، وتشديد العقوبات في حال استخدام الوسائل التقنية لارتكاب الجرائم التقليدية.

وعليه يمكننا القول، بأن هذه النصوص تشكل منظومة قانونية متماسكة تجمع بين التجريم الوقائي والملاحقة القانونية، ما يجعلها أداة فعالة في مواجهة الجرائم المعلوماتية ودعم جهود التحري الإلكتروني في تعقب مرتكبيها والحد من تأثيرها.

ثانياً: الإطار القانوني للتحريات الإلكترونية في إفريقيا: نظمت اتفاقية مالابو لسنة 2014، حيث تهدف إلى معالجة القضايا المتعلقة بالعمل في مجال المعلومات والعمليات الإلكترونية. وتهدف هذه الاتفاقية لتحقيق ما يلي:

-تحسين وتوحيد التشريعات المتعلقة بالدول الأعضاء، وضمان مواكبة القوانين لتطور التكنولوجيا والاتصالات. يتم ذلك مع الحفاظ على المبادئ الأساسية وحماية حقوق الإنسان والحريات العامة.

-بناء الثقة والتعاون المستدام مع الهيئات القانونية والثقافية والمؤسسات القيادية والمجتمع الدولي بهدف تعزيز الأمن والشراكة الفعالة.

-التأكيد على أهمية حماية البيانات الشخصية والخصوصية، باعتبار ذلك جزءاً أساسياً ضمن بيئة التعاملات الإلكترونية، حيث يجب أن يتم هذا بما يتماشى مع المبادئ القانونية الأساسية ويلبي احتياجات الجهات الفاعلة في القطاعين العام والخاص.

- تعزيز استخدام الأنظمة الإلكترونية والاتصالات، مما يساهم في تقليل التكاليف وزيادة الكفاءة الاقتصادية.

- دعم جهود الحكومات في إعادة تأسيس أطر تساهم في التنمية المستدامة و/أو تقديم حلول للمشكلات التي تؤثر على رفاهية واقتصاد سكانها.

- العمل على تعزيز الاعتراف القانوني بالعمليات والإجراءات الإلكترونية، مع تطوير البنية التحتية القانونية اللازمة لتحقيق الشفافية وحماية البيانات وضمان موثوقية التعاملات الإلكترونية. كما تهدف إلى معالجة قضايا تتعلق بالممارسات المرتبطة بالخدمات الهاتفية وجوانب أخرى مشابهة⁵⁶.

تهدف الاستراتيجيات الإفريقية إلى تعزيز الأمن الوطني من خلال العمل على تطوير الأسس اللازمة لدعم المؤسسات الوطنية. ويأتي ذلك إدراكا لأهمية البنية التحتية للمعلومات في الدول، والتي تُعد العامل الأساسي لمواجهة التحديات التي تواجهها. بالإضافة إلى ذلك، تحظى الخطط العلمية والتقنية بتركيز خاص، بهدف تحقيق تقدم واضح في مجال الهيئات والقطاعات الحيوية التي تخدم المجتمع. إلى جانب ذلك، يجب تعزيز التعاون بين مختلف الجهات لتحقيق تكامل أكبر بين الأنظمة الإلكترونية وتطبيقات الأمن الوطني، مما يستدعي إطلاق برامج شاملة ومدرسة تهدف إلى رفع مستوى الجاهزية. يأتي هذا استجابة للتحديات العامة التي تواجه الدول في الحفاظ على استقرارها وأمنها في ظل التطور التكنولوجي المستمر.

أما فيما يتعلق بحوكمة الأنظمة، فلا بد من وضع آليات صارمة لضمان توافق الجهات المعنية مع المعايير الوطنية، إن الهدف من ذلك هو إنشاء بنية تحتية قوية للأمان السيبراني، مما يمنع أي اختراق أو تعرض للمعلومات الحساسة. ومن ضمن الإجراءات التي ينبغي اتخاذها:

- مواجهة محاولات التخريب الإلكتروني مثل التلاعب أو الاختراق أو التدمير المتعمد للبيانات الهامة.

- منع الإنتاج غير القانوني أو توزيع المحتوى المحمي بحقوق الملكية الفكرية، إلى جانب الحد من القرصنة الرقمية.

- تأمين البيانات الشخصية، والتصدي لأي استغلال أو استخدام غير مشروع لها.

- تطوير إطار قانوني متكامل يضمن حماية المواطنين والمؤسسات وفقا للمعايير الدولية .

وعليه، فإن هذه التحديات تفرض ضرورة اتخاذ تدابير استباقية، وتعزيز الشفافية لتوفير بيئة رقمية آمنة ومستدامة لجميع الأطراف⁵⁷.

المطلب الثالث: الجهات المختصة بمباشرة التحريات الإلكترونية

⁵⁶ - مريم لوكال، "قراءة في اتفاقية الاتحاد الإفريقي حول الامن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014"، مجلة الدراسات القانونية والاقتصادية، جامعة امحمد بوقرة - بومرداس، الجزائر، المجلد 04، العدد 03، 2021، ص661.

⁵⁷ - المرجع نفسه، ص ص: 664-665.

تختلف الجهات المعنية بالتحقيق في الجرائم الإلكترونية من بلد إلى آخر. ففي العديد من الدول، توجد مؤسسات متخصصة بمكافحة هذا النوع من الجرائم، مثل الوكالة الوطنية للأمن في الولايات المتحدة الأمريكية. إضافة إلى ذلك، تسهم منظمة الشرطة الجنائية الدولية، التي تعمل تحت مظلة هيئة التعاون الدولي، بدور أساسي في التصدي للجرائم الإلكترونية على مستوى عالمي. وسننطلق من هنا للحديث عن الهيئات المعنية في التحقيق في التشريع الجزائري:

الفرع الأول: الهيئات الوطنية المختصة بمباشرة التحريات الإلكترونية

سنتناول في هذا الفرع، الجهات المختصة بسلطة التحقيق في الجرائم الإلكترونية، والتي تتمتع بخصائص تميزها عن الجرائم التقليدية. كما يلي:

أولاً: الضبطية القضائية كهيئة مختصة بمباشرة التحريات الإلكترونية: يلجأ المشرع الجزائري إلى تخصيص ضبطية قضائية مختصة بالتحري والتحقق في الجرائم الإلكترونية، لكونها جرائم معقدة وصعبة الإثبات، حيث يكون عمل هذه الضبطية بعد وقوع الجريمة⁵⁸، أي أن هذه الضبطية لا عمل لها إلا بعد وقوع الجريمة، على عكس الضبطية الإدارية والتي تكمن مهمتها في منع وقوع الجريمة⁵⁹. وقد قسم المشرع الجزائري الضبطية القضائية إلى:

أ- مباشرة التحريات الإلكترونية على مستوى جهاز الشرطة: أنشأت المديرية العامة للأمن مخبر مركزي بمركز الشرطة شاطوناف بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة وهران، وتحتوي على فروع تقنية من بينها خلية الاعلام الآلي وفرق متخصصة مهمتها التحقيق والكشف على جرائم الانترنت⁶⁰. بالإضافة إلى إنشاء ثلاثة مخبر جديدة قيد الإنجاز في مدن بشار، ورقلة، وتمنراست بهدف توسيع نطاق هذا الفرع ليغطي كافة أنحاء الوطن، يوجد أيضا مخبر متخصص يحمل اسم الأدلة الرقمية والآثار التكنولوجية والذي يندرج ضمن مخبر الشرطة العلمية. هذا المخبر يُركز على خدمة ثلاث ولايات رئيسية هي الجزائر، وهران، وقسنطينة، ويُعتبر مركزا متقدما لدعم العمليات المتعلقة بالأمن الرقمي. يتخصص المخبر في التحقيق بالجرائم الإلكترونية عبر جمع وتحليل الأدلة الرقمية لتحديد التهديدات التقنية ومكافحتها. ويتم تنظيم المهام في المخبر ضمن ثلاثة أقسام رئيسية:

- قسم يتولى استغلال البيانات الرقمية الناتجة عن الحواسيب والشبكات.
- قسم آخر متخصص في تحليل الأدلة المستمدة من الأجهزة المحمولة.
- قسم معني بتحليل الأصوات باستخدام تقنية متطورة للكشف عن الجرائم الإلكترونية.

58- حازم حسن الجمل، الحماية الجنائية الامن الالكتروني، دار الفكر والقانون، القاهرة-مصر، 2015، ص62.

59- المرجع نفسه، ص63.

60 - عبد القادر فلاح، نادية آيت عبد المالك، "التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الاستاذ الباحث

للدراستات القانونية والسياسية، جامعة محمد بوضياف-المسيلة، الجزائر، المجلد 04، العدد 02، 2019، ص 1695.

إن تحقيق النجاح في عمليات الضبطية القضائية يعتمد إلى حد كبير على التنسيق الوثيق بين جهاز الشرطة والسلطات القضائية، مع أهمية توفير تدريب مناسب لعناصر الشرطة في مجال مكافحة الجرائم الإلكترونية، بالإضافة إلى اعتماد أحدث التقنيات لضمان دقة جمع وتحليل الأدلة الرقمية.

تشير الضبطية القضائية إلى الإجراءات التي تتخذها الشرطة في الجرائم للتصدي للجرائم المعلوماتية. كما توجد فرق متخصصة على مستوى أمن الولايات تابعة لمصالح الشرطة القضائية، تضم خبراء تقنيين متخصصين في مجالات الحوسبة، أمن المعلومات، التحقيق الرقمي، وغيرها من المجالات ذات الصلة⁶¹.

ب-مباشرة التحريات الإلكترونية على مستوى جهاز الدرك الوطني: يعد الدرك الوطني من الأجهزة التي تعمل على مكافحة الجريمة الإلكترونية، وذلك بواسطة المعهد الوطني للأدلة الجنائية وعلم الجرائم الكائن مقره ببوشاوي، وهو تابع لقيادة الدرك العامة، قسم الاعلام ولإلكترونيك الذي يختص بالتحقيق والكشف عن الجرائم الإلكترونية.

يعد هذا المعهد مؤسسة عامة ذات طابع إداري، تأسس بموجب المرسوم الرئاسي رقم 183-04 بتاريخ 26 جوان 2004. كما يُعتبر المعهد أداة مستوحاة من الخبرات التطبيقية والتحليل الحديثة المدعومة بالتكنولوجيا المتقدمة، حيث يساهم في توجيه التحقيقات وكشف الحقائق بالاعتماد على الأدلة العلمية والتحليلية. كما يوفر دعماً تقنياً للوحدات القضائية والشرطة، مما يعزز من كفاءة ودقة سير عملية تحقيق العدالة.

تتم إجراءات الضبطية القضائية تحت إشراف وكيل الجمهورية المختص، الذي يُعد ممثل النيابة العامة لدى المحكمة. يُشرف الوكيل على سير التحقيقات الجنائية ويتخذ القرارات القانونية المناسبة بناءً على الأدلة المتوفرة. كما أنه المسؤول عن منح الصلاحية لمصالح الأمن لتولي التحقيقات المباشرة⁶².

من ناحية أخرى، يمتلك الدرك الوطني وحدات متخصصة ضمن القيادة العامة تنفذ مهامها وتُجري التحقيقات اللازمة في مختلف المجالات، بما في ذلك الجرائم الإلكترونية. وتنقسم هذه الوحدات إلى:

-المصالح المركزية للتحريات الجنائي.

-المصالح والمراكز العلمية والتقنية.

-هياكل التكوين.

61 - المرجع نفسه، ص 1696.

62-المرجع نفسه.

-المعهد الوطني لعلم الاجرام.

ثانيا: صلاحيات الضبطية القضائية كهيئة مختصة بمباشرة التحريات الالكترونية: إن الاختصاص النوعي في النظام القضائي يعني تحديد نوع معين من الجرائم التي يتم التحقيق فيها من قبل أعضاء الضبطية القضائية، مثل الجرائم الالكترونية ويساعد هذا الاختصاص على تركيز الجهود والموارد القضائية في مجال المعلوماتي⁶³.

نستنتج من ذلك أن النظام القضائي يعتمد على تخصيص أجهزة متخصصة لكل نوع من التحقيقات، بهدف ضمان الوصول إلى نتائج دقيقة وسريعة، مع تفادي أي تدخل أو خلط بين القضايا. بالإضافة إلى ذلك، هناك ما يعرف بالاختصاص الإقليمي الذي يباشر فيه ضابط الشرطة القضائية مهامه المتعلقة بالتحري والتحقيق في الجرائم الإلكترونية. وتتمثل صلاحية الضبطية القضائية في⁶⁴:

-مراقبة الانترنت ووسائل التواصل الاجتماعي: تملك الضبطية القضائية صلاحية مراقبة الانترنت للبحث عن أنشطة غير قانونية وغير مشروعة التي تهدد سلامة أمن الوطن.

-تتبع الجرائم الالكترونية: كما لها صلاحية التعاون مع وكالات أمنية دولية لتتبع الجرائم الالكترونية التي تتجاوز الحدود الوطنية.

-إصدار أوامر الاعتقال وتقديم الدعم الفني للتحقيقات: يمكن أن تقوم الشرطة أو الدرك الوطني بالتحقيق الالكتروني وجمع الأدلة الرقمية وتحليلها إلى جانب إصدار أوامر الاعتقال وذلك تحت إشراف وكيل جمهورية مختص.

-التعاون مع مزودي الخدمات الالكترونية: تتعاون الضبطية القضائية مع شركات تقنية والمعلوماتية للحصول على معلومات تساعد على حل القضايا.

-حظر الوصول: يمكن للشرطة الالكترونية منع الوصول إلى مواقع غير مشروعة.

-اعتراض المراسلات وتسجيل الاصوات والتقاط الصور: لقد نصت المواد 114 إلى 119 قانون الإجراءات الجزائية لسنة 2025، بالسماح للضبطية القضائية اللجوء إلى اعتراض المراسلات وتسجيل الاصوات والتقاط الصور في الجرائم المعلوماتية بشرط الحصول على إذن وكيل الجمهورية المختص، أو قاضي التحقيق.

-عملية التصدي للجريمة الالكترونية: يقوم جهاز الدرك الوطني بالتصدي للجرائم باستخدام التقنيات الرقمية الحديثة كما له صلاحية تقديم الدعم للمؤسسات الحكومية لتعزيز أمن أنظمتها

⁶³-طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية-مصر، دون سنة نشر، ص343.

⁶⁴ - فائق نور الايمان بن عمار، التحري والتحقيق في الجرائم الالكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس-مستغانم، الجزائر، 2024/2023، ص 27.

الالكترونية وحماية بياناتها، كما يعمل أيضا على تقوية التعاون لدولي في مجال مكافحة الجرائم الالكترونية.

الفرع الثاني: الهيئة غير القضائية للتحقيق في الجريمة الالكترونية

بعد التطرق إلى الجهات القضائية والأجهزة المعنية بمكافحة الجرائم الإلكترونية، سنتناول في هذا الفرع الهيئات غير القضائية المكلفة بالتحقيق في الجرائم المعلوماتية. من بين هذه الهيئات تبرز الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، والتي تضطلع بدور حيوي في التحري عن هذا النوع من الجرائم.

أولاً: مفهوم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: لقد هذا المشرع الجزائري حذو باقي التشريعات المقارنة وقام بالبحث عن هيئات متخصصة تقوم بمساعدة الدولة وتنتهج منهج وقائي، وقد لجأ المشرع إلى فكرة السلطة الإدارية⁶⁵، حيث أنشئت الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال بموجب نص المادة 13 من القانون رقم 04-09 المؤرخ في 05 أوت 2009، حيث نصت على: "تنشأ الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم".

صدر التنظيم الذي كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها سنة 2015، الذي جاء فيه تحديد مقر الهيئة بمدينة الجزائر مع إمكانية نقله إلى أي مكان آخر عبر التراب الوطني، وذلك بقرار من وزير الدفاع الوطني، وتتمتع بالشخصية المعنوية والاستقلالية المادية تحت سلطة وزارة الدفاع الوطني⁶⁶.

تأسست هذه الهيئة للعمل على مكافحة الجرائم التي ترتكب باستخدام تكنولوجيا المعلومات والاتصالات، كما تهدف إلى حماية المجتمع من جرائم الانترنت وتعمل أيضا على توعية الناس بأخطار هذه الجرائم وكيفية الوقاية منها.

يلعب مجلس التوجيه دورا محوريا في تقييم حالة التهديد المرتبطة بهذه الجرائم، بهدف تحديد الإجراءات الرقابية الواجب اتخاذها. كما يتولى إعداد تقرير سنوي يعرض نشاطات المجلس والمخرجات المتعلقة بمهامه المنوطة به، حيث يجتمع مجلس التوجيه في السنة مرتين بناء على استدعاء من رئيسه وهذا في دورة عادية، أما دورة غير عادية يمكن اجتماعه بطلب من الرئيس أو أحد أعضائه.

⁶⁵ - سهيلة بوزبرة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية"، المجلة النقدية للقانون والعلوم السياسية، جامعو مولود معمري-تيزي وزو، الجزائر، المجلد 17، العدد 02، 2022، ص502.

⁶⁶ - مرسوم رئاسي رقم 15-261 مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 53، الصادرة بتاريخ 8 أكتوبر 2015.

أما المديرية العامة للهيئة، والتي تتولى السهر على حسن سير الهيئة، وذلك لضمان فعاليات وسلامة عمل الهيئة وتحقيق أهدافها بنجاح، بالإضافة إلى إعداد مشروع الميزانية، تنشيط وتنسيق عمليات الوقاية من الجرائم وإعداد وتنفيذ برنامج عمل الهيئة، وتتولى أيضا كل المهام المتصلة بالإعلام والاتصال ومكافحتها⁶⁷.

يتبين مما سبق، أن الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال تعد مؤسسة عمومية ذات طابع إداري، تتميز بالاستقلالية وتمتلك شخصية معنوية خاصة بها. ومن أبرز النتائج المترتبة على امتلاكها لهذه الشخصية المعنوية ما يلي:
أ-دمة مالية مستقلة: تتمتع الهيئة بقدرة مالية مستقلة باعتبارها شخصية معنوية، ما يمنحها استقلالية فيما يتعلق بإدارتها المالية.

ب-الأهلية القانونية: تُمنح الهيئة أهلية قانونية تمكنها من ممارسة الأنشطة القانونية المرتبطة بمهامها، وذلك ضمن القوانين واللوائح المطبقة وقانونها الأساسي. هذه الأهلية تشمل الحقوق والصلاحيات التي تتيح لها أداء واجباتها على أكمل وجه.

ج-الموطن: مقر الهيئة، الذي تحدده النصوص التشريعية، يقع في مدينة الجزائر، ويعتبر المكان الرسمي الذي تنطلق منه أنشطتها.

د-تحمل المسؤولية عن الأضرار: بحكم تمتعها بالشخصية المعنوية، تتولى الهيئة الوطنية مسؤولية التعويض عن الأضرار التي قد تسببها للغير، سواء كانت تلك الأضرار مادية أو معنوية. تنعكس هذه الخصائص على طبيعة عمل الهيئة ودورها في الوقاية من الجرائم التي تستهدف تكنولوجيا الإعلام والاتصال

ثانيا: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بالإعلام والاتصال: نصت المادة 14 من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها⁶⁸، على أنه تتولى الهيئة مجموعة من المهام نذكر منها:

أ-الوقاية من جرائم الاعلام والاتصال: هي عملية التوعية لمستخدمي التكنولوجيا حول خطورة جرائم الاختراق والتجسس على الاتصالات والرسائل الالكترونية، ويعد هذا أمر بالغ الأهمية في عصرنا الرقمي الحالي. وذلك باتخاذ عدة إجراءات لتحقيق هذه الغاية، مثل توفير موارد تثقيفية عبر الانترنت، وتشجيع المستخدمين على تحديث أنظمة التشغيل والتطبيقات الخاصة بهم بانتظام، وغيرها من الإجراءات⁶⁹.

67 - أنظر المادتين 9 و10 من المرسوم الرئاسي رقم 19-172 مؤرخ في 06 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 37، الصادرة بتاريخ 9 جوان 2019.

68 - أنظر نص المادة 14 من القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ب-مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال: تتمثل طرق مكافحة الجريمة الالكترونية فيما يلي:

1-مساعدة السلطات القضائية الداخلية: من مهام الهيئة مساعدة السلطات القضائية ومصالح الشرطة في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الاعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، وعليه تتدخل الهيئة بطلب من الجهات القضائية المختصة، ولقد سحب المشرع الجزائري بموجب المرسوم الرئاسي رقم 19-172، اختصاص المراقبة الالكترونية من جميع الهيئات الأخرى وخوله لهذه الهيئة بصفتها مساعد للجهة القضائية⁷⁰.

2-تعزيز وتنسيق جهود الوقاية من الجرائم المرتبطة بتكنولوجيا الاعلام والاتصال: يتطلب هذا الأمر تضافر الجهود بين جهات متعددة لمواجهة الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات. وتتولى الهيئة القيام بدور محوري في هذا المجال من خلال تعزيز الوعي العام وتوفير الحماية ضد الجرائم الإلكترونية. كما يشمل دورها تقديم الدعم اللازم لمصالح الأمن والدرك الوطني، وكذلك لجميع الإدارات المركزية للدولة، وذلك عبر تبادل المعلومات والموارد والتعاون في التحقيقات والعمليات الأمنية ذات الصلة.

3-دعم السلطات القضائية الأجنبية: وفقا للفصل السادس من القانون رقم 09-04 السالف الذكر، وتحت عنوان التعاون والمساعدة القضائية الدولية، يمكن الاستفادة من إجراءات التعاون الدولي من خلال تبادل المعلومات وطلب تدابير تحفظية، وهو ما يعكس أهمية التعاون العابر للحدود في مواجهة الجرائم الإلكترونية وتعزيز العدالة على نطاق عالمي.

4-تبادل المعلومات: نصت المادة 17 من القانون رقم 09-04 السالف الذكر، على أنه: "تتم استجابة طلبات المساعدة الرامية لتبادل المعلومات أو إتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل". يشمل هذا تقديم المعلومات والوثائق التي تطلبها السلطة القضائية الجزائرية، أو تلك التي تطلبها دولة أجنبية من الجزائر بشأن جريمة، كما أنها تساعد أيضا على تعرف الجهات القضائية على الماضي الجزائري (صحيفة السوابق القضائية) لشخص المتهم، ويتضح ذلك بواسطة اتفاقات تبادل المعلومات بين الدولتين الطالبة والمطلوب منها⁷¹.

⁶⁹ بن عنصر سهام، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص: قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري - تيزي وزو، الجزائر، 2015، ص 51.

⁷⁰ - أمال حابت، "دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال"، مجلة الدراسات الحقوقية، كلية الحقوق والعلوم السياسية، جامعة سعيدة الجزائر، المجلد 6، العدد 1، ص 483-465.

5-طلب الإجراءات التحفظية: هو أحد الإجراءات القضائية المرتبطة بالدعوى الجزائية، يتم التقدم به من الدولة الطالبة إلى الدولة المطلوب منها تنفيذ الإجراء، وذلك وفقاً لما ورد في المادتين 16 و 17 من القانون رقم 04-09 السالف الذكر. يمكن أن تشمل هذه الإجراءات إصدار أوامر مؤقتة من المحكمة مثل منع السفر، تجميد الأموال، وغيرها من التدابير، وفقاً للقوانين الداخلية والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل. كما أن طلبات المساعدة القضائية الدولية لها شروط محددة وفق المادة 18 من ذات القانون، ومن أبرز هذه الشروط:

- إمكانية رفض الطلب إذا ترتب عليه مساس بالسيادة الوطنية أو الإخلال بالنظام العام.
- الامتنال لطلب المساعدة مع ضمان الحفاظ على سرية المعلومات المرسلة وعدم استخدامها في قضايا غير تلك المحددة في الطلب.
- كفالة المراقبة الوقائية للاتصالات الإلكترونية لمكافحة الجرائم المتعلقة بالإرهاب والتخريب وأي تهديد لأمن الدولة.
- دعم تدريب المحققين المختصين في مجالات التحريات التقنية المرتبطة بتكنولوجيا المعلومات والاتصالات .
- تحديث الأطر القانونية في مجال اختصاص التكنولوجيا والإعلام، وهو جزء مهم من عملية تطوير القوانين المنظمة لهذا المجال .
- الملاحظ أنه مما سبق طرحه، أن المشرع الجزائري أغفل الحديث عن دور الهيئة للوقاية من الجرائم المتصلة بالإعلام والاتصال، ومكافحتها في الحالات الاستعجالية والطارئة⁷².

⁷¹ - المرجع نفسه، ص 47.

⁷² - المرجع نفسه، ص 48.

خلاصة الفصل الأول

تطرقنا من خلال هذا الفصل إلى الإطار المفاهيمي والتشريعي للتحريات الإلكترونية بوصفها مستحدثاً إجرائياً فرضته الطفرة الرقمية. واستهلالاً، يُعنى الفصل بضبط الماهية القانونية للجريمة المعلوماتية وتحديد خصائصها الجوهرية العسية على القياس التقليدي، مع استعراض أنماطها المستحدثة وصورها السلوكية المستهدفة للأنظمة المعالجة آلياً للمعطيات.

كما تناولنا من خلال دراسة هذا الفصل، التمييز الإجرائي بين منظومة التحريات الإلكترونية والآليات التقليدية للاستدلال، مع إبراز التمايز في الوسائط المعتمدة والأساليب المنهجية. وانتقالاً إلى الشق التنظيمي، فقد تم التفصيل في المرجعيات القانونية الوطنية والاتفاقيات الدولية الحاكمة لهذه التحريات، مع تبيان الاختصاص النوعي والحصري للجهات الضبطية والقضائية المنوط بها مباشرة هذه الإجراءات، لضمان مواءمتها مع مبدأ الشرعية الإجرائية، وتحقيق الردع الفاعل دون المساس بالحقوق المصونة قانوناً.

الفصل الثاني

آليات التحريات الالكترونية
ودورها في مواجهة الجريمة
المعلوماتية في ظل الذكاء
الاصطناعي

تمهيد

يشهد عالمنا اليوم ثورة هائلة في مجال الرقمنة والتكنولوجيا، حيث أصبحت هذه التحولات جزءاً لا يتجزأ من حياتنا اليومية. لقد ساهمت التكنولوجيا في توفير خدمات متعددة تسهل علينا أداء أعمالنا وتلبية احتياجاتنا اليومية، كما فتحت لنا آفاقاً واسعة لتطوير مهاراتنا وتعزيز قدراتنا. ومع ذلك، فإن هذا الانفتاح على التكنولوجيا، وخصوصاً الإنترنت⁷³، دفع السلطات القانونية والتنظيمية إلى وضع استراتيجيات مبتكرة لمكافحة هذه الظاهرة، حيث يلعب التحقيق في الجرائم الإلكترونية دوراً محورياً يتمثل في جمع الأدلة الرقمية وتحليل البيانات الإلكترونية لتحديد الجناة.

في هذا السياق نوضح أساليب ووسائل توثيق الجرائم وتحديد الأدوات المستخدمة فيها وترتكز عمليات التحقيق على تقنيات وأدوات متقدمة لتحليل البيانات واستخلاص الأدلة التي تساهم في الكشف عن مرتكبي هذه الجرائم ووضع حد لها، وذلك بإمكانية الاعتماد على الذكاء الاصطناعي مع ضرورة الحفاظ على مشروعية الإجراءات.

- المبحث الأول: وسائل وأساليب التحريات الإلكترونية

- المبحث الثاني: التحديات القانونية والعملية للتحريات الإلكترونية

⁷³ - سبق وأن تناولنا هذه النقطة من خلال الفصل الأول من مذكرتنا، حيث ناقشنا كيف أدى هذا التطور التكنولوجي إلى ظهور نوع جديد من الجرائم يعرف بالجريمة الإلكترونية. كما قدمنا تعريفات لمفهوم الجرائم الإلكترونية وكيفية التعامل معها.

المبحث الأول: وسائل وأساليب التحريات الإلكترونية

إن التطور التكنولوجي وخصائص أنظمة المعالجة الآلية، سيؤديان بلا شك إلى تغيير العديد من المفاهيم المرتبطة بإجراءات وأساليب الحصول على الأدلة الرقمية. هذا يستدعي بالضرورة إعادة النظر في بعض الأساليب التقليدية والعمل على إدخال تعديلات على القواعد الإجرائية في قانون الإجراءات الجزائية، بما يتناسب مع طبيعة البيئة التقنية الحديثة. وهذا ما سنوضحه من خلال هذا المبحث.

المطلب الأول: المراقبة الإلكترونية وتتبع الاتصالات

تعتبر المراقبة الإلكترونية وتتبع الاتصالات من أحدث وأدق الوسائل المستخدمة في مجال التحري الرقمي، وذلك بسبب طبيعتها القانونية المزدوجة. فهي من ناحية أداة تقنية لا غنى عنها للكشف عن الأدلة الرقمية المخفية وتعقب المجرمين في العالم الافتراضي، ومن ناحية أخرى، تنطوي على انتهاك مباشر للحق في الخصوصية وحماية سرية المراسلات التي يضمنها الدستور. بناءً على هذا التوازن المعقد بين الكفاءة العملية والحفاظ على الحقوق القانونية، يركز هذا المطلب على مناقشة الأحكام المنظمة لإجراءات المراقبة الإلكترونية، مع تسليط الضوء على الآليات القانونية والتقنية المستخدمة في عمليات تتبع الاتصالات واعتراضها.

الفرع الأول: المراقبة الإلكترونية

تُعد المراقبة الإلكترونية واحدة من أبرز وسائل التحري الحديثة التي تبنتها التشريعات المعاصرة بهدف الكشف عن الأدلة الرقمية غير الظاهرة. وعليه، نخصص هذا الفرع لبحث المفهوم القانوني للمراقبة الإلكترونية، مع التركيز على الشروط والضوابط الإجرائية التي تنظم تطبيقها ضمن البيئة الرقمية.

أولاً: تعريف المراقبة الإلكترونية: نصت المادة 20 من الاتفاقية المتعلقة بمكافحة الجريمة المنظمة عبر الحدود الوطنية، والتي سنتها منظمة الأمم المتحدة في إطار مكافحة الجريمة المنظمة على أنه: "تقوم كل دولة طرف، ضمن حدود إمكانياتها ووفقاً للشروط المنصوص عليها في قانونها الداخلي، إذا كانت المبادئ الأساسية لنظامها القانوني الداخلي تسمح بذلك، باتخاذ ما يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب، وكذلك ما تراه مناسباً لاستخدام أساليب تحري خاصة أخرى مثل المراقبة الإلكترونية، أو غيرها من أشكال المراقبة"⁷⁴. ونجد في نص هذه المادة دعوة لاعتماد أسلوب المراقبة ضمن ما يسمح به القانون من أجل الحد من الجرائم.

74 - عبد الحليم بن بادة، "المراقبة الإلكترونية بين الحق في الخصوصية ومشروعية الدليل الإلكتروني"، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمن ميرة-بجاية، الجزائر، المجلد 10، العدد 3، 2019، ص 390.

تبنى المشرع الجزائري مصطلح "المراقبة الإلكترونية" من هذه المادة، ولم يضبط تعريفا له، لا في مواد قانون الإجراءات الجزائية، ولا في مواد القانون 09-04، وترك ذلك للفقه. وقد عُرِّفت، على أنها: "عملية مراقبة سرية للمراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو المشاركين في ارتكاب الجريمة"⁷⁵.

استنادا إلى هذا التعريف، يمكن اعتبار المراقبة الإلكترونية وسيلة لتتبع بيانات محددة بهدف الوصول إلى الحقيقة واكتشاف أدلة تسهم في حل قضايا معينة.

نجد تعريفا آخر للمراقبة الإلكترونية جاء فيه، أنها: "إجراء تحقيق خلسة ينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا، بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها، ويتضمن من ناحية استراق السمع، ومن ناحية أخرى الحفاظ على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض". أي أن المراقبة الإلكترونية هي تعد على خصوصيات الفرد، والاستماع إلى محادثاته الخاصة بأمر من السلطات المختصة، من أجل بلوغ الحقيقة وكشف ملبسات الجريمة الواقعة⁷⁶.

يمكننا استنتاج من التعريفات السابقة، أن المراقبة الإلكترونية تمثل عملية توظيف التقنيات الحديثة للرصد والتسجيل الإلكتروني بهدف جمع المعلومات والأدلة المرتبطة بجريمة معينة.

ثانيا: خصائص إجراء المراقبة الإلكترونية: تتمثل أساسا فيما يلي:

أ- **سرية إجراء المراقبة الإلكترونية:** تهدف إلى تحقيق نتائج دقيقة وفعالة مع الحفاظ على الهدف المنشود، إضافة إلى ضمان حماية خصوصية المحادثات والاتصالات. كما تسعى إلى تعزيز تنفيذ القانون بشكل صحيح وتوفير الحماية اللازمة للأفراد. ولضمان تحقيق هذا التوازن، تم تحديد جملة من الشروط التي تشمل: الحصول على إذن قانوني للقيام بالمراقبة، والتصريح بهوية الشخص الذي يتم مراقبته.

ب- **الاعتماد على أجهزة خاصة في إجراء المراقبة الإلكترونية:** لقد كان للتطور الذي شهده عالم التكنولوجيا والمعلوماتية، أثر كبير في تسهيل عملية المراقبة الإلكترونية، حيث أدى إلى ظهور أجهزة ومعدات مراقبة إلكترونية حديثة ومتطورة تساهم بشكل كبير في تسهيل عملية مراقبة الاتصالات، حيث لا يمكن أن تكون مراقبة من دون هذه الأجهزة المتخصصة⁷⁷.

ج- **هدف المراقبة الإلكترونية هو الحصول على دليل غير مادي:** إن الهدف الرئيسي للمحققين الجنائيين الذين يتخذون هذا الإجراء هو الحصول على أدلة من شأنها أن تسهم في كشف غموض

⁷⁵ - رشيدة بوبكر، المرجع السابق، ص 44.

⁷⁶ - عبد الحليم بن بادة، المرجع السابق، ص 391.

⁷⁷ - كريم معروف، سعاد بن حليمة، "الإجراءات المستحدثة في البحث والتحقيق للكشف عن الجرائم التي ترتكب في الفضاء الإلكتروني"، مجلة الدراسات الاستراتيجية والعسكرية، المركز العربي الديمقراطي، برلين، ألمانيا، العدد 13، ديسمبر 2021، ص 7.

الجريمة الالكترونية، وتأكيد الأدلة التي يتم الحصول عليها من خلال التحقيقات والتحريات، وبالتالي ضمان إسناد الجرائم المرتكبة في الفضاء الافتراضي إلى مرتكبيها⁷⁸.

د-مساس إجراء المراقبة الالكترونية بحق الشخص في سرية المراسلات والاتصالات الالكترونية: إن عملية المراقبة والتنصت على الاتصالات تؤدي بالضرورة إلى انتهاك حق الشخص في حماية خصوصياتها، لكنها من جهة أخرى تمكن المحققين من معرفة أفكار المشتبه به ونواياه والتعرف على مشاعره مما يمكنهم من معرفة الحقيقة والوصول إليها⁷⁹.

ثالثا: شروط إجراء المراقبة الالكترونية: تتمثل شروط إجراء المراقبة الإلكترونية فيما يلي:

أ-يجب أن يتضمن تصريح المراقبة المحادثات أو الاتصالات التي ستتم مراقبتها، وهوية الشخص الذي تتم مراقبته، ولكي تكون المراقبة الإلكترونية قانونية، يجب أن تكون بتصريح مكتوب من طرف السلطة القضائية.

ب-يجب تحديد ساعات المراقبة، وذلك لأن تمديد مدة المراقبة يشكل إفشاء لأسرار المواطنين دون مبرر، وقد حدد المشرع الجزائري مدة المراقبة القابلة للتجديد بستة أشهر في نص المادة 4 من القانون 04-09 السالف الذكر.

ج-يجب على مشغلي المراقبة أن يسجلوا فقط ما هو مصرح به من قبل سلطة المراقبة، ويحظر عليهم تسجيل ومراقبة أي شيء يتجاوز ذلك.

د-يجب أن تكون الأشرطة المسجلة عند تنفيذ أوامر المراقبة مختومة، لمنع التلاعب أو التغيير.

ه-يجب أن تتم عملية المراقبة بشكل شفاف ونزيه، كما يتعين على جهات التحقيق تقديم معلومات كافية حول أسباب وأساليب المراقبة المستخدمة.

و-يجب أن يكون طرفي المراقبة هما: المراقب الإلكتروني والمتمثل في المحقق الجنائي وقاض التحقيق أو ضابط الشرطة القضائية، أو أي جهاز مكلف بالتحقيق والتحري في الجرائم الالكترونية، والطرف الثاني هو المراقب ويتمثل في المشتبه به⁸⁰.

رابعا: حالات اللجوء إلى إجراء المراقبة الالكترونية: نصت المادة 4 من القانون رقم 09-04 السالف الذكر، على الحالات التي يتم فيها اللجوء إلى المراقبة الإلكترونية، وتمثلت فيما يأتي:

⁷⁸- عبد الحليم بن بادة، المرجع السابق، ص 394.

⁷⁹- كريم معروف، سعاد بن حليمة، المرجع السابق، ص 6.

⁸⁰- المرجع نفسه، ص 8.

-في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب، أو الجرائم التي تمس بأمن الدولة.

-في حال توفر معلومات عن احتمال وقوع اعتداء على المنظومة المعلوماتية التي تهدد الدفاع الوطني، أو مؤسسات الدولة، أو الاقتصاد الوطني.

-أن تكون المراقبة الإلكترونية من مقتضيات التحري والتحقيق الجنائي، بحيث يستحيل الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إليها.

-في حالة تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما نصت الفقرة 05 من المادة 04 من القانون 04-09، على أنه: "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة...". أي أنه لا يحق إجراء المراقبة ما لم يكن هناك تصريح مكتوب من قبل السلطات المعنية.

الفرع الثاني: تتبع الاتصالات

يعد تتبع الاتصالات من أدق آليات التحري التقني التي تتيح لجهات التحقيق اقتفاء الأثر الرقمي للجريمة وضبط أدلتها. وتأسيساً على ذلك، نخصص هذا الفرع لبيان الأحكام القانونية والشروط الإجرائية التي وضعها المشرع لضبط هذا الإجراء وحماية حرمة الحياة الخاصة

أولاً: الاعتراض والالتقاط الإلكتروني: الاعتراض والتسجيل والالتقاط والتسريب، هي مصطلحات متنوعة يمكن تلخيصها في مفهوم واحد وهو المراقبة. هذا المصطلح يشير ببساطة إلى المراقبة القانونية لشخص، أو مكان، أو محادثة، أو وثيقة، أو وسيلة اتصال صوتية أو مرئية نتيجة الاشتباه في القيام بنشاط غير قانوني.

وقد اختلفت الآراء الفقهية حول طبيعة هذا الإجراء. فمن جهة، يرى البعض أنه يدخل ضمن إطار التفتيش ويخضع لضوابط وشروط إجراءات التفتيش. بينما يرى آخرون أنه يُعتبر جزءاً من إجراءات المراقبة وله قواعده الخاصة.

نظم المشرع الجزائري ضمن قانون الإجراءات الجزائية لسنة 2025، في الباب الثاني "في التحقيقات"، في الفصل الرابع منه اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وذلك ضمن المواد من 114 إلى 119. كما يلي:

أ-اعتراض المراسلات: الاعتراض يعني الاستلاء، ولا يتأتى ذلك إلا عن طريق المواصلات السلكية واللاسلكية، دون الرسائل والخطابات والمطبوعات والطرود، لدى مكاتب البريد، ونظراً للتطور الذي عرفه مجال الاتصال فإن المشرع لم يقصر الاعتراض على المكالمات الهاتفية، بل وسعه لمختلف أنواع الاتصال السلكية واللاسلكية.

ب-تسجيل الأصوات والتقاط الصور: ونميز بين:

1-تسجيل الأصوات: يُعتبر تسجيل الأصوات توثيقاً مهماً في العديد من السياقات القانونية، وهي عبارة عن عملية تسجيل المحادثات التي تجري بين المتهمين، ورغم أن المشرع الجزائري أعطى للمتهم الحق في الصمت⁸¹، إلا أنه بطريقة غير مباشرة أورد استثناءاً عن هذا الحق في المطة الثانية من المادة 114 من قانون الإجراءات الجزائية، أين أصبح من الممكن أخذ اعتراف الشخص ضد نفسه بشكل خفي دون رضاه وموافقته، عن طريق تسجيل كل ما يتفوه به من كلام بصفة خاصة أو سرية.

والجدير بالذكر، أن التشريعات اختلفت في المعيار الذي يجعلنا نميز بين ما يعد حديثاً خاصاً، وما هو حديث عام، فهناك من أخذ بطبيعة المكان الذي يدور فيه الحديث، والبعض الآخر اعتمد على طبيعة الحديث ذاته⁸². غير أن المشرع الجزائري قد عبر عن موقفه بوضوح من خلال المطة الثانية من المادة 114 من قانون الإجراءات الجزائية، حيث ركز على مسألة المكان سواء كان عاماً أو خاصاً، مع التشديد على ضرورة أن يكون الحديث سرىاً وخاصاً.

2-التقاط الصور: يُعرف التقاط الصور، بأنه: "حفظ الصورة على مادة معينة موجودة داخل أجهزة أو آلة التصوير، ليتم رؤيتها فيما بعد، بهدف التحقيق في جريمة أو أمر ما يتعلق بها"⁸³، تعد عملية التصوير وحفظ الصور أداة تهدف إلى كشف الحقائق، مع الالتزام بالضوابط القانونية التي تحكمها.

الجدير بالذكر أن المشرع الجزائري لم يقتصر على منح قاضي التحقيق صلاحية تسجيل الأصوات فقط، بل وسع صلاحياته لتشمل أيضاً إمكانية التقاط الصور، من خلال المطة الثانية من نص المادة 114 من قانون الإجراءات الجزائية.

ثانياً: الشروط الموضوعية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور: تتمثل فيما يلي:

أ-السلطة المختصة بإجراء هذه العمليات: من الطبيعي أن تكون هذه العمليات حصرية بجهاز معين في الدولة، وذلك للحفاظ على حق الفرد في حماية خصوصيته، ولهذا كان أمر اعتراض المراسلات وتسجيلها والتقاط الصور من اختصاص قاضي التحقيق، والذي وإن كان لا يقوم بالعملية بشكل مباشر-إلا أنها تتم تحت مراقبته، ويقوم بها من يملك الخبرة في التعامل معها⁸⁴.

81 - عمارة فوزي، "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية"، مجلة العلوم الإنسانية، جامعة الإخوة منتوري-قسنطينة¹، الجزائر، العدد 33، 2010، ص 237.

82 - نبيلة قيشاح، "ضمانات المراقبة الإلكترونية في التشريع الجزائري"، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور-خنشلة، الجزائر، المجلد 10، العدد 2، 2022، ص 1098.

83 - المرجع نفسه، ص 1099.

84 - فوزي عمارة، المرجع السابق، ص 238.

يقتصر دور القاضي على ضمان تطبيق القواعد القانونية بشكل صحيح خلال هذه الإجراءات. وبالرجوع إلى القانون رقم 25-14 من قانون الإجراءات الجزائية، نجد أن هذه الإجراءات تنفذ بموجب إذن من وكيل الجمهورية، وذلك أثناء مرحلة التحري بشرط أن تكون من دواعي التحري ضرورة اللجوء إلى هذا الإجراء.

أما بالنسبة للجهة المكلفة بالعملية، تتمثل في ضابط الشرطة القضائية لإنجاز العمليات، أو لقاضي التحقيق، أو ضابط الشرطة القضائية الذي يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلوكية واللاسلكية، لتكفل الجوانب التقنية. وهذا ما جاء ضمن نص المادة 117 من قانون الإجراءات الجزائية.

ب-توقيت ومكان تنفيذ هذه العمليات: لم يُحدد قانون الإجراءات الجزائية الجزائي قواعد دقيقة تتعلق بتوقيت ومكان هذه الإجراءات. فهو يتيح تنفيذها في أي وقت، سواء خلال ساعات النهار أو الليل، وفي أي موقع، سواء كان مكانا خاصا أم عاما.

ج-عدم مسؤولية القائم والمشرف على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: لقد سبق لنا أن ذكرنا أن المشرع الجزائي قد ضمن حق الفرد في حماية خصوصية وسرية اتصالاته، إلا أن ما يتعرض له الشخص من انتهاك لخصوصيته عن طريق تسجيل صوته أو التقاط صورة له خلصة ليلا أو نهارا كإجراء قانوني تفرضه خطورة الموقف، وضرورة من ضرورات التحقيق الجنائي لكشف جريمة ما، فهذا لا يترتب عليه أي مساءلة قانونية ولا يتحمل القائمون بها المسؤولية الجنائية، وذلك تحت مبدأ "الضرورات تبيح المحظورات"⁸⁵.

ثالثا: الشروط الشكلية لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: تتمثل فيما يلي:

أ-صدور إذن مكتوب: إن ضابط الشرطة القضائية لا يمكنه القيام بإجراء الاعتراض إلا بالحصول على إذن من وكيل الجمهورية المختص أو قاضي التحقيق، وذلك طبقا لأحكام المواد 114 إلى 119 من قانون الإجراءات الجزائية.

ب-تحرير محضر الاعتراض: نصت المادة 118 من قانون الإجراءات الجزائية، على أن: "يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري. ويذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاؤها منها". أي أنه يجب أن تكون كل عملية اعتراض أو تسجيل أو تصوير موثقة بمحضر كتابي يتم من خلاله تدوين كافة تفاصيل العملية بشكل دقيق.

ج-تحديد مدة المراقبة: يجب تحديد المدة اللازمة لعملية الاعتراض، والتي حددها المشرع بمدة أقصاها أربعة أشهر قابلة للتجديد، وهذا ما نصت عليه المادة 116 من قانون الإجراءات الجزائية.

يجب أن تُنفذ جميع العمليات السابقة تحت إشراف وكيل الجمهورية أو قاضي التحقيق حسب الحالة، وفي كل الأحوال يجب عدم المساس بالسِر المهني. إذا تم اكتشاف جرائم أخرى غير تلك المذكورة في إذن القاضي، فإن ذلك لا يشكل سببا لإبطال الإجراءات المؤقتة.

المطلب الثاني: التفتيش الإلكتروني وضبط الأدلة الرقمية

ساهم التطور التكنولوجي والانتشار الواسع للوسائل الرقمية في ظهور أنواع جديدة من الجرائم، الأمر الذي فرض الحاجة إلى تبني أساليب مبتكرة للتحري، من بينها التفتيش الإلكتروني. فلم يعد هذا النوع من التفتيش يقتصر على المواقع والأماكن المادية، بل تجاوزها ليُطال الأنظمة المعلوماتية مثل الأجهزة الحاسوبية والهواتف المحمولة، بهدف العثور على الأدلة الرقمية. وبالنظر إلى الطبيعة الخاصة لهذه الأدلة الرقمية، التي تتسم بسهولة التلاعب بها وسرعة اختفائها، بات من الضروري التعامل معها وفق إجراءات دقيقة تكفل الحفاظ على سلامتها وتضمن حجيتها القانونية أمام القضاء، مع الحرص التام على احترام الحقوق والحريات الفردية.

الفرع الأول: تعريف التفتيش الإلكتروني وأهم وسائله

يُعتبر التفتيش أحد أبرز أدوات البحث والتحري التي تهدف إلى الكشف عن الحقيقة وجمع الأدلة. ومع التطور التقني، امتد نطاق التفتيش ليشمل الوسائل الحديثة، لا سيما في المجال الإلكتروني، مما تطلب تنويع أساليبه بما يتناسب مع طبيعة الجرائم الحديثة.

أولاً: تعريف التفتيش الإلكتروني: يُعد التفتيش الإلكتروني أحد الإجراءات القانونية التي تناولها المشرع الجزائري ضمن نصوص القانون 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها، فالهدف من سنّ هذا القانون هو وضع ضوابط وإجراءات تتلاءم مع الطبيعة الخاصة للجريمة المعلوماتية، مما يتطلب تسليط الضوء على التفتيش في البيئة الرقمية، مع الإشارة إلى مفهومه وأصوله من خلال استقراء التعريفات الفقهية والممارسات القضائية.

يُعرف التفتيش بوجه عام، على أنه: "عملية البحث عن أدلة مادية قد تقود إلى كشف حقيقة جريمة وقعت وربطها بأشخاص معينين، ويتم ذلك وفق إجراءات قانونية صارمة"⁸⁶.

⁸⁶ - علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، مصر، 2012، ص39.

بالرجوع إلى التعاريف الفقهية، نجد تنوعاً في صياغات مفهوم التفتيش الإلكتروني بحسب أبعاده المختلفة وتعدد مجالاته، فضلاً عن اختلاف الجرائم المرتبطة به وأحكام التعامل معها. وقد تم تعريف التفتيش الإلكتروني من قبل بعض الفقهاء، على أنه: "الاطلاع على محتويات أو أماكن يعتبرها القانون مستودعات سرية لأصحابها، سواء كانت عبارة عن أجهزة حاسوب، أنظمة معلوماتية، أو شبكات الإنترنت"⁸⁷.

إن التفتيش كإجراء من إجراءات التحقيق يقتضي صدور إذن قانوني من الجهات المختصة، مثل القضاء، ليتم تنفيذه من قبل ضباط الشرطة القضائية. ويُنظر له كإجراء مفاجئ، يُنفذ دون إخطار مسبق للمتهم بغرض منع أي محاولة لإخفاء الأدلة المرتبطة بالجريمة قيد التحقيق⁸⁸.

ثانياً: وسائل التفتيش الإلكتروني: تتمثل هذه الوسائل أساساً، فيما يلي:

أ- برنامج مالتيجو " Maltego " المستخدم أثناء المعاينة والتفتيش: يُعتبر هذا البرنامج واحداً من أبرز وأقوى الأدوات المخصصة لجمع المعلومات عن الأهداف التي يتطلع إليها الباحث إلى الحصول على بيانات بشأنها. يتميز البرنامج بفعالته العالية في تجميع المعلومات المتعلقة بالأفراد أو مجموعات، مع تقديم رؤية واضحة للروابط والتفاعلات بينهم، وذلك من خلال الاعتماد على مصادر متنوعة، مثل: البريد الإلكتروني، الشبكات الاجتماعية، المواقع الإلكترونية، أرقام الهواتف، وغيرها من البيانات ذات الصلة.

تُعد هذه الأداة نظاماً تفاعلياً متقدماً لاستنباط وتحليل البيانات، حيث توفر رسوماً بيانية مفصلة تُبرز تسلسل وترابط العلاقات بين مختلف العناصر والمعلومات. حيث يُساعد هذا النهج في الكشف عن الروابط المشتركة بين مجموعات متنوعة من البيانات التي يتم استرجاعها عبر الإنترنت. بالإضافة إلى ذلك، تُستخدم الأداة بشكل واسع في مجالات التحقيق الرقمي لتحليل العلاقات بين أجزاء متفرقة من المعلومات المستمدة من مصادر متعددة ومتفرقة في الشبكة العنكبوتية.

ب- برنامج "Forensic" المستخدم أثناء عمليات المعاينة والتفتيش: يُركز في جوهره على مكافحة الجرائم بمختلف أنواعها، والتي تتنوع بين جرائم القتل والسرقة والجنايات. وقد تم تخصيص قسم خاص بالجرائم الإلكترونية، ويُعرف بـ "Forensic Digital"، هذا القسم يُعنى بتتبع وتوثيق الأنشطة غير القانونية التي تحدث عبر الإنترنت أو باستخدام الأجهزة الإلكترونية، حيث يعمل فريق مختص من خبراء تقنية المعلومات على إدارة ومراقبة النظام لضمان كشف وحظر هذه الأنشطة غير المشروعة. هؤلاء الخبراء يمتلكون خبرة عالية تمكنهم من التصدي لأي تهديدات رقمية.

87 - المرجع نفسه، ص 39.

88 - هلالى عبد الله أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط1، دار النهضة العربية، القاهرة-مصر، 2012، ص46.

يعمل البرنامج على تصوير القرائن وجمع الأدلة باستخدام حزم برمجية متطورة صُممت خصيصا للمحققين الجنائيين، تلك البرامج تحتوي على أدوات قوية تمكنهم من تطوير ملفات متكاملة تحتوي على بيانات جاهزة للتحليل والمراجعة. كما يتضمن البرنامج مهام متعددة، مثل: التحري عن الأدلة الرقمية، استنساخها، تحليلها، فك التشفير، استعادة الملفات المحذوفة وكلمات المرور، وتحليل البريد الإلكتروني، ويوفر أيضا أدوات بحث متقدمة تساهم في إعداد تقارير دقيقة لعرضها على الجهات المختصة لمعالجة القضايا⁸⁹.

علاوة على ذلك، يعتمد التفتيش الإلكتروني على تقنيات متطورة تناسب طبيعة الجرائم المرتكبة. نذكر منها:

1- تقنية تتبع عنوان IP-TCP: يُعتبر العنوان IP هو العنصر المسؤول عن نقل حزم البيانات عبر شبكة الإنترنت وتوجيهها نحو الوجهة المحددة، إذ يُعد بمثابة هوية الجهاز المتصل بالشبكة. يتألف من أربعة أجزاء رقمية، حيث يمثل الجزء الأول الموقع الجغرافي، والجزء الثاني يشير إلى رمز مزود الخدمة، بينما الجزء الثالث يرمز إلى مجموعة الأجهزة المرتبطة، وأخيرا يُحدد الجزء الرابع الجهاز المعني بالاتصال⁹⁰.

في حال وقوع جريمة إلكترونية، يقوم ضباط الشرطة القضائية بالتركيز على فحص فضاء الاتصالات الإلكترونية، وهو يشمل أي عملية تراسل أو استقبال أو إرسال لإشارات أو نصوص أو صور أو أصوات أو بيانات بأي شكل عبر الوسائل الإلكترونية.

وفي هذا الإطار، تتعاون الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مع السلطات القضائية بموجب نص المادة 04 من المرسوم الرئاسي رقم 15-261⁹¹، حيث تعمل مصالح الشرطة القضائية كجزء من فرق تحقيق تُعنى بتتبع عنوان IP الخاص بالجهاز الذي يُشتبه في كونه مصدر الجريمة، لتحديد موقعه بدقة⁹².

2- تقنية تحليل البروكسي 'Proxy': يُعتبر البروكسي وسيطا بين المستخدم والشبكة، ويُستخدم عادة من قبل مزودي خدمات الاتصالات لإدارة الشبكة وضمان أمنها، بالإضافة إلى تحسين سرعة الوصول للمعلومات بفضل ما يُعرف بـ "ذاكرة التخزين المخبئية (Memory Cache)". فعندما يقدم المستخدم طلبا لزيارة صفحة معينة، يتحقق البروكسي مما إذا كانت هذه

⁸⁹ - إيناس محمد راضي، الأجهزة التحليلية الحديثة في كلية علوم الأدلة الجنائية، تم الإطلاع عليه بتاريخ 2026/03/21، على الساعة 20:00 سا، منشور على الرابط:

http://www.uobabylon.edu.iq/uobColeges/service_showrest.aspx?fid:

⁹⁰ - المرجع نفسه.

⁹¹ -مرسوم رئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 53، الصادرة بتاريخ 8 أكتوبر 2015.

⁹² - عبد الاله بن سعود محمد السراي، فاعلية الأساليب المستخدمة في اثبات جريمة التزوير الإلكتروني، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2011، ص51.

الصفحة مخزنة مسبقا في الذاكرة الجاهزة، وإذا كانت متوفرة يقوم بتقديمها مباشرة دون الحاجة إلى استرجاعها من شبكة الإنترنت. ومن بين ميزات هذا النظام أن الذاكرة المخزنة تحتفظ بسجل البيانات والعمليات السابقة، مما يمكن ضباط الشرطة القضائية بالتعاون مع مزودي الخدمات من الوصول إلى معلومات مفيدة واستخلاص الأدلة التي قد تُستخدم ضد المتهم⁹³.

ج- استعمال برامج التتبع المعلوماتي برنامج "TRACER - HACK": تعمل برامج التتبع على كشف محاولات الاختراق وتحديد هوية المسؤول عنها، بالإضافة إلى تنبيه الجهة المتضررة بشأن ذلك. عادة، تكون هذه البرامج نشطة في الخلفية، حيث ترصد محاولات القرصنة والاختراق فور حدوثها، وتقوم سريعا بإغلاق المنافذ المستخدمة من قبل المخترقين. بعدها تبدأ بملاحقة وتعقب الأثر للوصول إلى معلومات دقيقة مثل عنوان IP الخاص بهم ومزود خدمة الإنترنت، بالإضافة إلى بيانات أخرى ذات صلة. وتتضمن هذه البرامج شاشة رئيسية تعرض للمستخدم تقارير عن عمليات الاختراق، مما يساهم في دعم ضباط الشرطة القضائية للوصول إلى المجرمين المعنيين⁹⁴.

د- الاستعانة بنظام كشف الاختراق "Detection System Intrusion": يُرمز إلى هذا النظام اختصارا بـ I.D.S، وهو نظام يعتمد على مجموعة من البرامج المصممة لمراقبة العمليات الجارية على أجهزة الحاسوب أو الشبكات وتحليلها بهدف الكشف عن أي مؤشرات قد تشير إلى وجود تهديدات تمس أمن النظام أو الشبكة. يتحقق ذلك عبر تحليل حزم البيانات أثناء انتقالها عبر الشبكة، بالإضافة إلى مراقبة ملفات التشغيل المحددة. يُستفاد من هذا النظام أيضا من قبل ضباط الشرطة القضائية لتسجيل الأحداث فور وقوعها ضمن الأجهزة أو الشبكات، مما يساهم في توثيق الوقائع وتعزيز الإجراءات الأمنية⁹⁵.

هـ- العمل بنظام الترميز: هو نظام حاسوبي مصمم خصيصا ليكون هدفا للهجمات الإلكترونية عبر الشبكة، وذلك من خلال إظهار ضعف أو سهولة تخترق ظاهرة بهدف جذب المهاجمين. الغرض الأساسي من هذا النظام هو جمع أكبر قدر ممكن من المعلومات حول أساليب الهجوم المستخدمة وتحليلها بدقة. يتيح ذلك للجهات المختصة في التحري والتحقيق اتخاذ الإجراءات الوقائية اللازمة، فضلا عن تزويد فريق التحقيق بالبيانات المطلوبة والعديد من المعلومات التي تساعد في توضيح معالم الجريمة وفهمها⁹⁶.

الفرع الثاني: الجهات المختصة بإجراء التفتيش الإلكتروني

⁹³ - خالد عياد الحلبي، المرجع السابق، ص 206.

⁹⁴ - أسماء بن بريكة، نور الهدى بن سعيد، التفتيش الإلكتروني، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة عمار تليجي-الأغواط، الجزائر، 2024/2023، ص ص 12-13.

⁹⁵ - خالد عياد الحلبي، المرجع السابق، ص 209.

⁹⁶ - عبد الله بن سعود محمد السراني، المرجع السابق، ص 51.

يتطلب إجراء التفتيش الإلكتروني تدخل جهات مختصة قانوناً، لما له من مساس بالحياة الخاصة، لذلك حدّد المشرّع الجهات المخوّلة للقيام به وفق ضوابط قانونية دقيقة.

أولاً: الاختصاص النوعي للتفتيش الإلكتروني: يُقصد بالاختصاص النوعي للتفتيش تحديد الجهة المخوّلة قانوناً بإجرائه حسب طبيعة الجريمة، وذلك لضمان احترام الإجراءات القانونية وحماية الحقوق والحريات. حيث لا تعتبر إجراءات التفتيش الإلكتروني صحيحة وقانونية، إلا إذا تم تنفيذها من قبل الأشخاص أو الجهات التي يخوّلها القانون صلاحيات القيام بها. وقد اختلفت القوانين والإجراءات في هذا الصدد، حيث أن بعض التشريعات تسند هذه المهمة إلى النيابة العامة وبعضها الآخر إلى قاضي التحقيق أو ضباط الشرطة القضائية. أما بالنسبة للمشرّع الجزائري، فقد أوكل صلاحيات إجراء التفتيش إلى السلطات القضائية المتمثلة في النيابة العامة أو قاضي التحقيق، بالإضافة إلى ضباط الشرطة القضائية، وذلك وفقاً لأحكام نص المادة 75 من قانون الإجراءات الجزائية.

وقد أجاز المشرّع لوكيل الجمهورية وقاضي التحقيق وضباط الشرطة القضائية تسخير خبراء مؤهلين يمتلكون المهارات الفنية الضرورية لمعالجة الجرائم المتعلقة بالمعلوماتية. وبالإضافة إلى ذلك، سمح المشرّع للسلطات المخوّلة بالتفتيش التعاون مع مختصين وخبراء في مجال تقنية المعلومات لتقديم المشورة وتنفيذ إجراءات التفتيش بأساليب تقنية تتماشى مع القوانين الحديثة، بما يتوافق مع مقتضيات نص المادة 75 سالف الذكر⁹⁷.

هذا، ونشير إلى أنه نظراً لخصوصية جرائم تكنولوجيا المعلومات، فإن إجراءات التفتيش الإلكتروني كما هو محدد قانونياً تخضع لقواعد خاصة تختلف عن القواعد العامة المقررة في نصوص المواد 75 وما يليها من قانون الإجراءات الجزائية. حيث يُطبق هذا التباين في الإجراءات وفق حالتين رئيسيتين:

-الحالة الأولى: الجرائم الخاصة: عند التحقيق في جرائم مثل المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم المتعلقة بأنظمة معالجة البيانات، وكذلك تبييض الأموال والإرهاب ومخالفات قانون الصرف، فإن ضابط الشرطة القضائية غير ملزم بحضور المتهم أو شهود عند تنفيذ التفتيش. وفيما يتعلق بتفتيش مساكن المتهمين، يجوز للضابط المختص أن يقوم به خارج الأوقات المحددة في نص المادة 78 من قانون الإجراءات الجزائية، بشرط الحصول على إذن من وكيل الجمهورية وأن يتم التفتيش بحضوره.

-الحالة الثانية: الجرائم المعلوماتية: بالنسبة للتحقيقات المرتبطة بالجرائم المعلوماتية، يتميز الإجراء بمزيد من الضبط والدقة نظراً لارتباطه بتقنيات التكنولوجيا الحديثة. إذ يسمح القانون

97 - زيدان زريحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة-الجزائر، 2011، ص160.

لضباط الشرطة القضائية بإجراء عمليات تفتيش تخص المنازل التي تحتوي على أجهزة حاسب آلي بعد الحصول على موافقة مسبقة من وكيل الجمهورية. ويتم تنفيذ التفتيش بحضور شاهدين غير تابعين للجهاز الأمني أو بحضور ممثل يعينه صاحب المسكن إذا كان قيد التوقيف⁹⁸.

تُنفذ إجراءات التفتيش في مثل هذه الجرائم من قبل ضباط شرطة متخصصين لديهم الخبرة الكافية والحاصلين على إذن رسمي من الجهات القضائية. تتمتع شرطة الإنترنت بصلاحيات البحث والتحقيق باستخدام أدوات وتقنيات متطورة لضمان كشف الجرائم بطريقة قانونية ومنهجية. وتشترط القوانين أن تكون الجهات المنوطة بالتفتيش الإلكتروني مؤهلة ومدرّبة لمواجهة تحديات الجرائم المعلوماتية. لدعم هذه العمليات، قام المشرع الجزائري بتعزيز قدرات الأجهزة الأمنية بأنظمة حديثة لمكافحة الجرائم الإلكترونية. وتتولى "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها" الإشراف على تطوير هذه الأنظمة وتنظيم العمليات الأمنية لمكافحة هذا النوع من الجرائم⁹⁹.

كما توجد وحدات أمنية متخصصة ضمن جهاز الأمن الوطني مسؤولة عن الوقاية والتحقيق في الجرائم المعلوماتية، ومنها:

- المختبر المركزي للشرطة العلمية.

- المختبر الجهوي للشرطة العلمية في قسنطينة.

- المختبر الجهوي للشرطة العلمية في وهران.

ثانياً: الاختصاص الإقليمي للتفتيش الإلكتروني: يُقصد بالاختصاص المكاني للتفتيش تحديد النطاق الجغرافي الذي تمارس فيه الجهة المختصة صلاحياتها، وذلك لضمان صحة الإجراءات واحترام الحدود القانونية لكل سلطة.

إن الاختصاص الإقليمي النطاق الجغرافي الذي يزاوّل ضمنه ضباط الشرطة القضائية صلاحياتهم، حيث يحدد ذلك بالدائرة الإقليمية التي يمارسون فيها مهامهم الوظيفية. وقد قام المشرع الجزائري بتوسيع نطاق اختصاص ضباط الشرطة القضائية ليشمل كافة الإقليم الوطني¹⁰⁰. في هذا السياق، يبقى عمل ضباط الشرطة القضائية تحت إشراف وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك وفقاً لنص المادة 337 من قانون الإجراءات الجزائية.

98 - هروال نبيلة هبة، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، مصر، 2007، ص 100.

99 - سعاد رابح، "ضوابط مكافحة الجريمة المعلوماتية"، مجلة القانون العام الجزائري والمقارن، جامعة الجيلالي اليابس-سيدي بلعباس، الجزائر، المجلد 7، العدد 01، جوان 2021، ص 281.

100 - عبد الله أوهابيه، ضمانات الحرية الشخصية أثناء مرحلة البحث التمهيدي، الاستدلال، ط 1، الديوان الوطني للأشغال التربوية، الجزائر، 2004، ص 300.

تتميز الجرائم المعلوماتية بكونها عابرة للحدود الوطنية، إذ إنها غالباً ما تُرتكب بالتعاون بين أفراد من جنسيات مختلفة ودون التقيد بحدود جغرافية. يتجلى هذا الطابع الدولي في إمكانية ارتكاب الجريمة في دولة معينة وظهور نتائجها في دولة أخرى، مما أثار جدلاً فقهاً حول تحديد الاختصاص القضائي للبت في مثل هذه الجرائم وتنظيم عمليات التفتيش ذات الصلة. يضيف هذا التعقيد تحديات قانونية تتعلق بإمكانية النفاذ إلى البيانات المخزنة عبر أقاليم متعددة، ويستلزم تعاون مزودي خدمات الإنترنت مع السلطات القضائية للوصول إلى المحتويات ذات الصلة¹⁰¹.

أثارت بعض الاتجاهات الفقهية النقاش حول معيار تحديد الاختصاص في الجرائم المعلوماتية. هناك رأي يرى بأن الاختصاص يعود إلى محاكم الدولة التي تم فيها تحميل البيانات والتي تُعتبر دولة المصدر. ومع ذلك، تعرض هذا الرأي للانتقاد بسبب احتمالية أن يكون الفعل غير مجرم في دولة المصدر، وبالتالي يظل مرتكبوا هذه الجرائم بمنأى عن العقاب في تلك الحالة. لذلك ظهرت وجهة نظر أخرى تقضي بمنح الاختصاص للدولة التي تحققت فيها النتيجة النهائية للجريمة؛ غير أن هذا الطرح يواجه معضلة تتعلق بتوزيع العمليات بين عدة دول، مما قد يؤدي بدوره إلى تمكن الجناة من الإفلات من العقاب.

الفرع الثالث: ضبط الأدلة الرقمية

يُمثل ضبط الأدلة الرقمية الركيزة الأساسية للعدالة في العصر السيبراني؛ ونظراً لطبيعتها الحساسة وسرعة زوالها، يخضع ضبطها لقواعد إجرائية وتقنية صارمة تضمن سلامتها ومشروعيتها القانونية.

ويتسع هذا الفرع ليتناول مفهوم الضبط الرقمي وآلياته، إلى جانب استعراض أنواع الأدلة الرقمية الناجمة عن التفتيش الإلكتروني—سواء كانت مخزنة في الأجهزة المادية، أو منقولة عبر الشبكات، أو مستضافة في السحابة الرقمية—وكيفية التعامل معها دون تغيير طبيعتها الفنية.

أولاً: ضبط الدليل الرقمي الضبط: هو النتيجة المباشرة لعملية التفتيش الإلكتروني، ويُعد أحد إجراءات التحقيق الهادفة للوصول إلى الحقيقة وليس غاية في حد ذاته. يُثار تساؤل هام حول مدى إمكانية إخضاع النظم المعلوماتية للتفتيش، باعتبارها تحتوي بيانات مادية، إلى جانب كيفية التعامل معها بشكل قانوني وفعال.

أ- جمع آثار التفتيش الإلكتروني (الدليل الرقمي): يبدأ التحقيق الجنائي بتحديد مصدر الدليل الرقمي المتوقع جمعه، حيث يتم الحصول عليه بصورة رقمية أولية بهدف فحصه وتحليله. تختلف مصادر البيانات بناءً على نوعها وقد تتضمن أجهزة تخزين أو الأنظمة التقنية. تتم

101 - غنا محمد غنا، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الأنترنت، دار الفكر والقانون، المنصورة - مصر، 2010، ص180.

مقارنة توقيع الحاوية الأصلية بالبيانات المستنسخة للتأكد من صحتها وسلامتها، ويتم إنشاء نسخ احتياطية تُحفظ في مكان آمن لضمان عدم تلف البيانات المستخدمة أثناء العملية¹⁰².

يشمل الحصول على البيانات خطوات متعددة تهدف للتأكد من صحة وسلامة الدليل، سواء قبل أو بعد عملية تفتيش النظام. خلال هذه الخطوات، يُراعى عدم تعديل الدليل أو المساس به بأي شكل، ويمكن تحقيق ذلك من خلال نسخ البيانات وتحويلها دون الإخلال بمحتواها الأصلي¹⁰³.

ب- فحص البيانات الرقمية كأثر للتفتيش: يقوم المحقق الجنائي بفحص البيانات المستخرجة لفصل الأدلة المتعلقة بالقضية، ويتم ذلك بناءً على نوع الحاوية المستخدمة لتخزين البيانات. يتوجب على المحقق اختيار الأدوات المناسبة واستخدام الطريقة الصحيحة لاستخراج الدليل الرقمي والذي يلعب دوراً محورياً في بناء القضية.

ج- تحليل ومراجعة آثار التفتيش الإلكتروني: يُحلل المحقق الجنائي البيانات المستخرجة لتحديد الاستنتاجات وربط الأدلة ببعضها. تعد هذه الخطوة دقيقة وحاسمة، حيث يتم فيها التحقق من مدى مطابقة القواعد القانونية للتفتيش وصحة الإجراءات المتبعة. ومن الضروري أن يشترك أكثر من محقق في عملية التحليل لضمان وجود وجهات نظر متعددة وأساليب مختلفة قد تكشف عن أدلة جديدة تعزز القضية.

يُرافق كافة مراحل التحقيق تدوين مفصل لعمليات التفتيش وتحليل الأدلة، إذ تُحفظ هذه السجلات على هيئة محاضر وتقارير مرفقة بملف شامل لإثبات صحة الدليل الرقمي المستخرج من مسرح الجريمة المعلوماتي¹⁰⁴.

ثانياً: أنواع الأدلة الرقمية الناجمة عن التفتيش الإلكتروني: تمثل الأدلة الرقمية عنصراً مهماً في التحقيقات المتعلقة بالجرائم المعلوماتية، إذ يمكن أن تسهم بشكل كبير في إثبات الجريمة وربطها بالمتهم.

أ- ضبط جهاز الكمبيوتر وملحقاته: يعد ضبط جهاز الكمبيوتر وملحقاته خطوة ضرورية لتحديد إذا ما كانت الجريمة المرتكبة تُصنف كجريمة معلوماتية ولتحديد ارتباطها بالموقع أو الشخص الحائز على الجهاز. وتتنوع أشكال أجهزة الكمبيوتر ومواصفاتها، مما يتطلب من

102 - نعيم سعيدان، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، القانون الجنائي، كلية الحقوق، جامعة الحاج لخضر-باتنة، الجزائر، 2012، ص124.

103 - فاطمة الزهراء خبازي، الجريمة الإلكترونية في ظل الجرائم المرتبطة بتكنولوجيات المعلومات، تم التصفح بتاريخ 22 مارس 2026، على الساعة 19:08، منشور على الرابط: <http://salahgardafi.content.com.a2eb>

104 - حسني ثابت، الجريمة الإلكترونية في ظل تطور تكنولوجيات المعلومات، تم التصفح بتاريخ 22 مارس 2026، على الساعة 21:20، منشور على الرابط: <http://kenonaonline.com>

ضباط الشرطة القضائية امتلاك المعرفة الكافية للتعامل معها بشكل صحيح وسريع، إما بأنفسهم أو بمساعدة خبير تقني. ومن بين الملحقات نذكر:

1-الملحقات البرمجية(Software) : إذا كان الدليل الرقمي يعتمد على برنامج معين، فمن الضروري ضبط الأقراص الخاصة بتركيب هذا البرنامج لفحص الدليل الرقمي بشكل صحيح.

2-وسائل التخزين المتنقلة: تشمل هذه الوسائل الأقراص المدمجة (CDs)، أقراص الليزر، الأقراص الصلبة المحمولة، الأشرطة المغناطيسية وغيرها.

3-المودم: يعتبر المودم عنصرا أساسيا لربط أجهزة الكمبيوتر ببعضها عبر خطوط الهاتف.

ب-ضبط البريد الإلكتروني: يتضمن هذا الإجراء الوصول إلى صندوق البريد الإلكتروني الخاص بالمتهم بعد معرفة اسم المستخدم وكلمة المرور. يتم ذلك لفحص محتوى البريد الوارد والصادر، والرسائل المحفوظة أو المحذوفة. يمكن أيضا الاعتماد على برامج متخصصة لفحص الرسائل الإلكترونية داخل جهاز المتهم¹⁰⁵. ومع ذلك، تواجه المحققين تحديات عديدة أثناء ضبط أدلة البريد الإلكتروني، منها:

- كمية البيانات الهائلة التي يجب فحصها.

- احتمال انتهاك حقوق الخصوصية للأطراف الأخرى، وهو ما يستدعي اتخاذ تدابير وضمانات لحماية تلك الحقوق.

- إمكانية تخزين بعض البيانات على خوادم وأجهزة في دول أجنبية، الأمر الذي يتطلب تعاوناً بين السلطات المحلية والدولية¹⁰⁶.

ينص المشرع الجزائري في المادة 6 من القانون 04-09 المؤرخ في 5 أوت 2009، ويتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على أنه في حالة العثور على بيانات مخزنة قد تكون مفيدة في التحقيق المرتبط بجريمة ما، فإنه ليس من الضروري حجز كامل المنظومة المعلوماتية. بدلا من ذلك، يتم نسخ البيانات الضرورية وحفظها على وسيط إلكتروني قابل للحجز وفقا للإجراءات القانونية.

ج-محضر التفتيش الإلكتروني: إعداد محضر التفتيش الإلكتروني يُعد خطوة حاسمة لتوثيق الأدلة المستخلصة بشكل رسمي ومرتب. ويتضمن المحضر عدة عناصر أساسية:

105 - نهال عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان -الأردن، 2010، ص 42.

106 - عبد الصديق شيخ، "الوقاية من الجرائم الإلكترونية في ظل القانون رقم 04-09"، مجلة معالم الدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة يحي فارس-المدية، الجزائر، المجلد 04، العدد 01، 2020، ص199.

1-الرقم القضائي ووصف الواقعة: بداية، يتم تحديد الرقم القضائي الخاص بالواقعة بحسب تسلسل تسجيل القضايا. يُكتب الرقم بمداد مميز غالبا باللون الأحمر لتسهيل التعرف عليه وضمان عدم تكراره.

2-عنوان محضر التفتيش الإلكتروني: يجب أن يشتمل عنوان المحضر على تاريخ ووقت ومكان افتتاحه بالإضافة إلى بيانات المحقق والإجراءات التي قام بها قبل مباشرة التحقيق.

3-تاريخ ووقت افتتاح المحضر: يُوضح في البداية التاريخ الكامل اليوم، الشهر، السنة (حسب التقويمين الميلادي والهجري)، إلى جانب وقت البدء. يُعتبر هذا البيان مهما لتحديد توقيت الحادثة والتدخل الأمني.

4-مكان تحرير المحضر: يحتوي المحضر على بيانات تتعلق باسم المحقق وصفته ومؤهلاته، وهو أمر ضروري لمعرفة مدى أهليته لإجراء التحقيق. كما يتم ذكر اسم كاتب المحضر مع الإشارة إلى أداء القسم إن وُجد.

5-الإجراءات السابقة لبدء التحقيق: تتضمن توثيق كل الإجراءات التي تمت قبل بدء التحقيق الرسمي، مثل تلقي البلاغ وتفاصيل انتقال المحقق إلى مكان الحادث، بالإضافة إلى ملخص محضر الاستدلالات إن وجد.

6-مقدمة المحضر: تشكل مقدمة المحضر ملخصا شاملا ومختصا للواقعة، مع الالتزام بتقديم المعلومات التالية:

- كيفية تلقي البلاغ.

- عرض ملخص موجز عن الواقعة.

في هذه المرحلة، يُثبت وصول الأخبار المتعلقة بالواقعة للمحقق، ثم يقوم المحقق بتسجيل مضمون الواقعة، شرح كيفية حدوثها، ومناقشة الأطراف المتصلة بها بصورة شفاهية.

7-موضوع المحضر: يتضمن المحضر توثيق جميع الخطوات والإجراءات القانونية والفنية التي قام بها المحقق للكشف عن غموض الواقعة، والتوصل إلى مرتكبي الجريمة وضبط الأدلة الداعمة لربطهم بالجريمة. يمكن تقسيم هذه الإجراءات إلى قسمين:

- الإجراءات الميدانية، وتشمل جمع الأدلة المحسوسة أو المادية.

- الإجراءات المتعلقة بأقوال أطراف الواقعة، بما في ذلك الحجج والبراهين المستمدة من معاينة الأدلة المادية، وفحصها بالوسائل الحسية أو باستخدام التقنيات العلمية، لا سيما الأدلة الإلكترونية. تتجلى هذه الإجراءات بضبط الأدلة المادية من خلال:

-انتقال المحقق إلى مسرح الجريمة لمعاينته وجمع الآثار والأدلة ذات الصلة.

-وضع خطة عمل بالتعاون مع فريق البحث لتنفيذ الإجراءات اللازمة للقبض على المتهم وتفتيشه، في سياق الاتصال بأطراف الواقعة. تشتمل الواقعة (الجريمة) على عناصر رئيسية مثل: المجني عليه، الشهود، المتهم، والمضبوطات. ينبغي كذلك أن تقتصر مناقشة المتهم على محقق ذي خبرة، وأن تتم في غرفة مخصصة للتحقيق وليس من قبل معاوني المحقق.

-يجب على المحقق استخلاص إفادات واضحة من المتهم بشأن تفاصيل الحادثة.

-مواجهة المتهم بأقوال الشهود أو المجني عليه أو المتهمين الآخرين.

-مواجهة المتهم بالأدلة التي عُثر عليها في مسرح الجريمة أو التي كانت بحيازته.

-تحليل أقوال المتهم للكشف عن أي تناقضات أو تعارض في تصريحاته، مع تقديمه بتلك التناقضات عند الضرورة¹⁰⁷.

8-توقيع المحقق على المحضر: ألزم القانون المحقق بالتوقيع على كل صفحات المحضر، على أن يتم التوقيع أيضا من قبل الكاتب في نهاية التحقيق، حيث يُعد توقيع عضو النيابة العامة العامل الرئيسي في مصداقية المحضر وصحته، مما يضمن استبعاد أي شبهات تتعلق بالتزوير أو التحريف.

د-مشروعية الدليل المستخلص من التفتيش الإلكتروني: يُعتبر الهدف الرئيسي من عملية التفتيش هو البحث عن الأدلة المرتبطة بجريمة معينة، الأمر الذي يثير تساؤلات حول مدى مشروعية الأدلة المستخلصة عبر الوسائل الإلكترونية، وقيمتها القانونية أمام المحاكم، خصوصا أنها تختلف عن الأدلة المادية المعتادة.

يشترط في صحة الدليل المستخلص من التفتيش الإلكتروني توفر مجموعة من الشروط التي تتيح للقاضي قبوله كدليل قانوني ونظرا لأن التفتيش إجراء مطلوب من النيابة العامة في إطار تحرياتا وتحقيقاتها حول الجرائم، فإن هذه الشروط تتضمن:

1-الحصول المشروع على الدليل: ينبغي أن تكون إجراءات الحصول على الدليل الرقمي مطابقة لقواعد الدستور والقانون. هذا يعني ألا يتم انتهاك الحريات أو تجاوز القوانين تحت أي ظرف، كما يجب أن يُنفذ التفتيش بما يتوافق مع الضوابط القانونية دون استخدام الخداع أو التدليس للحصول على البيانات. وقد أتاح المشرع قوانين خاصة بجرائم أنظمة المعلومات، تضمن حماية الحريات الفردية المتوفرة على الحواسيب والإنترنت، كما أضاف ضمانات قانونية وقضائية للتفتيش الإلكتروني.

107 - عفيفي كامل عفيفي، جرائم الكمبيوتر، دون دار نشر، الإسكندرية-مصر، 2000، ص154.

2 -يقينية الدليل المستخلص: يشترط أن يكون الدليل الرقمي حاسما وغير قابل للشك. وفي حال وجود شك في مصداقية الدليل، يُفسر هذا لصالح المتهم. لذلك، يلعب خبرة المسؤولين عن التفتيش دورا مهما في تحديد مدى يقينية الدليل، وأيضا نوعية البرامج والأجهزة المستخدمة خلال العملية، مما يعزز صدقية الإجراءات¹⁰⁸.

والجدير بالذكر، أنه لا يمكن قبول أي دليل مستخلص من وسائل إلكترونية ما لم يُعرض للمناقشة أمام المحكمة لتقدير قيمته القانونية. عمليات المناقشة تلعب دورا محوريا في تكوين قناعة القاضي بشأن اعتماد هذا الدليل أو رفضه. إذ لا يكفي مجرد وجود محضر التفتيش لإثبات مشروعية الدليل، حيث يجب أن تتم مناقشته علنا والاستماع إلى تفاصيله وإجراءات استخلاصه. بالتالي، فإن المحكمة التي لم تستمع إلى المناقشة الكافية للدليل المستخرج من الوسائل الإلكترونية تفقد القدرة على الحكم بالدعوى بصورة عادلة وموثوقة، نظرا لاستحالة تقييم القيمة القانونية لهذا الدليل بشكل صحيح¹⁰⁹.

ه-حجية الدليل المستخلص وسائل التفتيش الإلكتروني: اشترط المشرع الجزائري أن يتم الحصول على الأدلة المُستخلصة من خلال التفتيش الإلكتروني بطريقة قانونية ومشروعة. إذ لا يجوز للقاضي الجنائي الاعتماد في حكمه إلا على دليل جرى الحصول عليه وفقا للقانون ودون أي انتهاك للإجراءات القانونية. ويعد صحة الدليل وعدم شوبه بأي بطلان ركنا أساسيا، باعتبار أن مشروعية الخصومة الجنائية تعتمد على أدلة سليمة قانونيا. ولا يمكن للقاضي أن يتجاهل هذه الضوابط، حيث تُعتبر إحدى ركائز العدالة الجنائية التي تُعزّز قرينة البراءة. وفي الوقت ذاته، يجب مراعاة حرية القاضي في تكوين قناعته، بصفته ممثلا لسلطة الدولة في تنفيذ العقوبات¹¹⁰.

أما عن موقف المشرع الجزائري تجاه الأدلة الإلكترونية، فقد نصت المادة 349 من قانون الإجراءات الجزائية، في فقرتها الأولى، على أنه يجوز إثبات الجرائم بأي وسيلة من وسائل الإثبات، بما فيها الإلكترونية، ما لم ينص القانون على خلاف ذلك. كما يتيح القانون للقاضي أن يبني حكمه تبعا لقناعته الشخصية. وبناءا على ذلك، تتوفر للقاضي عند الفصل في الجرائم المعلوماتية محاضر التفتيش الإلكتروني التي تعد من الأدلة القابلة للتقدير وفقا لتقديره الشخصي، بحيث يمكنه الأخذ بها إلى جانب بقية الأدلة المقدمة في القضية. وهذا يعكس السلطات الواسعة التي يمنحها المشرع للقضاة أثناء التحقيق القضائي.

بالإضافة إلى ما سبق، تُعتبر الضبطية القضائية ملزمة بالامتنثال لمبدأ الشرعية الجنائية والإجرائية في الدعاوى الجزائية. وبالتالي، لا يمكنها القيام بتفتيش إلكتروني دون الالتزام

108 - عبد الإله هلاي أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي-دراسة مقارنة، ط1، دار النهضة العربية، مصر، 1997، ص180.

109 - مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة القاهرة، 2008، ص259.

110 - أمال قارة، الجريمة المعلوماتية، رسالة ماجستير، القانون الجنائي والعلوم الجنائية، جامعة الجزائر 1، الجزائر، 2002، ص 196.

بالقواعد المنصوص عليها في قانون الإجراءات الجزائية، حتى لو تعلق الأمر بجرائم شديدة الخطورة أو أفعال إجرامية غير مشروعة، حيث تزداد صعوبة هذا الإجراء مع تعقيد الجرائم المعلوماتية وحدثاتها.

يُصنف التفتيش الإلكتروني ضمن الإجراءات المعقدة نظرا لطبيعة الأدلة الرقمية التي قد يسهل تعديلها أو تدميرها بسرعة. وقد تكون تلك الأدلة متصلة بدول أخرى، مما يُعقد عملية الحصول عليها بسبب اعتبارات سيادة الدول. بالإضافة إلى ذلك، فإن هذا النوع من التفتيش يتطلب مهارات ومعرفة تقنية وفنية دقيقة، والتي قد لا تكون متوفرة دائما لدى أفراد الشرطة والمحققين والقضاة.

في هذا السياق، انسجم المشرع الجزائري مع الجهود الدولية الرامية إلى مكافحة الجرائم المعلوماتية. لذلك، أقدم على وضع استراتيجية تضمنت إصدار نصوص قانونية خاصة بموجب القانون رقم 04-09، للحد من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال. كما قام بتعديل النصوص القانونية الحالية بما يتوافق مع طبيعة هذه الجرائم. وقد تم التركيز على الجانب العملي لمكافحة هذه الظاهرة من خلال إنشاء هيئات متخصصة وأجهزة وطنية أسندت إليها مهمة التصدي لهذه الجرائم.

يتجلى الدور الإيجابي للهيئة الوطنية المكلفة بالوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، بالإضافة إلى الجهود الفعالة للأجهزة الأمنية، التي تعمل بالتنسيق مع السلطات المختصة لجمع الأدلة اللازمة في القضايا المتعلقة بالجرائم المعلوماتية. تظل هذه الأدلة خاضعة لمبدأ حرية القاضي الجنائي في تكوين قناعته من أجل الوصول إلى الحقيقة الموضوعية.

أما إجراءات التفتيش في الجرائم المعلوماتية، فتعتبر أساسا لتحقيق العدالة والكشف عن كافة الملابسات المرتبطة بالجريمة. ويهدف هذا الإجراء بشكل رئيسي إلى ضبط الأدوات المستخدمة في ارتكاب الجريمة أو تلك التي نتجت عنها، مما يعكس أهميته البالغة ضمن مسار التحقيق الجنائي.

المطلب الثالث: توظيف الذكاء الاصطناعي في التحريات الإلكترونية

يُعتبر الذكاء الاصطناعي أحد فروع علوم الحاسوب التي تهدف إلى بناء أنظمة قادرة على تقليد القدرات البشرية، مثل التعلم، التحليل، واتخاذ القرارات. ومع إزدياد الجرائم الإلكترونية وتعدد أساليبها، برزت أهمية الاستعانة بالتقنيات الحديثة لتعزيز فعالية التحريات الرقمية، وعلى رأسها الذكاء الاصطناعي.

هذا، وقد ساهم توظيف الذكاء الاصطناعي في إحداث تحول جذري في مجال التحقيقات الإلكترونية، حيث بات من الممكن معالجة كميات هائلة من البيانات بسرعة ودقة متناهية، وهذا بدوره يمكن الجهات المختصة من الكشف عن الجرائم وتعقب مرتكبيها بكفاءة عالية وفعالية أكبر.

الفرع الأول: تعريف الذكاء الاصطناعي وبيان أهم مجالاته

يُعد الذكاء الاصطناعي من أبرز مخرجات تطور علوم الحاسوب في العصر الحديث، حيث أصبح يلعب دوراً متزايد الأهمية في مختلف المجالات، لاسيما في الميادين الأمنية والرقمية. ونظراً لتعدد استخداماته وتشعب تطبيقاته، فإنه من الضروري الوقوف على تعريفه وتحديد أهم مجالاته، تمهيدا لفهم دوره في التحريات الإلكترونية.

أولاً: تعريف الذكاء الاصطناعي: على الرغم من تزايد الاهتمام بمجال الذكاء الاصطناعي باعتباره مجالاً بحثاً خصباً، حيويًا وحديثاً، إلا أن الوصول إلى تعريف دقيق أو موحد لهذا المجال لا يزال بعيد المنال. فقد ركزت أغلب التعريفات، إما على الجوانب التقنية واستخدامات الذكاء الاصطناعي كتطبيق أو كأداة، أو على السمات التي تحاكي ذكاء الإنسان.

يُعرف الذكاء الاصطناعي، على أنه دراسة وتصميم أنظمة ذكية تستطيع فهم بيئتها وإتخاذ إجراءات تزيد من احتمالية نجاحها. بينما قدم العالم الأميركي جون مكارثي تعريفاً مختلفاً بقوله، إنه علم وهندسة إنشاء آلات ذكية، وخصوصاً برامج الكمبيوتر¹¹¹.

من جانب آخر، يرى البعض أن الذكاء الاصطناعي هو فرع من علم الحاسوب المرتبط بتخصصات أخرى مثل علم النفس وعلوم المعرفة، ويهدف إلى جعل الحواسيب تؤدي مهامها بكفاءة تضاهي كفاءة البشر، مع السعي لأن تفكر بذكاء عبر أداء مهام متنوعة مثل تشغيل السيارات ذاتية القيادة، لعب الشطرنج، إثبات النظريات الرياضية، إجراء العمليات الجراحية، وغير ذلك¹¹².

كما يرى فريق آخر، بأن الذكاء الاصطناعي هو مجموعة من السلوكيات والخصائص التي تجعل البرامج الحاسوبية تحاكي قدرات وأداء الدماغ البشري، مثل التعلم والاستنتاج والتفاعل مع مواقف غير مبرمجة مسبقاً. ويُعتبر الذكاء الاصطناعي امتداداً للجيل الحديث من علوم الحوسبة، حيث يسعى إلى محاكاة عمليات التفكير العقلي البشري.

ورغم اختلاف وجهات النظر، إلا أن التعريفات المختلفة تتفق على أن الذكاء الاصطناعي يتجسد في وجود تقنيات قادرة على التعلم وإتخاذ القرارات. فالذكاء الاصطناعي، سواء روبوتات أو أنظمة حوسبية رقمية، يمتاز بالقدرة على إنجاز مهام بشرية مثل التفكير، استنتاج المعاني،

111 - عبد الإله أحمد مطر الفالسي، "المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي"، مجلة الدراسات القانونية، كلية الحقوق، جامعة أسيوط، مصر، المجلد 9، العدد 8، 2021، ص 2844.

112 - المرجع نفسه، ص 2845.

التشخيص الطبي، البحث في الإنترنت، التعرف على الأصوات والكتابة اليدوية، والتفاعل مع البيئة المحيطة بشكل ذاتي¹¹³.

تشمل تطبيقات الذكاء الاصطناعي العديد من المجالات مثل التعلم الآلي، معالجة اللغة الطبيعية، التعرف على الصوت والصورة، الذكاء الروبوتي، والذكاء الاصطناعي في المجال المالي، وغيرها. هذه التطبيقات تتطلب توفر تقنيات الحوسبة العالية ومعالجة البيانات الضخمة لتمكين الأنظمة الذكية من التكيف مع البيئات المتغيرة والتفاعل معها بكفاءة ومرونة¹¹⁴.

ومع ذلك، لا يمكن مقارنة الذكاء الاصطناعي بشكل عام بالعقل البشري لأن لكل منهما مزاياه وقيوده الخاصة. إذ يتميز الذكاء الاصطناعي بتنفيذ المهام المحددة بسرعة ودقة أعلى من الإنسان وبقدرته الفائقة على تحليل كميات هائلة من البيانات بشكل فعال ودقيق. أما الذكاء البشري فيتفوق بالقدرة على التعلم العميق وتأقلم أفضل مع التغييرات وحل المشكلات بطريقة إبداعية وإبتكار حلول جديدة.

بشكل عام، يعتمد تقييم أداء الإنسان مقارنة بالذكاء الاصطناعي على نوعية المهام المطلوبة. ومع ذلك، في كثير من السيناريوهات تتعزز النتائج بشكل كبير عندما يعمل الإنسان مع الذكاء الاصطناعي لتحقيق أهداف مشتركة.

يُشير مصطلح الذكاء الاصطناعي أيضاً، إلى أي قدرة شبيهة بذكاء الإنسان يتم إعتماها في الحواسيب أو الروبوتات أو الأجهزة الأخرى. ومن بين التعريفات الأكثر شيوعاً للذكاء الاصطناعي، أنه القدرة على محاكاة القدرات العقلية للبشر، مثل التعلم من التجارب، التعرف على الأشياء، تعلم اللغات والتفاعل معها، اتخاذ القرارات، وحل المشكلات المعقدة. ويعتبره بعض الخبراء فرعاً من علوم الكمبيوتر يهدف إلى تطوير آلات تقوم بوظائف مشابهة لتلك التي يؤديها الإنسان ولكن بطريقة عالية الكفاءة والدقة.

ثانياً: مجالات تطبيق الذكاء الاصطناعي: تشهد مجالات تطبيق الذكاء الاصطناعي تحولاً جذرياً، حيث أصبح له دور بارز في مختلف القطاعات، ولا سيما تلك المرتبطة بالمجال القانوني، مثل العمل الشرطي والأمني. حيث تتجلى أهمية الذكاء الاصطناعي في هذه المجالات ضمن إطار استراتيجيات المدن الذكية التي تعتمد على تقنياته لضمان الأمن والنظام. من بين أبرز استخدامات الذكاء الاصطناعي نذكر:

أ- الاستعانة بتقنيات الذكاء الاصطناعي لتحليل الصور والفيديوهات: يمكن استخدام كاميرات المراقبة الذكية لتحليل الصور ومقاطع الفيديو بهدف تحديد أماكن تواجد الأشخاص المشتبه بهم

113 - خالد ممدوح إبراهيم، التنظيم القانوني للذكاء الاصطناعي، دار الفكر الجامعي، الإسكندرية - مصر، 2022، ص 22.

114 - بتشيم بوجمعة، الذكاء الاصطناعي في منظومة العدالة الحديثة على ضوء أحدث أحكام التشريع والقضاء المقارن إلى غاية سنة 2022، دار ألفا للوثائق، الجزائر، 2022، ص 38.

أو المطلوبين، مع إرسال تنبيهات تفاعلية فورية إلى مراكز التحكم. كما تُستخدم الطائرات الذكية بدون طيار للمراقبة الجوية والحد من ارتكاب الجرائم.

ب-توظيف الذكاء الاصطناعي في مكافحة الجرائم الحديثة: تتميز الجرائم الحديثة بتعقيدها الشديد مقارنة بالجرائم التقليدية، مما يجعل من الصعب كشفها وتتبعها وضبط مرتكبيها. هذا التعقيد يرجع إلى الطبيعة الخفية لهذه الجرائم وصعوبة جمع الأدلة والتحقيق مع مرتكبيها، الذين غالبا ما يتمتعون بمهارات عالية وذكاء تقني. للتصدي لهذا التحدي، لجأت بعض الجهات الأمنية إلى تقنيات الذكاء الاصطناعي، كما يظهر في مثال شرطة نيويورك التي أنشأت مركزا لإدارة الجريمة يعتمد على تحليل البيانات. حيث يتيح هذا المركز مراقبة الجرائم في المدينة والتنبيه باحتمال وقوعها بهدف الاستعداد للتصدي لها مسبقا¹¹⁵.

وفي هذا السياق، يسهم القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في تنظيم استخدام التكنولوجيا للأغراض الأمنية. حيث حدد القانون الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية، ضمن نص المادة 4 منه، التي جاء فيها: "يمكن القيام بعملية المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية:

أ-للوفاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة،
ب-في حالة توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج-لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة..."¹¹⁶.

ج-استخدام الذكاء الاصطناعي لتحليل بيانات شبكات التواصل الاجتماعي: أصبحت تطبيقات الذكاء الاصطناعي جزءا أساسيا من منصات التواصل الاجتماعي، حيث تُستخدم للتصدي للظواهر السلبية. إذ تولي الجهات الأمنية اهتماما متزايدا بوسائل التحليل الرقمي التي تعمل على فحص بيانات المستخدمين للكشف المبكر عن الأنماط المشبوهة والسلوكيات غير الطبيعية داخل البيئة الإلكترونية. حيث لم يعد دور الحاسوب مقصورا على ميادين البحث العلمي أو العمليات الحسابية فقط، بل بات عنصرا رئيسيا في التعامل مع التحديات الحديثة ومكافحة الجرائم الإلكترونية¹¹⁷.

الفرع الثاني: دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية

115 - الفلاسي عبد الإله أحمد مطر، المرجع السابق، ص13.

116 - القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

117 - الفلاسي عبد الإله أحمد مطر، المرجع السابق، ص 14.

أصبح الذكاء الاصطناعي أداة فعالة في مكافحة الجريمة الإلكترونية، لما يوفره من قدرات متقدمة في التحليل والكشف، مما يستدعي بيان دوره وأهم تطبيقاته في هذا المجال.

إن هذا الأخير أصبح بالغ الأهمية في عصرنا الحالي، نظرا للطبيعة التقنية المعقدة التي تتميز بها هذه الجرائم وصعوبة اكتشافها بسهولة. حيث يمكن للذكاء الاصطناعي أن يلعب دورا حيويا من خلال الاستفادة من التحليلات الرقمية والأنظمة الذكية، إذ يساهم تكامله مع تقنيات مثل التنقيب عن البيانات والشبكات العصبية في تعزيز دور الأجهزة الذكية في مجال أمن المعلومات.

يتيح الذكاء الاصطناعي تحليل البيانات المخزنة بشكل فعال وتدعيمها لإدارة أفضل للأمن السيبراني، بالإضافة إلى كشف شبكات التجسس ومحاولات التلاعب في البيانات. إن الهدف الأساسي من استخدام الذكاء الاصطناعي هنا هو تطوير وتحسين العمليات الرقابية، وبناء قواعد معرفية تساعد على فهم التهديدات والمخاطر التي تحيط بأمن المعلومات، مما يؤدي إلى كشف الجرائم الإلكترونية مبكرا أو حتى التنبؤ بها قبل وقوعها¹¹⁸.

أولا: دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية الواقعة على الأموال: تعتمد الجرائم الإلكترونية، التي تعد واحدة من أكثر الجرائم تحقيقا للعوائد المالية للمجرمين، بشكل رئيسي على أساليب القرصنة والابتزاز من أجل الحصول على الأموال. مع تطور البيئة الرقمية واستغلالها من قبل مرتكبي الجرائم، أصبح العالم الرقمي بحاجة ماسة إلى وجود أنظمة حماية قوية تحول بينه وبين هؤلاء الفاعلين. في هذا السياق، يبرز الذكاء الاصطناعي كأداة فعالة تساهم بدور محوري في مكافحة الجريمة الإلكترونية.

نتيجة للأهمية المتزايدة لدور الذكاء الاصطناعي، بات من الضروري تكامله في الأنظمة المالية والمحاسبية، من خلال توظيف الشبكات العصبية والخوارزميات المتقدمة التي صممت للتنبؤ بالجرائم قبل وقوعها. حيث تعمل هذه الخوارزميات عبر تحليل كميات ضخمة من البيانات المتنوعة، حيث تقوم بمسحها وفحصها وتنقيتها لفهم أنماط السلوك الإجرامي، مما يمكن الشركات المالية وأصحاب الأعمال من التعرف على التهديدات المحتملة واتخاذ التدابير الوقائية اللازمة في وقت مبكر.

علاوة على ذلك، تتيح التقنيات الذكية للحكومات تعزيز جهودها في مواجهة الجرائم الإلكترونية وتحسين سياساتها الأمنية لتحقيق توازن شامل في هذا المجال¹¹⁹.

يعمل الذكاء الاصطناعي بدقة متناهية وفق آليات وتقنيات متطورة تساهم في تنظيم العمليات الأمنية، وتجميع البيانات وتحليلها، والبحث عنها ضمن العالم الرقمي وأنظمة المعلومات. كل

118 - دولي الخضر، ناصري نفيسة، "دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية"، مجلة المؤشر للدراسات الاقتصادية، جامعة بشار، المجلد 2، العدد 2، 2018، ص 60.

119 - رانا مصباح عبد المحسن عبد الرزاق، "دور الذكاء الاصطناعي في مواجهة جريمة الإرهاب الإلكتروني-دراسة مقارنة"، المجلة الأكاديمية لجامعة نوز، العراق، المجلد 12، العدد 4، 2023، ص 17.

هذه الإمكانيات تفتح آفاقا جديدة لمواجهة التحديات المتعلقة بالجريمة الإلكترونية وتعزيز الأمن السبيرياني على كافة المستويات¹²⁰.

ثانيا: اقحام الشرطة الرقمية للذكاء الاصطناعي في مكافحة الجرائم الإلكترونية: تعتمد الشرطة الحديثة بشكل متزايد على تقنيات الذكاء الاصطناعي كوسيلة لتعزيز كفاءتها وتطوير أدواتها التكنولوجية المتقدمة، حيث يتمثل هذا التطور في دمج كافة الأنظمة التابعة للشركات والمؤسسات الخاصة تحت مظلة الرقابة الحكومية، مما يتيح للشرطة القدرة على التنبؤ بالجرائم المحتملة والتدخل لمنع وقوعها. علاوة على ذلك، يسهم الذكاء الاصطناعي في تحقيق تقدم كبير في مجال التحقيق الرقمي، حيث يُمكنه تحديد هوية الجاني عبر الرسائل والبيانات الرقمية الخاصة مثل رقم الهاتف، إلى جانب الكشف عن الأدلة وتحليل بيانات المجرمين، مما يعزز فعالية عمليات المراقبة¹²¹.

تتبنى بعض الدول المتقدمة استخدام تقنية بصمة الدماغ التي تستعمل في مسح دماغ المشتبه به قبل البدء في التحقيق الجنائي. تُمكن هذه التقنية من الكشف عما إذا كان الشخص المحتجز يملك معلومات مرتبطة بالجريمة قيد التحقيق، ما يجعل من الصعب على المتهم اللجوء إلى أساليب خداع أو تزييف للتأثير على نتائج التحقيق. ويختلف هذا النهج عن الأجهزة التقليدية لكشف الكذب التي تعتمد على تحليل الضغوط العصبية الناتجة عن التغيرات العاطفية للشخص الكاذب، إذ إن بصمة الدماغ توفر دقة أكبر دون الحاجة لخلق أي ضغط عصبي على المشتبه به¹²².

بالإضافة إلى ذلك، يعد جهاز الإنذار المبكر أحد الأدوات الاستراتيجية للحفاظ على الأمن والاستقرار. فهو يمثل مكونا رئيسيا في توقع وقوع الجرائم واتخاذ إجراءات وقائية لمنعها، مما يسهم في تعزيز سلامة المجتمع والحد من المخاطر الأمنية¹²³.

ثالثا: دور الذكاء الاصطناعي في مكافحة جرائم الإرهاب السبيرياني: يعد الإرهاب السبيرياني من أكثر الظواهر المثيرة للقلق، خصوصا خلال السنوات الأخيرة، حيث شهد العالم انتشارا واسعا لهذا النوع من التهديدات. يعتمد الإرهابيون بشكل متزايد على شبكة الإنترنت لتحقيق أهدافهم، باستخدام برمجيات خبيثة ومتطورة لاستهداف أنظمة الحاسوب، وعبر تقنيات معقدة، إذ يمكنهم تحويل الأجهزة إلى قنابل إلكترونية مؤقتة لتفجيرها في أماكن متعددة في وقت واحد، مما يشكل خطرا كبيرا على البنى التحتية الحيوية. فقد تتسبب الهجمات الإلكترونية في شلل الشركات التجارية، وتعطيل البنوك، بل وتأثر سلبا على أسواق المال والاقتصاد العالمي.

120 - نور أمينة الأخشن، محمد العيداني، "الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية"، مجلة القانون والعلوم البيئية، كلية الحقوق والعلوم السياسية، جامعة الجبالي بونعام-خميس مليانة، الجزائر، المجلد 2، العدد 2، 2023، ص537.

121 - حمزة قده، إيمان كحيط، توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، المؤتمر الدولي العام حول التكنولوجيا الرقمية من التأصيل إلى الابتكار، دون مجلد، جامعة أم القيوين، الإمارات العربية المتحدة، 2022، ص8.

122 - رانا مصباح عبد المحسن عبد الرزاق، المرجع السابق، ص18.

123 - سعود عبد القادر الشاعر، دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي -دراسة مقارنة، جامعة عجمان، الامارات العربية المتحدة، 2020، ص21.

إن الجدير بالذكر، أن المجرمين السيبرانيين ليس من الضروري أن يتواجدوا في نفس الدولة، مما يزيد من تحديات مكافحتهم. ففي هذا السياق، يشكل الذكاء الاصطناعي حلا محوريا في مواجهة الإرهاب السيبراني. تلعب تقنيات الذكاء الاصطناعي -منها شبكات التتبع والتصوير بالأقمار الاصطناعية- دورا هاما في تحديد مواقع المجرمين من خلال تحليل البيانات المستخرجة من الهواتف المحمولة وتحديد المواقع الجغرافية بدقة. كما يمكن نشر كاميرات مراقبة ذكية في الأماكن الحساسة للكشف عن الأنشطة غير القانونية عبر التعرف على الوجوه ومقارنتها مع قواعد البيانات التي تضم معلومات عن المطلوبين.

لا يقتصر دور الذكاء الاصطناعي على كشف الجرائم فقط، بل يمتد ليشمل التنبؤ بها قبل وقوعها، من خلال التحليل الإحصائي المعقد للبيانات، مما يساهم في بناء بيئة أمنية استباقية. إضافة إلى ذلك، تساعد هذه التقنيات في تقديم الدعم المباشر لرجال الأمن عبر توفير الحماية اللازمة أثناء العمليات الميدانية¹²⁴. وباستخدام الأنظمة الذكية لرصد وتتبع السلوكيات المريبة على الشبكات الإلكترونية، يصبح بالإمكان تعزيز القدرات الأمنية وتقليل الجرائم السيبرانية بشكل ملحوظ.

وعليه، يعد الذكاء الاصطناعي أداة استراتيجية فعالة لضمان الأمان والاستقرار في العصر الرقمي الذي يشهد تطورا متسارعا في التكنولوجيا وأساليب الاعتداء الإلكتروني¹²⁵.

رابعا: دور الذكاء الاصطناعي في تطوير الأجهزة الأمنية: ظلت الأجهزة الأمنية في الدول الفقيرة تعتمد على أنظمة تقليدية في مكافحة الجريمة. ومع التطور التكنولوجي السريع عالميا، لم تعد الأساليب البدائية كافية لمواجهة الجرائم التي أصبحت أكثر تعقيدا وتشابكا، إذ بات من الممكن أن تُرتكب إلكترونيا ومن مسافات بعيدة باستخدام الأجهزة الحديثة. وفي هذا السياق، لعب الذكاء الاصطناعي دورا مهما في تعزيز وتطوير المؤسسات الأمنية بشكل غير مسبوق. فقد أتاح هذا التطور فرصة كبيرة للجهات الأمنية للوصول إلى كم هائل من المعلومات المخزنة على منصات التواصل الاجتماعي، أنظمة المراقبة بالكاميرات، وبيانات الوسائل الإعلامية، مما يساهم في تتبع المجرمين والجرائم المحتملة¹²⁶.

كما يُستخدم الذكاء الاصطناعي في العديد من المهام الدولية، مثل دعم جهود قوات حفظ السلام عبر تقليل التصعيد بين الأطراف المتنازعة وتقليل الخسائر البشرية. كما يمكن

124 - سعود عبد القادر الشاعر، دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي الجرائم الإلكترونية (دراسة مقارنة)، جامعة عجمان، الإمارات العربية المتحدة، 2020، ص17.

125 - عمار ياسر زهير البابلي، "دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة"، مجلة الامن والقانون، أكاديمية دبي للنشر، الإمارات، المجلد 29، العدد 1، 2021، ص136.

126 - المرجع نفسه، ص 149.

استثماره في التنبؤ بمواقع الضربات الجوية المحتملة، مما يُمكن من تحذير السكان المدنيين في المناطق المستهدفة وتوفير حماية أفضل لهم¹²⁷.

المبحث الثاني: التحديات القانونية والعملية للتحريات الإلكترونية

أدى التطور المتسارع في مجالات تكنولوجيا المعلومات والاتصالات إلى تمكين الجهات المعنية من استخدام أدوات إلكترونية متقدمة وفعالة في تتبع الأنشطة الإجرامية الرقمية وجمع الأدلة اللازمة لإثباتها. ومع ذلك، فإن التوسع المستمر في الاعتماد على هذه الوسائل المستحدثة بات يثير تحديات مزدوجة الأبعاد والآثار؛ فمن منظور قانوني، تُبرز الحاجة الملحة إلى تحقيق توازن دقيق بين جهود مكافحة الجرائم الرقمية وضمان حماية الحقوق والحريات الفردية، وبشكل خاص الحق في الخصوصية وسرية المراسلات.

تأسيساً على هذا الطرح، يقتضي منا المنهج المتبع تقسيم هذا المبحث إلى ثلاثة مطالب رئيسية؛ نخصص **المطلب الأول** لبيان الإشكالات القانونية المرتبطة بحماية الحقوق والحريات الفردية، لننتقل في **المطلب الثاني** لرصد الصعوبات التقنية والعملية للتحريات الإلكترونية، على أن نستعرض في **المطلب الثالث والأخير** التحديات القانونية لاستخدام الذكاء الاصطناعي في هذه التحريات".

المطلب الأول: الإشكالات القانونية المرتبطة بحماية الحقوق والحريات الفردية

يُعتبر التطور التكنولوجي والانتشار المتزايد للوسائل الرقمية من العوامل الرئيسية التي أسهمت بشكل ملحوظ في تطوير أساليب التحري الحديثة. فقد أضحت التحريات الإلكترونية أداة ذات فعالية كبيرة في كشف الجرائم وجمع الأدلة. ومع ذلك، فإن استخدام هذه الوسائل يثير تساؤلات قانونية معقدة تتعلق بمدى الالتزام بحماية الحقوق والحريات الفردية، ولا سيما في ظل الإمكانية الكبيرة لانتهاك الحياة الخاصة للأفراد والتعدي على بياناتهم الشخصية. لذا، تبرز الحاجة إلى إيجاد توازن دقيق بين السعي لتحقيق متطلبات الأمن وصون الحقوق الأساسية.

الفرع الأول: عناصر الحق في الخصوصية الرقمية

أعلن الإعلان العالمي لحقوق الإنسان، إلى جانب العهد الدولي الخاص بالحقوق المدنية والسياسية، عن مجموعة من العناصر الجوهرية التي تشكل الحق في الخصوصية، وهو حق يُعتبر مشتركاً بين جميع الشعوب حول العالم. من خلال هذا السياق، نسعى لتناول هذه العناصر بالتفصيل فيما يلي:

أولاً: خصوصية الاتصالات والمراسلات الهاتفية السلكية واللاسلكية: إن الغاية من المراسلات هنا هي التجسيد المادي للأفكار الشخصية عبر البريد الإلكتروني أو أي وسيلة

127 - على شريف، دور الذكاء الاصطناعي في نشر وتعزيز ثقافة السلام في مناطق النزاعات المسلحة، المركز الديمقراطي العربي، برلين-ألمانيا، 2021، ص4.

مراسلة تعتمد على وسائط رقمية، مثل أقراص الحاسوب الآلي. لا شك أن الشكل الخارجي للمراسلة أو الوسيلة المستخدمة لنقلها لا يُعتبر أساسا للحماية، بل الأهمية تكمن في الخصوصية التي تحتويها ومدى حرص صاحبها على صونها من الاطلاع العلني. وبذلك تعتبر تلك المراسلات مشمولة بالحماية القانونية بنفس القدر الذي تحظى به الرسائل التقليدية¹²⁸.

تنتهك خصوصية هذه المراسلات إذا تم التنصت عليها أو تسجيلها دون أخذ موافقة أصحابها، أي بطريقة سرية وغير معلنة. كما أن الحصول عليها بطرق غير مشروعة، مثل سرقتها أو استخدامها لتحقيق أغراض تضر بصاحبها، يُعد خرقا للخصوصية. يصل هذا الضرر إلى حد التعدي إذا كان الشخص المسؤول على علم بطبيعتها السرية وحساسية مضمونها، ورغم ذلك أخل بالإجراءات اللازمة لحمايتها من التدخل الخارجي أو إفشاء محتواها¹²⁹.

ثانيا: خصوصية الحياة الصحية والبيانات الشخصية: يندرج التاريخ المرضي للإنسان ضمن خصوصية حياته الصحية، ويتضمن كافة الفحوصات التي أجراها، والنتائج المرتبطة بها، وجميع العلاجات التي خضع لها، بالإضافة إلى الرعاية الصحية التي تلقاها منذ بداية ظهور أعراض مرضه. هذا التاريخ يتم رقمته بشكل متزايد في المؤسسات الاستشفائية، التي باتت تعتمد على بنوك المعلومات لتنظيم عملياتها الإدارية من خلال تخزين الاستثمارات الطبية لكل مريض وربط بياناته بالحواسيب سواء على المستوى المحلي أو العالمي. وفي إطار حماية هذه البيانات، اعتبرها المشرع الجزائري، عبر قانون الصحة رقم 18-11¹³⁰، من الأمور الشخصية الحساسة التي غالبا ما يسعى الأفراد لعدم الكشف عنها لتجنب أي إحراج محتمل¹³¹.

عرفت اللجنة الوطنية للمعلوماتية والحريات هذه البيانات، بأنها كافة المعلومات المتعلقة بشخص طبيعي يمكن تحديد هويته بشكل مباشر أو غير مباشر من خلال رقم تعريفه أو عبر مجموعة من العناصر الخاصة به. وتشمل هذه البيانات أنواعا متعددة، مثل المعلومات المحددة للهوية كال بصمات، الأصابع، العين، الصوت، الوجه. بالإضافة إلى بيانات شخصية إضافية قد تكشف عن الحياة الجنسية، العائلية، الأصل العرقي أو الإثني، الآراء السياسية، أو السوابق العدلية. يتم تخزين هذه البيانات عادة ضمن قواعد بيانات المؤسسات العامة والخاصة¹³².

128 - صفية بشتان، الحماية القانونية للحياة الخاصة - دراسة مقارنة، أطروحة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري - تيزي وزو، الجزائر، 2012، ص 218.

129 - يحي الشريف نصير، مزغيش سعاد، "الآليات القانونية المكرسة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري"، مجلة البحوث في العقود وقانون الأعمال، جامعة الإخوة منتوري-قسنطينة¹، الجزائر، المجلد 07، العدد 02، 2022، ص 197.

130 - القانون رقم 18-11 المؤرخ في 2 جويلية 2018، المتعلق بالصحة، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 46، الصادرة بتاريخ 29 جويلية 2018.

131 - المرجع نفسه، ص 192.

132 - مفيدة مباركية، "الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري"، مجلة الشريعة والاقتصاد، جامعة العلوم الإسلامية - الأمير عبد القادر، قسنطينة، الجزائر، المجلد 07، العدد 01، 2018، جوان 2018، ص 426.

تندرج كل هذه المعلومات ضمن نطاق الحماية الجنائية التي أقرها المشرع الجزائري لضمان خصوصية الأفراد الرقمية، ولتجنب أي تهديد يتعلق بانتهاكها أو نشرها بصورة غير مشروعة¹³³. وفي العديد من الحالات، يتم تقديم هذه البيانات بموافقة صاحبها أو تصل إلى الهيئات بغرض معين. ومع ذلك، يكمن التهديد الحقيقي في إمكانية نشرها أو إفشائها بشكل غير قانوني أو بطريقة تُلحق الأذى بصاحبها¹³⁴.

ثالثا: خصوصية الذمة المالية: تشمل الذمة المالية للشخص جميع ممتلكاته وما تحتويه من أصول وخصوم، سواء الحاضرة مثل المدخول، أو المستقبلية كالإرث والوصية. وأي كشف لهذه المعلومات للعلن يعتبر انتهاكا لخصوصية الفرد، حيث يحرص كل منا على عدم الإفصاح عنها أو مشاركتها مع الآخرين لتجنب أن يصبح عرضة للاستغلال من قبل الخارجين عن القانون، أو أن يقع ضحية لجرائم السرقة أو النصب والاحتيال. ولهذا، تتبع المؤسسات المالية والبنوك سياسات صارمة لحماية خصوصية عملائها، من خلال تخصيص شيفرة خاصة لكل شخص للتأكد من سرية هويته ومقدار ثروته. بهذه الآلية، يتم تعزيز حماية الذمة المالية بحيث تبقى بيانات العملاء المالية آمنة ومحصنة، بما في ذلك المعلومات والمعاملات والاتفاقات التي تشملها¹³⁵.

الفرع الثاني: الأساس القانوني لحماية الخصوصية الرقمية في الدساتير والتشريعات الجزائرية

انطلاقا من كون الجزائر ملتزمة بتكريس الحق في الخصوصية الرقمية، وذلك بما يتوافق مع الإعلان العالمي لحقوق الإنسان، والميثاق العربي، وكذلك الميثاق الإفريقي لحقوق الإنسان والشعوب، أصبح من الضروري على الدولة تكييف تشريعاتها الوطنية لتتلاءم مع هذه المعايير الدولية. يأتي هذا التكيف استجابة لما أفرزته التطورات العلمية والتقدم التكنولوجي، بما يضمن لكل فرد حماية حياته الخاصة. وفي هذا السياق، سنركز في هذا الفرع على استعراض الدساتير والتشريعات المختلفة التي وضعها المشرع الجزائري في هذا الشأن، مقارنة بإجراءات الدول الأخرى التي صادقت على هذه الاتفاقيات الدولية.

أولا: الاعتراف الدستوري بالخصوصية الرقمية: طالما منح الدستور الجزائري أولوية كبيرة لمفهوم الخصوصية، وقد ظهر ذلك جليا عبر مختلف الدساتير التي اعتمدتها الدولة على مر السنوات. بداية مع دستور 1963، حيث نصت المادة 14 منه، على تجريم التعدي على حرمة المسكن وجاءت مكاملة بضمان سرية المراسلات لكل المواطنين¹³⁶.

133 - نفس المرجع، ص ص: 463 و 464.

134 - صيرينة بن سعيد، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا الإعلام والاتصال، أطروحة دكتوراه، قانون دستوري، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر -باتنة 1، الجزائر، 2015/2014، ص 132.

135 - جميلة سليمان، "الخصوصية الرقمية للفرد ومدى تأثير الإجراء السيبراني عليها"، مجلة القانون والعلوم السياسية، المركز الجامعي- النعامة، المجلد 09، العدد 02، 2023، ص ص: 90 و 91.

136 - أنظر دستور الجزائر لسنة 1963، المؤرخ في 10 سبتمبر 1963، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 64، 1963.

كما تضمن دستور الجزائر لسنة 1976، ضمن نص المادة 49 بشكل واضح وصريح على عدم جواز انتهاك الحياة الخاصة وضمان سرية المراسلات والاتصالات¹³⁷.

أما الدستور الجزائري لسنة 1989، فقد واصل الأخذ بهذا التوجه لحماية كرامة الإنسان وحرمة حياته ضد أي شكل من أشكال العنف الجسدي أو المعنوي¹³⁸. وقد شدد الدستور في حماية الخصوصية بإيراد ضمانات خاصة في نص المادة 37 منه، التي أكدت على عدم المساس بحرمة الحياة الخاصة، الشرف، والكرامة، بالإضافة إلى حماية سرية الاتصالات والمراسلات بمختلف أنواعها. علاوة على ذلك، أولى المشرع أهمية للتجاوزات المحتملة أثناء التحقيقات القضائية، فوضع قيودا صارمة لضمان احترام خصوصية الأفراد أثناء عمليات التفتيش، حيث لا يسمح بذلك إلا بناءً على موافقة المعني وبأمر كتابي صادر من الجهة القضائية المختصة.

هذا النهج استمر الأخذ به ضمن دستور 1996¹³⁹، حيث منحت المادة 38 منه حماية مشددة لحرمة الحياة الخاصة، وتم التركيز على سرية المراسلات والاتصالات بموجب نص المادة 39 منه. لم يكتف المشرع الجزائري بالاعتراف بالحق في الحياة الخاصة كحق دستوري مطلق، بل اعتبره واجبا على كل فرد احترامه أثناء ممارسة حقوقه الأخرى. كما شدد نص المادة 63 من نفس الدستور على ضرورة الحفاظ على الخصوصية وصونها¹⁴⁰.

برزت المادة 47 كمادة جديدة، في التعديل الدستوري لسنة 2020، التي كفلت حماية المعطيات الشخصية للأفراد واعتبرت ذلك حقا أساسيا يعكس استجابة المشرع للمتغيرات الحديثة المرتبطة بالعصر الرقمي. إضافة إلى ذلك، أكد نص المادة 81 من نفس التعديل حرص المشرع الجزائري على حماية الخصوصية، وشدد على أن لكل فرد الحق بممارسة حرياته في إطار احترام حقوق الآخرين، بما يشمل الحق في الشرف وحماية الحياة الخاصة، مع التركيز على حماية الطفولة والشباب¹⁴¹.

ثانيا: حماية الخصوصية الرقمية في ظل القوانين الداخلية: تعد الخصوصية حقا جوهريا مرتبطا بشخص الفرد، وقد انعكس اهتمام المشرع بحماية هذا الحق بوضوح في الأحكام القانونية الصارمة التي تهدف إلى التصدي لأولئك الذين ينتهكونه. سوف نتناول فيما يلي تحليل هذا الاهتمام بالتفصيل:

137 - أنظر الأمر رقم 97-76 المؤرخ في 22 نوفمبر 1976، المتضمن دستور الجزائر لسنة 1976، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 94، الصادرة بتاريخ 24 نوفمبر 1976.

138 - أنظر نص المادة 33 من المرسوم الرئاسي 89 - 18 المؤرخ في 28 فيفري 1989، المتضمن الدستور الجزائري لسنة 1989، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 09، الصادرة بتاريخ 01 مارس 1989.

139 - المرسوم الرئاسي رقم 96 - 438 المؤرخ في 07 ديسمبر 1996، المتضمن دستور الجزائر لسنة 1996، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 76، الصادرة بتاريخ 08 ديسمبر 1996.

140 - صبرينة بن سعيد، المرجع السابق، ص: 160 و 161.

141 - المرسوم الرئاسي رقم 20 - 442 المؤرخ في 30 ديسمبر 2020، المتضمن التعديل الدستوري لسنة 2020، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 82، الصادر بتاريخ 30 ديسمبر 2020.

أ-حماية الخصوصية الرقمية في ظل القانون المدني المعدل والمتمم¹⁴²: لم تتوقف الحماية المدنية للخصوصية الرقمية عند وضع قواعد المسؤولية المدنية المنصوص عليها في المادة 124 من القانون المدني المعدل والمتمم، بل تجاوزتها لضمان حماية أوسع لهذه الخصوصية. كما نصت المادة 47 من نفس القانون، صراحة على حق الأفراد في وقف أي اعتداء على حقوقهم الشخصية من دون الحاجة إلى إثبات الضرر، مع تمكينهم من المطالبة بالتعويض عن الأضرار التي تمس حقوقاً ملازمة للشخصية، مثل حرية الفرد، وسلامته الجسدية، وسمعته الأدبية، وحرمة منزله، واسمه¹⁴³. على اعتبار أن الخصوصية تُعد من ضمن هذه الحقوق الأساسية، فهي تتمتع بطبيعة الحال بنفس المستوى من الحماية المقررة لهذه الحقوق في إطار القانون.

كما أكدت المادتان 28 و48 من القانون المدني المعدل والمتمم، على حماية أحد مظاهر الحق في الخصوصية، وهو الحق في الاسم باعتباره جزءاً لا يتجزأ من شخصية الفرد بكل أبعادها المادية والمعنوية. وقد جعل المشرع من خلال هاتين المادتين أي استخدام غير مبرر لاسم الشخص أو انتحاله عملاً مكفولاً للحماية القانونية، ولم تقتصر هذه الحماية على منح المتضرر الحق في رفع الدعوى فقط، بل سهل أيضاً سبل لجوئه للقضاء¹⁴⁴.

ب-حماية الخصوصية الرقمية في ظل قانون العقوبات المعدل والمتمم¹⁴⁵: سعياً لتعزيز الحق في الخصوصية، ركّز المشرع الجزائري على وضع إطار قانوني قوي يهدف إلى حماية الأفراد من مختلف أشكال الاعتداء التي تنتهك حياتهم الشخصية، وضمان تمتّعهم بحياة آمنة بعيدة عن التطفل والانتهاكات الرقمية. يظهر هذا التوجه بشكل واضح في أحكام المادة 303 مكرر من الأمر رقم 66-156 المتعلق بقانون العقوبات، المعدّل والمكمل بموجب القانون رقم 06-23، حيث جرم المشرع أي انتهاك لحرمة الحياة الخاصة للأفراد باستخدام أي وسيلة تقنية، سواء كان ذلك من خلال اعتراض المكالمات أو المحادثات الهاتفية، أو التقاط الصور الشخصية ونشرها دون إذن مالكيها.

وفي إطار مواكبة التحولات الحديثة وحماية الفئات الأكثر عرضة للاحتياز الرقمي، أضاف المشرع الجزائري تعديلات جديدة على قانون العقوبات بموجب القانون رقم 06-24 الصادر بتاريخ 28 أبريل 2024. هذه التعديلات جرّمت صراحة أي انتهاك يرتكبه الزوج أو الخاطب بحق الحياة الخاصة لزوجته أو خطيبته، أو حتى التهديد بذلك، مع تشديد العقوبات الجزائية

¹⁴² - الأمر رقم 75 - 58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 78، الصادر بتاريخ 30 سبتمبر 1975، المعدل والمتمم بالقانون رقم 05-10 المؤرخ في 20 جوان 2005، المعدل والمتمم بالقانون رقم 07-05 المؤرخ في 13 ماي 2007.

¹⁴³ - محمد بن حيدة، حماية الحق في الحياة الخاصة في التشريع الجزائري، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد - تلمسان، الجزائر، 2016/2017، ص2.

¹⁴⁴ - فضيلة عاقل، الحماية القانونية للحق في الحياة الخاصة-دراسة مقارنة، أطروحة دكتوراه علوم في القانون الخاص، كلية الحقوق، جامعة الإخوة منتوري-قسنطينة1، الجزائر، 2011/2012، ص: 107 و108.

¹⁴⁵ - الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، الجريدة الرسمية، العدد 84، 2006.

واتخاذ تدابير تحفظية مثل منع الجاني من التواصل الرقمي مع الضحية. يعكس هذا النهج الحرص على تقديم حماية جنائية شاملة للفرد وخصوصيته في ظل البيئة الرقمية المتطورة

ج- حماية الخصوصية الرقمية في ظل القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية¹⁴⁶: خصص المشرع نصوصا تفصيلية لتحديد الضمانات والضوابط التي تحكم عملية مراقبة المكالمات والمحادثات الشخصية، بهدف ضمان احترام الحقوق والحريات. وفقا لأحكام نص المادة 114 من هذا القانون، يشترط أن يصدر الإذن بمراقبة المكالمات عن سلطة قضائية مختصة، وأن يتم حصر تلك الإجراءات في نطاق جرائم محددة ومعينة. بالإضافة إلى ذلك، ورد في نص نفس المادة تحديد المبررات القانونية التي تدعو إلى اتخاذ هذا الإجراء، مع توضيح الأماكن المشمولة به، فضلا عن تحديد المدة الزمنية المقررة له، والتي لا يجوز أن تتجاوز أربعة (4) أشهر كحد أقصى، مع إمكانية تمديدتها إذا تطلبت الظروف ذلك.

د- حماية الخصوصية الرقمية في ظل القانون رقم 88 - 09 المتعلق بالأرشفة الوطني¹⁴⁷: في سياق تعزيز حماية المعلومات الشخصية، باعتبارها أحد أسس الخصوصية الرقمية، سعى المشرع الجزائري إلى تأمين هذه الحقوق عبر أحكام قانونية واردة في التشريعات ذات الصلة. حيث تنص المادة 10 من قانون الأرشفة الوطني، في المطة الأولى منها، على حظر الاطلاع على المعلومات القضائية التي لا تحمل أي ارتباط بالحياة الخاصة للأفراد إلا بعد مرور خمسين عاما على اختتام الملف القضائي وإغلاقه. بالإضافة إلى ذلك، تشير المطة الثالثة من المادة ذاتها إلى حظر الإفصاح عن أي معلومات طبية مرتبطة بالحياة الخاصة للأفراد إلا بعد مرور 100 عام من تاريخ ولادة الشخص المعني، بهدف الحفاظ على الأمن العام واحترام شرف العائلات¹⁴⁸.

ه- حماية الخصوصية الرقمية في ظل القانون رقم 09 - 04: تماشيا مع الالتزامات التي تفرضها الاتفاقيات الدولية المصادق عليها، والتي تدعو إلى مراقبة الاتصالات الإلكترونية، قام المشرع الجزائري من خلال هذا القانون بإضفاء الشرعية على هذا الإجراء الاستثنائي بهدف منع وقوع الجرائم في المجال المعلوماتي. يأتي هذا الإجراء كأحد التدابير الوقائية، مع التأكيد على احترام سرية الاتصالات والمراسلات أثناء وضع الترتيبات التقنية اللازمة لتنفيذه، بما في ذلك عمليات المراقبة وتجميع وتسجيل المحتوى¹⁴⁹.

¹⁴⁶ - القانون رقم 25-14 المؤرخ في 3 أوت 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 54، الصادر بتاريخ 13 أوت 2025.

¹⁴⁷ - قانون رقم 88-09 المؤرخ في 26 جانفي 1988، المتعلق بالأرشفة الوطني، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 04، المؤرخة في 27 جانفي 1988.

¹⁴⁸ - محمد بن حيدة، المرجع السابق، ص 97.

¹⁴⁹ - أنظر نص المادة 03 من القانون 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 47، الصادرة بتاريخ 16 أوت 2009.

كما حرص المشرع الجزائري على تعزيز عدد من الضمانات لضمان تطبيق عملية مراقبة الاتصالات الإلكترونية بشكل قانوني وعادل. وفي هذا السياق، تم تجريم أي استخدام للمعلومات التي يتم الحصول عليها خارج نطاق التحريات والتحقيقات القضائية الضرورية، وذلك بهدف حماية خصوصية الأفراد المعنيين، وفرض عقوبات صارمة ضد أي انتهاك لهذا التشريع¹⁵⁰.

و- حماية الخصوصية الرقمية في ظل القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين¹⁵¹: سعى لحماية الخصوصية، قام المشرع بتجريم عملية جمع البيانات الشخصية واستخدامها بطرق غير قانونية. وقد ورد ذلك بوضوح في نص المادة 43 من هذا القانون، التي جاء فيها أنه لا يحق لمقدمي خدمات التصديق الإلكتروني جمع البيانات الشخصية الخاصة بالأفراد إلا إذا تم ذلك بموافقة صريحة ومباشرة من الشخص المعني. وفي حال قام مقدم الخدمة باستخدام هذه البيانات لأغراض أخرى غير تلك المحددة، أو قام بإفشاءها بطرق غير مشروعة، فإنه يعرض نفسه للعقوبات المنصوص عليها في نص المادة 71 من نفس القانون¹⁵².

ي- حماية الخصوصية الرقمية في ظل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المعدل والمتمم: توجه المشرع نحو حماية البيانات الشخصية المتداولة في المجال الرقمي من خلال هذا القانون، الذي جاء استجابة للتطورات السريعة التي شهدتها ميدان التكنولوجيا والتحديات الناتجة عن عدم كفاية الأساليب التقليدية لضمان حماية فعالة لخصوصية الأفراد. حيث تشير المادة 07 من هذا القانون إلى ضرورة الحصول على موافقة صريحة من الشخص المعني قبل معالجة بياناته ذات الطابع الشخصي. كما وضحت الفقرة الثالثة من المادة ذاتها حق الشخص في سحب موافقته في أي وقت، خاصة إذا ترتب على ذلك انتهاك لخصوصيته أو تهديد لأي من حقوقه أو حرياته. بالإضافة إلى ذلك، فرض هذا التشريع عقوبات جزائية وإدارية على المسؤولين عن معالجة البيانات في حال حدوث انتهاكات تتعارض مع الضوابط والشروط المنصوص عليها في القانون لضمان حماية البيانات واحترام الخصوصية¹⁵³.

ت- حماية الخصوصية الرقمية في ظل قوانين الاعلام: يعتبر الإعلام بجميع وسائله السمعية، البصرية، والمكتوبة الموجهة للجمهور مصدرا هاما للمعرفة ونقل المعلومات. ومع ذلك، في ظل التطورات الحالية التي يشهدها العالم، أصبح الإعلام أيضا محورا يثير القلق إزاء انتهاك

150 - بوحفارة علاء الدين، الحماية الجنائية للاتصالات الإلكترونية في ظل القانون 04 - 18، مذكرة ماستر ل.م.د، قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي - تبسة، الجزائر، 2021/ 2022، ص 21.

151 - قانون رقم 15-04 المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 06، الصادرة بتاريخ 10 فيفري 2015.

152 - رشيدة بوكري، الحماية الجنائية للحياة الخاصة في ظل تكنولوجيا المعلومات والاتصالات: دراسة مقارنة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2021، ص 91.

153 - أمينة مسياد، "آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون 18-07"، مجلة الباحث في العلوم القانونية والسياسية، جامعة محمد الشريف مساعديه-سوق أهراس، الجزائر، المجلد 03، العدد 05، شهر جوان 2021، ص ص 101 - 106.

حقوق الأفراد في حياتهم الخاصة وحررياتهم الأساسية. وفي هذا السياق، أصدر المشرع القانون العضوي رقم 12-05 المتعلق بالإعلام¹⁵⁴، الذي يهدف إلى مواكبة التغييرات وتجسيد أخلاقيات هذه المهنة، والتي يُطلب من الصحفي التحلي بها أثناء ممارسة نشاطه المهني.

يحدد هذا القانون مجموعة من المبادئ القانونية العامة بموجب نص المادة 92 منه. كما نصت المادة 93 بشكل صريح على منع انتهاك الحياة الخاصة، مؤكدة على ضرورة تعزيز الضمانات القانونية لحماية الحقوق الأساسية للأفراد داخل هذا المجال الدقيق التي تؤكد ضرورة احترام حياة الأشخاص، وشرفهم واعتبارهم، بمن فيهم الشخصيات العامة، سواء بشكل مباشر أو غير مباشر. ولم يكتفِ المشرع بذلك، بل أنشأ هيئة رقابية تُعنى بتنظيم وإدارة النشاط الإعلامي، وتتحمل مسؤولية فرض العقوبات على من يخالفون أخلاقيات وأدبيات مهنة الصحافة¹⁵⁵.

في ذات السياق، أصدر المشرع الجزائري القانون رقم 14-04 المنظم للنشاط السمعي البصري¹⁵⁶، نظرا لأهمية هذا القطاع وحساسيته، في ظل الفوضى الناجمة عن التحولات الاقتصادية، الاجتماعية، الثقافية والإعلامية التي تشهدها البلاد، إلى جانب التحديات التي يفرضها الانفجار التكنولوجي. هذه التحديات تبرز بوضوح في مسألة حماية خصوصية الأفراد أمام الانتهاكات في المجال المعلوماتي¹⁵⁷. وعليه، وضع نص المادة 48 من هذا القانون شروطا عامة تلزم جميع خدمات الاتصال السمعي البصري بعدم المساس بالحياة الخاصة أو الشرف والسمعة، سواء للأشخاص العاديين أو الشخصيات العامة.

الفرع الثالث: الإشكالات الإجرائية في الجرائم الإلكترونية

إن الطابع الفريد للجرائم الإلكترونية وخصوصيتها لم يقتصر تأثيره على القواعد الموضوعية فحسب، بل امتد ليشمل الإجراءات القانونية المطبقة عليها. فقد واجه القضاء تحديات عديدة ذات طابع إجرائي، أبرزها نقص الخبرة لدى سلطات البحث والتحري وعدم كفاءة الأساليب المستخدمة في التعامل مع الأبعاد الفنية والتقنية المرتبطة بتلك الجرائم. هذا القصور أثر سلبا على قدرة الأجهزة القضائية في مواجهة هذه الجرائم بفعالية.

154 - القانون العضوي رقم 12 - 05 المؤرخ في 12 جانفي 2012، المتعلق بالإعلام، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 01، الصادر بتاريخ 15 جانفي 2012.

155 - صونيا نايل، "أخلاقيات مهنة الصحافة على ضوء قانون الإعلام رقم 12 - 05"، مجلة الحقوق والحريات، جامعة محمد خيضر-بسكرة، الجزائر، المجلد 10، العدد 01، 2022، ص ص: 2020 - 2025.

156 - قانون رقم 14 - 04 المؤرخ في 14 فيفري 2014، المتعلق بالنشاط السمعي البصري، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 16، الصادرة بتاريخ 23 مارس 2014.

157 - بوعبدالله بن عجائمة، "قانون 14 - 04 المتعلق بالنشاط السمعي البصري في الجزائر: بين متغيرات المرحلة وضرورات التعديل"، مجلة أبحاث قانونية وسياسية، جامعة محمد صديق بن يحيى-جيجل، الجزائر، المجلد 07، العدد 02، ديسمبر 2022، ص 171.

بالإضافة إلى ذلك، تبرز مشكلة الاختصاص القضائي والقانون الواجب تطبيقه، خاصة في ظل الطبيعة العابرة للحدود لهذه الجرائم، حيث يمكن أن يُرتكب الفعل في دولة وتظهر آثاره في دولة أخرى. هذا الواقع يعقد عملية تحريك الدعوى العمومية ويعزز احتمالية إفلات الجناة من العقاب.

أولاً: نقص خبرة سلطات البحث والتحري في الجرائم الإلكترونية: قد يعاني الجهاز المسؤول عن التحقيق والتحري في الجرائم الإلكترونية، بما يشمل رجال الأمن والقضاة وأعضاء الهيئات المتخصصة، من قصور واضح في الخبرة والمعرفة المتعلقة باستخدام الحاسب الآلي وأنظمتها، سواء في جمع الأدلة أو في كيفية التعامل معها واستخراجها. هذا النقص يفضي أحياناً إلى فقدان الأدلة بسبب الأخطاء الفنية، أو تلفها نتيجة الإهمال، أو حتى تجاهل أدلة هامة نتيجة عدم إلمام هذه الفئة باللغة الرقمية المستخدمة في مجال المعلوماتية، على الرغم من الدور الجوهرى لهذه الأدلة في كشف الحقيقة¹⁵⁸.

بناءً عليه، فإن التعامل مع الجرائم الإلكترونية يتطلب وجود مختصين ذوي كفاءة عالية من رجال الضبط والخبراء والقضاة، وتوفير برامج تدريبية منتظمة تساهم في اطلاعهم على أحدث المستجدات التكنولوجية. هذا التدريب الدوري يساهم في تحسين وتطوير مهاراتهم ومعارفهم المتعلقة بالتعامل مع مسرح الجريمة الإلكترونية، فضلاً عن تمكينهم من جمع الأدلة وتحليلها بشكل فعال. وقد أكدت الصكوك الدولية ضرورة تعزيز التعاون في مجال التدريب ونقل الخبرات بهدف دعم قدرات أجهزة إنفاذ القانون بما يتلاءم مع التطورات المستمرة للأساليب الإجرامية والتقنيات الحديثة. كما دعت إلى الاستفادة من التجارب العلمية الأجنبية المتقدمة التي برهنت على نجاحها في مواجهة هذا النوع من الجرائم¹⁵⁹.

وفي ظل هذه الضرورة، يُوصى بالاستعانة بخبرات خارجية من متخصصين في علم المعلوماتية وتخصيص صلاحيات قضائية مؤقتة لهم، أو دمجهم بشكل دائم ضمن فرق البحث والتحري حتى يتم رفع كفاءة جهاز التحري التقليدي القائم. فالممارسات الحالية التي تعتمد على الأجهزة التقليدية تعاني من أوجه قصور تقلل من فعاليتها وتؤثر على مدى تحقق الشرعية. لذا، لتحقيق التوازن بين الفعالية والشرعية، يجب إعادة هيكلة منظومة التحقيق عبر تأهيل الفنيين والمعنيين تقنياً وقانونياً وتعزيز وعيهم بالإطار القانوني المرتبط بالجرائم الإلكترونية، وذلك لضمان قدرتهم على مواكبة كافة المستجدات المتعلقة بهذا النوع المعقد من الإجرام¹⁶⁰.

158 - فتية حيمر، "الجرائم المعلوماتية في الجزائر: المواجهة والتحدى"، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور-خنشلة، الجزائر، المجلد 12، العدد 01، 2025، ص280.

159 - فطيمة حايطي، إجراءات التحقيق في الجرائم الإلكترونية - دراسة مقارنة، أطروحة دكتوراه الطور الثالث، قانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون-تيارت، الجزائر، 2023/2022، ص: 338 و339.

160 - وفاء صدراتي، آليات مكافحة جريمة التزوير الإلكتروني، أطروحة دكتوراه، قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي - تبسة، الجزائر، 2021/2020، ص156.

ثانياً: إشكال تنازع الاختصاص والقانون الواجب التطبيق: يُعبر الاختصاص القضائي عن ممارسة السلطة القضائية في القيام بمهام المتابعة، التحقيق، وإصدار الأحكام بخصوص الجرائم، وذلك وفق القواعد القانونية التي حددها المشرع والقيود التي أقرها لهذه السلطات أثناء أداء وظائفها. وعلى خلاف الجرائم التقليدية التي يتم تحديد مكان ارتكابها بسهولة ضمن حدود إقليم معين.

تطرح الجرائم الإلكترونية إشكاليات خاصة فيما يتعلق بالاختصاص القضائي، نظراً لافتقارها إلى التجسيد المادي وكونها ذات طبيعة عابرة للحدود الجغرافية. هذه السمات تجعل من الصعب تحديد الهيئة القضائية المختصة بالبت في هذه الجرائم. فعلى سبيل المثال، قد ترتكب الأنشطة الإجرامية في دولة معينة، بينما تظهر نتائجها الضارة في دولة أخرى، وتُخزن البيانات المتعلقة بهذه الأنشطة على خوادم موجودة في دولة ثالثة. هذا الامتداد المكاني والتشتت الجغرافي للمكونات المتصلة بالجريمة الرقمية يؤديان إلى تعقيد عملية تحديد السلطة القضائية المناسبة ويتيحان للجناة فرصة التهرب من المساءلة القانونية، بسبب غياب معايير صارمة وحاسمة تُسند الاختصاص إلى جهة قضائية محددة.

يزداد التعقيد عندما يتعلق الأمر بجرائم ترتبط بالخصوصية الرقمية، حيث تتداخل العديد من المعايير لتحديد مكان الاختصاص القضائي، مثل موقع الضحية، أو مكان وجود الجهاز الحاسوبي الذي استخدم في ارتكاب الجريمة، أو الموقع الذي ظهرت فيه النتيجة الضارة، أو مكان إقامة الجاني.

للتعامل مع هذه الإشكالية -التي يُطلق عليها اسم تنازع الاختصاص بين أكثر من نظام قانوني وطني لملاحقة نفس الجريمة أو توزيع النشاط الإجرامي بين عدة دول- برزت الحاجة إلى إيجاد حلول مستحدثة تتماشى مع مبدأ الشرعية الجنائية. إذ تهدف هذه الحلول إلى تغليب اختصاص دولة محددة بناءً على معيار يحقق أكبر قدر من الفعالية والعدالة لضمان حسن سير الإجراءات القانونية.

وفي هذا السياق، يتفق معظم الباحثين على أن مبدأ الإقليمية يُعد الأكثر معقولية وقبولاً للتعامل مع الجرائم الإلكترونية. فاختصاص الدولة التي يرتكب فيها كل أو معظم أجزاء الجريمة ينسجم مع مبدأ السيادة ويضمن توافر الأدلة المتعلقة بالجريمة داخل نطاق الولاية القضائية للدولة المعنية، مما يسهل من عملية التحقيق والكشف عن الحقيقة¹⁶¹.

قد تبني المشرع الجزائري مبدأ الإقليمية من خلال نص المادة (3) من قانون العقوبات المعدل والمتمم، التي تنص على تطبيق القانون الجزائري على جميع الجرائم المرتكبة على أراضي

161 - عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية - دراسة مقارنة، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، الأردن، 2014، ص 96.

الجمهورية¹⁶². وبالتالي، فإن أي فعل يُعد جريمة ترتبط بتكنولوجيا الإعلام والاتصال يرتكب داخل حدود الدولة الجزائرية يجعل مقترفها- سواء أكان جزائرياً أم أجنبياً- خاضعاً للعقوبة وفقاً للقانون الجزائري. وتدعيماً لهذا المبدأ، نجد المشرع الجزائري قد أفرد نصوص المواد 335 - 342 من قانون الإجراءات الجزائية لسنة 2025، الذي يحدد كل من الاختصاص الإقليمي والنوعي في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المطلب الثاني: الصعوبات التقنية والعملية للتحريات الالكترونية

تواجه التحريات الإلكترونية تحديات متنامية نتيجة لتعقيد التقنيات الحديثة، لا سيما مع التوسع في استخدام وسائل التشفير وأساليب إخفاء الهوية، بالإضافة إلى التعقيدات التي تفرضها معاملات العملات الرقمية وصعوبة تتبعها. وهذا يستدعي من الجهات المختصة العمل على تطوير أدواتها وابتكار أساليب جديدة تواكب هذه التحولات، لضمان كفاءة وفعالية عمليات التحري. سنوضح في هذا المطلب أهم الصعوبات التي تواجه التحريات الالكترونية.

الفرع الأول: الصعوبات التقنية للتحريات الالكترونية

إذا كانت البيئة الرقمية قد منحت جهات التحقيق آليات مستحدثة لتعقب الجريمة، فإنها في الوقت ذاته فرضت عقبات وتحديات تقنية معقدة تحد من فاعلية هذه الإجراءات. وتأسيساً على ذلك، نخصص هذا الفرع لأبرز الصعوبات التقنية التي تواجه مصالح الضبطية القضائية أثناء مباشرة التحريات الإلكترونية.

أولاً: صعوبة اكتشاف الجريمة المعلوماتية: الجرائم المرتبطة باستخدام الإنترنت تمتاز بكونها خفية ومعقدة في غالب الأحيان، حيث يصعب على الضحية اكتشافها، رغم احتمال وقوعها أثناء تواجده على الشبكة. كما أن مرتكب الجريمة غالباً ما يمتلك مهارات تقنية عالية تسهم في تنفيذ جريمته بدقة وإخفاءها. مثال عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الجرائم¹⁶³.

كما أن وسيلة تنفيذها تتميز بالطابع الفني الذي يضيف عليها الكثير من التعقيد. بالإضافة إلى عدم الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقدان عملائهم، فضلاً عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة ثانية واحدة¹⁶⁴.

162 - تنص المادة 3 من قانون العقوبات المعدل والمتمم، على أنه: "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية".

كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في إختصاص المحاكم الجزائرية الجزائية طبقاً لأحكام قانون الإجراءات الجزائية".

163 - محمد عبيد الكعبي، "الجرائم الناشئة عن الاستعمال غير المشروع لشبكة الإنترنت"، دار النهضة العربية، القاهرة- مصر، 2007، ص 29.

164 - نهال عبد القادر المومني، "الجرائم المعلوماتية"، دار الثقافة للنشر والتوزيع، ط1، عمان، 2008، ص 54.

ثانيا: صعوبة إثبات الجريمة الإلكترونية: تقع الجريمة الإلكترونية في بيئة غير تقليدية، حيث تتجاوز إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة. ونظرا لما تتطلبه هذه الجرائم من تقنيات لارتكابها، فهي تستلزم أسلوبا خاصا في التحقيق والتعامل، الأمر الذي قد لا يتحقق بالقدر الكافي في بعض الجهات الأمنية والقضائية نظرا لنقص المعارف التقنية، وهو ما يتطلب تخصصا دقيقا لتحسين كفاءة الجهاز الأمني والقضائي في مواجهة هذه الظاهرة.

حيث لم تعد القوانين التقليدية قادرة على مواكبة السرعة الهائلة في التطور التكنولوجي الذي أدى إلى ظهور جرائم مستحدثة، وباتت النصوص القانونية الكلاسيكية عاجزة عن استيعابها أو مواجهتها، مما يشكل عائقا أساسيا أمام إثبات الجريمة المعلوماتية¹⁶⁵.

ثالثا: أسلوب ارتكاب الجريمة الإلكترونية: الجرائم الإلكترونية هي جرائم "هادئة"، تحتاج إلى قدرة علمية وفنية في التعامل مع جهاز الحاسوب وشبكة المعلومات الدولية (**الإنترنت**)، بما في ذلك إتقان تقنيات ارتكاب هذه الجرائم، كالاختراق سواء عن طريق استغلال ثغرات نظام التشغيل، أو استخدام البرمجيات الخبيثة، أو عن طريق كسر وسرقة كلمات السر. كما ظهرت تقنيات متطورة مثل تقنية "السلامي" (**Salami Technique**)، أو "حصان طروادة" (**Trojan Horse**) في ارتكاب عمليات الاختلاس المالي، وغيرها من الأساليب التقنية التي أفرزتها التكنولوجيا الحديثة¹⁶⁶.

الفرع الثاني: الصعوبات العملية للتحريات الإلكترونية

بالإضافة إلى التحديات التقنية البحتة، تواجه جهات التحقيق والبحث الجنائي مجموعة من الصعوبات العملية والميدانية التي تعيق سرعة الكشف عن الجرائم المعلوماتية وتحديد المتورطين فيها. بناءً على ذلك، سنوضح في هذا الفرع العقبات العملية التي تواجه أجهزة الضبط القضائي في الميدان.

أولاً: التعاون والتواطؤ على الأضرار: وهو أكثر تكرارا في الجرائم الإلكترونية عنه في الأنماط الأخرى للجرائم الخاصة، أو "جرائم أصحاب الياقات البيضاء"، وهم ذوو المناصب الرفيعة المستوى في الإدارات، وغالبا ما يكون متضمنا فيها متخصص في الحسابات يقوم بالجانب الفني في المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة (المجني عليها) لتغطية عملية التلاعب وتحويل المكاسب إليه، كما أنه من عادة من يمارس التلاعب بالحسابات تبادل المعلومات بصفة منتظمة حول أنشطتهم الإجرامية¹⁶⁷.

165 - محمد عبيد الكعبي، المرجع السابق، ص 40.

166 - عائشة بن قارة مصطفى، المرجع السابق، ص 44.

167 - إبراهيم الدسوقي عطية، الحماية الجنائية للمعلوماتية: دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2008، ص 769.

ثانياً: أعراض النخبة: يعتقد بعض المتخصصين في تقنية الحاسبات والإلكترونيات أن من مزايا مراكزهم الوظيفية ومهاراتهم الفنية، استخدام الحاسبات وبرامجها لأغراض شخصية، أو ممارسة بعض الهوايات الرائدة في فلك هذه التقنية، وهو ما يُعبر عنه بـ "أعراض النخبة"، ومن شأن ذلك تمادي بعضهم في استخدام نظم الحاسب بصورة غير مشروعة تصل إلى حد ارتكاب الجرائم الخطيرة¹⁶⁸.

ثالثاً: الأضرار: تقع الجرائم الإلكترونية في نطاق تقنية متقدمة يتزايد يوماً بعد يوم استخدامها في إدارة المعاملات الاقتصادية والمالية -الوطنية والدولية- والاعتماد عليها في تسيير معظم الشؤون العامة لأكثر الحكومات بما في ذلك الأمن والدفاع، ومن شأن ذلك أن يضيف أبعاداً غير مسبوقة على الخسائر والأضرار التي تنجم عن هذه الجرائم. والأدلة على ذلك أن حجم الخسائر المادية الناجمة عن هذه الجرائم يبلغ -وفقاً لتقديرات المركز الوطني لجرائم الحاسب في الولايات المتحدة الأمريكية- (N.C.C.D.C) في نهاية القرن الماضي حوالي 555 مليون دولار في السنة¹⁶⁹.

رابعاً: الصفة الدولية للجريمة المعلوماتية: يمكن اعتبار أن من أبرز السمات المميزة للجريمة الإلكترونية قدرتها على تخطي الحدود الجغرافية، مما يمنحها طابعاً دولياً بطبيعتها. بل إن هناك من يرى أنها جريمة ذات طبيعة عابرة للحدود. فمع التطور الكبير في شبكات المعلومات، لم تعد هناك حدود ملموسة أو مرئية تعيق انتقال البيانات بين الدول. وهذا يعود إلى الإمكانيات الهائلة التي توفرها الأنظمة الإلكترونية، حيث يمكنها نقل كميات ضخمة من المعلومات بين أجهزة تفصل بينها آلاف الأميال. ونتيجة لذلك، أصبحت الجرائم الإلكترونية قادرة على التأثير في عدة دول بشكل متزامن.

تتجلى هذه الإشكالية بشكل خاص في القطاع المصرفي، إذ أسفر الانتشار الواسع للمعاملات البنكية عبر الشبكات الدولية عن تصاعد ملحوظ في جرائم الاحتيال المرتبطة بالمعلوماتية. ويمكن أن يقوم الجاني الموجود في دولة معينة باختراق نظام إلكتروني في دولة أخرى بهدف ارتكاب جريمة تؤثر على شخص أو جهة في دولة ثالثة، كما يحدث في حالات الاحتيال الإلكتروني.

ومن القضايا الهامة ذات البعد الدولي للجرائم الإلكترونية نذكر قضية "نقص المناعة المكتسبة" ("الإيدز")، وتتلخص وقائعها في أنه عام 1989 قام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج، الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرضى نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس) من أمثلة حضان طروادة. حيث كان يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلي عن

¹⁶⁸ - Jack Bologna, Corporate Fraud: The Basics of Prevention and Detection, Butterworth-Heinemann, 1984, p. 11.

¹⁶⁹ - Martin Wasik, "Computer Crimes and Other Crimes Against Information Technology in the United Kingdom", Revue Internationale de Droit Pénal (R.I.D.P), 1991, p19.

العمل، ثم تظهر بعد ذلك على الشاشة عبارة يقوم الفاعل من خلالها بطلب مبلغ من المال يُرسل إلى عنوان في دولة "بنما" حتى يتمكن المجني عليه من الحصول على مضاد للفيروس. وفي عام 1990 تم إلقاء القبض على المتهم ويدعى "جوزيف بوب (Joseph Popp)" في ولاية "أوهايو" بالولايات المتحدة الأمريكية، وطلبت بريطانيا تسليمه لمحاكمته أمام القضاء الإنجليزي، وقد وافق القضاء الأمريكي على ذلك. وتظهر أهمية هذه القضية من ناحيتين :

الأولى: أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية.

الثانية: أنها المرة الأولى التي يُقدم فيها شخص للمحاكمة بتهمة إعداد فيروس¹⁷⁰.

المطلب الثالث: التحديات القانونية لاستخدام الذكاء الاصطناعي في التحريات الإلكترونية

إنه لمن الضروري توظيف تقنيات الذكاء الاصطناعي في تحليل البيانات، لما لها من دور في تحسين أداء جهاز الشرطة والعمل على تقديم أدلة جزائية جديدة تتسم بالدقة والموضوعية والثقة، مما يحقق نوعاً من الحماية الجزائية على نحو من شأنه أن يحسن من أداء نظام العدالة الجزائية، كما يمكن أن يتم الاستعانة به في تعزيز الرفاهية الاقتصادية والاجتماعية وممارسة حقوق الإنسان¹⁷¹، إلا أن الاستعانة الآمنة والقانونية بهذه التقنيات لم يخلُ من الإشكاليات، وبالتالي كان متاحاً كمنفذ على أيدي بعض المتخصصين في العقول الإنسانية وبعيدا عن حالة الحدس التي نالها الذكاء الاصطناعي بمحاولة تحديد طبيعته¹⁷²، وتأسيس المسؤولية المدنية والجزائية بتطبيقاته.

غير أن إشكاليات البحث في استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في البحث عن الجرائم ومحاولة الكشف عن مرتكبيها أو التنبؤ بها من جانب آخر، تتمثل في بعض الإشكاليات المتعلقة بحماية خصوصية الأفراد وحرمة حياتهم الخاصة، بما في ذلك حرمة بياناتهم الشخصية¹⁷³. وهو ما يطرح تساؤلات كثيرة بشأن الدولة لاستخدام البيانات المخزنة لديها للأغراض الأمنية أو القانونية، وكذلك حق الأفراد في محو بياناتهم الشخصية عقب استخدامها لأغراض معينة، فضلا عن إشكالية أخرى لا تقل أهمية عن سابقتها، وهي ما يتعلق بالأدلة الجنائية المستنبطة أو المستخلصة من تقنيات الذكاء الاصطناعي وتحليل البيانات.

الفرع الأول: الإشكاليات المتعلقة بالخصوصية وحماية البيانات

¹⁷⁰ - نائلة عادل فريد قورة، جرائم الحاسب الاقتصادية-دراسة نظرية تطبيقية، منشورات الحلبي القانونية بيروت-لبنان، 2005، ص 48.

¹⁷¹ - Kelley M. Saylor, *Artificial Intelligence and National Security*, CRS Report No. R45178, Congressional Research Service, Washington, D.C., Updated November 10, 2020, p.1

¹⁷² - محمود سلامة عبد المنعم الشريف، النظرية العامة للأدلة العلمية في المواد الجنائية: دراسة مقارنة، دار النهضة العربية، القاهرة-مصر، 2012، ص 45.

¹⁷³ - محمد عرفان الخطيب، "المسؤولية المدنية والذكاء الاصطناعي... إمكانية المساءلة؟ دراسة تحليلية معمقة بقواعد المسؤولية المدنية في القانون المدني الفرنسي"، مجلة كلية الحقوق الكويتية العالمية، المجلد 8، العدد 29، مارس 2020، ص 1.

إن تأثير الذكاء الاصطناعي قد مس الاعتماد على البيانات الحديثة وتفاصيل الحياة الخاصة للأفراد ومراقبتهم في جزء كبير منه، مما يسمح بشكل كبير في اختراق الخصوصية وسرية البيانات¹⁷⁴. وفيما يتعلق باستخدام تقنيات الذكاء الاصطناعي في الكشف عن الجرائم ومرتكبيها والتنبؤ المستقبلي بالجريمة، فإن هذا الاستخدام يتمخض عن إشكاليتين أساسيتين الأولى: تتعلق بتعارض هذا الاستخدام مع الحماية المقررة للحق في الخصوصية وحرمة الحياة الخاصة بالأفراد، والثانية: تتعلق بتعارض هذا الاستخدام مع الحق في حماية البيانات الشخصية للأفراد.

أولاً: التعارض مع الحق في الخصوصية وحرمة الحياة الخاصة: يُشكل الحق في الخصوصية وحرمة الحياة الخاصة إشكالية قانونية تتصل بشخصية الإنسان، وتقوم فكرة الحق على حماية الجانب غير العلني من حياة الإنسان من جانب حمائي شامل، ويقابل هذا الحق واجب الاحترام من قبل السلطات العامة للدولة والأفراد، ويقتضي في الوقت نفسه أن تكفل له الدولة الحماية الدستورية والقانونية مواجهة أي انتهاك غير مشروع.

وقد كان يقصد بهذا الحق ببدايته وجوب احترام الخصوصية المادية للإنسان بهدف توفير حماية للكيان المادي والممتلكات، لكن هذا المفهوم توسع بشكل كبير ليشمل الجوانب المعنوية كالأفكار والمشاعر والأحرار والمعلومات الشخصية¹⁷⁵.

يُثير استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم ومرتكبيها والتنبؤ بها إشكالية هامة وخطيرة تتعلق بتعارض هذا الاستخدام مع الحماية القانونية المقررة للحق في الخصوصية وحرمة الحياة الخاصة للأفراد، ومقتضى ذلك أن تطبيقات الذكاء الاصطناعي تخلو من الجانب القانوني والأخلاقي والقيمي، الذي يحد من جانب الحماية المقررة للخصوصية وحرمة حياة الأفراد الخاصة، فأنظمة الذكاء الاصطناعي التي تطبق تقنيات التعلم الآلي من الإحصائيات للعثور على أنماط كبيرة من البيانات وأجراء تنبأت مستقبلية.

بناءً على تلك الأنماط والتحليلات، عادة ما يتغير المنطق القانوني والأخلاقي وتفسير التعارض بين استخدام هذه التقنيات مع الحق في الخصوصية، والحق في حرمة الحياة الخاصة، وذلك يظهر في عدة جوانب:

أ- يعتمد البحث في تقنيات الذكاء الاصطناعي وتحليل البيانات في جانب كبير منه على متابعة ومراقبة أنشطة الأفراد، وذلك من خلال تتبع الشخص ومراقبة حركته ورصد أي تغييرات تطرأ على حياته بصفة عامة، ويتم ذلك دون الحصول على موافقة الشخص أو علمه، وهو ما يشكل انتهاكاً لحرمة الحياة الخاصة للأفراد. وحتى في حالة علم الأشخاص باستخدام ما يقومون به من أفعال وتحركات في الحصول على معلومات عنهم، فإنهم وبلا شك يرفضون هذه القيود التي تفرض عليهم إلكترونياً. وفي حال حصول السلطات على الموافقة على إتمام المتابعة

174 - يُعد الحق في حرمة الحياة الخاصة من الحقوق الدستورية الأصلية التي حرصت دساتير الدول المختلفة على كفالتها، والنص على صيانة حمايتها من أي انتهاك. وتبدو الحماية القانونية لهذا الحق ملحة بشكل خاص في مواجهة التقدم التكنولوجي المتسارع الذي بات يهدد الحرية الشخصية للإنسان.

175 - محمد نجيب حسني، شرح قانون الإجراءات الجنائية، ط3، دار النهضة العربية، مصر، 1990، ص676

والمراقبة، فإن الفرد سيغير من سلوكه التلقائي الذي يمكن أن يكشف عن حقيقة نواياه وأفكاره، مما يؤدي إلى فقدان قيمة المعلومات الناتجة عن تحليل البيانات التي تم الحصول عليها وتخزينها، ويترتب على ذلك تفرغ هذه الوسائل من محتواها ومضمونها.

ويظهر ذلك بصفة خاصة من خلال ما أشرنا إليه سابقاً من مفهوم "الشرطة التنبؤية" (Predictive Policing)، ووسائل تحليل بيانات الأفراد وتحركاتهم لرصد التغيرات التي تطرأ داخل المجتمع. على سبيل المثال: تستخدم الأجهزة الأمنية للوصول إلى ما تحتاج إليه من تنبؤات وإحصاءات، إضافة إلى تحليل ما يقوم به الأفراد من تحركات ولقاءات وغيرها، والتي ترصدها شبكات التواصل الاجتماعي بشكل تلقائي. كما يمكن للأجهزة الأمنية أن تستخدم معلومات هذه الشبكات في التوصل إلى نتائج كثيرة تتعلق بالرأي العام إتجاه قضية معينة. ولا يتأتى ذلك إلا نتيجة تحليل التفاعلات التلقائية للأفراد مع القضايا المعروضة للرأي العام، أو الحوادث المجتمعية التي يتناولها أفراد المجتمع بالتحليل والمناقشة¹⁷⁶.

على الرغم من أن هذه التحليلات قد تقدم نتائج موثوقة ودقيقة لأنها تعتمد على بيانات ومعلومات تلقائية يشاركها الأفراد أثناء تفاعلهم العفوي عبر المنصات الرقمية مثل: فيسبوك، انستغرام وإكس، فإن هناك احتمالاً لحدوث تلاعب أو استغلال موجه لهذه البيانات في سياق قضايا معينة. ويمكن أن يتجسد ذلك في تقييد التلقائية المفترضة في تلك النقاشات بهدف تشكيل توجهات الرأي العام بطرق محددة. هذا الأمر قد يؤدي إلى خروج نتائج منحرفة عن الواقع، ما ينعكس بدوره على كيفية تعامل سلطات الضبط الإداري داخل الدولة. وتبرز خطورة هذه الممارسات بشكل أكثر وضوحاً عندما يُنظر إلى الدور المتزايد لكاميرات المراقبة المنتشرة بشكل كبير في الأماكن العامة والخاصة. فبدلاً من اقتصار هدف هذه الأجهزة على كشف الجرائم، أصبحت تشكل تهديداً كبيراً لخصوصية الأفراد بسبب العدد الهائل منها والإمكانات التقنية التي تدعمها. ومن الجدير بالذكر أن التطورات الأخيرة في هذا المجال قد أدت إلى ظهور برامج متقدمة تخلّ الكاميرات الإبلاغ عن الأشخاص بناءً فقط على قيامهم بأفعال تُعتبر مشبوهة أو تخضع للتفسير الخاص من قبل النظام.

أضف إلى ذلك آليات التعرف على الوجه (Face Recognition)، التي استحدثتها وسائل التواصل الاجتماعي، والتي يمكن من خلالها تتبع الأشخاص ومراقبة تحركاتهم. وفي حين أن هذه التقنيات تكون مفيدة بشكل كبير للشرطة في عملها، إلا أنها تبدو إجراءات غير قانونية في كثير من الأحيان، كما أنها تُستخدم في أحيان كثيرة باعتبارها معصومة من الخطأ، وهو ما يهدد الحق في هذه الحساسية بشكل كبير¹⁷⁷.

¹⁷⁶ - رزق سعد علي، "استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم"، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات - مصر، المجلد 9، العدد 3، سبتمبر 2023، ص 1626.

¹⁷⁷ -David a Fahrenthold on pig way in small towers, www.Washington post, January 22;2016.

ب- يعتمد الذكاء الاصطناعي وتحليل البيانات في مجال الكشف عن الجريمة والتنبؤ باحتمالية وقوعها مستقبلا على بيانات تتعلق بالحمض النووي (DNA) للأشخاص والصفات الوراثية التي تميزهم عن غيرهم. ولا يتسنى للأجهزة الأمنية التوصل لهذه الصفات أو الجينات إلا باستخدام العنصر البشري في الحصول عليها أو المواد الصخرية لإجراء تحليل الدم، الأنسجة، واللعاب...، وإدخال هذه المواد محل الضبط لمعرفة الحمض النووي (DNA) للحالة، مما يسهل على أجهزة الضبط الاستدلال والوصول إلى صاحب الحمض النووي محل الاتهام. وتثير هذه المسألة عدة مخاطر:

1- الاعتماد على العنصر البشري: قد يؤدي ذلك إلى نتائج مضللة وغير صحيحة، فعند ضبط جريمة ما دون التوصل لفاعلها، وقيام سلطات الضبط بالحصول على أي دليل بيولوجي في مسرح الجريمة، فنقطة الدم أو لعاب الفاعل أو بقعة مني أو نسيج من جلد الجاني، تعتبر أجزاء بيولوجية وتخضع للفحص الدقيق من أجل الوصول إلى الحمض النووي للجاني، وذلك من خلال قيام المختص سواء كان كيميائيا أو شخصا له خبرة معينة لإدخال معطيات هذه المضبوطات للفحص، بحيث يهتدي إلى التابع الخاص بالبصمة الوراثية أو الحمض النووي، لكن تساؤلات تقوم في حين أن هذه التكنولوجيا تكون أداة رائعة للقبض على الأفراد المطلوبين، إلا أننا يجب أن نتذكر في ذات الوقت أن الكمبيوتر يحتوي على سجل لتحركات ملايين الأشخاص الأبرياء، مما يثير القلق بالاستخدام هذه الآليات الحديث، بشأن قيام هذا الشخص باستبدال العينة المضبوطة بغيرها، أو التلاعب بها عن إهمال أو دون قصد. فلا شك أن ذلك يؤدي إلى نتائج مغايرة تماما للنتيجة السليمة، وهو ما يتطلب الحيلة والحذر عند استخراج الحمض النووي، وأن تكون عملية الاستخلاص محاطة بهالة من الضمانات القانونية والشرعية التي تؤكد على صدق النتائج التي تنتهي إليها عملية تحليل الحمض النووي والجينات الوراثية. وقد رصدت بعض التقارير أن النتائج التي يذهب إليها تطبيق هذه التقنيات قد تتعارض مع الواقع، فعلى الرغم من أن الخوارزميات تنتشر بشكل واسع جدا، إلا أنها ليست منزهة من الخطأ حيث كشف تقرير حول مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل أن ضعف البيانات المخزنة في الخوارزميات مؤشر خطير ينعكس بالضرورة على النتائج التي تنتهي إليها¹⁷⁸.

2- التهديدات المتعلقة بالخصوصية الجينية: على الرغم من أهمية التحليل الجيني في خدمة العدالة الجزائية، بصفة خاصة في سرعة التوصل إلى الجناة وتحديد هويتهم تمهيدا لملاحقتهم، وهو ما يضمن أداء القانون الجزائي والقضاء الجزائي دوره بفاعلية، مما ينعكس إيجابا على حسن إدارة العدالة الجزائية¹⁷⁹، إلا أن الأمر لا يخلو من الصعوبات إذ ينطوي البحث بالضرورة

¹⁷⁸ - عماد عبد الرحيم الدحيات، "نحو تنظيم قانوني للذكاء الاصطناعي في حياتنا: إشكالية العلاقة بين البشر والآلة"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي لتأمنغست-الجزائر، المجلد 08، العدد 05، ديسمبر 2019، ص 14-31.
¹⁷⁹ - عبد الفتاح فرحات الجبالي، "المسؤولية المدنية والذكاء الاصطناعي: إمكانية المساءلة (دراسة تحليلية في ضوء قواعد المسؤولية المدنية في القانون المدني الفرنسي)"، مجلة كلية القانون الكويتية العالمية، الكويت، المجلد 8، العدد 1، مارس 2020.

على إخضاع شخص معين للفحص الجيني والحصول على عينة جينية جبرا عنه وتحليلها، وهو ما سيتبع الحصول على قدر كبير من المعلومات حول الشخص بشكل إجباري، وهو ما يشكل انتهاكا لحق الشخص للخصوصية الجينية من ناحية وإهدار حقوق الإنسان بصفة عامة من ناحية أخرى، وتثير هذه الحالة العديد من التساؤلات المتعلقة بالضمانات التي يكفلها القانون للشخص في حالة خضوعه للفحص الجيني الإجباري¹⁸⁰.

3- التهديدات المتعلقة بالحرية الفردية: إن الإجراءات التي تتبعها أجهزة الضبط الإداري والقضائي للحصول على البصمات الوراثية للأفراد بصفة عامة بغية التوصل إلى صاحب البصمة المعروفة أو المضبوطة في مسرح الجريمة¹⁸¹، عادة ما تحمل الكثير من التجاوزات في حق الأبرياء فهذه الحملات وإن كانت غايتها نبيلة، وهي تتمثل في حل اللغز في جريمة خطيرة ومعقدة ومروعة، إلا أنها تبدأ بأفضل النوايا وتنتهي دائماً بانتهاك الحقوق الفردية، فانضباط المكيفون بضبط صاحب البصمة الوراثية المضبوطة لن تحدهم أية حدود في البحث عنها فهم يشعرون بواجب ديني تقريبا لحل لغز الجريمة وهو ما يؤدي دائما إلى الاعتداء على الحقوق الشخصية، وقد أثار بعض الباحثين القانونيين إلى ضرورة المطالبة بسجل وطني للحمض النووي لكل مواطن كطريقة مثالية للقبض على المجرمين وإبعادهم عن الشارع¹⁸²، على أن يتقدم كل مواطن بشكل طوعي للحصول منه على الحمض النووي تمهيدا لحفظها داخل بنوك المعلومات، فينعكس ذلك بشكل كبير على معدلات الجريمة داخل أي مجتمع، ومن المحتمل أن يُثني الكثيرين عن ارتكاب الجرائم لكن هذه الفكرة تبدو محفوفة بالمخاطر، لاسيما إذا نظرنا إلى حماية سلك البيانات وكفالة عدم وصول الشركات لديها لاستخدامها في أغراض جزائية أو ربحية أو غيرها.

ثانيا: تعارض التحريات الالكترونية مع الحق في حماية البيانات الشخصية للأفراد: تشهد العديد من المعاملات التي يجريها الأفراد على أهمية وحيوية البيانات الشخصية، فالعديد من المعاملات تتم من خلال سلك البيانات، وهذه البيانات الشخصية يتم تخزينها ومعالجتها بطريقة تسهل استحضارها والاستعانة بها في العديد من العمليات الاستدلالية، فعلى مستوى الشركات التجارية مثلا تستطيع الشركات الرائدة في مجال المعلومات باستخدام تلك البيانات لعملائها في الاستدلال عن حجم مبيعاتها ونوع الطلب على منتجاتها، والأماكن التي تطلب فيها تلك المنتجات كثيرا على مستوى الدول والحكومات، كما تستطيع أن تستخدم بيانات المواطنين لديها والمقيمين

¹⁸⁰ -Zalnieriute, et al., The Rule of Law and Automation of Government DecisionMaking, Modern Law Review 82. 2019

¹⁸¹ -Mangani D, 5 AI Application I Banking to Look out for in Next 5 Years, available at:

[https://www.analyticsvidhya.com/blog/2017/04/5-ai-applicationsin-banking-to-lookoutfor-in-next-5-years/\(18/07/2021](https://www.analyticsvidhya.com/blog/2017/04/5-ai-applicationsin-banking-to-lookoutfor-in-next-5-years/(18/07/2021)
at 11h.02) .

¹⁸² - زين الهوشي, عندما يرتكب الذكاء الاصطناعي الجرائم, من يتحمل العقوبة؟ مقال منشور ,شاهد يوم 2021\08\03

في معرفة الرأي العام وتوجيهه، هذا، وتستطيع أيضا استخدام تلك البيانات في استخلاص نتائج مفيدة عن حالة الأشخاص وعلاقاتهم¹⁸³.

تشكل الثورة التكنولوجية الحالية في مجال معالجة البيانات الشخصية للأفراد خطرا كبيرا بالنظر إلى الآثار السلبية التي يمكن أن تترتب عليها، وقد بدت أهم مظاهر هذه السلبية في اختراق النظم الأمنية لحماية البيانات المخزنة داخل الوسائل الإلكترونية، مما قد يهدد بإتلاف أو تخزين البرمجيات التي تحتوي هذه البيانات والمعلومات أو انتهاك حرمة الحياة الخاصة للأفراد، وهو ما يهدد حقوق الإنسان بصفة خاصة إذ لم يتم استخدام البيانات وتوظيفها في إطار أخلاقي وقانوني، وقد يقود ذلك إلى رفض اجتماعي باستخدام تلك البيانات والاستفادة منها.

قد حرصت المواثيق الدولية والدساتير المختلفة على تضليل نصوص المواد التي تكفل حماية البيانات الشخصية للأفراد وعدم تداولها أو انتهاكها أو استخدامها لأغراض تخالف الغرض الأساسي الذي جمعت من أجله¹⁸⁴.

يمكن أن تستخدم تقنيات الذكاء الاصطناعي في تحليل البيانات في جانب كبير من عمل التحريات باستخدام البيانات الشخصية للأفراد، حيث تستخدم هذه البيانات في الاستدلال على مواقف الأفراد وسلوكياتهم المختلفة، وتتمثل هذه التقنيات في التنبؤ بما سيقوم به الأفراد في المستقبل القريب، وذلك اعتمادا على ما يتوافر من بيانات شخصية. كما تستطيع تقنيات الذكاء الاصطناعي والتطبيقات، تحليل البيانات الشخصية من مصادر متعددة حيث نجد في مواقع الانترنت ووسائل التواصل الاجتماعي مصدرا زائرا بالبيانات التي يقدمها الأفراد بشكل مجاني عند الحصول على أي تطبيق أو برنامج، علاوة على البيانات الحكومية والتي يقدمها الأفراد عند طلبهم أي خدمة من مؤسسات الدولة وذلك عند خضوعهم للتحقيق أو العقوبات، ولا شك أن لهذه البيانات قيمة كبيرة في تحديد التعامل مع الأفراد¹⁸⁵.

الفرع الثاني: إشكاليات اعتماد الدليل الجنائي المستمد من الذكاء الاصطناعي

يحتل الإثبات الجنائي أهمية خاصة في الخصوصية الجنائية، ويقوم على مجموعة الأدلة التي تؤكد وجود الحق أو تنفيه، وغم وجود حرية في الإثبات للوصول إلى الدليل، إلا أن هذه الحرية يجب أن تُمارس في إطار قانوني يمثل شرطا لقبول الدليل في الإدانة. وعلى كل حال فإن جميع الأدلة متروكة تقديرها للاقتناع الشخصي للقاضي الجزائي وذلك في حدود القانون¹⁸⁶.

تنقسم الأدلة بحسب علاقتها بالواقعة المراد إثباتها إلى أدلة مباشرة وأخرى غير مباشرة، وتعد الأدلة مباشرة إذا نصت على الواقعة مباشرة بحيث لا تحتاج إلى اجتهاد عقلي أو تأمل أو

¹⁸³ - العزاوي لمى عبد الباقي محمود، حاتم دعاء جليل، " الذكاء الصناعي والمسؤولية الجنائية الدولية"، مجلة /المفكر، كلية الحقوق والعلوم السياسية - جامعة محمد خيضر-بسكرة، الجزائر، المجلد 14، العدد 1، 2019.

¹⁸⁴ - Odile Siary, 2017, Quelle personnalité juridique pour les ROBOTS, article Village de la justice , site web village-justice.com. vu janvier 2020.

¹⁸⁵ - ذكاء الاصطناعي، مقال منشور، شوهه يوم 08\03\2021 على الساعة 14:32 على موقع [\https://ar.wikipedia.org/wiki](https://ar.wikipedia.org/wiki)

¹⁸⁶ - الذكاء الاصطناعي، والية عمله، مقال شوهه بتاريخ تعرف على تاريخ 01\09\2021 على الساعة 13:23 على موقع <https://technologyreview.ae>

استنتاج من جانب القاضي، بينما تحتاج الأدلة غير المباشرة إلى عملية ذهنية يباشرها العقل بواسطة المنطق. وقد استقر قضاء محكمة النقض على جواز استعانة المحكمة المختصة بدليل غير مباشر، طالما كان من شأنه أن يؤدي إلى الحقيقة بعملية تجريها المحكمة¹⁸⁷.

إذا تساهم تقنيات الذكاء الاصطناعي وتحليل البيانات -بالمفاهيم السابقة- بالتوصل إلى أدلة الجريمة بالإثبات أو النفي، وبإمكان جهات إنفاذ القانون أن تستعين بما في عملها حال وقوع الجريمة سواء في المراحل السابقة على تحريك الدعوى العمومية أو في إطار الدعوى العمومية، كما يجوز استخدامها للتنبؤ بالسلوك الإجرامي مما يعزز من فرصة منع الجريمة قبل ارتكابها وفرض بعض التدابير الوقائية.

أولاً: أطر الاستعانة بالأدلة المستخلصة بواسطة الذكاء الاصطناعي: تنقسم إجراءات الخصوصية الجزائية إلى قسمين، أولهما: الإجراءات الأولية السابقة على تحريك الدعوى العمومية، وثانيها: إجراءات الدعوى العمومية، والتي تبدأ بتحريكها بمعرفة الجهة المختصة. وترمي بعض هذه الإجراءات إلى التنقيب عن أدلة الجريمة ويستهدف بعضها الآخر الاحتياط من فرار المتهم أو إفساده الأدلة المتحصلة، وتعتبر مرحلة جمع الأدلة وفحصها والتأكد من نسبتها للمتهم¹⁸⁸.

أ- الاستعانة بتقنيات الذكاء الاصطناعي في مرحلة جمع الاستدلالات: تستهدف أعمال الاستدلال جمع المعلومات عن الجريمة ومرتكيها لتقديمه إلى سلطة التحقيق المختصة لاتخاذ قرار بشأنها، ولأعمال الاستدلال أهمية كبيرة¹⁸⁹، حيث يكون ممثل النيابة العامة هو أول من يصل إلى مكان ارتكاب الجريمة فيتخذ الإجراءات اللازمة للمحافظة على الأدلة فضلاً عن سؤال المتهم وضبطه، وتتميز أعمال الاستدلال بأنها تُثير الطريق لسلطة التحقيق بما تقدمه إليها من معلومات تفيد في كشف الحقيقة، فتستطيع سلطة التحقيق أن تتخذ القرار الملائم في شأن الدعوى العمومية، كما أن لهذه المرحلة أهميتها في توفير مرحلة المحاكمة الجزائية من خلال التمهيد لنظام التصالح¹⁹⁰. يحكم أعمال الاستدلال قاعدة أساسية مفادها أنه لا يصح اتخاذ أي إجراء ينطوي على تقييد حريات الأفراد أو المساس بحقوقهم الشخصية، يشير بعض الفقه إلى أن الواقع يشهد انطواء هذه المرحلة في الغالب على إجراءات تمس الحرية الفردية¹⁹¹، حيث يفترض خلو هذه المرحلة من صفتي الجبر والإكراه التي تنسم بها مرحلة التحقيق الأولية¹⁹².

187 - تأثير الذكاء الاصطناعي في سباق التسلح لمقال شوهده بتاريخ 2021\08\23 على الساعة 14:57 على موقع <https://futureuae.com/ar/home/index/2>

188 - ما هي استخدامات الذكاء الاصطناعي في التحقيقات ؟ مقال شوهده 2021\08\25 على الساعة 15:38 على الموقع <https://wikipedia.org/wiki>

189 - الخطر الوجودي من الذكاء الاصطناعي العام، مقال شوهده يوم 2021\08\29 على الساعة 13:32 <https://ar.org/wiki>

190 - الموقع الإلكتروني لمركز الذكاء الاصطناعي على الواب <https://skailab2021.univ-skikda.dz/index.php> موقع المدرسة الوطنية العليا للذكاء الاصطناعي على الواب: <https://services.mesrs.dz/ensia/rtl/index>

191 - F. Patrick Hubbard, 'Sophisticated Robots': Balancing Liability, Regulation, and Innovation, 66 Florida Law Review, 2014

192 - Fintechnews Singapore, the Potential of AI in Banking, available at: <http://fintechnews.sg/27160/ai/the-potential-of-ai-in-banking-report/> (15/07/2021 at 17h.00)

تبنّت سلطات الاستدلال في العديد من دول العالم المتقدمة فكرة استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم وتتبع مرتكبيها، كما استطاعت أجهزة الضبط في بعض الدول تقديم ما يسمى خرائط التنبؤ بالجريمة بواسطة الهواتف اللوحية ومكنها ذلك من توقع ارتكاب الجريمة والتنبؤ بها، ومن ثم معالجتها بإجراءات استباقية تتبعها الشرطة في موقع الحدث بحثاً عن الجريمة¹⁹³.

ب- الاستعانة بتقنيات الذكاء الاصطناعي في مرحلة التحقيق: تتسم إجراءات التحقيق الابتدائي بالأهمية والخطورة في الوقت نفسه، إذ تهدف إلى تحديد مدى توافر مبرر تقديم المتهم إلى المحاكمة الجزائية لإقرار الحق في العقاب أو نفيه، وهذا أمر يتوقف على إثبات وقوع الجريمة ونسبتها للمتهم. تبدو أهمية مرحلة التحقيق الابتدائي من عدة نواحي، فهي تؤدي إلى تحضير الدعوى العمومية وتحديد مدى قابليتها للنظر أمام قضاء الحكم، كما يتاح فيها جمع الأدلة قبل ضياعها. وتتجلى خطورة إجراءات التحقيق فيما تنطوي عليه من إجراءات تمس بحرية المتهم وكذلك الحاجة الملحة لتحقيق قدر من التوازن بين حق الدولة في العقاب وما تقتضيه من إتخاذ بعض الإجراءات الماسة بحرية المتهم، وحق هذا الأخير في ضمان حريته الشخصية والدفاع عنها¹⁹⁴.

تملك سلطة التحقيق سواء كانت النيابة العامة أو قاضي التحقيق إتخاذ مجموعة من الإجراءات لجمع الأدلة وفحصها والتأكد من نسبتها إلى المتهم أو عدم نسبتها إليه، وإذا كنا قد إنتهينا في المطلب السابق إلى نتيجة مفادها أن استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات يؤدي إلى توغل هذه الإجراءات على الحرية الشخصية وحرمة الحياة الخاصة للأفراد، كما أن من شأن الاستعانة به أن يحقق نتائج تتناقض مع الخصوصية الجينية والرقمية، وما يقتضيه ذلك أن يتم تقييد لجوء السلطات العامة بما في ذلك سلطة التحقيق إلى استخدامه بضرورة صدور أمر قضائي مسبب، ينطوي على بيان العلة من الاستعانة بهذه الوسائل المستحدثة في الكشف عن الجريمة والتوصل لأدلتها، ويكون هذا الأمر محل للرقابة في مضمونه والأسباب التي بني عليها من محكمة الموضوع، وبذلك يتفق استخدام هذه التقنيات الحديثة مع الضمانات التي كفلها الدستور وضمنها القانون لحرمة الحياة الخاصة والحرية الشخصية للأفراد.

ثانياً: طبيعة الأدلة المستخلصة بواسطة تقنيات الذكاء الاصطناعي: من خلال ما سبق توصلنا إلى أنه يجوز استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم أو التنبؤ بها مستقبلاً. ومع ذلك، يجب النظر بعناية في طبيعة هذه الأدلة وكيفية تقدير المحكمة الجنائية لها، بما يتوافق مع تأثيرها على الدراسات المتعلقة بعلم الإجرام. كما ينبغي تقييم مدى فعاليتها في تقليل معدلات الجريمة في الدول التي اعتمدت هذه التقنيات

أ- طبيعة الأدلة المستمدة من استخدام تقنيات الذكاء الاصطناعي: قسم الفقهاء الأدلة بحسب دلالتها على الواقعة محل الإثبات إلى أدلة مباشرة وأدلة غير مباشرة، فالأدلة المباشرة هي التي

¹⁹³ - Gentsch P. , AI in Marketing, Sales and Service. Palgrave Macmillan, Cham, 2019 .

¹⁹⁴ - PILacelpersonne Alliacé criminelle ce Prévention De la criminalise annules 1973 p.16

تفيد في إثبات الواقعة أو نفيها بطريقة مباشرة دون الحاجة إلى إجتهد أو استنتاج، ومن أمثلة الأدلة المباشرة إقرار المتهم وشهادة الشهود، وهي تحتاج إلى عمليات ذهنية أو فنية تؤيدها المحكمة أو جهة فنية مختصة، وتنطوي ضمن الأدلة غير المباشرة القرائن والدلائل وكذلك الخبرة الفنية التي تحصل عليها سلطات الاستدلال أو التحقيق¹⁹⁵.

بالنظر إلى الأدلة المستخلصة من استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات نجد أنها أدلة فنية تحتاج إلى خبرة فنية متخصصة لاستخلاص الدليل والمحافظة عليه، كما أنها تعتبر أدلة غير مباشرة على الواقعة المراد إثباتها.

ب- سلطة المحكمة المختصة في تقدير الأدلة المستخلصة بواسطة تقنيات الذكاء الاصطناعي: يحكم عملية الإثبات الجنائي عدة قواعد، من أهمها قاعدة حرية المحكمة في تكوين عقيدتها والاقتناع الذاتي للقاضي الجزائي¹⁹⁶، وذلك نزولا على مبدأ حرية الإثبات في المجال الجزائي، ويتجلى تطبيق هذه المبادئ في ثلاثة مراحل هامة: مرحلة جمع الأدلة، مرحلة مناقشة الأدلة بواسطة أطراف الدعوى ومرحلة تقدير قيمة أدلة الإثبات بمعرفة المحكمة الجزائية. إن حرية الإثبات ليست مطلقة من كل قيد، إنما هي حرية مقيدة بممارستها في حدود القانون، فإن خرجت عن الإطار المحدد لها قانونا تعرض الدليل الناتج عنها لجزاء إجرائي يؤدي إلى إهداره وعدم الإعتماد عليه أو الأخذ به، وما ذلك إلا تطبيق لمبدأ الشرعية الإجرائية التي يحدد معالمها القانون، واستنادا إلى مبدأ إقتناع القاضي وحرية الإثبات الجنائي، فإنه يجوز للمحكمة المختصة بنظر الدعوى أن تلجأ لذوي الخبرة في مجالات الذكاء الاصطناعي لاستخلاص الأدلة على وقوع الجريمة¹⁹⁷.

والجدير بالذكر، أنه فيما يتعلق ببناء الحكم على الأدلة المستخلصة من تقنيات الذكاء الاصطناعي وحدها، فإنه إذا لم يكن بالدعوى دليل على الواقعة سواها، فإننا نرى أنه يجوز للمحكمة ذلك مادامت قد انتهت إلى الاستعانة بهذه الوسائل في استخلاص الدليل، وتعذر عليها الحصول على أدلة أخرى تساندها، وإذا كنا قد انتهينا في فقرة سابقة إلى اعتبار الأدلة المستمدة بواسطة تلك التقنيات من الأدلة غير المباشرة، فإن النتيجة المنتقاة لذلك أن يكون للمحكمة السلطة الكاملة في تقدير تلك الأدلة، طالما أنها لا تدل دلالة مباشرة وقاطعة على ارتكاب

¹⁹⁵ - ولا يحول ذلك دون سلطة المحكمة في وزن وتقدير الاعتراف كدليل مقدم في الدعوى ، وتطبيق لذلك قضى بأن "الاعتراف في المسائل الجنائية لا يخرج عن كونه عنصرا من عناصر الدعوى التي تملك محكمة الموضوع كامل الحرية في تقدير حجيتها وقيمتها الدليلية " رزق سعد علي، المرجع السابق ص 1646

¹⁹⁶ - لبيان ذلك نضرب مثال يتضح به الحال ، اذا فرضنا قيام شخص بارتكاب جريمة قتل دون ان يخلف اي دليل يمكن الاستعانة به في الوصول الى مرتكب الجريمة وكان هذا الشخص يعلم بما يمثله الحمض النووي من اهمية في كشف امر الجريمة والوصول الى مرتكبيها ، فألقى منديل او قطعة قماش او لفافة تخص شخص اخر وبها دمائه او لعابه او ترك بعض خصال الشعر التي تخص غيره فان تحليل البصمة الوراثية في هذه الحالات سيؤدي حتما الى ارتكاب الآخر للجريمة ، وسيشير الى استبعاد القاتل الحقيقي ، وهو ما يناقض الواقع ويجافي الحقيقة ويدل ذلك على انه وان كانت البصمة الوراثية دليل مباشر على معرفة صاحبها الا انها دليل غير مباشر على انه مرتكب الجريمة ، رزق سعد علي ، المرجع السابق ص 1643

¹⁹⁷ - J. Larrieu, Les robots et la propriété intellectuelle, Propriété industrielle., n°2, 2013. A. Lebois, Quelle protection juridique pour 36 les créations des robots journalistes? Communication Commerce Electronique., n° 1, 2015. G. Loiseau., A. Bonnet, La responsabilité du fait de l'intelligence artificielle, op, cit.,

الجريمة أو نفي إرتكابها. وعليه فإنه يجوز للمحكمة أن تبسط سلطتها على الأدلة المستخلصة من هذه التقنيات مع التأكيد على القيمة الثبوتية لبعض الأدلة كالبصمة الوراثية والحمض.

ج- أثر الأدلة المستخلصة بواسطة الذكاء الاصطناعي على أبحاث علم الإجرام: تهتم دراسات وأبحاث علم الإجرام في جانب كبير منها بالبحث على أسباب وعوامل الظاهرة الإجرامية، على أمل التوصل إليها والحد منها أو على الأقل تقسيم وتحسين السياسة الجنائية التي تتبعها الدول المختلفة إتجاه الجريمة، وتستمد تلك الأبحاث مقدماتها من وسائل مختلفة أهمها الإحصائيات الجنائية والمقابلات والدراسات التي تجرى على شخصيات المجرمين وسلوكهم قبل إرتكاب الجريمة. فالسياسة الجنائية الرشيدة تتلقى نتائج تلك الدراسات والأبحاث وتعمل على الاستفادة منها في وضع تصور ناجح وسريع للوقاية من الجرائم مستقبلاً¹⁹⁸.

ومن ناحية أخرى، نجد أن قواعد الإجراءات الجزائية تسمح للمتهم بأن يدافع عن نفسه بما يشاء، وله في سبيل إثبات براءته أن يلجأ إلى وسائل أخرى مختلفة على غرار الإقرار. غير أننا نلاحظ أن إحاطة المتهم بالأدلة المستمدة من تقنيات الذكاء الاصطناعي وتحليل البيانات مثل كاميرات المراقبة، وأجهزة الهاتف الذكية والتسجيلات الصوتية، وغيرها، من الممكن أن تدفع الشخص إلى الإقرار بجرمه، إذ أنه يجد الأدلة تنطق بما لا يدع مجالاً للشك على إدانته، ومن ثم ليس له سبيل في التخلص من هذه الأدلة الدامغة سوى الإقرار بالجريمة، وإذا كانت هذه النتيجة مهمة وناجحة بالنسبة لسلطة التحقيق في إثبات الجريمة، إلا أنها في ذات الوقت تسدل الستار للبحث على أسباب الجريمة، إذ عادة ما تكفي سلطة التحقيق أو المحكمة بالحصول على الإقرار فقط¹⁹⁹، ثم توقيع العقوبة دون النظر إلى الأسباب التي دفعت الشخص إلى إرتكاب الجريمة، وتعتبر قاعدة التسليم بالإقرار أثراً من آثار قوانين القرون الوسطى التي كانت تعتبر الإقرار دليلاً قانونياً يجب الحصول عليه. ولهذه النتيجة أثر هام في القبض على المجرمين وعقابهم بلا شك لكن في الوقت نفسه قد تؤدي إلى آثار سلبية على أبحاث علم الإجرام التي تستهدف الوقوف على أسباب الجنوح إلى الجرائم ومن ثم الاهتمام بمعالجتها، وبالتالي منع الجريمة والوقاية منها على المدى البعيد²⁰⁰.

¹⁹⁸ -M. Soulez, Propriété intellectuelle - Le droit de la propriété intellectuelle à l'épreuve des technologies robotiques. 2016, JCP G, p. 972. M. Soulez, Questions juridiques au sujet de l'intelligence artificielle, Enjeux numériques., n°1 mars 2018. J. Larrieu, Robot et propriété intellectuelle, Dalloz, Paris, 2016 .

¹⁹⁹ . M. Zalnieriute, et al., The Rule of Law and Automation of Government Decision Making, Modern Law Review 82. 2019 .

²⁰⁰-Mangani D, 5 AI Application I Banking to Look out for in Next 5 Years, available at: [https://www.analyticsvidhya.com/blog/2017/04/5-ai-applicationsin-banking-to-lookoutfor-in-next-5-years/\(18/07/2021 at 11h.02\)](https://www.analyticsvidhya.com/blog/2017/04/5-ai-applicationsin-banking-to-lookoutfor-in-next-5-years/(18/07/2021 at 11h.02))

خلاصة الفصل الثاني

تمحور هذا الفصل حول رصد الآليات التقنية والوسائل المستحدثة في منظومة التحري الإلكتروني، مع تسليط الضوء على المقاربة التكنولوجية المتمثلة في إدماج تطبيقات الذكاء الاصطناعي لتعزيز النجاعة الإجرائية في الكشف والتحقيق وتتبع الأثر الرقمي.

بالموازاة مع ذلك، استقرئنا من خلال هذا الفصل جملة التحديات القانونية والعملية الناشئة عن هذا التطور، لا سيما الإشكالات المتعلقة بمدى مشروعية هذه الوسائل في إطار حماية الحقوق والحريات الأساسية كحرمة الحياة الخاصة، تليها العقوبات التقنية المقترنة بحجية الدليل الرقمي وضمان سلامته من التلاشي أو العبث (الموثوقية والمصادقية). وصولاً إلى المسألة القانونية حول المسؤولية الناشئة عن الاعتماد على خوارزميات الذكاء الاصطناعي في العمل الضبطي. وانتهينا إلى التأكيد على الحتمية التشريعية لـ مواكبة النصوص القانونية لهذه التحولات، عبر خلق أطر تنظيمية مرنة تتلاءم والخصوصية الإجرائية للجريمة المعلوماتية المعاصرة.

خاتمة

في ختام هذه الدراسة القانونية المعمقة، والتي عبّرنا في طياتها ممرّات الفضاء السيبراني المعقد، واستقرّأنا من خلالها ترسانة القوانين، خاصة الإجرائية منها، في مواجهة الإجرام المعلوماتي، يمكننا القول إن التحريات الإلكترونية لم تعد مجرد خيار تشريعي ترفي أو ترفاً فكرياً تبحث عنه الأنظمة القانونية، بل غدت حتمية وجودية فرضتها صدمة الحادثة الرقمية، وعجز الآليات الكلاسيكية للقوانين الجزائية عن مواكبة مجتمع المعرفة.

لقد كشفت هذه الدراسة عن عمق التحول البنيوي في مفهوم الجريمة في حد ذاته، إذ انسحبت معالم السلوك الجرمي من فضاءها المادي المحسوس لتتوطن في بيئة افتراضية هلامية، لا تحكمها جغرافيا، ولا تقيدّها حدود سياسية، وينفذها جناة يتميزون براديكالية الذكاء الفني والخداع التقني. هذا التحول استتبع بالضرورة ثورة موازية ومضادة في أدوات التنقيب والبحث الجنائي لضبط "الأثر الرقمي" الذي يتميز بطبيعته الافتراضية، وسرعة تلاشيّه، وسهولة تدميره وتحويله بضغطة زر واحدة من أي مكان في العالم. وهنا وجب التأكيد صراحةً على أن هذا الاندفاع اللوجستي والتقني لتقصي الأدلة الرقمية لا يجب أن يعمي المشرع عن الالتزام الأسمى بحماية المعطيات الشخصية والحياة الخاصة للأفراد؛ فالأمن الرقمي يفقد شرعيته القانونية والأخلاقية إذا بُني على استباحة البيانات الحميمة للمواطنين أو تجريدهم من حقوقهم الدستورية في الخصوصية وسرية شؤونهم الشخصية.

ومن خلال تفكيك البنية القانونية والمؤسسية لهذا الموضوع، واستقراء آليات التحري الإلكتروني وتداخلها مع الطفرة الخوارزمية وعصر الذكاء الاصطناعي، تمكنا من صياغة منظومة متكاملة من النتائج الجوهرية، يعقبها أفق استشرافي من الاقتراحات التي نراها كفيلة بتقويم الانحراف الإجرائي وتحسين العدالة الجنائية:

أولاً: نتائج الدراسة: توصلنا من خلالنا دراستنا لموضوع مذكرتنا هذه إلى مجموعة من النتائج نوجزها فيما يلي:

1- أثبتت الدراسة أن القواعد الإجرائية الكلاسيكية (كالمعينة العينية، والتفتيش المادي للأماكن، وضبط الأشياء المادية) تقف عاجزة بنيوياً أمام الجريمة المعلوماتية. هذا العجز تسبب في بروز ما يُعرف بـ "أزمة القانون الجنائي"، حيث يصطدم المحقق بقواعد "مبدأ الشرعية الجنائية الإجرائية" التي تمنعه من القياس أو التوسع في تفسير النصوص المقيدة للحرية، مما جعل الدليل الرقمي المستخلص عبر وسائل غير منصوص عليها محل طعن دائم بالبطلان.

2- إن إقرار آليات مستحدثة مثل المراقبة الإلكترونية وتتبع الاتصالات يواجه عقبة عملية بالغة التعقيد على الساحة الدولية، تتمثل في اصطدامه الصارم بقواعد "السيادة الوطنية والإقليمية" للدول. فالجريمة المعلوماتية عابرة للحدود بطبيعتها (حيث قد يقع الفعل في دولة، وتتحقق النتيجة في دولة ثانية، وتُخزن البيانات في خوادم دولة ثالثة)، وهو ما يفرز تنازعا حادا

في الاختصاص القضائي، ويجعل من إجراءات المساعدة القانونية المتبادلة والإنبات القضائية التقليدية آليات بطيئة وببيروقراطية تخدم الجاني وتمنحه الوقت الكافي لمحو أثر جريمته.

3- يشكل إقام تقنيات الذكاء الاصطناعي والأنظمة الخوارزمية في منظومة التحريات الإلكترونية قفزة نوعية، إذ نقل السياسة الجنائية من "استراتيجية رد الفعل اللاحق" إلى "استراتيجية التنبؤ الاستباقي" عبر تحليل السلوكيات الشاذة في الشبكة وقمع الجريمة قبل استفحال أثرها. ومع ذلك، أسفر هذا التوظيف عن إشكالات قانونية بالغة الخطورة، أبرزها تراجع "الدور البشري" للمحقق، وضبابية المساءلة القانونية عن الأخطاء الخوارزمية، وغياب الشفافية التقنية فيما يُعرف فقها بمعضلة "الصندوق الأسود" (Black Box)، مما يهدد مبدأ اليقين القضائي وافترض البراءة.

4- كشفت الدراسة أن المشرع -في سعيه الحثيث لتعزيز الفعالية الإجرائية وتوسيع صلاحيات الضبطية القضائية والجهات المختصة-، قد غلب كفة الهاجس الأمني على حساب الحقوق والحريات الفردية. فإجراءات مثل اعتراض المراسلات، والتفتيش الإلكتروني عن بُعد للأنظمة، واختراق الحواسيب، تمثل سياسا مباشرا وخطيرا بالحق في الخصوصية وحرمة الحياة الخاصة وسرية البيانات الشخصية للمواطنين، ما لم تحط بضمانات تشريعية صارمة وقاطعة.

ثانيا: الاقتراحات: بناء على ما أسفرت عنه هذه الدراسة من نتائج موضوعية وإجرائية، نتقدم بجملة من الاقتراحات الرامية إلى تقويم المنظومة التشريعية والمؤسسية. نوجزها فيما يلي:

1- ندعو المشرع إلى ضرورة صياغة نصوص إجرائية رقمية مستقلة ومرنة في قانون الإجراءات الجزائية، تتجاوز التعديلات الترقيعية الجزئية. إذ يجب وضع تنظيم قانوني دقيق ومفصل يحدد شروط وضوابط "التفتيش الإلكتروني عن بُعد"، وكيفية التعامل مع البيانات المشفرة، وتحديد القيمة الإثباتية للأدلة المستخرجة من الفضاء الافتراضي لضمان عدم إفلات المجرمين تقنيا.

2- من الضروري إحاطة آليات المراقبة الإلكترونية واعتراض المراسلات بتدابير حمائية مشددة، فلا يجوز مباشرة هذه الإجراءات الخطيرة إلا بناء على أمر قضائي مكتوب، مسبب، ومحدد الصلاحيات، ولمدة زمنية قصيرة جدا لا تقبل التمديد إلا في أضيق الحدود ولجرائم على قدر عال من الخطورة. مع تفعيل الجزاء الإجرائي الصارم المتمثل في "بطلان الدليل الرقمي بطلانا مطلقا ومن النظام العام". إذا استخلص بناء على انتهاك غير مبرر لحرمة الحياة الخاصة.

3- ضرورة السعي نحو الانضمام إلى الاتفاقيات الدولية المتخصصة (مثل اتفاقية بودابست للجرائم الإلكترونية) وتفعيل الأطر الإقليمية الموحدة، من أجل خلق منظومة تعاون أمني

وقضائي "فوري ومباشر" يتجاوز البيروقراطية التقليدية للإنابات القضائية، مما يتيح تجميد البيانات الرقمية وحجزها وتتبع الجناة عبر الحدود في الوقت الحقيقي.

4-من الضروري الأخذ بعين الاعتبار والاهتمام بتأهيل العنصر البشري عبر إنشاء معاهد ومراكز تدريب تخصصية مشتركة (قانونية-هندسية) لرجال الضبطية القضائية والقضاة، لمواكبة تقنيات التشفير وفك الرموز. بالإضافة إلى دعم الجهات المختصة (كالهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال) بالميزانيات اللوجستية الباهظة اللازمة لشراء برمجيات النسخ الجنائي والتحليل الرقمي المتطورة، لتقليص الفجوة التقنية بين ذكاء المجرم المعلوماتي وقدرات الدولة.

5-كما نقترح وضع إطار قانوني وأخلاقي وطني ودولي صارم يحكم استخدام خوارزميات الذكاء الاصطناعي في مجال البحث الجنائي. ويجب التأكيد نصا على أن هذه الأنظمة الذكية تظل مجرد "أدوات مساعدة واستشارية" للمحقق والقاضي، ولا يمكنها بأي حال من الأحوال أن تحل محل العقيدة الإنسانية واليقين الوجداني للقاضي البشري، مع إلزام الشركات المطورة بتقديم خوارزميات قابلة للتفسير والمراجعة (Explainable AI).

قائمة المصادر والمراجع

1-الدساتير الجزائرية

- دستور الجزائر لسنة 1963، المؤرخ في 10 سبتمبر 1963، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 64، 1963.
- الأمر رقم 97-76 المؤرخ في 22 نوفمبر 1976، المتضمن دستور الجزائر لسنة 1976، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 94، الصادرة بتاريخ 24 نوفمبر 1976.
- المرسوم الرئاسي 89 - 18 المؤرخ في 28 فيفري 1989، المتضمن الدستور الجزائري لسنة 1989، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 09، الصادرة بتاريخ 01 مارس 1989.
- المرسوم الرئاسي رقم 96 - 438 المؤرخ في 07 ديسمبر 1996، المتضمن دستور الجزائر لسنة 1996، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 76، الصادرة بتاريخ 08 ديسمبر 1996.
- المرسوم الرئاسي رقم 20 - 442 المؤرخ في 30 ديسمبر 2020، المتضمن التعديل الدستوري لسنة 2020، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 82، الصادر بتاريخ 30 ديسمبر 2020.

2-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

3-القوانين والأوامر

- القانون العضوي رقم 12 - 05 المؤرخ في 12 جانفي 2012، المتعلق بالإعلام، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 01، الصادر بتاريخ 15 جانفي 2012.
- الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم 48، الصادر بتاريخ 10 يونيو 1966.
- قانون رقم 88-09 المؤرخ في 26 جانفي 1988، المتعلق بالأرشفة الوطني، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 04، المؤرخة في 27 جانفي 1988.
- قانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 47، الصادرة بتاريخ 16 أوت 2009.

- قانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 34، 2018، المعدل والمتمم بالقانون رقم 25-11 المؤرخ في 24 جويلية 2025، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 48، الصادرة بتاريخ 24 جويلية 2025.

- القانون رقم 18-11 المؤرخ في 2 جويلية 2018، المتعلق بالصحة، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 46، الصادرة بتاريخ 29 جويلية 2018.

- قانون رقم 15-04 المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 06، الصادرة بتاريخ 10 فيفري 2015.

4-المراسيم الرئاسية

- مرسوم رئاسي رقم 19-172 مؤرخ في 06 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 37، الصادرة بتاريخ 9 جوان 2019.

- مرسوم رئاسي رقم 15-261 مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 53، الصادرة بتاريخ 8 أكتوبر 2015.

ب-المراجع

1-الكتب

- أحمد حسين الهضيبي، قانون مكافحة جرائم تقنية المعلومات المصري: دراسة تحليلية مقارنة، دار الفكر العربي، القاهرة، 2020.
- أحمد عبد الإله المراغي، "الجريمة الإلكترونية ودور القانون الجنائي في الحد منها - دراسة تحليلية تأصيلية مقارنة"، المركز القومي للإصدارات القانونية، القاهرة، 2017.
- أوهابية عبد الله، ضمانات الحرية الشخصية أثناء مرحلة البحث التمهيدي، الاستدلال، ط 1، الديوان الوطني للأشغال التربوية، الجزائر، 2004.
- أيوب بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية: دراسة مقارنة، مشورات الحلبي القانونية، لبنان، 2009.
- باطلي غنية، الجريمة الإلكترونية: دراسة مقارنة، ط 1، الدار الجزائرية، الجزائر، 2016.

- بتشيم بوجمعة، الذكاء الاصطناعي في منظومة العدالة الحديثة على ضوء أحدث أحكام التشريع والقضاء المقارن إلى غاية سنة 2022، دار ألفا للوثائق، الجزائر، 2022.
- بوكر رشيدة، الحماية الجنائية للحياة الخاصة في ظل تكنولوجيا المعلومات والاتصالات: دراسة مقارنة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2021.
- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة-مصر، 2008.
- حازم حسن الجمل، الحماية الجنائية الامن الالكتروني، دار الفكر والقانون، القاهرة-مصر، 2015.
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان -الأردن، 2011.
- خالد ممدوح إبراهيم، التنظيم القانوني للذكاء الاصطناعي، دار الفكر الجامعي، الإسكندرية -مصر، 2022.
- رشيد عادل، علم المعلومات والمكتبات، دار الفكر العربي، بيروت، 2010.
- زكريا فؤاد، المعجم الفلسفي للمصطلحات التقنية، دار العلم للملايين، القاهرة-مصر، 2007.
- زيدان زيحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة-الجزائر، 2011.
- داود حسن طاهر، جرائم نظم المعلومات، دار الفكر العربي، الرياض-المملكة العربية السعودية، 2000.
- سامي فؤاد، الجرائم المعلوماتية في القانون المقارن، دار الثقافة القانونية، القاهرة-مصر، 2018.
- سراج الدين الرويب، آلية الإنترنت في التعاون الدولي الشرطي، ط1، الدار المصرية اللبنانية، مصر، 2001.
- طارق إبراهيم الدسوقي، أمن المعلومات والبحث الجنائي في جرائم الإنترنت، دار الجامعة الجديدة، الإسكندرية، مصر، 2011.
- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية-مصر، دون سنة نشر.
- عبد الاله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في اثبات جريمة التزوير الإلكتروني، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2011.
- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، دار النهضة العربية، عمان، 2009.
- عفيفي كامل عفيفي، جرائم الكمبيوتر، دون دار نشر، الإسكندرية-مصر، 2000.

- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، مصر، 2012.
- غانم المرضي الشمري، الجرائم المعلوماتية: ماهيتها، خصائصها وكيفية التصدي لها قانونياً، الدار العلمية الدولية، الأردن، 2016.
- غنا محمد غنا، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة -مصر، 2010.
- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت: الجريمة المعلوماتية، ط1، دار الثقافة للنشر والتوزيع-عمان، الأردن، 2007.
- محمد عبيد الكعبي، "الجرائم الناشئة عن الاستعمال غير المشروع لشبكة الانترنت"، دار النهضة العربية، القاهرة-مصر، 2007.
- محمد نجيب حسني، شرح قانون الإجراءات الجنائية، ط3، دار النهضة العربية، مصر، 1990.
- محمود سلامة عبد المنعم الشريف، النظرية العامة للأدلة العلمية في المواد الجنائية: دراسة مقارنة، دار النهضة العربية، القاهرة-مصر، 2012.
- محمود مرسي، الجريمة المعلوماتية: دراسة جنائية مقارنة، دار النهضة، القاهرة-مصر، 2012.
- مسدور عبد السلام، الجريمة المعلوماتية: دراسة مقارنة بين التشريع الجزائري والفرنسي، دار النهضة العربية، الجزائر، 2015.
- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة القاهرة، 2008.
- موسى مصطفى محمد، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، مصر، 2005.
- نائلة عادل فريد قورة، جرائم الحاسب الاقتصادية-دراسة نظرية تطبيقية، منشورات الحلبي القانونية بيروت-لبنان، 2005.
- نبيل الزهيري، مصطلحات معلوماتية عربي-إنجليزي، دار الفكر، عمان، 2012.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار النهضة العربية، عمان، 2008.
- هروال نبيلة هبة، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، مصر، 2007.
- هلال عبد الاله أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط1، دار النهضة العربية، القاهرة-مصر، 2012.
- يعيش تمام شوقي، الجريمة المعلوماتية-دراسة تأصيلية مقارنة، مطبعة الرمال، ط1، الوادي، الجزائر، 2019.

2-1- أطروحات الدكتوراه

- بشاتن صفية، الحماية القانونية للحياة الخاصة -دراسة مقارنة، أطروحة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري - تيزي وزو، الجزائر، 2012.
- بن حيدة محمد، حماية الحق في الحياة الخاصة في التشريع الجزائري، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد - تلمسان، الجزائر، 2016/2017.
- بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا الإعلام والاتصال، أطروحة دكتوراه، قانون دستوري، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر -باتنة 1، الجزائر، 2014/2015.
- حايطي فطيمة، إجراءات التحقيق في الجرائم الإلكترونية - دراسة مقارنة، أطروحة دكتوراه الطور الثالث، قانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون-تيارت، الجزائر، 2022/2023.
- صدراتي وفاء، آليات مكافحة جريمة التزوير الإلكتروني، أطروحة دكتوراه، قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي - تبسة، الجزائر، 2020/2021.
- عاقللي فضيلة، الحماية القانونية للحق في الحياة الخاصة-دراسة مقارنة، أطروحة دكتوراه علوم في القانون الخاص، كلية الحقوق، جامعة الإخوة منتوري-قسنطينة1، الجزائر، 2011/2012.
- عمر محمد أبو بكر بن يونس، "الجرائم الناشئة عن استخدام الإنترنت"، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2004.

2-2- رسائل الماجستير

- بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، رسالة تخرج لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2012/2013.
- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر-باتنة، الجزائر، 2012-2013.
- قارة أمال، الجريمة المعلوماتية، رسالة ماجستير، القانون الجنائي والعلوم الجنائية، جامعة الجزائر 1، الجزائر، 2002.
- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية - دراسة مقارنة، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، الأردن، 2014.

2-3-مذكرات الماستر

- بن بريكة أسماء، بن سعيد نور الهدى، التفتيش الإلكتروني، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي-الأغواط، الجزائر، 2024/2023.
- بن عمارة فاتن نور الايمان، التحري والتحقيق في الجرائم الالكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس-مستغانم، الجزائر، 2024/2023.
- بن عنصر سهام، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص: قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري - تيزي وزو، الجزائر، 2015.
- بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص: قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي - برج بوعريريج، الجزائر، 2021.

3-المقالات

- الأخشن نور أمينة، العيداني محمد، "الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية"، مجلة القانون والعلوم البيئية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي بونعامة-خميس مليانة، الجزائر، المجلد 2، العدد 2، 2023.
- الدحيات عماد عبد الرحيم، "نحو تنظيم قانوني للذكاء الاصطناعي في حياتنا: إشكالية العلاقة بين البشر والآلة"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي لتامنغست-الجزائر، المجلد 08، العدد 05، ديسمبر 2019.
- العزاوي لمى عبد الباقي محمود، حاتم دعاء جليل، "الذكاء الصناعي والمسؤولية الجنائية الدولية"، مجلة المفكر، كلية الحقوق والعلوم السياسية -جامعة محمد خيضر-بسكرة، الجزائر، المجلد 14، العدد 1، 2019.
- بن بادة عبد الحليم، "المراقبة الالكترونية بين الحق في الخصوصية ومشروعية الدليل الالكتروني"، المجلة الاكاديمية للبحث القانوني، جامعة عبد الرحمن ميرة-بجاية، الجزائر، المجلد 10، العدد 3، 2019.
- بن عجائمة بوعبدالله، "قانون 14 - 04 المتعلق بالنشاط السمعي البصري في الجزائر: بين متغيرات المرحلة وضرورات التعديل"، مجلة أبحاث قانونية وسياسية، جامعة محمد صديق بن يحي-جيجل، الجزائر، المجلد 07، العدد 02، ديسمبر 2022.
- بوزبرة سهيلة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية"، المجلة النقدية للقانون والعلوم السياسية، جامعو مولود معمري-تيزي وزو، الجزائر، المجلد 17، العدد 02، 2022.

- بوضياف أسهمان، "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري في ظل القانون 04-09"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية"، جامعة محمد بوضياف-المسيلة، الجزائر، المجلد 15، العدد 01، 2022.
- بومعزة مروة، "الأنتربول وآليات عمله في إطار مكافحة الجريمة"، مجلة البيان للدراسات القانونية والسياسية، جامعة البشير الإبراهيمي-برج بوعريريج-الجزائر، المجلد 5، العدد 2، 2020.
- حابت أمال، "دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، مجلة الدراسات الحقوقية، كلية الحقوق والعلوم السياسية، جامعة سعيدة الجزائر، المجلد 6، العدد 1.
- حيمر فتيحة، "الجرائم المعلوماتية في الجزائر: المواجهة والتحدي"، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور-خنشلة، الجزائر، المجلد 12، العدد 01، 2025.
- دولي الخضر، ناصري نفيسة، "دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية"، مجلة المؤشر للدراسات الاقتصادية، جامعة بشار، المجلد 2، العدد 2، 2018.
- رابح سعاد، "ضوابط مكافحة الجريمة المعلوماتية"، مجلة القانون العام الجزائري والمقارن، جامعة الجيلالي الياصب-سيدي بلعباس، الجزائر، المجلد 7، العدد 01، جوان 2021.
- رانا مصباح عبد المحسن عبد الرزاق، "دور الذكاء الاصطناعي في مواجهة جريمة الإرهاب الإلكتروني-دراسة مقارنة"، المجلة الأكاديمية لجامعة نوروز، العراق، المجلد 12، العدد 4، 2023.
- رزق سعد علي، "استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم"، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات -مصر، المجلد 9، العدد 3، سبتمبر 2023.
- سليمان جميلة، "الخصوصية الرقمية للفرد ومدى تأثير الإجراء السيبراني عليها"، مجلة القانون والعلوم السياسية، المركز الجامعي-النعامة، المجلد 09، العدد 02، 2023.
- شيخ عبد الصديق، "الوقاية من الجرائم الإلكترونية في ظل القانون رقم 04-09"، مجلة معالم الدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة يحي فارس-المدينة، الجزائر، المجلد 04، العدد 01، 2020.
- عبد الإله أمحد مطر الفالسي، "المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي"، مجلة الدراسات القانونية، كلية الحقوق، جامعة أسيوط، مصر، المجلد 9، العدد 8، 2021.

- عبد الفتاح فرحات الجبالي، "المسؤولية المدنية والذكاء الاصطناعي: إمكانية المساءلة (دراسة تحليلية في ضوء قواعد المسؤولية المدنية في القانون المدني الفرنسي)"، مجلة كلية القانون الكويتية العالمية، الكويت، المجلد 8، العدد 1، مارس 2020.
- عمار ياسر زهير البابلي، "دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة"، مجلة الامن والقانون، أكاديمية دبي للنشر، الإمارات، المجلد 29، العدد 1، 2021.
- عمارة فوزي، "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية"، مجلة العلوم الإنسانية، جامعة الإخوة منتوري-قسنطينة 1، الجزائر، العدد 33، 2010.
- عمر أبو الفتوح حمامي، "الحماية الإجرائية للمعلوماتية وأثرها في الإثبات الجنائي: دراسة مقارنة"، مجلة الفكر القانوني والاقتصادي، جامعة بنها، يناير 2017.
- غنام محمد غنام، "الدليل المستمد من الحاسب الآلي ومدى حجته في الإثبات الجنائي"، مجلة الحقوق، جامعة الكويت، المجلد 26، العدد 1، 2002.
- فلاح عبد القادر، آيت عبد المالك نادية، "التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف-المسيلة، الجزائر، المجلد 04، العدد 02، 2019.
- قيشاح نبيلة، "ضمانات المراقبة الإلكترونية في التشريع الجزائري"، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور-خنشلة، الجزائر، المجلد 10، العدد 2، 2022.
- مباركية مفيدة، "الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري"، مجلة الشريعة والاقتصاد، جامعة العلوم الإسلامية-الأمير عبد القادر، قسنطينة، الجزائر، المجلد 07، العدد 01، 2018، جوان 2018.
- محمد عرفان الخطيب، "المسؤولية المدنية والذكاء الاصطناعي... إمكانية المساءلة؟ دراسة تحليلية معمقة بقواعد المسؤولية المدنية في القانون المدني الفرنسي"، مجلة كلية الحقوق الكويتية العالمية، المجلد 8، العدد 29، مارس 2020.
- مريم لوكال، "قراءة في اتفاقية الاتحاد الإفريقي حول الامن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014"، مجلة الدراسات القانونية والاقتصادية، جامعة امحمد بوقرة - بومرداس، الجزائر، المجلد 04، العدد 03، 2021.
- مسياد أمينة، "آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون 07-18"، مجلة الباحث في العلوم القانونية والسياسية، جامعة محمد الشريف مساعديه-سوق أهراس، الجزائر، المجلد 03، العدد 05، شهر جوان 2021.
- معروف كريم، بن حليلة سعاد، "الإجراءات المستحدثة في البحث والتحقيق للكشف عن الجرائم التي ترتكب في الفضاء الإلكتروني"، مجلة الدراسات الاستراتيجية والعسكرية، المركز العربي الديمقراطي، برلين، ألمانيا، العدد 13، ديسمبر 2021.

- مهادوي حنان، "التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري"، مجلة الفكر القانوني والسياسي، جامعة محمد لمين دباغين سطيف 2، المجلد 6، العدد 2، 2022.
- نايل صونيا، "أخلاقيات مهنة الصحافة على ضوء قانون الإعلام رقم 12 - 05"، مجلة الحقوق والحريات، جامعة محمد خيضر-بسكرة، الجزائر، المجلد 10، العدد 01، 2022.
- يحي الشريف نصير، مزغيش سعاد، "الآليات القانونية المكرسة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري"، مجلة البحوث في العقود وقانون الأعمال، جامعة الإخوة منتوري-قسنطينة 1، الجزائر، المجلد 07، العدد 02، 2022.

4-الروابط

- مكتب الأمم المتحدة المعني بالمخدرات والجريمة (<http://www.cdonu.org>).
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (<https://esttf.motrans.gov.iq>).

ثانياً: المصادر والمراجع باللغة الأجنبية

- Jack Bologna, Corporate Fraud: The Basics of Prevention and Detection, 1984.
- Martin Wasik, Computer Crimes and Other Crimes Against Information Technology in the United Kingdom, 1991.
- Kelley M. Sayler, Artificial Intelligence and National Security, CRS Report, 2020.
- David A. Fahrenthold, Washington Post, 2016.
- Zalnieriute et al., The Rule of Law and Automation of Government Decision Making, Modern Law Review, 2019.
- Mangani D, 5 AI Application in Banking, 2017/2021.
- Odile Siary, Quelle personnalité juridique pour les ROBOTS, Village de la justice, 2017.
- F. Patrick Hubbard, 'Sophisticated Robots': Balancing Liability, Regulation, and Innovation, 2014.
- Fintechnews Singapore, the Potential of AI in Banking, 2021.
- Gentsch P., AI in Marketing, Sales and Service, 2019.
- J. Larrieu, Les robots et la propriété intellectuelle, 2013/2016.
- Lebois, Quelle protection juridique pour les créations des robots journalistes?, 2015.

- G. Loiseau & A. Bonnet, La responsabilité du fait de l'intelligence artificielle.
- M. Soulez, Propriété intellectuelle - Le droit à l'épreuve des technologies robotiques, 2016.

فهرس المحتويات

رقم الصفحة	العناوين
	شكر
	إهداء
8	مقدمة
12	الفصل الأول: الإطار المفاهيمي والقانوني للتحريات الالكترونية في مواجهة الجريمة المعلوماتية
13	المبحث الأول: ماهية الجريمة المعلوماتية والتحريات الالكترونية
13	المطلب الأول: مفهوم الجريمة المعلوماتية
13	الفرع الأول: تعريف المعلوماتية
13	أولاً: التعريف اللغوي للمعلوماتية
14	ثانياً: التعريف الاصطلاحي للمعلوماتية
14	ثالثاً: التعريف التشريعي للجريمة معلوماتية
14	أ-تعريف التشريع الفرنسي للمعلوماتية
15	ب-تعريف التشريع المصري للمعلوماتية
15	ج-تعريف التشريع الأمريكي للمعلوماتية
15	د-تعريف المعلوماتية حسب اتفاقية بودابست
15	هـ-تعريف المشرع الجزائري للمعلوماتية
16	رابعاً: تعريف الجريمة المعلوماتية في الفقه
17	الفرع الثاني: خصائص الجريمة المعلوماتية
17	أولاً: صعوبة اكتشاف الجريمة الالكترونية
18	ثانياً: صعوبة إثبات الجريمة الالكترونية
18	أ- فضاء الجريمة
18	ب - صعوبة الاحتفاظ بآثار الجريمة
18	ثالثاً: الجريمة الالكترونية عابرة للحدود الوطنية
18	المطلب الثاني: صور وأشكال الجريمة المعلوماتية
19	الفرع الأول: صور الجريمة المعلوماتية
19	أولاً: الاختراق غير المشروع للأنظمة المعلوماتية
19	ثانياً: التلاعب بالبيانات أو التعديل غير القانوني
19	ثالثاً: تعطيل أو إفساد نظم المعلومات
19	رابعاً: جرائم التشهير الإلكتروني ونشر المحتوى غير القانوني
19	الفرع الثاني: أشكال الجريمة المعلوماتية
20	أولاً: الاحتيال الإلكتروني
20	ثانياً: الجرائم المرتبطة بالملكية الفكرية الرقمية

20	ثالثا: الاحتيال عبر البريد الإلكتروني(Phishing)
20	رابعا: انتهاك سرية البيانات
20	المطلب الثالث: مفهوم التحريات الالكترونية وتمييزها عن التحريات التقليدية
20	الفرع الأول: مفهوم التحريات الالكترونية والتحريات التقليدية
21	أولا: تعريف التحريات الالكترونية
21	ثانيا: تعريف التحريات في شكلها التقليدي
22	الفرع الثاني: التمييز بين التحريات الالكترونية والتحريات التقليدية
24	المبحث الثاني: الأساس القانوني للتحريات الالكترونية
25	المطلب الأول: الإطار القانوني للتحريات الالكترونية في الجزائر
25	الفرع الأول: القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال
26	أولا: مراقبة الاتصالات الإلكترونية
26	ثانيا: القواعد الإجرائية
26	أ-تفتيش المنظومات المعلوماتية
27	ب-حجز المعطيات المعلوماتية
28	ج-التعاون والمساعدة القضائية الدولية
28	الفرع الثاني: التحريات الالكترونية في ظل قانون الإجراءات الجزائية
29	الفرع الثالث: القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المعدل والمتمم
30	الفرع الرابع: قانون العقوبات الجزائري المعدل والمتمم
31	أولا: جريمة الدخول أو البقاء عن طريق الغش إلى نظام معالجة البيانات
32	ثانيا: جرائم الاعتداء على المعطيات الموجودة داخل نظم المعلوماتية
33	المطلب الثاني: الإطار القانوني الدولي والاقليمي للتحريات الإلكترونية
33	الفرع الأول: اتفاقية بودابست لمكافحة الجريمة المعلوماتية
33	أولاً: المحافظة المؤقتة على البيانات المخزنة
33	ثانيا: آليات جمع المعلومات الخاصة بالمشتبه بهم
34	ثالثا: إجراءات التفتيش الرقمي
34	الفرع الثاني: دور المنظمات الدولية في مكافحة الجريمة المعلوماتية
34	أولا: الإنترنت ومكافحة الجريمة المعلوماتية
35	أ-الوصول المباشر إلى المعلومات
35	ب-الربط الإلكتروني
35	ج-تنزيل البيانات
35	1-الاتصال بواسطة جهاز X400
36	2-الاتصال عبر الهاتف الدولي وأجهزة الفاكس

36	ثانياً: الأمم المتحدة ومكافحة الجريمة المعلوماتية
36	أ-المؤتمر السابع للأمم المتحدة لمنع الجريمة ومعاملة المجرمين
36	ب-المؤتمر الثامن للأمم المتحدة الذي عُقد في هافانا، كوبا
37	ج-المؤتمر التاسع للأمم المتحدة
37	د-المؤتمر الثاني عشر للأمم المتحدة حول الجريمة والعدالة الجنائية
37	هـ-المؤتمر الثالث عشر للأمم المتحدة حول الجريمة والعدالة الجنائية
38	و-المؤتمر الخامس عشر للقانون الجنائي في ريو دي جانيرو بالبرازيل عام 2017
38	الفرع الثالث: الإطار القانوني الإقليمي للتحريات الإلكترونية
39	أولاً: الإطار القانوني للتحريات الإلكترونية في الدول العربية
39	أ-نطاق تطبيق الاتفاقية
39	ب-مبدأ السيادة المرسخ
39	ج-عنصر التجريم
40	ثانياً: الإطار القانوني للتحريات الإلكترونية في إفريقيا
42	المطلب الثالث: الجهات المختصة بمباشرة التحريات الإلكترونية
42	الفرع الأول: الهيئات الوطنية المختصة بمباشرة التحريات الإلكترونية
42	أولاً: الضبطية القضائية كهيئة مختصة بمباشرة التحريات الإلكترونية
42	أ-مباشرة التحريات الإلكترونية على مستوى جهاز الشرطة
43	ب-مباشرة التحريات الإلكترونية على مستوى جهاز الدرك الوطني
44	ثانياً: صلاحيات الضبطية القضائية كهيئة مختصة بمباشرة التحريات الإلكترونية
45	الفرع الثاني: الهيئة غير القضائية للتحقيق في الجريمة الإلكترونية
45	أولاً: مفهوم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال
46	أ-دعوة مالية مستقلة
46	ب-الأهلية القانونية
46	ج-الموطن
47	د-تحمل المسؤولية عن الأضرار
47	ثانياً: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بالاعلام والاتصال
47	أ-الوقاية من جرائم الاعلام والاتصال
47	ب-مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال
47	1-مساعدة السلطات القضائية الداخلية
47	2-تعزيز وتنسيق جهود الوقاية من الجرائم المرتبطة بتكنولوجيا الاعلام والاتصال
48	3-دعم السلطات القضائية الأجنبية
48	4-تبادل المعلومات
48	5-طلب الإجراءات التحفظية

50	خلاصة الفصل الأول
51	الفصل الثاني: آليات التحريات الالكترونية ودورها في مواجهة الجريمة المعلوماتية في ظل الذكاء الاصطناعي
53	المبحث الأول: وسائل وأساليب التحريات الالكترونية
53	المطلب الأول: المراقبة الالكترونية وتتبع الاتصالات
53	الفرع الأول: المراقبة الالكترونية
53	أولاً: تعريف المراقبة الإلكترونية
53	ثانياً: خصائص اجراء المراقبة الالكترونية
53	أ-سرية إجراء المراقبة الإلكترونية
53	ب-الاعتماد على أجهزة خاصة في إجراء المراقبة الالكترونية
53	ج-هدف المراقبة الالكترونية هو الحصول على دليل غير مادي
54	د-مساس إجراء المراقبة الالكترونية بحق الشخص في سرية المراسلات والاتصالات الالكترونية
54	ثالثاً: شروط اجراء المراقبة الالكترونية
54	رابعاً: حالات اللجوء إلى إجراء المراقبة الالكترونية
55	الفرع الثاني: تتبع الاتصالات
55	أولاً: الاعتراض والالتقاط الالكتروني
55	أ-اعتراض المراسلات
56	ب-تسجيل الأصوات والتقاط الصور
56	1-تسجيل الأصوات
56	2-التقاط الصور
56	ثانياً: الشروط الموضوعية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور
56	أ-السلطة المختصة بإجراء هذه العمليات
57	ب-توقيت ومكان تنفيذ هذه العمليات
57	ج-عدم مسؤولية القائم والمشرف على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور
57	ثالثاً: الشروط الشكلية لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور
57	أ-صدور إذن مكتوب
57	ب-تحرير محضر الاعتراض
58	ج-تحديد مدة المراقبة
58	المطلب الثاني: التفتيش الالكتروني وضبط الادلة الرقمية
58	الفرع الأول: تعريف التفتيش الالكتروني وأهم وسائله
58	أولاً: تعريف التفتيش الالكتروني

59	ثانيا: وسائل التفتيش الإلكتروني
59	أ-برنامج مالتيجو " Maltego " المستخدم أثناء المعاينة والتفتيش
59	ب-برنامج "Forensic" المستخدم أثناء عمليات المعاينة والتفتيش
60	1-تقنية تتبع عنوان TCP – IP
61	2-تقنية تحليل البروكسي 'Proxy'
61	ج-استعمال برامج التتبع المعلوماتي برنامج "TRACER –HACK"
61	د-الاستعانة بنظام كشف الاختراق "Detection System Intrusion"
62	هـ-العمل بنظام الترميز
62	الفرع الثاني: الجهات المختصة بإجراء التفتيش الإلكتروني
62	أولا: الاختصاص النوعي للتفتيش الإلكتروني
64	ثانيا: الاختصاص الإقليمي للتفتيش الإلكتروني
64	الفرع الثالث: ضبط الأدلة الرقمية
65	أولا: ضبط الدليل الرقمي الضبط
65	أ-جمع آثار التفتيش الإلكتروني (الدليل الرقمي)
65	ب-فحص البيانات الرقمية كأثر للتفتيش
65	ج-تحليل ومراجعة آثار التفتيش الإلكتروني
66	ثانيا: أنواع الأدلة الرقمية الناجمة عن التفتيش الإلكتروني
66	أ- ضبط جهاز الكمبيوتر وملحقاته
66	1-الملحقات البرمجية (Software)
66	2-وسائل التخزين المتنقلة
66	3-المودم
66	ب-ضبط البريد الإلكتروني
67	ج-محضر التفتيش الإلكتروني
67	1-الرقم القضائي ووصف الواقعة
67	2-عنوان محضر التفتيش الإلكتروني
67	3-تاريخ ووقت افتتاح المحضر
67	4-مكان تحرير المحضر
67	5-الإجراءات السابقة لبدء التحقيق
67	6-مقدمة المحضر
68	7-موضوع المحضر
69	د-مشروعية الدليل المستخلص من التفتيش الإلكتروني
69	1-الحصول المشروع على الدليل
69	2 -يقينية الدليل المستخلص
69	هـ-حجية الدليل المستخلص وسائل التفتيش الإلكتروني
71	المطلب الثالث: توظيف الذكاء الاصطناعي في التحريات الإلكترونية

71	الفرع الأول: تعريف الذكاء الاصطناعي وبيان أهم مجالاته
71	أولاً: تعريف الذكاء الاصطناعي
73	ثانياً: مجالات تطبيق الذكاء الاصطناعي
73	أ- الاستعانة بتقنيات الذكاء الاصطناعي لتحليل الصور والفيديوهات
73	ب- توظيف الذكاء الاصطناعي في مكافحة الجرائم الحديثة
74	ج- استخدام الذكاء الاصطناعي لتحليل بيانات شبكات التواصل الاجتماعي
74	الفرع الثاني: دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية
75	أولاً: دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية الواقعة على الأموال
75	ثانياً: اقحام الشرطة الرقمية للذكاء الاصطناعي في مكافحة الجرائم الإلكترونية
76	ثالثاً: دور الذكاء الاصطناعي في مكافحة جرائم الإرهاب السيبراني
77	رابعاً: دور الذكاء الاصطناعي في تطوير الأجهزة الأمنية
77	المبحث الثاني: التحديات القانونية والعملية للتحريات الإلكترونية
78	المطلب الأول: الإشكاليات القانونية المرتبطة بحماية الحقوق والحريات الفردية
78	الفرع الأول: عناصر الحق في الخصوصية الرقمية
78	أولاً: خصوصية الاتصالات والمراسلات الهاتفية السلكية واللاسلكية
79	ثانياً: خصوصية الحياة الصحية والبيانات الشخصية
79	ثالثاً: خصوصية الذمة المالية
80	الفرع الثاني: الأساس القانوني لحماية الخصوصية الرقمية في الدساتير والتشريعات الجزائرية
80	أولاً: الاعتراف الدستوري بالخصوصية الرقمية
81	ثانياً: حماية الخصوصية الرقمية في ظل القوانين الداخلية
81	أ- حماية الخصوصية الرقمية في ظل القانون المدني المعدل والمتمم
82	ب- حماية الخصوصية الرقمية في ظل قانون العقوبات المعدل والمتمم
82	ج- حماية الخصوصية الرقمية في ظل القانون رقم 14-25 المتضمن قانون الإجراءات الجزائية
83	د- حماية الخصوصية الرقمية في ظل القانون رقم 88 - 09 المتعلق بالأرشيف الوطني
83	هـ- حماية الخصوصية الرقمية في ظل القانون رقم 09 - 04
84	و- حماية الخصوصية الرقمية في ظل القانون رقم 04-15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين
84	ي- حماية الخصوصية الرقمية في ظل القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المعدل والمتمم

84	ت-حماية الخصوصية الرقمية في ظل قوانين الاعلام
85	الفرع الثالث: الإشكالات الإجرائية في الجرائم الإلكترونية
86	أولاً: نقص خبرة سلطات البحث والتحري في الجرائم الإلكترونية
86	ثانياً: إشكال تنازع الاختصاص والقانون الواجب التطبيق
89	المطلب الثاني: الصعوبات التقنية والعملية للتحريات الإلكترونية
89	الفرع الأول: الصعوبات التقنية للتحريات الإلكترونية
89	أولاً: صعوبة اكتشاف الجريمة المعلوماتية
89	ثانياً: صعوبة إثبات الجريمة الإلكترونية
90	ثالثاً: أسلوب ارتكاب الجريمة الإلكترونية
90	الفرع الثاني: الصعوبات العملية للتحريات الإلكترونية
90	أولاً: التعاون والتواطؤ على الأضرار
90	ثانياً: أعراض النخبة
91	ثالثاً: الأضرار
91	رابعاً: الصفة الدولية للجريمة المعلوماتية
92	المطلب الثالث: التحديات القانونية لاستخدام الذكاء الاصطناعي في التحريات الإلكترونية
92	الفرع الأول: الإشكاليات المتعلقة بالخصوصية وحماية البيانات
93	أولاً: التعارض مع الحق في الخصوصية وحرمة الحياة الخاصة
96	ثانياً: تعارض التحريات الإلكترونية مع الحق في حماية البيانات الشخصية للأفراد
97	الفرع الثاني: إشكاليات اعتماد الدليل الجنائي المستمد من الذكاء الاصطناعي
98	أولاً: أطر الاستعانة بالأدلة المستخلصة بواسطة الذكاء الاصطناعي
98	أ- الاستعانة بتقنيات الذكاء الاصطناعي في مرحلة جمع الاستدلالات
99	ب- الاستعانة بتقنيات الذكاء الاصطناعي في مرحلة التحقيق
100	ثانياً: طبيعة الأدلة المستخلصة بواسطة تقنيات الذكاء الاصطناعي
100	أ- طبيعة الأدلة المستمدة من استخدام تقنيات الذكاء الاصطناعي
100	ب- سلطة المحكمة المختصة في تقدير الأدلة المستخلصة بواسطة تقنيات الذكاء الاصطناعي
101	ج- أثر الأدلة المستخلصة بواسطة الذكاء الاصطناعي على أبحاث علم الإجرام
103	خلاصة الفصل الثاني
105	خاتمة
109	قائمة المصادر والمراجع
118	فهرس المحتويات
128	ملخص الدراسة

ملخص

ملخص

يسلط الضوء من خلال هذه الدراسة على ماهية الجريمة المعلوماتية والتحريات الإلكترونية، وذلك من خلال توضيح الفرق الجوهرى بينها وبين الأساليب التقليدية في تتبع "الأثر الرقمي" العابر للحدود. حيث تستعرض الأطر القانونية الوطنية والدولية، مع إبراز دور الجهات الأمنية والفنية المتخصصة في مكافحة هذا النمط الإجرامي المتطور.

كما تعرج على آليات المراقبة الإلكترونية وتفتيش النظم المعلوماتية، مبرزة دور الذكاء الاصطناعي في الانتقال من مرحلة رد الفعل إلى "الوقاية الاستباقية" عبر التحليلات التنبؤية والتعرف الآلي. حيث تناقش الدراسة بعمق التحديات القانونية المتمثلة في الموازنة بين فعالية التحري وحماية الحق في الخصوصية، فضلاً عن المعوقات التقنية كالتشفير والشبكة المظلمة.

تصل هذه الدراسة في الختام، إلى التحذير من مخاطر "الأخطاء الخوارزمية" وانعدام الشفافية في تقنيات الذكاء الاصطناعي، مشددة على ضرورة إحاطة هذه الوسائل بـ ضمانات قضائية صارمة لضمان عدم تقويض الحريات الأساسية بدعوى الأمن السيبراني.

ختاماً، إن التحدي الحقيقي والرهان الأكبر الذي يواجه السياسة الجنائية المعاصرة في الألفية الرقمية، ليس في مدى قدرتها على ابتكار وترخيص أدوات تحرٍ رقمية أكثر توغلاً وشراسة، بل في مدى نجاحها في الحفاظ على إنسانية العدالة وضماناتها الحرفية؛ بحيث لا يتحول السعي المشروع وراء تحقيق الأمن الرقمي والسيبراني إلى مسوغ ومبرر لتقويض صرح الحقوق والحريات الفردية، فالقانون ما وجد إلا لحماية الإنسان، وحريته هي غايته الأسمى.

الكلمات المفتاحية: التحريات الإلكترونية، المراقبة الإلكترونية، الحق في الخصوصية، التفتيش ارقمي، الأمن السيبراني.

Abstract

This study sheds light on the nature of cybercrime and electronic investigations by clarifying the fundamental difference between them and traditional methods in tracking cross-border "digital evidence." It reviews national and international legal frameworks, highlighting the role of specialized security and technical authorities in combating this evolving criminal pattern.

The study also addresses the mechanisms of electronic surveillance and the inspection of information systems, highlighting the role of artificial intelligence in transitioning from a stage of reaction to "proactive prevention" through predictive analytics and automated recognition. Furthermore, the study deeply discusses the legal challenges of balancing the effectiveness of investigation with the protection of the right to privacy, as well as technical obstacles such as encryption and the Dark Web.

In conclusion, this study warns of the risks of "algorithmic errors" and the lack of transparency in artificial intelligence techniques, stressing the necessity of surrounding these means with strict judicial guarantees to ensure that fundamental freedoms are not undermined under the pretext of cybersecurity. In conclusion, the true challenge and greatest bet facing contemporary criminal policy in the digital millennium is not its ability to innovate and license more invasive and aggressive digital investigation tools, but rather its success in preserving the humanity of justice and its professional guarantees; so that the legitimate pursuit of achieving digital and cyber security does not turn into a pretext and justification for undermining the structure of individual rights and freedoms, for the law was only created to protect the human being, and their freedom is its ultimate goal.

Keywords: Digital Forensics, Electronic Surveillance, Right to Privacy, Digital Search and Seizure, Cybersecurity.

الجمهورية الجزائرية الديمقراطية



République Algérienne

الديمقراطية الشعبية

l'Enseignement Supérieur et de la

Ministère de

وزارة التعليم العالي و البحث العلمي recherche Scientifique

جامعة الشاذلي بن جديد Université Chadli Bendjedid El tarf

2026\06\30

استمارة معلومات حول الأطروحة أو المذكرة

الاسم:....نور الهدى-بسمة

اللقب:....زياني-مويسي.....

الكلية: كلية الحقوق والعلوم السياسية.....

القسم:....الحقوق.....

التخصص:قانون جنائي وعلوم جنائية.....

المستوى:السنة الثانية ماستر.....

عنوان المذكرة أو الأطروحة:التحريات الالكترونية في مواجهة الجريمة
المعلوماتية.....

المؤطر:الأستاذة مقدم رشا.....

الكلمات المفتاحية: التحريات الالكترونية; المراقبة الالكترونية;الحق في الخصوصية;
التفتيش الرقمي;الامن السيبراني

تاريخ المناقشة للأطروحة (اليوم والشهر والسنة): 17. / 06. / 2026

السنة الجامعية: 2025\2026.....

الملخص كاملا بجميع اللغات المتوفرة:

يسلط الضوء من خلال هذه الدراسة على ماهية الجريمة المعلوماتية والتحريات الإلكترونية، وذلك من خلال توضيح الفرق الجوهرية بينها وبين الأساليب التقليدية في تتبع "الأثر الرقمي" العابر للحدود. حيث تستعرض الأطر القانونية الوطنية والدولية، مع إبراز دور الجهات الأمنية والفنية المتخصصة في مكافحة هذا النمط الإجرامي المتطور.

كما تعرج على آليات المراقبة الإلكترونية وتفتيش النظم المعلوماتية، مبرزة دور الذكاء الاصطناعي في الانتقال من مرحلة رد الفعل إلى "الوقاية الاستباقية" عبر التحليلات التنبؤية والتعرف الآلي. حيث تناقش الدراسة بعمق التحديات القانونية المتمثلة في الموازنة بين فعالية التحري وحماية الحق في الخصوصية، فضلاً عن المعوقات التقنية كالتشفير والشبكة المظلمة.

تصل هذه الدراسة في الختام، إلى التحذير من مخاطر "الأخطاء الخوارزمية" وانعدام الشفافية في تقنيات الذكاء الاصطناعي، مشددة على ضرورة إحاطة هذه الوسائل بـ ضمانات قضائية صارمة لضمان عدم تقويض الحريات الأساسية بدعوى الأمن السيبراني.

ختاماً، إن التحدي الحقيقي والرهان الأكبر الذي يواجه السياسة الجنائية المعاصرة في الألفية الرقمية، ليس في مدى قدرتها على ابتكار وترخيص أدوات تحرٍ رقمية أكثر توغلاً وشراسة، بل في مدى نجاحها في الحفاظ على إنسانية العدالة وضماناتها الحرفية؛ بحيث لا يتحول السعي المشروع وراء تحقيق الأمن الرقمي والسيبراني إلى مسوغ ومبرر لتقويض صرح الحقوق والحريات الفردية، فالقانون ما وجد إلا لحماية الإنسان، وحرية هي غايته الأسمى.

Abstract

This study sheds light on the nature of cybercrime and electronic fundamental difference between them investigations by clarifying the and traditional methods in tracking cross-border "digital evidence." It reviews national and international legal frameworks, highlighting the role of specialized security and technical authorities in combating this evolving criminal pattern.

The study also addresses the mechanisms of electronic surveillance and the inspection of information systems, highlighting the role of artificial intelligence in transitioning from a stage of reaction to "proactive prevention" through predictive analytics and automated recognition. Furthermore, the study deeply discusses the legal challenges of balancing the effectiveness of investigation with the protection of the right to privacy, as well as technical obstacles such as encryption and the Dark Web.

In conclusion, this study warns of the risks of "algorithmic errors" and the lack of transparency in artificial intelligence techniques, stressing

