الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de L'Enseignement Supérieur et de la Recherche Scientifique
المركز الجامعي عبد الحفيظ بو الصوف ميلة

معهد الحقوق

القســـــم: الحقـــــوق
الشعبـــة: الحقـــــوق
التخصص: قانون جنائي

الرقم التسلسلي:
الـــــــــــرمز:

آليـــــات مكافحـــــة الجريمـــــــــة الإلكترونيـــــة في التشريـــــع الجزائـــــــــــــــــــــري

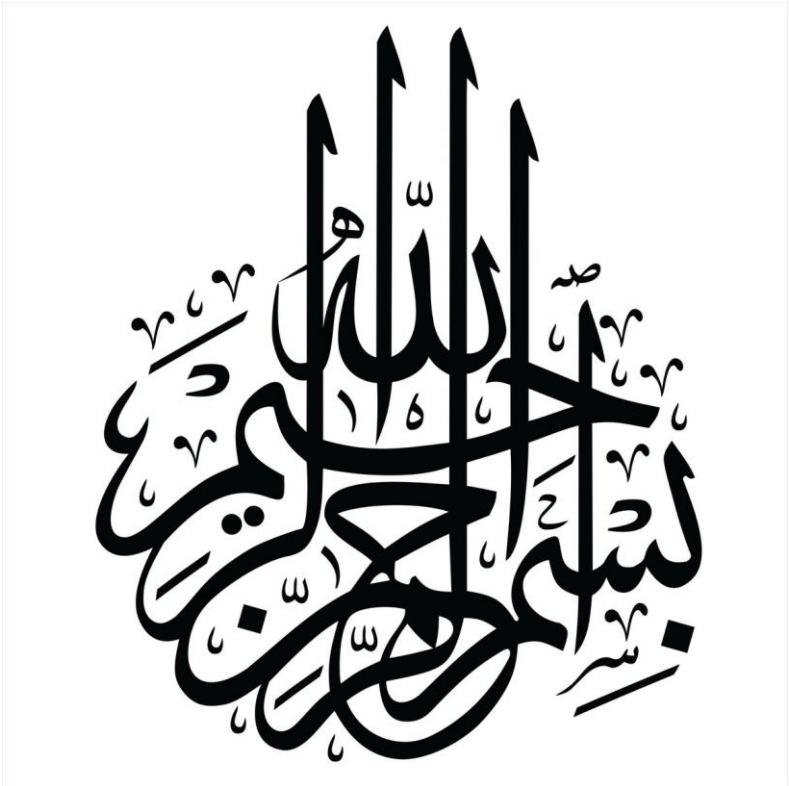
مذكرة ضمن متطلبات نيل شهادة الماستر

إعداد الطالبين:

- حسام بن ميسية
- عبد المولى حملاوي

لجنة المناقشة	
سهام بوكلاب	مشرفا ومقررا
عبد الرؤوف بن الشيهب	رئيسا
إيمان بغدادي	مناقشا

السنة الجامعية 2025/2024


بسم الله الرحمن الرحيم

قال الله تعالى

﴿يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ إِلَّا أَنْ تَكُونَ تِجَارَةً عَنْ تَرَاضٍ مِنْكُمْ وَلَا تَقْتُلُوا أَنْفُسَكُمْ إِنَّ اللَّهَ كَانَ بِكُمْ رَحِيمًا وَمَنْ يَفْعَلْ ذَلِكَ عُدْوَانًا وَظُلْمًا فَسَوْفَ نُصْلِيهِ نَارًا وَكَانَ ذَلِكَ عَلَى اللَّهِ يَسِيرًا﴾

[النساء : 29 - 30]

إهـــــداء

إلى كلّ من أمدّ هذا البحث بقُوّة العطاء والاستمرار

والدي الكريمين حَفِظَهُما الله

أخي وأخواتي وأبنائهم جميعا

حسام بن ميسية

إهـــــداء

أهدي ثمرة هذا العمل إلى والدي الكريمين حَفِظَهُما الله

إخوتي وأخواتي وأبنائهم جميعا

عبد المولى حملاوي

شكـــرٌ وتقديـــرٌ

أتقدّم بجزيل الشّكر و العرفان إلى كلّ

من كان له إسهامٌ في إنجاز هذا البحث ...

إلى أستاذتنا المشرفة التي أحاطته بتوجيهاتها المعرفيّة

و المنهجيّة واقتراحاتها السّديدة ...

ولأعضاء لجنة المناقشة الذين تجشَّموا عناء قراءته وتنقيحه...

مقدمة

شهد العالم خلال العقود الأخيرة تحولاً جذريًا في مختلف مجالات الحياة نتيجة التطورات التكنولوجية المتسارعة، وعلى رأسها الثورة الرقمية التي أحدثت طفرة غير مسبوقة في أساليب التواصل وتبادل المعلومات، والمعاملات الاقتصادية والاجتماعية.ورغم ما وفرته هذه الثورة من مزايا هائلة للبشرية، فإنها صاحبتها تحديات أمنية وقانونية مستجدة، من أبرزها ظاهرة **الجريمة الإلكترونية**، التي تمثل أحد أخطر إفرازات العصر الرقمي.

فبخلاف الجريمة التقليدية، التي تُرتكب في واقع ملموس وبوسائل محسوسة، فإن الجريمة الإلكترونية تُرتكب في الفضاء الافتراضي، وبوسائل تقنية متقدمة يصعب أحيانًا تتبعها أو ضبط مرتكبيها ما يفرض تحديات قانونية وإجرائية غير مسبوقة على الجهات المعنية بمكافحتها. فالمجرم الإلكتروني لا يحتاج إلى كسر قفل أو اقتحام مكان مادي، بل يكفيه امتلاك حاسوب واتصال بشبكة الإنترنت لينفذ هجماته ويخترق الحسابات،أو يبتز الأفراد،أو يعبث بأنظمة المعلومات، أو يتجسس على أسرار المؤسسات، أو ينشر أفكارًا متطرفة تهدد الأمن العام.

وأمام هذه الظاهرة المستحدثة، وجدت مختلف الدول نفسها مضطرة إلى مواكبة هذه التغيرات عبر تطوير منظومتها القانونية والأمنية بما يسمح بالتصدي الفعال لهذا النوع من الجرائم، وقد كانت الجزائر من بين هذه الدول التي أولت اهتمامًا متزايدًا بهذا الملف، فعملت على إدراج نصوص قانونية جديدة في تشريعاتها، واستحدثت آليات مؤسساتية وتكنولوجية لمكافحة هذا الخطر المتزايد. غير أن هذا الجهد رغم أهميته،لا يخلو من إشكالات متعددة، سواء على مستوى المفاهيم، أو على صعيد التطبيق العملي أو من حيث التنسيق بين الأجهزة الأمنية والقضائية، أو حتى من حيث وعي المجتمع بخطورة هذه الظاهرة وسبل الوقاية منها.

وانطلاقًا من هذه المعطيات، يحاول هذا البحث تسليط الضوء على الإطارين **المفاهيمي والقانوني** للجريمة الإلكترونية في الجزائر، وتحليل الأطر المؤسسية المكلفة بمكافحتها، وتحديد أهم الصعوبات التي تعترض سبيل مواجهة هذه الظاهرة المستجدة، خاصة في ظل التطور المتسارع لوسائل التكنولوجيا وأساليب الإجرام الرقمي.

الإشكالية الرئيسية للبحث:

ما هو الإطار القانوني والمؤسساتي الذي تبنته الجزائر لمكافحة الجريمة الإلكترونية ؟ وهل هذه المنظومة كافية وفعالة لمواجهة التحديات المتزايدة التي تطرحها هذه الظاهرة المعقدة؟

الأسئلة الفرعية:

1. ما المقصود بالجريمة الإلكترونية؟ وما أبرز خصائصها التي تميزها عن الجريمة التقليدية؟
2. ما هي العقوبات التي أقرها المشرع الجزائري لمرتكبي الجرائم الإلكترونية؟
3. ما هو دور الأجهزة الأمنية (الشرطة والدرك) في البحث والتحري عن هذه الجرائم؟
4. كيف تتعامل الأجهزة القضائية مع الجريمة الإلكترونية من حيث التحقيق والمحاكمة؟

الفرضية الرئيسية:

رغم الجهود القانونية والمؤسساتية التي بذلتها الجزائر في مجال مكافحة الجريمة الإلكترونية، إلا أن فعالية هذه الجهود تظل محدودة في ظل التحديات التقنية والتنظيمية الراهنة.

الفرضيات الفرعية:

1. الخصائص غير التقليدية للجريمة الإلكترونية تعيق عمليات التتبع والإثبات.
2. العقوبات الجزائية الحالية قد لا تتناسب مع تطور أساليب الجريمة الرقمية.
3. ضعف التنسيق بين الجهات الأمنية والقضائية يؤثر سلبًا على فعالية المكافحة.
4. غياب التكوين المتخصص في المجال الرقمي داخل المؤسسات الأمنية والقضائية يعد من أبرز العوائق.

أهداف الدراسة:

- توضيح المفاهيم المتعلقة بالجريمة الإلكترونية وخصائصها القانونية.
- تحليل المنظومة القانونية الجزائرية الخاصة بمكافحة الجريمة الإلكترونية.

- إبراز دور الأجهزة الأمنية والقضائية في ملاحقة مرتكبي هذه الجرائم.
- تسليط الضوء على أهم الإشكالات العملية المرتبطة بتطبيق القانون في هذا المجال.
- تقديم مقترحات عملية من شأنها تعزيز فعالية مكافحة الجريمة الإلكترونية.

أهمية الدراسة:

تكتسي هذه الدراسة أهمية نظرية وعملية في آنٍ واحد، فمن الناحية النظرية، تساهم في إثراء المكتبة القانونية بمقاربة تحليلية حديثة لظاهرة مستجدة، وتساعد الباحثين والمهتمين بالقانون الجنائي وتقنيات التحري الرقمي على فهم تعقيدات الجريمة الإلكترونية. أما من الناحية العملية، فهي توجه صناع القرار والمؤسسات الأمنية والقضائية نحو أهم النقاط الواجب تطويرها أو مراجعتها لتعزيز حماية المجتمع من هذه الجرائم.

منهجية الدراسة:

اعتمدت هذه الدراسة على **المنهج الوصفي التحليلي**،لتوضيح مفاهيم الجريمة الإلكترونية واستعراض النصوص القانونية ذات الصلة، بالإضافة إلى **المنهج المقارن** في بعض المواضع لبيان نقاط القوة والقصور في التشريع الجزائري مقارنة ببعض الأنظمة القانونية الأخرى.كما تم توظيف **المنهج القانوني التطبيقي** لتحليل مدى تطبيق النصوص القانونية في الواقع العملي، بالاستناد إلى التقارير الرسمية وبعض السوابق القضائية.

صعوبات الدراسة:

- **ندرة المراجع** المتخصصة التي تتناول الجريمة الإلكترونية في السياق الجزائري بوجه خاص.
- **قلة الدراسات الميدانية** والبيانات الإحصائية الرسمية حول معدلات الجريمة الإلكترونية وآليات المكافحة.
- **صعوبة الحصول على معلومات دقيقة** حول طريقة عمل الأجهزة الأمنية والقضائية، بسبب حساسية الموضوع.
- **الطابع المتجدد للجريمة الإلكترونية**، مما يصعب مواكبة جميع المستجدات التقنية والتشريعية.

الدراسات السابقة:

الدراسة الأولى بعنوان: "الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري"، من إعداد: عيمور راضية، منشورة في المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 6، العدد 1، لسنة 2022.

هدفت هذه الدراسة إلى تسليط الضوء على ماهية الجريمة الإلكترونية وسبل مكافحتها في التشريع الجزائري، وذلك في ظل التوسع الكبير في استخدام تكنولوجيا المعلومات وظهور جرائم مستحدثة ذات طابع إلكتروني. وقد اعتمدت الباحثة المنهج التحليلي الوصفي لمختلف النصوص القانونية ذات الصلة من أجل إبراز جهود المشرع الجزائري في مواجهة هذا النوع من الجرائم. وتوصلت الدراسة إلى مجموعة من النتائج، من أبرزها:

- تبني المشرع الجزائري سياسة مزدوجة للتصدي لظاهرة الإجرام المعلوماتي.
- استحداث قوانين خاصة تتماشى مع الخصوصية التقنية والواقعية للجرائم الإلكترونية.

ومن أهم التوصيات التي خلصت إليها الدراسة: ضرورة تفعيل التعاون التشريعي والقضائي والأمني مع الدول العربية، بل ومع الدول الغربية الأكثر خبرة في مجال مكافحة الجريمة الإلكترونية، بهدف الاستفادة من تجاربها وتعزيز فعالية المنظومة الوطنية في هذا المجال.

الدراسة الثانية بعنوان: "الآليات العقابية لمكافحة الجريمة الإلكترونية في الجزائر"، من إعداد: بَهلول سمية ودمّان ذبيح عماد، منشورة في مجلة الحقوق والعلوم السياسية، المجلد 7، العدد 1، لسنة 2020.

هدفت هذه الدراسة إلى تسليط الضوء على خطورة الجريمة الإلكترونية وبيان مختلف الآليات العقابية التي اعتمدها المشرّع الجزائري لمكافحتها والوقاية من آثارها السلبية على الأفراد والمؤسسات وحتى على أمن الدولة واستقرارها. وقد ركزت الدراسة على تحليل النصوص القانونية المستحدثة ذات الصلة، والتي تُظهر بوضوح سعي المشرّع إلى إيجاد منظومة ردعية فعالة تشمل عقوبات صارمة وهيئات وطنية متخصصة لمواجهة هذا التهديد.

وتوصلت الدراسة إلى أن الجزائر أولت اهتمامًا متزايدًا بالجريمة الإلكترونية من خلال سنّ نصوص قانونية تُقرّ عقوبات ردعية، وتعزيز دور الأجهزة القضائية والأمنية في التعامل معها.

ومن أبرز التوصيات التي طرحتها الدراسة: ضرورة تطوير المنظومة العقابية باستمرار، وتكثيف التنسيق بين مختلف الهيئات المتدخلة في مكافحة الجريمة الإلكترونية، من أجل التصدي الفعّال لهذا النمط الإجرامي المستحدث.

الدراسة الثالثة بعنوان: "آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري"، من إعداد: عقباش بريزة ومبارك حنان، تحت إشراف د. هدفي العيد، مذكرة ماستر أكاديمي في تخصص قانون الإعلام الآلي والإنترنت، جامعة محمد البشير الإبراهيمي – برج بوعريريج، السنة الجامعية 2020–2022.

سعت هذه الدراسة إلى تحليل الإطار القانوني والمؤسساتي الذي تبناه المشرع الجزائري لمكافحة الجريمة الإلكترونية، بالنظر إلى التوسع السريع لهذا النوع من الجرائم وتهديده المباشر لأمن الأفراد والمؤسسات والدولة. وبيّنت الدراسة أن المشرع الجزائري حاول سد الفراغ التشريعي في مجال الجريمة المعلوماتية عبر إدراج نصوص قانونية ذات طابع ردعي، وإنشاء هيئات وطنية متخصصة، إلى جانب تفعيل دور القطب الجزائي الوطني لمكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.

وتوصلت الدراسة إلى أن فعالية هذه الآليات تظل رهينة بتطوير مستمر للتشريعات، وتكوين القضاة المختصين، وتعزيز التعاون الدولي،إضافة إلى إنشاء مراكز متخصصة لدراسة الجريمة الإلكترونية.

ومن أبرز التوصيات التي قدمتها الدراسة:

- تحيين القوانين الجزائية القائمة لتشمل الجرائم المعلوماتية المستحدثة.
- إعادة النظر في بعض المواد القانونية كالمادة 32 مكرر 322 لتوضيح دور الهيئات القضائية المختصة.
- تفعيل دور القطب الجزائي الوطني مع احترام الحياة الخاصة والحريات الدستورية.

الفصل الأول: الإطار المفاهيمي والقانوني للجريمة الإلكترونية

شهِد العالم خلال العقود الأخيرة ثورة رقمية هائلة غيَّرت من أنماط الحياة والمعاملات في شتى المجالات،وأدت إلى بروز جرائم مُستحدثة تتَّخِذُ من الوسائل التكنولوجية مجالًا لتنفيذ أفعالها، وهو ما عُرف بالجريمة الإلكترونية.هذا النوع من الجرائم يتميز بخصائص فريدة تميّزه عن الجرائم التقليدية من حيث طبيعتها الافتراضية ووسائل ارتكابها وصعوبة تتبُّع مرتكبيها، الأمر الذي فرض على المشرّعين وضع أُطر قانونية وتنظيمية جديدة للتصدِّي لها.

وفي هذا الفصل، سنُسلِّطُ الضوء على المفهوم العام للجريمة الإلكترونية، من خلال الوقوف عند معناها اللغوي والاصطلاحي،ثم إبراز أهم خصائصها، لننتقِل لاحقًا إلى تحليل المنظومة القانونية الجزائرية الخاصَّة بمكافحة هذه الجرائم،من حيث العقوبات المقرَّرة لها،والقواعد القانونية والإجراءات المتبعة في مكافحتِها.

المبحث الأول: ماهية الجريمة الإلكترونية

تُعدُّ الجرائم الإلكترونية من أبرز التحديات القانونية المعاصرة التي فرضتها الطفرة التكنولوجية وانتشار الوسائط الرقمية في مختلف مناحي الحياة.ومع تزايُد الاعتماد على الأنظمة المعلوماتية في المجالات الاقتصادية والاجتماعية والإدارية، ظهرت صور جديدة من الجرائم التي تختلِفُ عن الجرائم التقليدية في طبيعتها وأدواتها وطُرق تنفيذها. وهو ما استدعى إعادة النظر في المفاهيم القانونية الكلاسيكية لمسايرة هذه الظواهر المُستحدثة،من خلال تحديد ماهية الجريمة الإلكترونية وخصائصها كمدخل ضروري لفهم سُبل مكافحتِها وملاحقة مرتكِبيها.

المطلب الأول: التعريف اللغوي والاصطلاحي للجريمة الإلكترونية

قبل التطرُّق إلى الإشكاليات القانونية والواقعية المرتبطة بالجريمة الإلكترونية، لا بد من الوقوف عند مفهومها من حيث اللغة والاصطلاح، وذلك لما يُشكِّله هذا المفهوم من أهمية في تحديد طبيعتها وتمييزها عن غيرها من الأفعال الجرمية التقليدية.فاختلاف الوسائط والأساليب المُستخدمة في ارتكاب هذه الجريمة ينعكس على طبيعة المصطلحات المُستعملة، سواء في السياق اللغوي أو القانوني،مما يستدعي توضيح هذه المفاهيم بشكل دقيق يُمهِّدُ للمعالجة القانونية الصحيحة.

الفرع الأول: التعريف اللغوي للجريمة الإلكترونية

نتعرَّض لتعريف الجريمة ، ثم الجريمة الإلكترونية .

أولا : تعريف الجريمة

جَرَمَ :الجُرْم والجَريمة تعني الذَّنْب، ويُقال منه: "جَرَمَ"، و"أَجْرَمَ"، و"اجْتَرَمَ". والجُرْمُ . بالكسر . يُطلق أيضًا على الجسد. و"جَرَمَ" تعني كذلك"كَسَبَ"،وبابهما (ضرب). قال الله تعالى: ﴿**وَلَا يَجْرِمَنَّكُمْ شَنَآنُ قَوْمٍ عَلَىٰ أَلَّا تَعْدِلُوا۟ ۚ اعْدِلُوا۟ هُوَ أَقْرَبُ لِلتَّقْوَىٰ**﴾[1]أي: لا يحملنّكم بغض قوم على أن تظلموا، ويُقال: "لا يَجْرِمَنَّكم" أي لا يَكْسِبَنَّكم.

[1]سورة المائدة، الآية 8.

ومن التعبيرات أيضًا: "تَجَرَّم عليه"،أي ادَّعى عليه ذنبًا لم يفعله. قال تعالى: ﴿**سَيُصِيبُ الَّذِينَ أَجْرَمُواْ صَغَارٌ عِندَ ٱللَّهِ وَعَذَابٌ شَدِيدٌ بِمَا كَانُواْ يَمْكُرُونَ**﴾[1]

وأيضا من الناحية اللغوية، تُشتق كلمة "جريمة" من الفعل "جرم"، الذي يعني كسب أو قطع ويُقال "جرم جرماً" أي أذنب[2] و"الجريمة" تعني الجناية أو الذنب، وهي مصدر "الجارم"، أي الذي يجرم نفسه أو قومه شرًّا[3]،كما أن الجريمة تُشير إلى التعدي على القيم أو على الآخرين.[4]

كما تأتي بمعنى الجز : يُقال جزمت صوف الشاة أي جزرته ، كانت في الأصل بمنزلة لا بد ولا محالة ، فجرت على ذلك وكثرت حتى تحولت إلى معنى القسم وصارت بمنزلة حقا ، لذلك يُجاب عنه باللام ، كما يجاب بها عن القسم ، يقولون لا جرم لأتينك .[5]

ثانيا : الجريمة الالكترونية

من الناحية اللغوية، يُشتق مصطلح "الجريمة الإلكترونية" من كلمتين: "الجريمة" التي تُشير إلى الفعل غير المشروع الذي يُعاقِب عليه القانون، و"الإلكترونية" نسبة إلى الوسط الذي تُرتكب فيه، أي الفضاء الرقمي المُعتمِد على التكنولوجيا الحديثة، لاسيما الإنترنت والحواسيب. وبالتالي، فالجريمة الإلكترونية هي كل فعل ضار يُرتكب باستخدام الوسائط الإلكترونية الحديثة[6]

الفرع الثاني: التعريف الاصطلاحي للجريمة الإلكترونية

وُضعت عدة تعاريف للجريمة الإلكترونية،منها ما هو فقهي، ومنها ما هو قانوني :

أوّلا : التعريف الفقهي

يمكن تعريف الجرائم الإلكترونية بأنها: "الجرائم التي تُرتكب من قِبل أفراد أو مجموعات بدافع إجرامي،بهدف إلحاق الضرر عمدًا بسُمعة الضحية أو التسُبب في أذى جسدي أو نفسي لها،سواء بشكل

---

[1] سورة الأنعام، الآية 124.

[2] ابن منظور، **لسان العرب**، دار إحياء التراث العربي، بيروت، 1999، ص 91.

[3] محب الدين الفيروزآبادي، **القاموس المحيط**، دار الكتب العلمية، بيروت، 2007، ص 88.

[4] الإمام محمد أبو زهرة، **الجريمة والعقوبة في الفقه الإسلامي**، دار الفكر العربي، القاهرة، 1998، ص 199.

[5] الجوهري إسماعيل بن حماد ، **الصحاح في اللغة** ، دار العلم للملايين ، ط 4 ، م 1، بدن تاريخ (ب.ت) ، ص120.

[6] **معجم المصطلحات الجنائية**، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، 2008، ص 142.

مباشر أو غير مباشر، وذلك باستخدام وسائل الاتصال الحديثة مثل الإنترنت (كغُرف الدردشة والبريد الإلكتروني) أو الهواتف المحمولة (كالرسائل النصية القصيرة ورسائل الوسائط المتعددة .)" [1]

عرّفها **ليوكفيلدت وفينسترا وستول** كمصطلح عام يشمل جميع أشكال الجريمة التي تلعبُ فيها تكنولوجيا المعلومات والاتصالات (ICT) دورًا أساسيًا . [2]

ويرى الأستاذ Rosenblatt أن الجريمة الإلكترونية هي "نشاط غير مشروع يستهدِف نسخ المعلومات المخزنة داخل الحاسوب أو الوصول إليها أو تغييرها أو حذفها،أو تحويلها عن طريقه[3]"

ومن التعريفات التي وضعها أنصار الاتجاه الضيق أنَّ الجريمة المعلوماتية هي : " كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازماً من ناحية؛ وملاحقته من ناحية أخرى " كما عرفها هذا الاتجاه بأنها : " هي التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط". أما أصحاب الاتجاه المُوسَّع فيعرِّفون الجريمة المعلوماتية بأنها : " كل سلوك إجرامي يتم بمساعدة الكمبيوتر" أو هي كل جريمة تتم في محيط أجهزة الكمبيوتر".[4]

كما تُعرَّف الجريمة الإلكترونية في القانون على أنَّها : كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يُرتكب باستخدام الحاسب الآلي " [5] .

وعُرِّفت أيضا: " بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخُّل التقنية الالكترونية.[6]

---

[1] زينب ياقوت ،" **واقع الجريمة عبر الفايسبوك وسبل الحد من انتشارها: دراسة حالة الجزائر**" مجلة الدراسات و البحوث القانونية ، جامعة محمد بوضياف ، المسيلة ، الجزائر ، *المجلد 7، العدد 2، 2022*، ص289

[2] Leukfeldt, R. and Veenstra S., & Stol W,(2013). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 January – June 2013, Vol 7 (1)p5.

[3] حمزة بن عقون، **السلوك الإجرامي للمجرم المعلوماتي**، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب جامعة باتنة، ،2011/2012 ص14

[4] محمود إبراهيم غازي، **الحماية الجنائية للخصوصية والتجارة الالكترونية**، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014م، ص 118.

[5] عبد الفتاح بيومي حجازي ، **مكافحة جرائم الكومبيوتر والأنترنيت في القانون العربي النموذجي** ، دار الكتب القانونية ، مصر ، الطبعة (ط)1 ،2007 ص 04 .

[6] عبابنه محمد احمد ، **جرائم الحاسوب و أبعادها الدولية**، دار الثقافة ، عمان ، الأردن ، ط1، 2005، ص17 .

جانب من الفقه نظر إليها من زاوية وقوع الجريمة ؛ أي أن الأجهزة الالكترونية تكون هي محل الجريمة فعرَّفها على أنها : " أفعال غير مشروعة، تهدف للوصول لمعلومات معينة أو حذفها أو نسخها أو تغييرها.[1] في حين نظر إليها جانب آخر من زاوية تقنية ، فعرَّفها على أنها : " الجرائم الإلكترونية تعني كل الجرائم التي تكون المعرفة بتقنية الحواسيب أساسا لارتكابها.[2]

ولا نستطيع إغفال أهمية أي تعريف من التعريفات السابقة للجريمة الالكترونية، نظرا لخصوصية الزاوية التي ينظر إليها كل تعريف في الجريمة الالكترونية، ولأهمية ذلك نستطيع أن نوسع تعريف الجريمة الالكترونية بأنها أية جريمة تُرتكب بواسطة نظام الكتروني أو شبكة الكترونية أو تُرتكب ضد أي نظام الكتروني في البيئة الالكترونية.

ثانيا : التعريف القانوني للجريمة الإلكترونية

عرَّفها المشرع الجزائري بموجب الفقرة –أ– من المادة 02 من القانون رقم 09–04 [3] والتي جاء فيها ما يلي : " يُقصد في مفهوم هذا القانون الجرائم المتصلة بتكنولوجيات الإعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدَّدة في قانون العقوبات أو أي جريمة أخرى تُرتكب أو يسهُل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية . " "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى تُرتكب أو يُسهل ارتكابها عن طريق منظومة معلوماتية أو اتصالات إلكترونية ."

كما عرّفها المشرع أيضا بموجب الفقرة –3– من المادة 211 مكرر 22 من القانون 21–11 [4] على أنها : " يُقصد في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال أي جريمة تُرتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال . "

---

[1] عياد سامي علي حامد، **الجريمة المعلوماتية وإجرام الإنترنت**، دار الفكر الجامعي، مصر ، 2007، ص40 .

[2] نفس المرجع ، ص40–41

[3] القانون 09–04 المؤرخ في 14 شعبان 1430 الموافق لـ 5 غشت 2009 **المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتهما** ، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية (ج.ر) عدد 47 صادر بتاريخ 16 غشت 2009 .

[4] القانون 21–11 المؤرخ في 16 محرم 1443 الموافق لـ 25 غشت 2021 يتمم الأمر 66–156 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 **يتضمن قانون الإجراءات الجزائية** ، ج.ر عدد 65 صادر بتاريخ 26 غشت 2021 .

المطلب الثاني: خصائص الجريمة الإلكترونية وأركانها

بعد الوقوف على مفهوم الجريمة الإلكترونية،أصبح من الضروري التعمُّق أكثر في خصائصها التي تجعلها مختلفة تمامًا عن الجرائم التقليدية، سواء من حيث طريقة ارتكابها أو الوسائل المستعملة فيها، أو من حيث طبيعة التحديات التي تفرضها على أجهزة العدالة ، وفي هذا الإطار نتناول أولًا أبرز الخصائص التي تنفرِد بها الجريمة الإلكترونية مع بيان صورها ، قبل الانتقال إلى دراسة أركانها التي تُبنى عليها المسؤولية الجزائية.

الفرع الأول : خصائص الجريمة الإلكترونية وصوَّرِها

تتميز الجرائم الإلكترونية بخصائص متفرِّدة عن غيرها من الجرائم العادية ، الأمر الذي ساهم في تعدُّد صُوَّرِها حسب ما سيتم توضيحه .

أوّلا : خصائص الجريمة الالكترونية [1]

ما يُميِّزُ الجرائم الالكترونية تفرُّدها بطبيعة خاصة ، لا وجود لها في عالم الجرائم التقليدية ، ساعد في ذلك انتشار تقنية المعلومات و التطور التكنولوجي ، ما أضفى عليها مجموعة من الخصائص والسمات وهي على النَّحو التالي :

1. جرائم مُتجدِّدة دائمة التطوُّر

إن من أبرز سمات الجريمة الإلكترونية أنها تتَّسِم **بمرونة عالية وقدرة هائلة على التطوُّر**، فهي لا ترتبِط بأنماط إجرامية ثابتة كما هو الحال مع الجرائم التقليدية، بل تتغير بتغُّير التقنيات والبرمجيات والأدوات المستعملة في الحياة اليومية.

هذا التطور لا يأتي فقط من التقدُّم التكنولوجي، وإنما أيضًا من **الابتكار الإجرامي** الذي يبديه مرتكبو هذا النوع من الجرائم، حيث يسعون دائمًا إلى استغلال الثغرات الجديدة في الأنظمة الإلكترونية أو استخدام وسائل لم تكن محسوبة من قبل، مثل الاستعانة ببرمجيات الذكاء الاصطناعي أو خوارزميات تعلم الآلة في تنفيذ الاحتيال أو التجسُّس.

[1] الكعبي محمد عبيد ، **الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الانترنيت** ، دار النهضة العربية ، القاهرة طبعة2، 2009، ص39

يُضاف إلى ذلك أن بعض الجرائم تتطوَّر من حيث الوسيلة فقط، فمثلاً الاحتيال المالي الذي كان يتم وجهًا لوجه، أصبح الآن يتم عن طريق البريد الإلكتروني أو مواقع الويب المزيفة، مع الحفاظ على ذات النتيجة الجنائية. هذا التغير الدائم يجعل من الجريمة الإلكترونية **ظاهرة متحرّكة تستلزِم رقابة ومتابعة دائمة من قبل الجهات التشريعية والتنفيذية**، كما تتطلب تكييفًا مُستمرًا لمناهج التكوين الأمني والقضائي .

2. جرائم تستلزِم المعرفة و الدراية

لا يستطيع أي شخص عادي ارتكاب الجريمة الإلكترونية، بل يتطلَّب الأمر **مستوى معينًا من الكفاءة التقنية والمعرفة المعلوماتية** .فالجاني غالبًا ما يكون خبيرًا في التعامُل مع الحواسيب، متمكنًا من تقنيات البرمجة أو الشبكات أو الحماية المعلوماتية، ويُطلق عليه في بعض الأدبيات اسم "المجرم الذكي."

هذا الشرط المعرفي يجعل من هذه الجرائم **أكثر نخبوية من غيرها**، حيث نجد أن مرتكبيها ينتمون إلى فئات عمرية وشبابية، ويستغلون معارفهم التكنولوجية لتحقيق أغراض إجرامية، أحيانًا بدافع الربح المادي، وأحيانًا بدافع الشهرة أو الانتقام أو الإيديولوجيا.وما يزيد في تعقيد الأمر أنَّ هذا النوع من الجريمة لا يمكن تفكيكه أو تتبُّعه إلا بواسطة **خبراء في التكنولوجيا الرقمية**، ممَّا يفرِضُ على الأجهزة الأمنية تكوين فرق مختصة في الأمن السيبراني والطب الشرعي الرقمي، وهو ما يتطلَّب موارد بشرية ومادية كبيرة .

3.جرائم هادئة الأداء

خلافًا للجرائم التقليدية التي تعتمِدُ على العنف أو القوة الجسدية،فإن الجريمة الإلكترونية [1] **تتِمُّ في هدوء وصمت تام**، دون الحاجة إلى اختراق فعلي لمكان مادي أو استخدام وسائل عنيفة. فالمجرم الإلكتروني لا يحمل سلاحًا، ولا يترك أثارًا مادية مرئية، بل يعتمد على أدوات رقمية مثل الفيروسات أو الروابط المُزيَّفة،أو الشفرات الخبيثة التي تُنفِّذُ المهام بشكل خفي.هذه "النعومة" لا تعني أن الجريمة أقل خطرًا، بل العكس،لأنها **قد تمُرُّ دون أن ينتبِه لها الضحية أو السلطات المختصة إلا بعد فوات الأوان** . ويكفي أن نعرف أن الكثير من ضحايا الجرائم الإلكترونية لا يكتشفون الاختراق أو الاحتيال إلا بعد أيام

[1] الصغير جميل عبد الباقي، **الأنترنيت و القانون الجنائي الأحكام الموضوعية للجرائم المتعلقة بالانترنيت**، دار النهضة العربية ، القاهرة ، مصر 2001، طبعة1، ص19

أو أسابيع، وقد لا يكتشفونه أبدًا.هذا ما يجعل الجريمة الإلكترونية من أكثر أنواع الجرائم تهديدًا للأمن السيبراني، خاصة أنها تتم بطرق متطورة وغير محسوسة،ويصعب توثيقها أو إثباتها كما هو الحال في الجرائم التقليدية .

4. جرائم يندمِجُ فيها الفضاء الالكتروني مع العالم الواقعي

لم تعُد الجريمة الإلكترونية مُجرَّد فعل يتم في فضاء افتراضي معزول عن الواقع،بل أصبحت **تترك آثارًا ملموسة في الحياة الواقعية** .فمثلاً عندما يتم اختراق حساب مصرفي وسرقة الأموال فإنَّ الضرر يقع فعليًا في الحياة الواقعية، ويؤثر على الاقتصاد والأفراد.كما أنَّ بعض الجرائم التي تبدأ عبر الإنترنت تتحوَّل لاحقًا إلى أفعال مادية،مثل الابتزاز أو الاستغلال الجنسي أو حتى القتل،وهو ما يسمى في بعض الأدبيات بـ "التحوُّل من الافتراضي إلى الواقعي"

من هنا تظهر خطورة الجريمة الإلكترونية في قُدرتِها على **طمس الفوارق بين العالم الرقمي والعالم المادي**،ممَّا يزيد من تعقيد التحقيقات الأمنية، لأنَّ الأدلة أحيانًا تكون رقمية بحتة،وتتطلَّب إجراءات قانونية وفنية خاصَّة لاستخراجها وحمايتها .

5. جرائم تتخطَّى حدود الزمان و المكان .

تتميز الجريمة الإلكترونية بقُدرتِها على تجاوُز القيود التقليدية للزمان والمكان،فالجاني يمكن أن يرتكب جريمته في أي لحظة،ومن أي مكان في العالم، دون أن يتحرَّك من مكانه. وهذا يعني أنَّ **المسافة الجغرافية لم تعُد عائقًا** أمام تنفيذ هذه الجرائم .

كما أنَّ الجريمة لا ترتبِطُ بوقت مُحدَّد،بل يمكن أن تُنفَّذ أو تستمِر على مدار الساعة.هذه الخاصية تطرح **تحديات كبيرة أمام التشريعات الوطنية** لأنَّها تفترِض أحيانًا وجود أكثر من دولة معنية بالجريمة: دولة يوجد فيها الجاني،وأخرى يوجد فيها الضحية، وربما دولة ثالثة تحتوي الخوادم المستعملة في الجريمة.هذا التداخُل يفرِض **تعاونًا دوليًا في المجال القانوني والأمني**،وإلاَّ فإنَّ الكثير من الجرائم تبقى دون عقاب،بسبب إشكالات الاختصاص القضائي أو غياب الاتفاقيات الدولية الملائمة[1].

[1] يوسف أمير فرج ، **الإثبات الجنائي للجريمة الالكترونية و الاختصاص القضائي بها – دراسة مقارنة للتشريعات العربية و الأجنبية** – مكتبة الوفاء القانونية ، الإسكندرية ، طبعة 1، 2016، ص78.

6. جرائم صعبة الإثبات و الملاحقة

من أبرز العقبات التي تواجِهُ أنظمة العدالة في التعامُل مع الجرائم الإلكترونية هي **صعوبة إثباتِها وملاحقة مرتكِبيها** فعلى عكس الجرائم التقليدية التي قد تترُك أدلة مادية كالبصمات أو شهود العيان،فإن الجريمة الإلكترونية **تترك وراءها آثارًا رقمية** غير مرئية تحتاج إلى أدوات وخبرات متخصِّصة لاكتشافها.

وقد يعمل الجاني على إخفاء هويته باستخدام برامج التخفِّي (VPN) أو الشبكات المُظلِمة (Dark Web) أو حسابات وهمية،ممَّا يُعقِّدُ من عملية التتبُّع والكشف عن المصدر الحقيقي للهجوم. إضافة إلى ذلك، فإنَّ العديد من هذه الجرائم تتجاوز الحدود الجغرافية للدول،مما يجعل التعاوُن القضائي الدولي ضرورة، وفي غيابه، قد يُفلت الجناة من العقاب، خصوصًا إذا كانوا يتواجدون في بلدان لا تتعاون قضائيًا أو لا تعترِف بالجرائم المعلوماتية ضمن قوانينها[1].

7. خصوصية الضرر الناجم عن الجرائم الالكترونية

الجرائم الإلكترونية ليست جرائم بسيطة أو محدودة الأثر،بل هي **جرائم قادرة على التسبُّب في أضرار بالغة الخطورة** سواء على المستوى الفردي أو المؤسسي أو حتى الدولي.فهي قد تؤدي إلى[2]:

- **خسائر مالية ضخمة**:كما في حالات الاحتيال البنكي أواختراق أنظمة الشركات؛
- **انتهاك الخصوصية**:من خلال تسريب بيانات شخصية أو ابتزاز الضحايا بصور أو معلومات حساسة؛
- **أضرار اقتصادية وسياسية**،كما في الهجمات السيبرانية التي تستهدف البنى التحتية أو الأنظمة الحكومية الحساسة.بل إن بعض الجرائم الإلكترونية قد تؤدي إلى **حروب سيبرانية** بين الدول في ظل الاعتماد المتزايد على التكنولوجيا في قطاعات الدفاع والطاقة والاتصالات.

8. جرائم تتميَّز بسُرعة التنفيذ و سهولة إتلاف الأدلة من قبل الجناة

أحد أخطر جوانب الجرائم الإلكترونية هو **سُرعة تنفيذها الشديدة**، إذ يمكن للمجرم تنفيذ فعل إجرامي كامل في ثوانٍ معدودة،دون أن يُضطر للتنقُّل أو التواصُل المباشر مع الضحية.كما أن الجناة يمتلكون القدرة على **إتلاف الأدلة الرقمية بسهولة**، من خلال حذف الملفات أو تشفيرها، أو تدمير

---

[1] النادي محمد إبراهيم سعد ، **جرائم الانترنيت بين الشريعة الإسلامية و القوانين الوضعية – دراسة مقارنة** – مكتبة الوفاء القانونية ، الإسكندرية ط1، 2017، ص168.

[2] نفس المرجع ، ص170 .

الأقراص الصلبة، أو استخدام أدوات إلكترونية لمسح سجلات التصفُّح والمعاملات.وبما أن هذه الأدلة تتعلق بالبيئة الرقمية،فإنَّ **مرور الوقت يُمثِّلُ تهديدًا حقيقيًا لسلامتها**، فكل تأخير في كشف الجريمة قد يؤدي إلى فقدان الدليل أو تعديله،الأمر الذي يزيد من صعوبة التحقيق والمحاكمة[1].

9. خصوصية وسائل وطُرق توثيق الدليل الجنائي

توثيق الأدلة في الجرائم الإلكترونية يتِمُّ وِفق قواعد **التحقيق الجنائي الرقمي**، وهي إجراءات دقيقة تهدِفُ إلى استخراج الأدلة من الأجهزة والأنظمة الرقمية **مع الحفاظ على سلامتِها القانونية والفنية** ويُعد التوثيق في هذا السياق تحديًا كبيرًا، لأنه يتطلَّب[2]:

- استخدام أدوات مُخصَّصة لتحليل وتفريغ محتوى الأقراص الصلبة أو الشبكات ؛
- ضمان عدم تغيير أو تلف البيانات أثناء جمعها؛
- إعداد تقارير تقنية دقيقة يمكن اعتمادها قضائيًا.ويُفرض على المحقق الرقمي أن يتعامل **بحذر واحترافية شديدة**، لأن أي خلل في توثيق الأدلة قد يؤدي إلى رفضِها أمام الجهة القضائية ، ممَّا يُعطِّلُ مسار العدالة.وهنا تظهر الحاجة إلى تكوين مهني مُتخصِّص في مجال الأدلة الرقمية إضافة إلى سن قوانين دقيقة لضبط إجراءات إثباتِها.

10. جرائم غاية في الدقة

الجرائم الإلكترونية تتِّسِمُ بدرجة **عالية من الدِقَّة والتخطيط**، إذ أن الجُناة لا يتصرفون بعشوائية بل يدرسون خطواتهم بدقة،مُستعينين ببرمجيات وأدوات متقدِّمة.في حالات عديدة، تتم البرمجة المُسبقة للهجوم الإلكتروني (مثل الفيروسات أو برامج الفدية) بطريقة تجعلُها **تستهدِفُ أنظمة مُحدَّدة**، أو تنتظِرُ توقيتًا مُعينًا للتنفيذ، ممَّا يعكِس مستوى عالٍ من الدقة والتنظيم.هذه الجرائم تُدار في الغالب من طرف **عصابات إلكترونية مُنظَّمة أو محترفين مستقلين**، لديهم خبرات مُتقدِّمة في التعامُل مع الشبكات، وتشفير البيانات، واستخدام الثغرات الأمنية.وقد تشمل الجريمة الواحدة عدة مراحل، تبدأ

[1] الشوايكة محمد أمين ، **جرائم الحاسوب و الانترنيت الجريمة المعلوماتية** ، دار الثقافة للنشر و التوزيع ، عمان ، الأردن . 2011، ص221 .

[2] الدسوقي محمد كمال محمد ، **الحماية الجنائية لسرية المعلومات الإلكترونية – دراسة مقارنة** –دار الفكر و القانون للنشر والتوزيع ، القاهرة ، 2015، ص17

بالاستطلاع،ثم التسلُّل، ثم جمع المعلومات، ثم التنفيذ النهائي، وكل مرحلة تتِمُّ **بأسلوب علمي دقيق يصعُب رصدُه أو إيقافه دون تدخُّل تقني مُتخصِّص**[1].

ثانيا : صور الجريمة الالكترونية

الجرائم الالكترونية ليست نوعا واحدا،وإنما تختلف حسب الأساس والمعيار الذي يستند إليه الفقهاء في تقسيمهم لهذه الجرائم، فبعضهم يقسمها إلى جرائم تُرتكب على نظم الحاسوب وأخرى تُرتكب بواسطته وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المُتَّبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة،وغيرهم يؤسس تقسيمه على تعدُّد محل الاعتداء، وتعدُّد الحق المُعتدى عليه فتُوزَّع جرائم الحاسوب وفق هذا التقسيم إلى جرائم تقع على الأموال بواسطة الحاسوب وتلك التي تقع على الحياة الخاصة[2].

ويصف الأستاذ " يونس عرب " تصنيف الجريمة الالكترونية تبعا لمساسها بالأشخاص والأموال بأنه الشائع في الدراسات والأبحاث الأمريكية كما أنه المعيار المُتبع في تقسيم الجرائم الإلكترونية في مشروعات القوانين النموذجية وأشار في هذا الصدد إلى مشروع نموذجي يسمى :" Model State Computer Crime Code[3]

وفي نطاق هذا القانون النموذجي تُقسَّم الجرائم الإلكترونية إلى :

1- الجرائم الواقعة على الأشخاص.

2- الجرائم الواقعة على الأموال عدا السرقة.

3- جرائم السرقة والاحتيال.

4- جرائم التزوير والمقامرة والجرائم المنافية للآداب.

---

[1] عرب يونس خالد ، **دليل أمن المعلومات والخصوصية جرائم الكمبيوتر والأنترنيت** ، منشورات اتحاد المصارف العربية ، ط1، 2002 ، ص269.

[2] الطائي، جعفر حسن جاسم، **جرائم تكنولوجيا المعلومات**، دار البداية، الطبعة الأولى، 2007، ص 131.

[3] عرب، يونس ،**إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات**، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – ابو ظبي 10-12 /2/ 2002 ص 10 – 13 .

5- الجرائم الماسة بالمصالح الحكومية.

وتبعاً لهذا التقسيم الوارد ضمن مشروع القانون النموذجي الأمريكي فإن تصنيف الجريمة جاء على النحو الآتي:[1]

أولاً: طائفة الجرائم التي تستهدِفُ الأشخاص:

الجرائم غير الجنسية التي تستهدف الأشخاص،وتشمل هذه الطائفة جرائم القتل بالحاسب الآلي وجرائم الإهمال المرتبط بالكمبيوتر والتي تسبب الوفاة والتحريض على الانتحار والتحضير المتعمد عبر الإنترنت وهنالك جرائم التحرش عبر وسائل الاتصال والقدح والذم والشتم والتحقير .

وتشمُل هذه الطائفة ضمن التقسيم مجموعة جرائم تحريض القاصرين على أنشطة جنسية غير مشروعة وإفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية ومحاولة إغواء القاصرين بارتكاب أنشطة جنسية غير مشروعة والتحرش الجنسي بالقاصرين أو تلقي ونشر المعلومات عبر الإنترنت عن القاصرين، من أجل أنشطة جنسية غير مشروعة.

ثانياً: الجرائم المتعِلقة بالأموال عدا السرقة:

تشمل هذه الطائفة الاقتحام غير المصرَّح به مع نظام الحاسب الآلي لارتكاب فعل معين في الموقع المُقتحَم ضد البيانات والبرامج والمخرجات، لتخريب الحاسب الآلي من خلال نشر الفيروسات، ويدخُل فيها أيضا استخدام اسم الغير أو العلامة التجارية دون ترخيص وهذه طائفة واسعة في التجارة الالكترونية.

ثالثاً: طائفة جرائم الاحتيال والسرقة:

هذه الطائفة من أكبر وأوسع الجرائم انتشارا حتى الآن, وهي تشمل جرائم الاحتيال عن طريق التلاعُب بالمعطيات والنُّظم واستخدام الكمبيوتر للحصول على البطاقات المالية للغير عبر انتحال الصفات أو المعلومات داخل الكمبيوتر.

رابعاً: طائفة جرائم التزوير:

[1] عرب يونس ، المرجع السابق، ص13-14

وتشمل هذه الطائفة تزوير البريد الإلكتروني وتزوير الهوية،أو تزوير بطاقات الائتمان أو تزوير التوقيع الإلكتروني والبصمة الإلكترونية وبطاقات الدفع الإلكتروني.

خامساً: طائفة جرائم المقامرة والجرائم الضارة بالصحة:

تشمل هذه الطائفة تملُّك وإدارة مشروعٍ للمقامرة على الإنترنت أو استخدام الحاسب الآلي وشبكة الإنترنت للترويج للكحول ومواد الإدمان الأخرى كالحشيش والأفيون وسائر المخدرات المعروفة عالمياً ومحلياً.

سادساً: الجرائم الإلكترونية الماسَّة بالحكومة:

تشمل هذه الطائفة من الجرائم قطاع واسع بحيث تضم كافة جرائم تعطيل الأعمال الحكومية أو تعطيل تنفيذ القانون، أو تهديد السلامة العامة ويشمل ذلك: الإرهاب الإلكتروني والأنشطة الثأرية وأنشطة التدمير والاختراق الإلكتروني .[1]

الفرع الثاني: أركان الجريمة الالكترونية

سنتناول في هذا المطلب الأركان الثلاثة لأية جريمة للوقوف عند مدى توافُقها واختلافِها مع الجريمة محل البحث، وهي الركن الشرعي والمادي والمعنوي .

ثالثا: الركن الشرعي (القانوني)

الركن الشرعي للجريمة،هو النّص القانوني الذي يُحدّد قواعد القانون الجزائي من حيث التجريم والعقاب والبنيان الجوهري لأي جريمة .[2]

ويقوم هذا الركن بالنّسبة **للجريمة الإلكترونية** كغيرها من جرائم القانون على مبدأ **الشَّرعية الجزائية** الذي يستمِدُّ أساسه ابتداءً من المادة 43 من الدستور [1] : " لا إدانة إلاّ بمقتضى قانــونٍ صادرٍ

[1] عرب يونس ، المرجع السابق، ص14 .

[2] أحمد عبد الظاهر الطيب ، **الجديد في الموسوعة الجنائية – دراسة لأهم جرائم قانون العقوبات والتشريعات الجنائية الخاصة** – دار النهضة العربية ، القاهرة ، مصر ، **1997** ، ص ، **329** .

قبل ارتكاب الفعل المُجرَّم. " والمادة **الأولى** من **قانون العقوبات** : " لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون . "

فتحديدُ الأفعال التي تُعَدُّ جرائم،وبيان أركانها،وتحديد الجزاءات المُقرّرة لها من حيث نوعِها أو مقدارِها،كلّ ذلك يجب أن يرد صراحة في نص قانوني مكتوب يضعه المشرع سلفا .[2]

إن الركن الشرعي يعني السند القانوني لتجريم الفعل،وإعمالا لذلك فإنه من غير الممكن بحال الاجتهاد من القاضي الجزائي، فلا يجوز القياس في التجريم[3]

ولأنَّ الجرائم الإلكترونية حديثة وذات تقنية عالية،ووضع نصوص خاصة بها ليس بالأمر السهل وعلى الرغم من ذلك فقد سارت الجزائر على نهج العديد من الدول [4] في تجريم الأفعال التي تشكل مساسا بالمنظومات المعلوماتية سواء بموجب تشريعات خاصة على نحو ما جاء به القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما،أو بموجب التشريعات الجنائية العامة على نحو ما جاء به قانون العقوبات الذي استحدث قسما خاصًا لها بموجب

---

[3] المادة **43** من المرسوم الرئاسي 20-442 المؤرخ في 15 جمادى الأولى 1442 الموافق لـ 30 ديسمبر 2020 **يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020 في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية** ، ج.ر عدد 82 صادر بتاريخ 30 ديسمبر 2020 .

[2] محمود نجيب حسني ، **شرح قانون العقوبات – القسم العام** – دار النهضة العربية ، القاهرة ، مصر ، ط**5** ، **1982** ص ، **82** .

[3] المضحكي، حنان ريحان مبارك، **الجرائم المعلوماتية–دراسة مقارنة**–منشورات الحلبي الحقوقية، ط 1، 2014، ، ص56

[4] هناك بعض الدول وضعت قوانين لمثل تلك الجرائم ، وتعد دولة السويد أول دولة تضع قوانين خاصة لهذه الجرائم، حيث أصدرت وفي عام 1973 قانون البيانات وبعد ذلك وبين عامي (1976-1985) سنت الولايات المتحدة الأمريكية قانون لحماية أنظمة الحاسب الآلي، فتبعتها فرنسا والتي قامت في عام 1988 بتطوير قوانينها الجنائية لتتوافق مع ما استُحدث من جرائم، وأما فيما يخص الدول العربية فقد قامت بعضها بسن بعض القوانين في هذا المجال مثل السعودية التي أصدرت في العام 2007 نظامي التعاملات الالكترونية ونظام مكافحة الجرائم المعلوماتية والإمارات العربية المتحدة التي أصدرت القانون الإتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات / **أنظر** : في ظل غياب القوانين والتشريعات التي تحاسب المتورطين فيها، الجريمة الالكترونية في فلسطين مباحة" مقال منشور على الإنترنت، تاريخ الاطلاع: 12-4-2025، على الساعة :16-55 على الرابط التالي http://www.alqudsalraqmi.ps/atemplate.php?id=392

المواد من 394 مكرر إلى 394 مكرر 7 بموجب القانون 04-15 [1] وكذا القانون 21-11 المعدل والمتمم لقانون الإجراءات الجزائية لاسيما المادة 211 مكرر 22، فمختلف هذه النصوص حدَّدت مفهوم هذه الجريمة والأفعال التي تدخل في ارتكابها ، لتُشكل بذلك الأساس القانوني الذي يجرم مختلف الأفعال التي تُرتكب في العالم الافتراضي بوصفها جرائم إلكترونية .

ثانيا : الركن المادي

يمثّل الرُّكن المادي للجريمة بصفة عامّة،المظهر الخارجي للسلوك الإجرامي وما يترتّب عنه من ضرر.[2] والذي يُقرِّر المشرع لأجله جزاءً جنائيا . هذا المظهر الخارجي لا يكون له وجود في العالم الخارجي إلاّ بقيام الشخص أو عدم قيامه بأفعال مادية محسوسة كما حدّدتها نصوص التجريم ، فكلّ جريمة إذًا لابُدَّ لها من ماديات تتجسّد فيها الإرادة الإجرامية لمرتكبها .[3] ومن ثمَّة يُشترط لاكتماله ضرورة توافُر عناصره من سلوك جرمي (فعل أو امتناع عن فعل) ونتيجة جرمية وعلاقة سببية بينهما.

1- السلوك الجرمي:

إنّ السلوك الإجرامي يُعبِّر عن نشاط الجاني،والنشاط إمّا أن يكون بعمل إيجابي في صورة القيام بعمل يمنعه القانون،وينبني على حركة عضوية إرادية ونتيجة ورابطة سببية.[4] إذ القاعدة العامَّة في قانون العقوبات أنّه ينهى بأوامره عن ارتكاب بعض الأفعال التي يرى المشرع أنّ لها خطورة على المجتمع فيُقرِّر عقابا لكلّ من يرتكبها .

ويثور التساؤل في هذا المقام هل السلوك الجرمي والذي ينصرِفُ على كافَّة الجرائم التقليدية ينطبِقُ على الجريمة الالكترونية محل البحث ؟

---

[1] تم إضافة القسم السابع بعنوان : " **جرائم المساس بأنظمة المعالجة الآلية للمعطيات** " بموجب القانون **15/04** المؤرخ في **4** ربيع الثانية **1435** الموافق لـ **4** فبراير **2014** يعدل ويتمم الأمر 66-166 المؤرخ في 08 صفر 1386 الموافق لـ 8 يونيو 1966 المتضمن **قانون العقوبات** ، ج.ر عدد **71** صادر بتاريخ **10** نوفمبر **2004** .

[2] محمود محمود مصطفى، **شرح قانون العقوبات** –**القسم العام** –دار النهضة العربية ، القاهرة ، مصر، **1974** ، ص **38**

[3] علي عبد القادر القهوجي ، **قانون العقوبات – القسم العام –** الدار الجامعية ، بيروت ، لبنان ، **1994** ، ص **173** .

[4] Salvage Ph , **droit pénal général** , 3éme **édition , 1994 , p 34** .

بما أنَّ الجاني في الجرائم الالكترونية يختلف عن الجاني في غيرها من الجرائم من حيث كونه ذا خبرة كافية في مجال استخدام التقنيات الحديثة .[1] فإن السلوك الجرمي الذي سيصدُر منه في مجال ارتكاب الجريمة الالكترونية حتما سيختلِف عن الجاني التقليدي.

وبالرجوع لأحكام قانون العقوبات ، يُلاحَظ أنَّ المشرع قد حدَّد بموجب المواد من **394** مكرر إلى **394** مكرر **2** من القانون **04-15** طائفة الأفعال التي تشكل السلوك الجرمي لهذه الجريمة فيما يلي :

- أفعال الدخول والبقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات .

- الإدخال أو الإزالة أو التعديل بطريق الغش لمعطيات في نظام المعالجة الآلية للمعطيات .

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

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

2- النتيجة الجرمية

النتيجة الإجرامية هي آخر حلقات الفعل الإجرامي،تتجسّد في الأثر المُترتّب على السلوك الإجرامي الذي يأخذه المشرع بعين الاعتبار في التكوين القانوني للجريمة .[2] وهي أيضا الأثرُ المادي المُتمخِّض عن السلوك الإجرامي والمُعتد به قانونا .[3]

والنتيجة الجرمية في الجرائم التقليدية هي ما يترتَّب على الفعل الذي أتاه الجاني، فلا يكفي قيام الجاني بسلوكه الإجرامي مهما بلغت جسامته، بل لا بد من أن ينتُج عن هذا السلوك نتيجة، ففي جريمة القتل لا بد من أن ينتج عن سلوك الجاني وفاة المجني عليه، فإذا لم تنتج الوفاة عن فعل القتل لا نكون أمام جريمة قتل وإنما نكون أمام جريمة شروع في القتل.

---

[1] هروال نبيلة هبة، **الجوانب الإجرائية لجرائم الأنترنت**، دار الفكر الجامعي، طبعة 1، 2007، ص45 .

[2] محمود محمود مصطفى ، **قانون العقوبات – القسم العام –** دار الفكر العربي ، القاهرة ، **1979** ، ص **124** .

[3] محمد عوض ، **قانون العقوبات – القسم العام –** دار الجامعة الجديدة للنشر ، الإسكندرية ، مصر ، **2000** ، ص **59**

أما النتيجة الجرمية في الجريمة الالكترونية، فيثور النقاش بشأنها فيما إذا كانت نتيجة الفعل الجرمي في العالم الإفتراضي أم في العالم الحقيقي،وفي الحقيقة فإن الفرضيتان مُحتملتا الحدوث في الجرائم الإلكترونية، فمن الممكن حدوثها بالعالم الحقيقي، مثل إزهاق روح إنسان كانت حياته مُستمِرَّة عن طريق جهاز كمبيوتر، فباختراق هذا الكمبيوتر(جريمة الكترونية) فإن نتيجتها تكون بالعالم الحقيقي بقتل هذا الإنسان.[1] ويبقى في كل الحالات الركن المادي مُتوافِر، وكما سبق وأشرنا،فإن النتيجة الجرمية تشكل مشكلة في موضوع التوقيت والاختصاص،بحيث يمكن أن تدخُل دولتين وثلاثة في ذات الجريمة، ممَّا يُشكِّلُ تنازُعا في تطبيق القوانين.[2]

إنَّ الجرائم الإلكترونية هي من جرائم الخطر[(3)]، وهي التي لا يستلزِم نموذجها القانوني نتيجة مُعيّنة ، كون الاهتمام فيها مُنصبّ على السلوك بذاته ، فمُجرَّد احتمال وقوع الضرر كاف لقيام الجريمة وفي هذا الصدد خوَّل القانون 09-04 بموجب الفقرة –ب– من المادة 4 منه للأعوان المُكلّفين بالبحث والتحرّي عن جرائمه حق القيام بالمُراقبة الالكترونية لمُجرّد وجود احتمال وقوع اعتداء على منظومة معلوماتية من شأنِه أن يُهدّد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني . فالتجريم في هذا القانون جاء وقائيا لتفادي إلحاق الضرر بالمُتغيّرات أعلاه أي النظام العام ، الدفاع الوطني ، مؤسسات الدولة والاقتصاد الوطني .

3- علاقة السببية

رابطة السببية:مفادُها إسناد النتيجة المُعاقب عليها إلى سلوك الفّاعل عن طريق الرّبط بينهما فلا يكفي لقيام الركن المادي أن يقع سلوك إجرامي من الفاعل وأن تحصُل نتيجة عن ذلك السلوك، بل يلزمُ أيضا أن تُسند النتيجة إلى ذلك السلوك؛ أي لابُدَّ أن يكون بينهما صلة سببية تُحمِّل على القــول بأنّ سلوك الفاعل هو الذي تسبّب بتلك النتيجة الضّارة . [(4)]

---

[1] هروال نبيلة هبة ، المرجع السابق، ص47 .

[2] نفس المرجع ، نفس الصفحة .

[3] محمد عوض ، المرجع السّابق ، ص **59** .

[4] سميــر عالية ، **شرح قانون العقوبات – القسم العام –** المؤسسة الجامعية للدراسات والنشر والتوزيع ، بيروت ، لبنان **1998** ، **ص 208** / نبيل صقر ، عز الدين قمراوي ، **الجريمة المنظّمة–التهريب والمخدرات وتبييض الأموال في التشريع الجزائري** ، دار الهدى ، عين مليلة، الجزائر **2008** ، ص **31** .

فيجب أن تتحقّق علاقة السببية بين سلوك الجاني وبين النتيجة التي ترتبت على فعله، أي أن النتيجة الجرمية سببُها سلوك الجاني،ففي جريمة القتل وفاة المجني عليه سببه سلوك الجاني الإجرامي.

وقد نستطيع تطبيق ذات القواعد العامة المطبقة على الجرائم العادية على الجرائم الالكترونية فيما يتعلَّق بعلاقة السببية إذا انطبقت عليها، ففي جريمة سرقة الشيء المعلوماتي،فاختلاس الشيء المعلوماتي يتحقَّق بالنشاط المادي الصادر عن الجاني سواء بتشغيله للجهاز للحصول على المعلومة أو البرنامج أو الاستحواذ عليها،وهو ليس في حاجة لاستعمال العنف لانتزاع الشيء،وتشغيله الجهاز لاختلاس المعلومة تتحقق النتيجة بحصوله عليها، فرابطة السببية إذن مُتوافِرة بين نشاطه المادي والنتيجة الإجرامية[1].

ثالثا: الركن المعنوي

الركن المعنوي ركن أساسي لا يمكن للجريمة أن تتكوّن قانونا من دونه إلاّ إذا ورد نصٌّ صريح يُعبّر عن نيّة المشرع في إقصائه من بنيان الجريمة . [(2)]

ويقوم الركن المعنوي على عنصر القصد الجرمي – كما هو مفهومه في الجرائم العادية – يعني العلم بعناصر الجريمة، بالتالي فإن هذا الركن يتكون من علم وإرادة،وأما العلم فهو فهم الأحداث والأمور كما هي في الواقع،أي أنه يسبق الإرادة، وأما الإرادة فهي التوجُّه لفعل ولتحقيق الفعل الجرمي.

ففي الجرائم الالكترونية حتى ولو كانت النتيجة الجرمية بسبب صدفة أو فضول، أي أن الجاني لم يقصد ابتداءً أن يرتكب الجريمة، إلا أنَّ الركن المعنوي يبقى متوافرا، حيث أن الأجدر بالفاعل أن يتراجع عن فعله لا أن يستمر، وبالتالي فإن استمراره يجعل الركن المعنوي متوافر.

وبالرجوع لأحكام قانون العقوبات،يُلاحظ أن المشرع قد تطلَّب الركن المعنوي في هذه الجرائم حسب ما نصت عليه المادة 394 مكرر 2 التي جاء فيها : " ... كل من يقوم عمدا ... "

---

[1] قشقوش، هدى حامد، **جرائم الحاسب الالكتروني في التشريع المقارن**، دار النهضة العربية، القاهرة، مصر ، **1992** ص 61 – 62 .

2. محمود نجيب حسني ، **النظرية العامّة للقصد الجنائي** ، دار النهضة العربية ، القاهرة ، مصر، ط**2** ، **1986** ص **129** .

المبحث الثاني: المنظومة القانونية لمكافحة الجريمة الإلكترونية في التشريع الجزائري

مع التطوُّر المتسارِع في مجال تكنولوجيا المعلومات والاتصالات، برزت أنواع جديدة من الجرائم التي لم تكن مألوفة في الماضي، وهو ما دفع المشرّع الجزائري إلى مراجعة منظومته القانونية وتكييفها مع التحديات المُستجدَّة. ومن هذا المنطلق، أقرّ القانون مجموعة من العقوبات التي تهدِف إلى مواجهة الجرائم الإلكترونية والتصدِّي لها بفعالية. وتتنوَّع هذه العقوبات بحسب طبيعة الفعل المُرتكب وخطورته حيث تشمل عقوبات سالبة للحرية وأخرى مالية، لتُشكِّل بذلك إطارًا ردعيًا وتشريعيًا مُتكامِلًا لمواجهة التعدِّي على النظم المعلوماتية والمعطيات الرقمية.

المطلب الأول: العقوبات الجزائية للجريمة الإلكترونية

أولى المشرع الجزائري أهمية خاصة لمواجهة الجرائم الإلكترونية، نظرًا لخطورتها وتعدُّد أوجُهها وذلك من خلال إصدار القانون رقم 09-04 المتعلق **بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**.هذا القانون جاء لسد الفراغ التشريعي في ميدان الجرائم المعلوماتية، وقد نص على **مجموعة من العقوبات الجزائية** إلى جانب تلك التي نص عليها قانون العقوبات. تتنوَّع هذه الأخيرة بين عقوبات أصلية تتراوح بين العقوبات السالبة للحرية والمالية إلى جانب بعض العقوبات التكميلية حسب نوع الجريمة وخطورتها .

الفرع الأول:العقوبات الأصلية للجريمة الإلكترونية

العقوبات الأصلية حسب **المادة 4** من **قانون العقوبات** [1] هي : " العقوبات التي يجوز الحُكم بها مُنفصلة دون أن تقترِن بها أيّة عقوبة أخرى . " وتنقسم بخصوص الجريمة الإلكترونية إلى :

أوّلا : العقوبات السالبة للحرية

تُعتبر العقوبات السالبة للحرية – كالسجن والحبس – من أبرز الوسائل الزجرية التي اعتمدها المشرع لمواجهة الجرائم الإلكترونية. وتكمُن خطورة هذه الجرائم في أنَّها قد تُرتكب من **أي مكان في العالم**، ممَّا يفرِض تشديد العقوبات ، وتختلف هذه العقوبات التي تُفرض على الجاني بصفته شخصا طبيعيا باختلاف الفعل المرتكب وخطورته حسب ما حددته المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات والمادة 11 من القانون 09-04 على النَّحو الآتي بيانه :

1. جريمة الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك، وتتمثل عقوبتها السالبة للحرية في الحبس من **ثلاثة (3) أشهر إلى سنة (1) واحدة** ؛

2. جريمة تخريب نظام اشتغال المنظومة المعلوماتية ، تتمثل عقوبتها السالبة للحرية في **الحبس من ستة (6) أشعر إلى سنتين (2)** ؛

3. جريمة الإدخال بطريق الغش لمعطيات في نظام المعالجة الآلية أو الإزالة أو التعديل بطريق الغش للمعطيات التي يتضمنها، تتمثل عقوبتها السالبة للحرية في الحبس من **ستة (6) أشهر إلى ثلاث (3) سنوات** ؛

4. جريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، تتمثل عقوبتها السالبة للحرية في الحبس من **شهرين (2) إلى ثلاث (3) سنوات** ؛

5. جريمة حيازة أو إفشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها من ارتكاب إحدى هذه الجرائم، وتتمثل عقوبتها السالبة للحرية في في الحبس من **شهرين (2) إلى ثلاث (3) سنوات** ؛

[1] المعدلة بالمادة **2 من القانون 06-23** المؤرخ في **29** ذي القعدة **1427** الموافق لـ **20** ديسمبر **2006** يعدل ويتمم الأمر 66-156 **المتضمن قانون العقوبات** ، ج.ر عدد **84** صادر بتاريخ **24** ديسمبر **2006** .

6. المحاولة أو الاشتراك في ارتكاب إحدى هذه الجرائم، يُعاقب عليها بنفس العقوبة السالبة للحرية المقررة للجريمة الأصلية ؛

7. مضاعفة العقوبة السالبة للحرية،وذلك في حالة حذف أو تغيير معطيات المنظومة المعلوماتية أو استهداف الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام ؛

8. عرقلة حُسن سير التحريات القضائية،وتتمثل عقوبتها السالبة للحرية حسب المادة 11 من القانون 09-04 في الحبس من ستة (6) أشهر إلى خمس (5) سنوات .

*ثانيا :*العقوبات المالية – الغرامة –

الغرامةُ الماليةُ، من أقدم العقوبات الأصلية التي أصبحت السِّمة الغالِبة للعقاب لما أثبتته من فعالية في استرجاع الدولة لحقوقها المالية جرّاء مُخالفة أحكام القوانين . فهي دين يقع على عاتق المحكوم عليه يُدفع إلى خزينة الدولة . حيث تقوم على فكرة إلزام المحكوم عليه بدفع مبلغ مُحدَّد بقدر مُحدَّد من النقود لفائدة الخزينة العامَّة،فتُنشئ بذلك علاقة دائنية بين المحكوم عليه والدولة التي تستفيد منها باعتبارها إحدى مصادر إيرادات خزينتها العامّة .[1]

ونظراً للطابع المالي لبعض الجرائم الإلكترونية، خاصة الاحتيال والنصب وسرقة البيانات البنكية، أقرّ المشرع عقوبات مالية صارمة في حق الشخصين الطبيعي والمعنوي ، تتناسب مع خطورة الفعل تهدِف إلى [2] :

- ردع الجناة .
- تعويض الضحايا .

[1] سليمان عبد الله ، **شرح قانون العقوبات الجزائري–القسم العام–ج1**، ديوان المطبوعات الجامعية ، الجزائر، **1998 ص 463– 465** .

[2] سلاطنية بلقاسم، **الجرائم الإلكترونية في التشريع الجزائري**، دار هومة، الجزائر، 2018، ص. 120 .

- تقويض الدافع المالي للجريمة .

وبالرجوع لقانون العقوبات والمادة 11 من القانون 09-04 ، يُلاحظ أن المشرع قد حدد الغرامات المالية المحكوم بها على مرتكب الجريمة الإلكترونية على النحو الآتي :

1. جريمة الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك ، وتتراوح غرامتها المالية بين 50.000 إلى 100.000 دينار جزائري ؛

2. جريمة تخريب نظام اشتغال المنظومة المعلوماتية،وتتراوح غرامتها المالية بين 50.000 إلى 150.000 دينار جزائري .

3. جريمة الإدخال بطريق الغش لمعطيات في نظام المعالجة الآلية أو الإزالة أو التعديل بطريق الغش للمعطيات التي يتضمنها، وتتراوح غرامتها المالية بين 500.000 إلى 2.000.000 دينار جزائري ؛

4. جريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية،وتتراوح غرامتها المالية بين 100.000 إلى 5.000.000 دينار جزائري .

4. جريمة حيازة أو إفشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها من ارتكاب إحدى هذه الجرائم ، وتتراوح غرامتها المالية بين 100.000 إلى 5.000.000 دينار جزائري ؛

5. المحاولة أو الاشتراك في ارتكاب إحدى هذه الجرائم ، يُعاقب عليها بنفس الغرامة المالية المقررة للجريمة الأصلية .

6. مضاعفة الغرامة المالية ، وذلك في حالة حذف أو تغيير معطيات المنظومة المعلوماتية أو استهداف الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام ؛

7. تحديد غرامة الشخص المعنوي بما يُعادِلُ **خمس (5) مرات** الغرامة المقررة للشخص الطبيعي وذلك بعد الاعتراف الصريح بمسؤوليته الجزائية عن هذه الجرائم .

8. عرقلة حُسن سير التحريات القضائية ، وتتراوح غرامتها المالية بين 50.000 إلى 500.000 دينار جزائري؛ متى كان مرتكب الجريمة شخصا طبيعيا ، أما إذا كان مرتكب الجريمة الإلكترونية شخصا

معنويا، فيُعاقب بالغرامة المقررة وفقا للقواعد العامة المنصوص عليها في المادة 18 مكرر[1] من قانون العقوبات والتي تتراوح بين **واحد (1) إلى خمس (5) مرات** الحد الأقصى للغرامة المقررة للشخص الطبيعي .

الفرع الثاني : العقوبات التكميلية للجريمة الإلكترونية

العقوبات التكميلية حسب المادة 4 [2] من قانون العقوبات هي : " العقوبات التي لا يجوز الحكم بها مُستقلّة عن عقوبة أصلية فيما عدا الحالات التي ينصُّ عليها القانون صراحة ، وهي إمّا إجبارية أو اختيارية . " فبالإضافة إلى العقوبات الأصلية، أقرّ المشرع **عقوبات تكميلية**، مُقيّدا الحكم بها بمراعاة حقوق الغير حسن والنية . وهي العقوبات التي من شأنِها أن تُساهم في تضييق الخناق على مُرتكبي الجرائم الإلكترونية [3] . تتمثل هذه الأخيرة متى كان مرتكب الجريمة الإلكترونية **شخصا طبيعيا** حسب ما نصت عليه المادة 394 مكرر 6 من قانون العقوبات فيما يلي :

1- مصادرة الأجهزة والبرامج و والوسائل المستخدمة ، **و**المصادرة حسب المادة 15[4] من قانون العقوبات هي" الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال مُعيّنة أو ما يُعادِل قيمتها عند الاقتضاء."

وتنصبُّ المصادرة في الجرائم الإلكترونية على مختلف الأجهزة والبرامج والوسائل الإلكترونية (أجهزة، برمجيات، وسائط تخزين...) التي استُعملت أو كانت مُعدّة لارتكاب الجريمة .

2- إغلاق المواقع التي تكون محلا لجريمة من الجرائم الإلكترونية المعاقب عليها وفقا للقسم السابع المتعلق بجرائم المساس بالمعالجة الآلية للمعطيات

3- إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتُكِبت بعلم مالكها .

المطلب الثاني: القواعد القانونية والإجراءات الخاصة بالمكافحة

[1] الباب الأول مكرر 1 ، **العقوبات المطبقة على الشخص المعنوي** ، المواد من 18 مكرر إلى مكرر 3 مضافة بموجب القانون 04-15 ، المصدر السابق .

[2] المعدلة بالمادة **2** من القانون **23/06** المعدل والمتمم ، المصدر السّابق .

[3] زيان عبد العزيز، **الجرائم المعلوماتية بين القانون الجزائري والاتفاقيات الدولية**، دار الخلدونية، الجزائر، 2021 ص. 90-107.

[4] المعدلة بالمادة **5** من القانون**23/06** المعدل والمتمم ، المصدر السّابق .

تواجِه الجريمة الإلكترونية صعوبات مُتعدِّدة عند مكافحتها، نظرًا لتداخُلها مع تقنيات مُعقدة وحدود دولية مُتداخِلة. ولهذا، لم يكتفِ المشرّع الجزائري بتحديد العقوبات فقط، بل أرفق ذلك بجملة من القواعد القانونية والإجراءات الخاصة التي تهدِفُ إلى تسهيل عمليات الكشف والتحقيق والمتابعة. تشمل هذه الإجراءات تنظيم طرق جمع الأدلة الرقمية، وضبط آليات التعاون بين الجهات القضائية والأمنية بالإضافة إلى التنسيق مع المنظمات الدولية المختصَّة،بما يضمن التعامُل الفعّال مع هذا النوع من الجرائم الذي يتطلَّب سرعة واستجابة قانونية دقيقة ومدروسة.

الفرع الأول: التشريعات الجزائرية المتعلقة بالجريمة الإلكترونية

أمام الانتشار الواسع للجرائم الإلكترونية وتنوُّع صوَرها، سعت الجزائر إلى وضع إطار تشريعي خاص لمكافحتها، من خلال قوانين جديدة وتعديلات على القوانين الموجودة، تهدِفُ إلى تنظيم استعمال تكنولوجيا الإعلام والاتصال، حماية المعلومات والمعطيات الشخصية، وتجريم مختلف أشكال الاعتداءات الرقمية.

أولاً: القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

هذا القانون يُعد أول لبنة تشريعية أساسية في الجزائر لمعالجة الجرائم المعلوماتية. وقد جاء استجابة لحاجة ملحة آنذاك نتيجة تنامي الاعتداءات الإلكترونية وغياب تأطير قانوني واضح لها. وقد كان الهدف من سنه هو وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ضمن **تسع عشرة (19) مادة** مُوزعة على **ستة (6) فصول**، كل ذلك في إطار مراعاة سرية المراسلات والاتصالات،ولمقتضيات حماية النظام العام ومستلزمات التحريات والتحقيقات القضائية فكان من **أبرز محاوره :**

- حصر نطاق ومجال تطبيقه في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة بموجب القسم السابع مكرر من قانون العقوبات تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات " أو أي جريمة أخرى تُرتكب أو يسهُل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ؛

- وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية ، وذلك من خلال :

- تحديد الحالات التي تسمح باللُّجوء إلى المراقبة الإلكترونية .
- تحديد القواعد الإجرائية لتفتيش المنظومات المعلوماتية .
- تحديد التزامات مقدمي الخدمات في مساعدة السلطات .

– استحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما وتحديد طبيعتها القانونية والمهام المنوطة بها .

– تعزيز سُبل التعاون والمساعدة القضائية الدولية في مكافحتها .

ثانيا : القانون 04-15 المتضمن تعديل قانون العقوبات

بموجبه أدرج المشرع **القسم السابع مكرر** لمدونة **قانون العقوبات** تحت **عنوان " المساس بالمعالجة الآلية للمعطيات "** ضمن **المواد من 394 مكرر إلى 394 مكرر 7**، وذلك من خلال :

– تحديد الأفعال التي تُرتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات بوصفها جرائم إلكترونية ؛

– تحديد العقوبات الأصلية والتكميلية المقرَّرة لمرتكِبيها سواء كانوا أشخاصا طبيعيين أو معنويين .

– النص على تشديد العقوبة متى توفَّرت بعض ظروف التشديد .

– العقاب على الاشتراك والشروع في ارتكاب إحدى الأفعال المُعاقب عليها بموجب هذا القسم .

ثالثا : القانون 06-22 [1] **المعدل والمتمم لقانون الإجراءات الجزائية**

يُعد هذا القانون من بين أهم الآليات التشريعية الإجرائية التي استحدث المشرع بموجبها آليات جديدة واستثنائية في مجال البحث والتحري وجمع الاستدلالات عن الجرائم الخطيرة والعابرة للحدود الوطنية والتي تُعدُّ الجريمة الإلكترونية أحد أخطر صورها . كان ذلك من خلال تعديل **الباب الثاني** من **الكتاب الأول** من هذا القانون ، بإضافة **فصل رابع** تحت عنوان " **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور** " يشمل **المواد من 65 مكرر 5 إلى 65 مكرر 10** ، و**فصل خامس** تحت عنوان " **التسرب** " ويشمل **المواد من 65 مكرر 11 إلى 65 مكرر 118** ، وقد نظم المشرع بموجب هذه

[1] المؤرخ في 29 ذي القعدة 1427 الموافق لـ 20 ديسمبر 2006 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 8يونيو 1966 **المتضمن قانون الإجراءات الجزائية** ، ج.ر عدد 84 صادر بتاريخ 30 ديسمبر 2006

المواد الضوابط القانونية الموضوعية والإجرائية عند اللجوء لمثل هذه الإجراءات والحماية المقررة للقائمين بها كونها إجراءات في غاية الأهمية والخطورة .

ويكمُن وجه التقاطُع بين هذا القانون والقانون 09-04 في إمكانية الاستعانة بهذه الإجراءات الاستثنائية في مواجهة الجرائم الإلكترونية التي نظم أحكامها القانون 09-04 .

رابعا : القانون رقم 15-04 [1] المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين

كان الهدف من سن هذا القانون الذي جاء هذا تدعيما للقانون 09-04 لتحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين وذلك ضمن **82 مادة موزعة على خمسة (5) أبواب** لحماية مختلف التصرُّفات التي يتم التصديق عليها أو توقيعها إلكترونيا، فكان من أهم **محاوره الرئيسية :**

- تحديد مبادئ المماثلة وعدم التمييز تجاه التوقيع الإلكتروني .
- تحديد آليات إنشاء التوقيع الإلكتروني الموصوف والتحقُّق منه .
- تفعيل آلية التصديق الإلكتروني والسلطات المخولة بها .
- استحداث السلطة الحكومية والاقتصادية للتصديق الإلكتروني.
- ضبط النظام القانوني لتأدية خدمات التصديق الإلكتروني .

وتكمن العلاقة بين هذا القانون والقانون 04-09 في الفضاء الرقمي الذي تتم فيه عمليات التوقيع والتصديق الإلكترونيين والتي قد تكون محلا لجريمة أو جرائم إلكترونية .

خامسا : القانون رقم 18-04 [2] المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية

كان من أهداف سن هذا القانون،الذي ضم **190 مادة** موزعة على **خمسة (5) أبواب** ترقية وتطوير الاتصالات الإلكترونية واستعمالها ، فكان من أهم محاوره :

[1] المؤرخ في 11 ربيع الثاني 1436 الموافق لـ أول فبراير 2015 ، ج.ر عدد 6 صادر بتاريخ 10 فبراير 2015 .
[2] المؤرخ في 24 شعبان 1439 الموافق لـ 10 مايو 2018 ، ج.ر عدد 27 صادر بتاريخ 13 ماي 2018 .

- إخضاع نشاطات البريد والاتصالات لرقابة الدولة وإلزامِها بالسهر على أمن وسلامة شبكات الاتصالات الإلكترونية واحترام مبادئ الأخلاق والآداب العامة.

- تحديد النظام القانوني للاتصالات الإلكترونية .

- إقرار عقوبات إدارية وجزائية في حق المخالفين لأحكام هذا القانون في شقِّها الإلكتروني لاسيما تلك المتعلقة بانتهاك سرية المراسلات المرسلة إلكترونيا .

- إنشاء سلطة مستقلة لرقابة نشاط الاتصالات السمعية البصرية .

ويكمُن وجع التقاطُع بين هذا القانون والقانون 09-04 في إمكانية توجيه الاتصالات السلكية واللاسلكية الإلكترونية لارتكاب جرائم إلكترونية .

سادسا : القانون 18-05 [1] يتعلق بالتجارة الإلكترونية

جاء هذا القانون الذي احتوى على **50 مادة** موزعة على **ثلاثة أبواب** خصيصا لحماية مختلف المعاملات التجارية في شكلها الإلكتروني ، محددا من خلال **الباب الأول** نطاق تطبيقه من حيث الأشخاص بحيث شملت الحماية كل شخص متمتع بالجنسية الجزائرية أو مقيم في الجزائر إقامة شرعية وكل شخص معنوي خاضع للقانون الجزائري وكذا متى كان محل العقد التجاري الإلكتروني موجودا في الجزائر أو تم تنفيذ المعاملة التجارية الإلكترونية في الجزائر ، أما من حيث موضوعه فقد منع هذا القانون مختلف المعاملات الإلكترونية المتعلقة بلعب القمار والرهان والبناصيب والمشروبات الكحولية التبغ ، المنتجات الصيدلانية ، المنتجات التي تمس بحقوق الملكية الفكرية والصناعية والتجارية وكذا السلع والخدمات المحظورة أو التي تستوجب عقد رسمي .

كما حدد هذا القانون ضمن **الباب الثاني** مختلف الضوابط القانونية لممارسة التجارة الإلكترونية من حيث تحديد التزامات المستهلك الإلكتروني ، المورد الإلكتروني ، آليات الدفع الإلكتروني ، الإشهار الإلكتروني ، في حين عالج في **الباب الثالث** مختلف الجرائم التي ترتكب في مجال التجارة الإلكترونية محددا الجهات المخولة بمعاينة هذه الجرائم وكذا العقوبات المطبقة على مرتكبيها .

ويكمن وجه التقاطُع بينه وبين القانون **09-04** في السعي نحو توفير بيئة و حماية كافية لمختلف المعاملات التي تتم في الشكل الإلكتروني .

[1] المؤرخ في 24 شعبان 1439 الموافق لـ 10 يونيو 2018 ، ج.ر عدد 28 صادر بتاريخ 16 يونيو 2018 .

سابعا : القانون 18-07 [1] المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

جاء هذا القانون الذي احتوى على **76 مادة** موزعة على **سبعة (7) أبواب** لتحقيق عدة أهداف ذات صلة بالوقاية من الجرائم الإلكترونية من خلال :

- تحديد نطاق المعالجة الآلية للمعطيات الشخصية ، وحصرها في مختلف العمليات المنجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستحراج أو الاطلاع أو الاستعمال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط أو الإغلاق أو التشفير أو المسح أو الإتلاف .
- تحديد الإجراءات المسبقة للمعالجة والتزامات القائمين بها مع تحديد الجزاءات الإدارية والجزائية المقررة في حالة المخالفة .
- تحديد آليات معالجة المعطيات ذات الطابع الشخصي في مجال الاتصالات الإلكترونية .

ويكمُن وجه التقاطُع بين هذا القانون والقانون **09-04** في اعتبار الأول أكثر خصوصية في مجال احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة والتي أصبحت مجالات خصبا لارتكاب الجرائم الإلكترونية مقارنة بالأول الذي كانت أحكامه عامة .

ثامنا : القانون 21-11 المعدل والمتمم لقانون الإجراءات الجزائية

قصد مكافحة الجريمة بصفة عامة والجريمة الإلكترونية بصفة خاصة [2] لجأ المشرع إلى تعديل مختلف النصوص العقابية لاسيما في شقها الإجرائي، وذلك سعيا منه لمواكبة مختلف التطورات الحاصلة في عالم المعلوماتية والتكنولوجيا ، فإلى جانب الأقطاب الجزائية ذات الاختصاص المحلي ، والتي كان معقودا لها اختصاص النظر في هذه الجرائم،استحدث المشرع آلية عمل جديدة تعمل هي الأخرى على وضع حد للإجرام الإلكتروني،وذلك من خلال إنشائه للقطب الجزائي الوطني المتخصص من خلال

[1] المؤرخ في 25 رمضان 1439 الموافق لـ 10 يونيو 2018 ، ج.ر عدد 34 صادر بتاريخ 10 يونيو 2018 .

[2] عون فاطمة الزهراء ، **الإجراءات التشريعية المستحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري – القطب الجزائي الوطني نموذجا –** مجلة حقوق الإنسان والحريات ، جامعة ابن باديس ، مستغانم ، الجزائر ، المجلد 7 ، العدد 2 2022 ، ص 557 .

إضافة الباب السادس لقانون الإجراءات الجزائية تحت عنوان " **القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال** "

وقد نظمت **المواد من 211 مكرر 22 إلى 211 مكرر29** آليات عمل هذا الأخير من خلال تحديد ضوابط الاختصاص النوعي والمحلي له،وكذا تحديد الإجراءات المتبعة من طرفه وعلاقته مع مُختلف الجهات القضائية ذات الاختصاص الجزائي .

وعن دوافع استحداثِه ، فتكمُن في الحاجة إلى هيئة متخصصة لمكافحة الجرائم الإلكترونية تزامُنا مع التقدم السريع لتقنية المعلومات وآثارها السلبية على المستوى المالي والاقتصادي والاجتماعي[1] ، فكان الإنشاء بدافع تفعيل الرقابة على مُرتكِبيها ، يُضاف إلى ذلك فشل ومحدودية الوسائل التقليدية في البحث والتحري عنها[2]. فهذا القانون يُعدُّ بحق قفزة نوعية في مجال مكافحة الجريمة الإلكترونية الآخذة في الانتشار، يكمن وجه التقاطُع بينه وبين القانون 09-04 في اعتباره أداة إجرائية لقمع الجرائم المتصلة بالعالم الافتراضي .

تاسعا : المرسوم الرئاسي 20-05 [3] المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية

كان الهدف من سنه هو وضع منظومة وطنية لأمن الأنظمة المعلوماتية ، بحيث تشكل هذه الأخيرة – المنظومة – أداة الدولة في مجال أمن الأنظمة المعلوماتية، كما تشكل الإطار التنظيمي لإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق جهودها، والتي تم وضعها لدى وزارة الدفاع الوطني . نص هذا المرسوم ضمن **أربعة فصول** موزعة على**43 مادة** على إنشاء هيئتين وطنيتين في مجال حماية أمن الأنظمة المعلوماتية :

- المجلس الوطني لأمن الأنظمة المعلوماتية والمكلف بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة علبها وترخيصها .

---

[1] عون فاطمة الزهراء ، المرجع السابق ، ص 558 .

[2] بن عميور آمنة ، بوحلايس إلهام ، " **القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال** " عدد خاص بفعاليات الملتقى الدولي حول " **القانوني الجنائي للأعمال نحو توجه جديد للتجريم المعقد يوم 14 أكتوبر 2021** " مجلة البحوث في العقود وقانون الأعمال ، جامعة قسنطينة ، الجزائر ، المجلد 7 ، العدد 1 ، 2022 ، ص 72

[3] المؤرخ في 24 جمادى الأول 1441 الموافق لـ 20 جانفي 2020 ، ج.ر عدد 4 صادر بتاريخ 26 جانفي 2020 .

- وكالة أمن الأنظمة مكلفة بتنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية .

ويكمُن وجه التقاطُع بين هذا المرسوم –باعتباره نصا تنظيميا– وبين القانون 09-04 في تعزيز دور الدولة في مجال حماية الأمن المعلوماتي ، وتوحيد جهود تأمين الفضاء السيبراني للدولة ، وتوفير الإطار القانوني والتنظيمي اللازم لحماية البنية التحتية الحساسة والقدرات الوطنية كأحد الأهداف العامة للقانون09-04 .

الفرع الثاني: الإجراءات القانونية لمتابعة الجريمة الإلكترونية والتطوُّرات المستقبلية لمكافحتها

تتنوَّع هذه الإجراءات بتنوع، وتتطور بنسق كبير حسب ما سيتم تفصيله .

أولًا: الإجراءات القانونية لمكافحة الجريمة الإلكترونية

تُعدّ الجريمة الإلكترونية من الجرائم المعقدة التي تتطلب آليات قانونية دقيقة ومتكاملة لمواجهتها فبفضل الطبيعة غير التقليدية لهذه الجرائم، وسرعة تطورها، واعتمادها على وسائل رقمية غير ملموسة ظهرت ضرورة تطوير مجموعة من الإجراءات القانونية التي تواكب هذا التحول. وتتجسد هذه الإجراءات فيما يلي[1]:

1- التحقيق الجنائي في الجرائم الإلكترونية

التحقيق الجنائي في الجريمة الإلكترونية يمثل المرحلة الأولى والأساسية في عملية المتابعة القانونية، حيث تبدأ السلطات المختصة في جمع المعلومات الأولية المتعلقة بالواقعة، ثم تُباشر إجراءات التحري والتحقيق بهدف تحديد طبيعة الجريمة، مرتكبها، والأدلة الرقمية المتعلقة بها. وتختلف هذه التحقيقات عن التحقيقات التقليدية، لأنها تعتمد بدرجة كبيرة على وسائل فنية وتقنية، مثل تحليل البيانات الرقمية، واسترجاع الملفات المحذوفة، وتتبع عناوين الإنترنت، ورصد حركة الحسابات المشبوهة.

ولضمان نجاح التحقيق، يتم التعاون مع خبراء مختصين في الأمن السيبراني، والبرمجة، وتحليل الشبكات الإلكترونية،إذ إنهم وحدهم القادرون على تحليل طبيعة الفعل الإجرامي واستخلاص الأدلة بشكل

[1] حسين بن سعيد الغافري، **التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت** ، دار النهضة العربية، القاهرة 2009 ، ص.17

سليم. ويجب أن تتم هذه العمليات ضمن إطار قانوني واضح، يُحترَم فيه مبدأ الشرعية الإجرائية ويُحفظ فيه الدليل الرقمي دون الإخلال بسلامته أو قابليته للإثبات.

2- التعاون الدولي

الجريمة الإلكترونية، بطبيعتها،لا تعترِف بالحدود الجغرافية، حيث يمكن أن يُرتكب الفعل الإجرامي في بلد معين، وتُستهدف ضحيته في بلد آخر، وتُخزّن بياناته في خوادم تقع في دولة ثالثة. ولذلك، فإن التعاون الدولي يُعد من أهم مرتكزات مكافحة هذه الظاهرة. ويتم هذا التعاون من خلال اتفاقيات ثنائية أو متعددة الأطراف، تُنظّم إجراءات تبادُل المعلومات وتسليم المجرمين والمساعدة القانونية المتبادلة.

كما تلعب المنظمات الدولية دورًا محوريًا في هذا الجانب، من خلال تنسيق الجهود بين الدول وتوفير قواعد بيانات مشتركة، وتقديم المساعدة الفنية في التحقيقات. وفي هذا السياق، يُلاحظ أن الجزائر وإن لم تصادق بعد على اتفاقية بودابست المتعلقة بالجريمة السيبرانية،فإنها تُشارك في عدة آليات دولية وإقليمية للتعاون الأمني والقضائي، خاصة على مستوى العالم العربي وإفريقيا.

3- تحديث التشريعات الوطنية

نظرا للتطوُّر المستمر للوسائل والأساليب الإجرامية في الفضاء الرقمي، أصبح من الضروري تعديل النصوص القانونية بصفة دورية لمواكبة التحديات الجديدة. وقد قام المشرع الجزائري في هذا الإطار بتعديل قانون العقوبات، حيث أضاف مواد جديدة تجرّم الأفعال الإلكترونية، مثل الدخول غير المشروع إلى أنظمة المعالجة الآلية للمعطيات، وتزوير المعطيات الإلكترونية، والاحتيال عن طريق الوسائل التقنية.

كما صدرت قوانين خاصة تُنظم حماية البيانات الشخصية وتضبط استخدام التكنولوجيات الحديثة بطريقة قانونية تحترم خصوصية الأفراد، مثل القانون رقم 18-07 الذي يتناول حماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي. وقد سعت الدولة من خلال هذه النصوص إلى تعزيز الحماية القانونية للفضاء المعلوماتي وردع أي سلوك إجرامي يُرتكب عبره.

4- مراقبة الاتصالات الإلكترونية

تُعد مراقبة الاتصالات الإلكترونية وسيلة وقائية وتحقيقية في آن واحد، وتُستخدَم بشكل خاص عندما تتوفر مؤشرات قوية على احتمال ارتكاب جريمة إلكترونية خطيرة. وتتم هذه المراقبة وفقًا لضوابط صارمة يحددها القانون، إذ لا يجوز اللجوء إليها إلا بناءً على إذن مُسبق من السلطة القضائية المختصة وغالبًا ما يكون وكيل الجمهورية أو قاضي التحقيق.

وتُستعمل هذه الآلية في قضايا ترتبِط بالأمن القومي،أو الجرائم المنظمة، أو التهديدات الموجهة ضد نظم المعلومات الحيوية. ويُشترط دائمًا أن تتم عملية المراقبة مع احترام تام للحقوق الأساسية لاسيما الحق في الخصوصية والحرية الفردية،وأن تُستخدم المعلومات المستخلصة منها حصريًا في الإطار القانوني المشروع[1].

ثانيًا: التطوُّرات المستقبلية لمكافحة الجريمة الإلكترونية

إن الواقع الحالي والتطوُّر السريع للتكنولوجيا يُفرضان على الدول ومنها الجزائر أن تنظر إلى المستقبل من زاوية استباقية، من خلال وضع استراتيجيات تشريعية وتقنية تُمكنها من الاستجابة الفورية والفعالة لأي مُستجدات في عالم الجريمة الإلكترونية. وتتمثل أبرز هذه التوجُّهات فيما يلي[2]:

1- تطوير التشريعات لتشمُل تقنيات جديدة

لقد أصبح من الضروري أن تشمل النصوص القانونية الجرائم التي تُرتكب بواسطة أدوات مُستحدثة، مثل الذكاء الاصطناعي، والطائرات بدون طيار، والعملات المشفرة، والواقع الافتراضي. فهذه الوسائل تُستخدم اليوم في تنفيذ جرائم غير تقليدية تتطلَّب نصوصًا قانونية دقيقة، سواء فيما يتعلق بتحديد المسؤولية أو بضبط آليات الإثبات والمعاقبة.

2- تعزيز القدرات التقنية للأجهزة الأمنية والقضائية

[1] حسين بن سعيد الغافري،مرجع سابق، ص18

[2] حسن جوخدار ،**التحقيق الابتدائي في قانون أصول المحاكمات الجزائية- دراسة مقارنة** - دار الثقافة للنشر والتوزيع عمان، ،2008 ، ص 56 .

يتطلَّب التعامُل مع الجريمة الإلكترونية مستوى عالٍ من التكوين والاحترافية، سواء لدى القضاة أو المحامين، أو الضبطية القضائية. ولهذا،بات من الضروري وضع برامج تكوين مُتقدِّمة في مجال التحقيق الرقمي، والأدلة الإلكترونية، وتحليل البيانات. كما أصبح من المهم إنشاء مُختبرات جنائية رقمية مُجهَّزة بأحدث الوسائل التقنية، تسمح بتحليل الأجهزة الرقمية واسترجاع المعلومات منها بطرق علمية مُعتمدة.

3- ترسيخ الوعي الرَّقمي لدى المواطنين

لا تقتصِرُ مكافحة الجريمة الإلكترونية على الجانب الأمني أو القانوني فقط، بل تمتدُّ إلى الجانب التوعوي أيضًا. فالكثير من الجرائم تنجح بسبب ضُعف وعي الضحية أو عدم معرفته بكيفية حماية نفسه إلكترونيًا. ولذلك، وجب على الدولة والمؤسسات التعليمية والإعلامية أن تلعب دورًا رئيسيًا في توعية الأفراد، وخاصة فئة الشباب، بمخاطر الاستعمال السيئ للإنترنت، وضرورة الحفاظ على الخصوصية وعدم التفاعُل مع مصادر مشبوهة.

4- التحول نحو قضاء إلكتروني متكامل

في ظل التحوُّل الرقمي الذي يشهدُه العالم، أصبح من الضروري رقمنة الإجراءات القضائية من خلال اعتماد أنظمة إلكترونية تُمكِّنُ من رفع الدعاوى، وتقديم الوثائق، ومتابعة الملفات عبر الإنترنت. كما يجب تفعيل استخدام التوقيع الرقمي والتبادُل الإلكتروني للمذكرات والقرارات القضائية بين مُختلف الهيئات. فمثل هذه الإجراءات تُسهم في تسريع البت في القضايا وتُعزز الشفافية وتُقلِّلُ من فُرص التلاعب[1].

[1] حسن جوخدار، حسن جوخدار، مرجع سابق، ص56-57.

خلاصة الفصل الأول:

يُظهِرُ التحليل المفاهيمي والقانوني للجريمة الإلكترونية أنها تمثل تطورًا نوعيًا في عالم الجريمة يفرِضُ تحديات جديدة على المنظومات القانونية الوطنية والدولية. فهي جرائم تتميز بطابعها غير المادي وتستغِلُّ الفضاء الرقمي والوسائط الإلكترونية لتنفيذ أفعال غير مشروعة، غالبًا ما يكون من الصعب كشفها أو ملاحقتها بسبب الطبيعة المعقدة والتقنية التي تُنفَّذُ من خلالِها.

وقد حاول المشرّع الجزائري، عبر مجموعة من النصوص القانونية، خاصة القانون 09-04 ونصوص لاحقة له التصدِّي لهذا النوع من الجرائم من خلال سن عقوبات جزائية مناسبة، سواء سالبة للحرية أو مالية، كما أقرَّ مجموعة من الإجراءات الخاصة لمتابعة هذه الأفعال الإجرامية، بما في ذلك التعاوُن مع الأجهزة الأمنية والسلطات القضائية، وكذا الاستعانة بالإمكانات التقنية لكشف الأدلة الرقمية.

غير أنَّ التطوُّر السريع للجرائم الإلكترونية يتطلَّب مواكبة تشريعية مُستمِرَّة وتحديثًا دائمًا للمنظومة القانونية،من أجل إحكام السيطرة عليها وضمان حماية المجتمع من مخاطِرها المتزايِدة .

الفصل الثاني: الأجهزة المكلفة بمكافحة الجريمة الإلكترونية وآليات الملاحقة

تُشكِّلُ الجريمة الإلكترونية أحد أبرز التحديات التي تواجه الأنظمة القانونية والأمنية الحديثة، نظرًا لطبيعتها المعقدة وسرعة تطورها واعتمادها الكبير على التكنولوجيا العابرة للحدود. فلم تعُد الجرائم تُرتكب فقط في الواقع المادي،بل أصبحت الفضاءات الافتراضية مسرحًا واسعًا للعديد من الجرائم المُستحدثة التي تُهدِّدُ أمن الأفراد والدول،مثل اختراق النظم المعلوماتية، وسرقة المعطيات الشخصية، والابتزاز الرقمي ونشر البرمجيات الخبيثة، وغيرها.

وفي هذا الإطار لم يعُد من الممكن التصدِّي لهذه الظاهرة بالاعتماد على الوسائل التقليدية، بل أصبح من الضروري إشراك أجهزة أمنية وقضائية مُتخصِّصة تتوفَّرعلى الكفاءات التقنية والمعرفية اللاَّزمة لملاحقة مُرتكبي هذه الأفعال، وضمان تطبيق القانون في بيئة رقمية تزداد تعقيدًا يومًا بعد يوم.

وعليه، سيُعنى هذا الفصل بدراسة مُختلف الهيئات التي تتولى مسؤولية مكافحة الجريمة الإلكترونية في الجزائر، سواء في الشق الأمني من خلال الشرطة والدرك الوطني،أو في الجانب القضائي عبر النيابة العامة والمحاكم المُختصَّة. كما يتناول هذا الفصل بالتفصيل آليات التنسيق والتحقيق والإجراءات القانونية المُتَّبعة في هذا السياق، ممَّا يسمح بفهم شامل لبنية منظومة الردع والمتابعة في مواجهة التهديدات السيبرانية في الجزائر .

المبحث الأول: الأجهزة الأمنية المكلفة بالبحث والتحري

تُعد الأجهزة الأمنية حجر الزاوية في منظومة مكافحة الجريمة الإلكترونية، نظرًا لما تتطلَّبه هذه الجرائم من تدخُّل تقني وميداني سريع لجمع الأدلة وتعقُّب مرتكِبيها. ولقد أولى المشرّع الجزائري أهمية خاصة لهذه الأجهزة، حيث منحها صلاحيات قانونية مُحددة تُمكّنها من أداء مهامها بكفاءة، في إطار من التنسيق مع الجهات القضائية والهيئات التقنية المُتخصِّصة.

المطلب الأول: دور الشرطة القضائية في مكافحة الجريمة الإلكترونية

تلعب الشرطة القضائية دورًا أساسيًا في التصدِّي للجرائم الإلكترونية، انطلاقًا من تلقي الشكاوى مرورًا بفتح التحقيقات، ووصولًا إلى تقديم المتهمين أمام الجهات القضائية المختصَّة. وقد تمَّ تكليف وحدات مُتخصِّصة ضمن جهاز الشرطة، مثل **فرقة مكافحة الجرائم السيبرانية**، التي تملك أدوات تحليل رقمي وتقني مُتطوِّر،ممَّا يُعزِّزُ من قُدرتِها على الوصول إلى مرتكبي هذه الجرائم، سواء داخل أو خارج التراب الوطني، في إطار التعاوُن الأمني الدولي.

الفرع الأول: آليات التحري والتقصي عن الجرائم الإلكترونية

في إطار تعديل من قانون الاجراءات الجزائية الجزائري بالقانون 06-22 جاء المشرع بإجراءات مُستحدثة للكشف عن للجرائم الماسَّة بأنظمة المعالجة للمعطيات وهي:

أوَّلا : أسلوب اعتراض المراسلات و تسجيل الأصوات والتقاط التصور

مكَّن المشرع الجزائري بموجب المواد 65 مكرر 5 إلى 65 مكرر 11 ضباط الشرطة القضائية من صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية، وهي إجراءات تُباشَر بشكل خفي،على الرغم من تناقُضها مع النصوص المقررة لحماية الحق في الحياة الخاصة[1].

يُقصد بالتقاط الصور: " التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والخاصة ، أما تسجيل الأصوات، فيتم

[1] خلفي عبد الرحمن ، **محاضرات في قانون الإجراءات الجزائية** ، دار الهدى عين مليلة ، الجزائر ، 2010 ، ص72-73.

عن طريق وضع رقابة على الهواتف وتسجيل الأحاديث التي تتم عن طريقها، كما يتم أيضًا عن طريق وضع ميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضًا عن طريق التقاط الإشارات السلكية أو الإذاعية " [1]

إن ما يهُمُّ هو أن مثل هذه الإجراءات قد تمس بالحرية الشخصية، خصوصًا إذا علمنا أن سرية المراسلات هي حق دستوري كرسته المادة 47 من المرسوم الرئاسي 20-442 : " لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة " وأكَّدته بدورها المادة 3 من القانون 09-04 التي جاء فيها : "مع مراعاة الأحكام القانونية التي تخُصُّ سرية المراسلات والاتصالات، يمكن لمُقتضيات حماية النظام العام أو مُستلزمات التحريات أو التحقيقات القضائية الجارية، وفقًا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية "

ويُعد هذا الإجراء الحديث من أهم إجراءات التحقيق، حيث مكّن المشرع ضابط الشرطة القضائية من ممارسته للكشف عن الجرائم التي حدَّدها على سبيل الحصر في المادة 65 مكرر 5 من قانون الإجراءات الجزائية تباشرُه الجهة القضائية في بعض الجنايات والجنح التي وقعت أو قد تقع في القريب العاجل، بمعنى أنه إجراء للتحري والتحقيق،وكل ما يتمخُّض عنه يُعد دليلًا ضد كل شخص قامت تحريات جدية بشأن ضلوعه في ارتكاب الجريمة أو امتلاكه لأدلة تتعلق بها، وأن في مراقبة أحاديثه الهاتفية ما يُفيد في إظهار الحقيقة، بعد أن تعذَّر الوصول إليها بوسائل البحث العادية.

ونظرا لخصوصية هذا الإجراء فقد قيد المشرع اللجوء إليه بجملة من الضوابط الموضوعية والشكلية :

1- مباشرة التحري بإذن من وكيل الجمهورية

لم يسمح المشرع بإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا بإذن مكتوب من وكيل الجمهورية المختص، وتباشر هذه العمليات تحت مراقبته.

[1] حسن صادق المرصفاوي، **المرصفاوي في التحقيق الجنائي**، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر،1990 ص.78 .

ويجب أن يتضمن الإذن حسب المادة 65 مكرر 7 كل العناصر التي تسمح بالتعرُّف على الاتصالات المطلوب التقاطها والأماكن المقصودة سواء أكانت سكنية أو غير سكنية، كما يجب أن يتضمن نوع الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها ، وبالتالي، فإن الإذن المُسلَّم من قِبل وكيل الجمهورية للتحقيق في جريمة ما لا يصلح للتحقيق في جريمة أخرى، إلا بإذن جديد.كذلك، يجب أن يتضمَّن الإذن كل الأماكن التي تُوضَع فيها الترتيبات التقنية من أجل التقاط وتسجيل وتثبيت الكلام المتفوَّه به بصفة خاصة من شخص أو عدة أشخاص .

وعند مباشرة التحريات والتحقيقات، يُحرِّرُ ضابط الشرطة القضائية المأذون له أو المُناب من طرف القاضي المختص، محضرًا عن كل عملية اعتراض للمراسلات وتسجيل الأصوات والتقاط الصور، وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتسجيل الصوتي أو السمعي البصري. ويُذكر في المحضر تاريخ وساعة بداية هذه العمليات وانتهائها، ويجب أن يشمُل المحضر توقيع محرره في نهايته[1].

بعد ذلك، يُصنَّف أو ينسِخُ ضابط الشرطة القضائية المأذون له أو المناب، المراسلات أو الصور أو المحادثات المسجلة المفيدة في إظهار الحقيقة في محضر يُودع بملف المتهم وتُنسخ وتُترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء، بمساعدة مترجم يُسخّر لهذا الغرض حسب ما نصت عليه المادة 65 مكرر 10 من القانون 06-22 السابق الإشارة إليه .

2- التزام السر المهني:

تكون إجراءات التحري والتحقيق سرية، ومن ثم فإنها تُباشر ضمن الضمانات الممنوحة للمتهم والسرية تعني التزام من هو قائم بالتحري أو مُكلَّف بإجراء من إجراءاته أو ساهم فيه بالمحافظة على السر المهني، وقد صارت السرية اليوم وسيلة لحماية الحريات الشخصية، وليس فقط وسيلة لتسهيل قمع المتهم كما في السابق[2].

وقد نصَّ المشرع صراحة بموجب المادة 65 مكرر 6 على أنَّ هذه العمليات تتم بمراعاة السر المهني ودون المساس به . فالضابط المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور ملزم

[1] كمال كمال الرخاوي، **إذن التفتيش فقها وقضاء**، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2000، ص 271 .

[2] سهيلة بوزبرة، **مواجهة الصفقات العمومية المشبوهة**، مذكرة ماجستير في القانون الخاص، كلية الحقوق جامعة جيجل الجزائر ، 2008 ، ص .127 .

قانونًا بكتمان السر المهني تطبيقا لما نصت عليه المادة 11 من قانون الإجراءات الجزائية : " تكون إجراءات التحري والتحقيق سرية ما لم ينص القانون على خلاف ذلك، ودون الإضرار بحقوق الدفاع... "

فكل شخص يُساهم في هذه الإجراءات ملزم بكتمان السر المهني تحت طائلة العقوبات المنصوص عليها في قانون العقوبات. لذلك، فإن التحري عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات يتم بسرية مُطلقة، ويُمنع منعًا باتًا إخبار المُشتبه فيه بهذه التحريات، أو أي شخص آخر كذلك، يُمنع على ضابط الشرطة المأذون له أو المُناب أن يُفصِح عن مضمون محضر التحريات لأي شخص كان، وإلاَّ وقع تحت طائلة الجزاء الجنائي بتُهمة إفشاء السر المهني ، ويجب على ضباط الشرطة القضائية ومرؤوسيهم عدم إفشاء الأسرار التي جمعوها أثناء التحريات، لأن سمعة المواطنين لا يجوز أن تظل مهددة ببيانات غير مؤكدة[1].

ثانيا : أسلوب التسرُّب

يُعتبر التسرُّب تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006 ونظم أحكامها بموجب المواد من 65 مكرر 11 إلى مكرر 18 ، وذلك عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 12 منه ومنها الجريمة الإلكترونية .

والتسرب هو قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم[2].

فالتسرب إذًا،هو قيام المأذون له بالتحقيق في الجريمة بمراقبة الأشخاص المشتبه في ارتكابهم جريمة، أو التوغُّل داخل جماعة إجرامية بإيهامهم أنه شريك لهم، ويُسمح لضباط وأعوان الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة، وأن يرتكبوا –عند الضرورة– بعض الجرائم، دون أن يكونوا مسؤولين جزائيًا وذلك بهدف مراقبة الأشخاص المشتبه فيهم وكشف أنشطتهم الإجرامية، مع إخفاء هويتهم الحقيقية[3].

---

[1] عمار حشمان ، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة تخرج لنيل شهادة ماستر تخصص إدارة التحقيقات الاقتصادية و المالية،جامعة قاصدي مرباح ورقلة ،2018-2019 ،ص57.

[2] محمد حزيط ، **قاضي التحقيق في النظام القضائي الجزائري** ، ط2، دار هومة ، الجزائر ، 2009، ص115.

[3] بن حريقة محمد الأمين، **وسائل و أساليب التحري في مجال مكافحة الجرائم الالكترونية** ، مذكرة مقدمة لنيل شهادة الماستر في القانون القضائي كلية الحقوق و العلوم السياسية ، جامعة عبد الحميد بن باديس ، مستغانم 2019–2020، ص40 .

ويُشترَط لصحة العملية [1] حصول الضابط المُكلَّف بالتسرُّب على إذن من وكيل الجمهورية المختص[2] ويجب أن تتم العملية تحت إشرافه ومراقبته. فإن قرر قاضي التحقيق مباشرة هذا الإجراء وجب عليه أولاً إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح الإذن المكتوب لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه حسب ما نصت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية ، وذلك تحت طائلة البطلان المطلق. فيجب أن يكون الإذن مكتوبًا، يتضمَّن كل ما يتعلَّق بعملية التسرُّب، وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرُّب.

ولهذا، يجوز لضابط أو عون الشرطة القضائية المُرخَّص له بإجراء عملية التسرب، والأشخاص الذين يُسخَّرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيًا، القيام بما يلي :

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصَّل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها؛
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخريب أو الإيواء أو الحفظ أو الاتصال .

ويُحظر على المتسرِّب إظهار هويته الحقيقية في أي مرحلة من مراحل الإجراءات، مهما كانت الأسباب إلا لرؤسائه السلميين، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم ويعرّض العضو المكشوف عن هويته للخطر، وهو ما أكده المشرع بموجب المادة 65 مكرر 13 حيث نصت صراحة على أنه" :**لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات .** "

ورغم أن المشرع أجاز مثل هذه الأفعال التي تُعتبر في حقيقتها جرائم، من أجل خلق وتعزيز الثقة في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم، والنجاح في إيهامهم بأنهم شركاء أو فاعلون، إلاَّ أن المشرع منع هؤلاء الضباط أو الأعوان من تحريض المشتبه فيهم على ارتكاب الجريمة. بمعنى أنه يُمنع على الضباط والأعوان المتسربين أن يخلقوا الفكرة الإجرامية

[1] عبد الرحمن خلفي، **المرجع السابق** ، ص 74-75 .

[2] شهاوي قدري عبد الفتاح ، **مناط و تحريات – الاستدلالات و الاستخبارات** – منشاة المعارف ، مصر ،1998، ص191.

للشخص الموضوع تحت المراقبة ويدفعوه لارتكاب الجريمة، فذلك الفعل ممنوع تحت طائلة بطلان الإجراء[1].

وحماية للضابط المتسرَّب ، فقد عاقب المشرع بموجب المادة 65 مكرر 14 كل من يكشف هويته بالحبس من سنتين(2) إلى خمس (5) سنوات، وبغرامة من 200,000 دج إلى 2,000,000 دج، وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس (5) سنوات إلى عشر(10) سنوات والغرامة من 500,000 دج إلى 2,000,000 دج. وإذا تسبَّب هذا الكشف في وفاة أحد هؤلاء الأشخاص، فتكون العقوبة الحبس من عشر(10) سنوات إلى عشرين (20) سنة، والغرامة من 1,000,000 دج إلى 5,000,000 دج.

الفرع الثاني: التعاون مع الهيئات الدولية لمكافحة الجرائم الإلكترونية

يُعتبر التعاوُن الدولي و الوطني آلية لمكافحة الجرائم العابرة للحدود الوطنية بصفة عامة والجرائم الالكترونية بصفة خاصة ، نظرا لما تنطوي عليه هذه الجريمة المُستحدثة من مميزات وخصائص يصعُب معها على الدولة منفرِدة مكافحتها أو الحد منها ومن آثارِها ، وبمقتضى هذه الضرورة أصبحت الدول تُوحِّدُ جهودها وسياستها من أجل الكشف عن مرتكبي هذه الجريمة الخطيرة وتوقيع الجزاء المناسب عليهم،حيث أن التعاوُن الدولي يتم بعدة أشكال وفي مجالات مختلفة .

أولا: أشكال التعاوُن دولي لمكافحة الجريمة الالكترونية

هناك الكثير من تصنيفات التعاوُن الدولي لمكافحة الجريمة الالكترونية ، لكن من خلال دراستنا هذه ميزنا بين شكلين ونمطين لهذا التعاوُن :

1- التعاوُن الدولي الاتفاقي

من أجل إيجاد الأساس القانوني للتعاوُن الدولي لمكافحة الجريمة الالكترونية عُقِدت في سبيل ذلك مجموعة من الاتفاقيات الدولية العالمية منها والإقليمية،والتي اشتملت على مجموعة من أنواع الجرائم الالكترونية وطرق مُكافحتها ومُجابهتها على المستوى الدولي، وفي هذا الصدد هناك اتفاقيتان :

[1] بن حريقة محمد أمين ، المرجع سابق،ص 41.

1-1- اتفاقية بودباست:

بعد اقتناعِها الكامل بالخطر القادم وَّقعت ثلاثون دولة أوروبية في 2001.11.23 على اتفاقية الجريمة الالكترونية في **بودباست** من أجل مكافحة جرائم الأنترنيت ، وهي أولى الاتفاقيات التي تعاطت مع الطابع الدولي للجريمة الالكترونية[1]، كما أنها الاتفاقية الوحيدة المُتعددة الأطراف المعنية بمكافحة الجرائم المرتكبة باستخدام أو ضد الكمبيوتر وباستخدام شبكة الانترنيت ، وهي بمثابة ركيزة أساسية منذ دخلت حيز النفاذ في 10-7-2004 على مستوى الدول الأعضاء للاتحاد الأوروبي [2] . ما يميز هذه الاتفاقية على الرغم من كونها إقليمية أنه يمكن للدول غير الأعضاء في الاتحاد الأوروبي الانضمام اليها.[3]

وقد تناولت هذه الاتفاقية الجوانب الأساسية في الجريمة الإلكترونية الدولية،من خلال تسهيل التعاون الدولي، تسليم المجرمين، تقديم المساعدات القانونية المتبادلة، والتحقيق في البيانات والمعلومات الإلكترونية[4].

1-2- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات [5]

دعت هذه الاتفاقية إلى تعزيز التعاوُن العربي لمكافحة الجريمة الالكترونية ، والتي تُهدِّدُ أمن ومصالح وسلامة المجتمعات العربية ، فأصبحت الحاجة مُلحَّة إلى تبنِّي سياسة عربية مُشتركة لمكافحة هذه الجريمة،وقد تضمَّنت هذه الاتفاقية ضرورة التزام الدول الأطراف بتجريم مُختلف أشكال الجرائم الالكترونية الواردة في الاتفاقية بما يتوافق والنُّظم القانونية الداخلية للدول .

---

[1] وسام الدين محمد العلكة ، **التعاون الدولي في مواجهة جرائم الانترنيت**، مجلة آداب البصرة ، مجلة علمية فصلية محكمة تصدر عن كلية الآداب ، جامعة الصرة ، العراق ، العدد 66 ، 2013 ، ص371

[2] خالد الشرقوني السموني ، **مكافحة الجريمة الالكترونية على المستويين الوطني و الدولي** ، المجلة المغربية للإدارة و التنمية ، الرباط ، المغرب العدد112 2012 ، ص133

[3] لوكال مريم ، **الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي في ضوء قانون حماية المعطيات** ، مجلة العلوم القانونية و السياسية ، جامعة الوادي ، الجزائر ، المجلد 10، العدد1، 2019 ص1307

[4] ايمن بن ناصر بن جماد العباد ، **المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي – دراسة مقارنة** – مكتبة القانون والاقتصاد الرياض ، 2015، ص201 .

[5] ديباجة ، **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.الموافق عليها من طرف مجلس وزراء الداخلية والعدل بالقاهرة** بتاريخ 2010.12.21 .

2- التعاوُن الدولي المؤسساتي:

لم تعُد الاتفاقيات الدولية وحدها كافية لمجابهة الخطر الناجم أو المتوقَّع من الجرائم الالكترونية فسعت الدول لإنشاء مؤسسات وهياكل مُهمتها محاربة الإجرام المنظَّم العابِر للحدود والذي يضمُّ بين أشكاله الجريمة الالكترونية،وتعتبر المنظمة الدولية للشرطة الجنائية (الانتربول) من أكبر الهياكل الدولية الرَّائدة في هذا المجال .

2-1- المنظمة الدولية للشرطة الجنائية :

من بين وظائف **الأنتربول** في مجال مكافحة الجريمة الالكترونية أن يقوم بتعقُّب مجرمي المعلوماتية بصفة عامة وشبكة الانترنيت بصفة خاصة،وتتبُّع الأدلة الرَّقمية وضبطِها و إجراء عمليات التفتيش العابرة لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال للبحث عن الأدلة و البراهين على ارتكاب الجريمة الالكترونية التي تحتويها هذه الأنظمة المعلوماتية .[1]

وفي المجال الدولي لمكافحة الجريمة الالكترونية،استحدث **الأنتربول** منصَّات لتبادُل المعلومات مُخصَّصة لأجهزة نفاذ القانون والدول الأعضاء وهي:

أ- **منصَّة تبادُل المعارف المتَّصلة بالجريمة الالكترونية :** تساهم هذه المنصة في إنشاء شبكة دولية تضم خبراء مختصين لتبادُل المعرفة والخبرات في هذا المجال،حيث يمكن لأجهزة إنقاذ القانون والحكومات والمنظمات الدولية و الخبراء من شركات الأمن السيبيراني المشاركة من أجل تبادل المعلومات الميدانية الغير المشروطة و المتعلقة بالجريمة الالكترونية، فمن خلال هذه المصنة تُنَاقَش أحدث اتجاهات الجريمة الالكترونية و استراتيجيات الوقاية منها و تقنيات الكشف عنها وأساليب التحقيق فيها؛

ب- **منصَّة التعاوُن لمكافحة الجريمة الالكترونية :** تُنسِّقُ هذه المنصة عمليات أجهزة إنفاذ القانون على المستوى العالمي و التي ترمي إلى التصدي للجريمة الالكترونية ، فتشمل منتديات متعددة و مستقلة تسمح للجهات الميدانية المعنية بتعميم المعلومات الاستخبارية في إطار بيئة تفاعلية آمنة كما تحسن هذه المنصة من كفاءة الدول الأعضاء و فعاليتها على المستوى الميداني و تمكنها من امتلاك رؤية للتهديدات والاتجاهات الالكترونية بمجملها حتى تكون قادرة على تركيز مواردها بأفضل شكل مع تجنُّب ازدواجية الجهود.

[1] شنتير خضيرة ، **الآليات القانونية لمكافحة الجريمة الالكترونية – دراسة مقارنة** – أطروحة دكتوراه ، كلية الحقوق و العلوم السياسية ، جامعة أحمد دراية ، أدرار 2020-2021، ص210 .

2-2- المنظمة العربية لمكافحة الجريمة المعلوماتية

تم الاتفاق على إنشاء المنظمة العربية لمكافحة الجرائم المعلوماتية والأنترنيت وهي منظمة عربية غير حكومية علمية ومهنية ، ولها اهتمامات طابع قانوني و اقتصادي ، تعني بتنظيم مختلف الأطر القانونية و الإجرائية و المؤسسية لمكافحة الجرائم التي تتم عبر الانترنيت وكافة جرائم المعلومات وتهدف هذه المنظمة إلى مكافحة الجرائم الالكترونية بجميع أشكالها " الأجهزة و البرامج و الشبكات والمعلومات و البيانات والأموال ووسائل الاتصال و الجرائم ضد السمعة و الجرائم ضد الشخصية " وأيضا تهتم بمكافحة الجرائم ضد الإنسانية و جميع أشكال الجرائم ضد الأمن القومي ، وتسعى على العموم لمكافحة جميع الجرائم التي يكون أداة لارتكابها الحاسب أو الانترنيت أو يكونا أحد أهدافها.[1]

ثانيا: مجالات التعاوُن الدولي لمكافحة الجريمة الالكترونية

تقوم الدول ومن بينها الجزائر ببذل جهودها في مختلف المجالات من أجل تكريس فعلي للتعاوُن الدولي في هذا النوع الخطير من الاجرام ، وبهذا المعنى يشمل تكاثف الجهود الدولية لمجابهة الجريمة الالكترونية بمختلف أنواعها التعاوُن الدولي القضائي الإجرائي،إضافة تعاوُن في مجال خاص بالجريمة الإلكترونية نظرا لطبيعتها الفنية و التقنية وهو التعاوُن الدولي الفني .

1- التعاوُن الدولي القضائي و الإجرائي:

إنَّ الطبيعة غير المادية للجريمة الالكترونية تصعب من مهام أجهزة إنفاذ القانون متابعة وملاحقة مرتكبها خاصة إذا كانت الجريمة الالكترونية تعدت حدود الدولة الواحدة ، ولا يمكن للدولة المتضررة أن تحصُل على المعطيات و البيانات الالكترونية الموجودة في نظام معالجة في كمبيوتر يتواجد بإقليم أو أقاليم دول أخرى إلا بتعاوُن هذه الأخيرة،كما لا يمكنها الشروع أو مواصلة التحقيقات والإجراءات القضائية اللازمة في سبيل ملاحقة الجناة ، والذين قد يهربون إلى دولة أخرى بعد ارتكابهم لجريمتهم أو يكونون متواجدين أصلا في إقليم دولة أخرى أثناء ارتكابهم لها، وأمام هذه المعضلات أتت الاتفاقيات الدولية من أجل تسيير الكشف عن الجريمة الالكترونية ومعاقبة مرتكبيها،فقضت بضرورة تعاوُن الدول من أجل تبادُل المعلومات بين الدول،و تبادُل المساعدة و تسليم المجرمين.

---

[1] فيصل بدري ، **مكافحة الجريمة الالكترونية في القانون الدولي و الداخلي** ، رسالة دكتوراه ، جامعة الجزائر 01 2017-2018، ص91 .

1-1- تبادُل المعلومات

تُعدُّ الوقاية من خلال تبادُل المعلومات عنصرًا أساسيًا، وقاعدة جوهرية لمكافحة الجريمة الإلكترونية، وضمان إقامة نظام مواجهة فعال،[1]وفي إطار قواعد الاتفاقية، وبموجب **المادة 26** فقرة – أ- من اتفاقية مكافحة الجريمة المعلوماتية لعام 2001،يمكن للدول الأطراف أن تُرسِل معلوماتها لمثيلتها استباقيًا دون طلب مُسبق من الأطراف عن الانتهاكات التي تمس الأمن أو الأدلة، أو الطريق المتبع أو التحقيق أو التحريات المتعلقة بهذه الجريمة الإلكترونية، وهذا من خلال قنواتها الرسمية.

كما يمكن حسب **المادتان 31 و 32** من ذات الاتفاقية للدولة الطرف أن تطلُب من الدولة الطرف الأخرى الحصول على المعلومات، والبيانات والملفات من حاسوب كومبيوتر خاص بالضحية، كما يجوز للدولة الطرف الحصول على موافقة الدولة الأخرى في الحصول على المعلومات الخاصة أو السرية والتي تكون على ملفات عامة.

1-2- المساعدة المتبادَلة

نصَّت **الاتفاقية الأوروبية** الخاصة بجرائم تقنية المعلومات لعام **2010** على ضرورة تبادُل الدول الأطراف المساعدة فيما بينها، والتي تتمثل في مجال الأدلة المختلفة، الخاصة بالأدلة الإلكترونية، سواء منها الجنائية، أو المتعلقة بالجريمة.

ومن جانبها أيضًا نصت اتفاقية **بودباست** لعام 2001 في **الفصل الثالث** منها على مجموعة من الإجراءات العامة المرتبطة بالمساعدة المتبادلة الخاصة بالأدلة الرقمية،كما أوجبت على الدول أن تُوفِّر لمثيلاتها من الدول الأخرى الوسائل المناسِبة للتعاوُن القضائي، كما ألزمت الدول بموجب المادة 32 منها باتباع إجراءات سريعة وتدابير ناجعة من أجل مواجهة الجرائم المعلوماتية المستحدثة،كما خولت للدولة الطرف أن تطلُب من الدولة الطرف الأخرى في إطار المواد من 27 إلى 35 إخطارها في إطار المساعدة في المسائل العاجلة .

وبالرجوع لأحكام التشريع الجزائري وتحديدا القانون **09-04** يُلاحظ أن المشرع الجزائري قد أخذ بنظام المساعدة القضائية الدولية المتبادلة،حيث خول بموجب **المادة 16** منه للسلطات المختصة

[1] عبد الله جعفر كوفلي ، **العمل الأمني الناجح "دراسة نظرية تحليلية** ، دار الحليج للنشر و الطباعة ، عمان ، الأردن ، 2019، ص112 .

وفي إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم الإلكترونية، تبادُل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في شكلها الإلكتروني .

وفضلا عن ذلك أجاز وفي حالة الاستعجال وبمراعاة ما أوردته الاتفاقيات الدولية وما يفرضه مبدأ المعاملة بالمثل ، قبول طلبات المساعدة القضائية متى وردت عن طريق وسال الاتصال السريعة بما فيها أجهزة الفاكس والبريد الإلكتروني، وذلك في حدود ما توفره هذه الأخيرة من شروط كافية للتأكُد من صحتها

وفي ذات السياق أجازت **المادة 17 من ذات القانون** تبادُل المعلومات واتخاذ الإجراءات التحفظية وفقا لما حددته الاتفاقيات الدولية ذات الصلة والاتفاقيات الثنائية ومبدأ المعاملة بالمثل .

وما تجدُر الإشارة إليه في هذا الصدد هو أن المشرع الجزائري قد كان حريصا بخصوص قبول طلبات المساعدة،بحيث قيَّد تنفيذ هذه الطلبات أو الاستجابة لها حسب ما نصت عليه **المادة 18** من القانون أعلاه بقيد موضوعي مفادُه المحافظة على سرية المعلومات المبلَّغة أو شرط عدم استعمالها في غير ما هو موضح في الطلب .

1-3- تسليم المجرمين:

عرَّف القانون الدولي العام تسليم المجرمين بأنَّه: " إجراء التعاوُن الثنائي بين الدول في المسائل الجنائية، والذي يهدف إلى نقل شخص متهم بارتكاب جريمة،أو محكوم عليه بعقوبة جنائية من دولة إلى أخرى لملاحقته، أو تنفيذ الحكم الصادر بحقه.[1]

ويُعدُّ تسليم المجرمين في الجرائم الإلكترونية ووفقًا لما ورد في الاتفاقيات الدولية، من أهم الوسائل لملاحقة مرتكبي الجرائم، وخصوصًا ما ورد في **اتفاقية بودباست لعام 2001**،التي اعتبرت تسليم المجرمين التزامًا دوليًا وضروريًا في الجرائم الإلكترونية، وفقًا لما نصت عليه **المادة 24 من الاتفاقية** والتي تناولت الأحكام والإجراءات المتعلقة بالتسليم.

[1] مجاهدي خديجة صافية ، **اليات التعاون الدولي لمكافحة الجريمة المنظمة** ، أطروحة دكتوراه ، كلية الحقوق و العلوم السياسية ، جامعة مولود معمري ، تيزي وزو ، 2018،ص240 .

2- **التعاوُن الدولي الفني**

لا يقتصِرُ التعاوُن الدولي في مجال مكافحة الجريمة المعلوماتية على المساعدة الجنائية العادية فحسب، إذ أن التغيُّر السريع الذي يطرأ على طبيعة هذه الجريمة يتطلَّب كذلك مساعدة فنية عاجلة وفعالة بين الدول .

فالعناصر البشرية المؤهلة، ومراكز الدعم الفني والمساعدة التقنية ليست كلها موجودة بصورة موحدة في الدول، بالتالي فالجريمة الإلكترونية تحتاج إلى وجود تعاوُن دولي في المجال الفني، وكل دولة تُدعِّم وتوفِّر بصورة سريعة كل الإمكانيات للدول الأخرى حتى تستطيع مواجهة هذا النوع من الجرائم.

وقد أكدت **اتفاقية بودباست** لعام 2001 في **مادتها 35** على أهمية هذا النوع من التعاوُن من خلال إنشاء شبكة اتصال دائمة ومباشرة بين الدول، وذلك من خلال خدمات المساعدة الفورية لتسهيل الإجراءات المتعلقة بالجريمة الإلكترونية سواء في مجال التحري، أو الضبط، أو الحجز، أو تأمين الأدلة أو التحقيق، أو جمع المعلومات قبل فتح الدعوى، وهذا ما أكدت عليه المادة 35 من الاتفاقية.

كما نصَّت الاتفاقية العربية لمكافحة الجريمة المعلوماتية في مادتها 31 على التعاوُن بين الدول الأعضاء في المساعدة الفنية في الفقرة الثانية من المادة . يتمُّ هذا التعاوُن في عدة مجالات كالدعم الفني المتخصِّص، وتبادُل المساعدة التقنية، والتكوين، والبحث العلمي، وتبادل الأجهزة، والمعدات، والبرامج وكذا تبادُل المعلومات في مجال الجريمة المعلوماتية، وتنظيم اللقاءات، والندوات، والدورات التدريبية المشتركة بين الجهات، والهيئات، والمراكز المتخصصة،وكذا المؤسسات العلمية، والبحثية، والتعليمية العاملة في مجال الجريمة المعلوماتية.

المطلب الثاني: دور الهياكل الخاصة بمكافحة الجريمة الإلكترونية

إلى جانب جهاز الشرطة، يُعد الدرك والأمن الوطني أحد الفاعلين الأساسيين في منظومة مكافحة الجريمة الإلكترونية،علاوة على الدور الحيوي الذي تقوم بها الهيئة الوطنية لمكافحة الجرائم المتصلة بتنكنولوجيات الإعلام والاتصال وكذا القطب الجزائي الوطني المتخصص .

الفرع الأول: دور الدرك والأمن الوطني في مكافحة الجريمة الإلكترونية

لقد أولت الدولة الجزائرية، وعلى رأسِها مؤسسة الدرك الوطني، أهمية بالغة لمجال الأمن السيبراني، وكرَّست له جهودًا مُعتبرة، وذلك في إطار تنفيذ السياسة الأمنية للدولة، التي تراعي إلى جانب مُقتضيات الدفاع الوطني، التحوُّلات العميقة التي مسَّت بيئة التهديدات، من خلال انخراطِها في عالم الرقمنة، وما فرضه من تطوُّرات جديدة، جعلت من الضروري تطوير أدوات الدفاع الوطني، بما يتماشى مع التحوُّل الرقمي، الذي فرض تحديات كبيرة على الأمن، نتيجة تطوُّر الجرائم وتنوُّعها[1].

وفي ظل كل ذلك، أصبحت حماية الفضاء السيبراني ضرورة قصوى، لتحقيق الأمن بمفهومه الشامل، الذي يعد جوهر السياسة الأمنية، التي تنتهجُها الدولة الجزائرية. وتعد مؤسسة الدفاع الوطني أحد أهم الفاعلين في هذا المجال، بالنظر للمهام الحساسة التي تقوم بها في تنفيذ السياسة الأمنية للدولة. وتحقيقًا لذلك، تم تبني استراتيجية وقائية، من أجل التصدِّي للمخاطر المرتبطة باستخدام تكنولوجيا الإعلام والاتصال، وتأمين البنية التحتية للمعلومات، ضمن ما يسمى بالأمن السيبراني[2].

وتهدِفُ هذه الاستراتيجية إلى تنظيم الفضاء السيبراني، وضمان الاستخدام الآمن لتكنولوجيا الإعلام والاتصال، وحماية الأنظمة المعلوماتية الوطنية من كل تهديد أو هجوم، ما يسمح بالحفاظ على الأمن والاستقرار داخل المجتمع، وحماية الحريات الأساسية. هذه الاستراتيجية تقوم على مرتكزات تقنية وذلك من خلال حِرصها الدائم على التأقلم مع التطوُّر التكنولوجي، عمِلت مؤسسة الدفاع الوطني على تطوير قدراتها المادية والبشرية،من أجل التصدي للجرائم السيبرانية، وذلك بتوفير الوسائل التقنية اللازمة، بما فيها الأجهزة، والبرامج، وقواعد البيانات، والمخابر الجنائية، ووضعها تحت تصرف مختلف

---

[1] بارة سمير ، " **الدفاع الوطني والسياسات الوطنية للامن السيبراني في الجزائر ، الدور و التحديات** " المجلة الجزائرية للأمن الإنساني جامعة باتنة 1 ، الجزائر ، المجلد2، العدد2، 2017،ص431-432 .

[2] نفس المرجع ، ص432 .

الهياكل التابعة لها،من أجل تسهيل عمليات التحقيق، والبحث، والتحري، حول الجرائم المعلوماتية، وكذا ضمان جاهزية الأجهزة الأمنية، لمواجهة التحديات التي فرضها تطور تكنولوجيا الإعلام والاتصال[1].

ويعدّ الدرك الوطني،من بين الهيئات الأمنية التي سخّرت إمكانيات ضخمة،من أجل تحسين أدائه، وجعله يتماشى مع التحوُّلات الحاصلة في بيئة الأمن، وتوسيع مجال عمله ليشمل مكافحة الجريمة الإلكترونية، التي أصبحت تؤرق المجتمع. وهو ما مكَّنه من تحقيق نتائج إيجابية في عدة مجالات منها[2]:

- إفشال محاولات تسريب مواضيع امتحان شهادة البكالوريا.
- استعمال التطبيقات الحديثة، مثل تطبيق "طريقي"، للإبلاغ عن حوادث المرور.
- استعمال البرامج الإلكترونية لإعادة تمثيل الحوادث.
- تطوير منظومة اليقظة التكنولوجية، من أجل متابعة مختلف مستجدات تكنولوجيا الإعلام والاتصال.

إنَّ اضطلاع جهاز الدرك الوطني بالمهام المنوطة به يتطلب وجود جهاز عملياتي باعتباره من أهم مُتطلَّبات الأمن السيبراني، حيث يتيح الكشف عن الأخطار السيبرانية،والتصدِّي لها، بالاعتماد على الإمكانيات المادية، والموارد البشرية المتخصِّصة، وهو ما أدركته الدولة الجزائرية، من خلال إنشائها لعدة هياكل مُتخصِّصة في هذا المجال، منها[3]:

أوّلا : مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية و مكافحتها للدرك الوطني

أُنشئ هذا المركز سنة 2008 ويهدِفُ الى تأمين منظومة المعلومات لخدمة الأمن العمومي واعتُبِر بمثابة مركز توثيق ، يتواجد مقره ببئر مراد رايس،يعكف هذا المركز على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة و تحديد هوية أصحابها، سواء كانوا أشخاصا فرادى أو عصابات وذلك من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها ، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك و حتى الأفراد.[4]

---

[1] بارة سمير ، المرجع السابق، ص435 .

[2] المرجع نفسه ، الصفحة نفسها .

[3] المرجع نفسه ، الصفحة نفسها .

[4] ادريس عطية ، **مكانة الأمن السيبراني في منظومة الأمن الوطني** ، مجلة مصداقية ، المدرسة العليا العسكرية للإعلام والاتصال ، الجزائر المجلد 1، العدد1 ، ص122 .

ويُعتبر هذا المركز نقطة اتصال وطني ، يعمل على توفير المساعدة التقنية للمحققين ويتم فيه حفظ الأدلة ويوجه التحقيقات باستخدام التكنولوجيا الرقمية،إضافة الى معاينة الجرائم ومراقبة البحث عن الجرائم خصوصا على مستوى الإرهاب و القرصنة المعلوماتية .[1]

كما يهدِفُ مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها،وقد تمكَّنت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها وكذا من خلال الملتقيات ذات الطابع الوطني والدولي و تبادُل الخبرات مع دول أخرى وأن تُوفِّر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، وذلك من أجل الفهم الصحيح للجريمة الالكترونية والتصدي لها.[2]

ومن بين مهام هذا المركز كذلك، ضمان المراقبة الدائمة والمستمرة على شبكة الانترنيت،لقيام بمراقبة الاتصالات الالكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية بالإضافة الى المشاركة في عمليات التحري والتسرُّب عبر شبكة الأنترنيت لفائدة وحدات الدرك الوطني والسلطات القضائية،وكذا المشاركة في قمع الجرائم المعلوماتية من خلال التعاوُن مع مختلف مصالح الأمن والهيئات الوطنية ، كما يضطلِعُ هذا المركز بمساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة .[3]

وتشير إحصائيات متعلِّقة بالجرائم الالكترونية في الجزائر[4]، إلى أن هذا النوع من الإجرام يعرف ارتفاعا رهيبا ما جعل المصالح الأمنية تُحذِّرُ وتؤكد أنَّ الجريمة انتقلت من العالم الحقيقي إلى الافتراضي العابر للحدود، وفي هذا الصدد سجلت مصالح الدرك الوطني ومصالح الشرطة قرابة 8 آلاف جريمة الكترونية خلال سنة 2020 تورَّط فيها 1028 شخصا .

وفي ذات السياق ، بينت عملية تحليل المعطيات للجرائم المسجلة أن القذف و السب عبر الفضاء الافتراضي احتل الصدارة بنسبة تفوق 55 بالمائة ، تليها الجرائم ضد الأمن العمومي ، ثم الأفعال الماسة

---

[1] سفيان حديدان ، **الدخول أو البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات** ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية جامعة محمد بوضياف ، المسيلة ، الجزائر ، المجلد2، العدد8 ، 2017، ص309 .

[2] سمير بارة ، المرجع السابق ، ص271 .

[3] رابح سعاد ، **ضوابط مكافحة الجريمة المعلوماتية** ، مجلة القانون العام الجزائري و المقارن ، جامعة جيلالي اليابس سيدي بلعباس ، الجزائر المجلد 7 ، العدد1 ، 2021،ص281 .

[4] سميحة بلقاسم و حميد بوشوشه ، **الجريمة الالكترونية بعد الاجرام في الجزائر "واقعها و اليات مجابهتها** " ، مجلة العلوم الإنسانية لجامعة جامعة العربي بن مهيدي ، أم البواقي، الجزائر ، المجلد 10، العدد1، 2023 ، ص552 .

بالحياة الخاصة وإفشاء الأسرار، وأخيرا الابتزاز و النصب و الاحتيال و الاستغلال الجنسي والأفعال المخالفة للآداب العامة و قضايا مشابهة .

ثانيا : المعهد الوطني للأدلة الجنائية وعلم الإجرام

التابع للدرك الوطني والموضوع تحت وصاية وزارة الدفاع الوطني والذي يضطلع بالمهام الآتية [1]:

- إجراء الخبرات التقنية في الميدان الجنائي الرقمي .
- تقديم المساعدة التقنية في مجال مكافحة الجريمة السيبرانية .
- تصميم قواعد البيانات، والمشاركة في مختلف التظاهرات العلمية، والملتقيات، والأيام الدراسية، داخل وخارج الوطن .

ثالثا : المجلس الوطني لأمن الأنظمة المعلوماتية

هو من الهياكل المُستحدثة على مستوى مصلحة الدرك الوطني ، يتولى حسب **المادة 5** من **المرسوم الرئاسي 20-05** المتعلق بإنشائه في إطار إعداد الاستراتيجية الوطنية في مجال أمن الأنظمة المعوماتية على وجه الخصوص المهام الآتية :

- البث في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قِبل الوكالة وتحديدها .
- دراسة مخطط عمل الوكالة وتعزيز نشاطاتها والموافقة عليها .
- دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها .
- الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية .
- الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني .
- الموافقة على تصنيف الأنظمة المعلوماتية .

[1] بارة سمير ، المرجع السابق ، ص436 .

- اقتراح ملاءمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية عند الحاجة ؛
- إبداء الرأي المطابق في أي مشروع أو نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية .

رابعا : وكالة أمن الأنظمة المعلوماتية

تمَّ استحداثها بموجب **المرسوم الرئاسي 20-05**،حيث اعتبرتها **المادة 17** منه مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية ، مقرها الجزائر العاصمة تتولى هذه الأخيرة حسب **المادة 18 من ذات المرسوم** المهام الآتية :

- تحضير عناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس.
- تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المحددة من قِبل المجلس .
- اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية .
- إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية .
- متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية .
- السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية .
- تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الأنظمة المعلوماتية .
- مرافقة الإدارات والمؤسسات والهيئات بالتشاور مع الهياكل المختصة في هذا المجال في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية .
- جرد الأنظمة المعلوماتية وعرضها على المجلس للموافقة على تصنيفها .
- إعداد و تحيين خارطة الأنظمة المعلوماتية المصنفة .
- اقتراح مشاريع نصوص تشريعية أو تنظيمية في مجال أمن الأنظمة المعلوماتية بعد الرأي المطابق للمجلس.

- إعداد و تحديث المرجعيات والإجراءات والأدلة العلمية وتقديم توصيات في ميدان أمن الأنظمة المعلوماتية .
- اعتماد منتجات أمن الأنظمة المعلوماتية والتصديق عليها .
- اعتماد منظومات إنشاء وفحص الإمضاء الإلكتروني .
- تحديد معاييروإجراءات منح علامة الجودة أو التصديق أو اعتماد المنتجات ومقدمي الخدمات في مجال أمن الأنظمة المعلوماتية طبقا للتشريع والتنظيم المعمول بهما .
- القيام بنشاطات التكوين والتوجيه ذات الصلة بأمن الأنظمة المعلوماتية .

الفـــرع الثـــاني : دور الأمـــن الـــوطني فـــي مكافحـــة الجريمـــة الالكترونيـــة

يقـوم هـذا الأخيـر بمهامـه عبـر المراكـز و الوحـدات و المصـالح التـي اسـتحدثتها الدولـة الجزائريـة فـي اطـار اسـتراتيجيتها لمكافحـة الجريمـة الالكترونيـة و التصـدي لهـا، والتـي سـنتطرق لها تباعا في النقاط التالية:

أولا : المصحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامَّة للأمن الوطني

في إطار مجهودات المديرية العامة للأمن الوطني لمجابهة الإجرام السيبيراني، تمَّ إنشاء المصلحة المركزية للجريمة الالكترونية التي عمِلت على تكييف التشكيل الأمني لمديرية الشرطة القضائية استجابة من مصالح الأمن الجزائرية لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الالكترونية هذه المصلحة [1] عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص بمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني والتي أُنشِأت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015 وتتمثل مهام هذه المصلحة فيما يلي:

- مساعدة مصالح الشرطة القضائية في مجال التحريات التقنية .
- المشاركة في حماية الأنظمة المعلوماتية و الفضاء السيبراني الوطني.
- التعاون و المشاركة في التحقيقات و التحريات ذات البعد الوطني و الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال.

[1] سميحة بلقاسم وحميد بوشوشه ، المرجع السابق ، ص548 .

- اليقظة المعلوماتية و البحث عن الشبكات المفتوحة،عن كل محتوى غير شرعي يشكل في حد ذاته جريمة في قانون العقوبات او يكون مخالف للنظام العام .
- المساهمة في التكوين المتخصص لعناصر الشرطة المتواجدين على مستوى فرق مكافحة الجريمة المعلوماتية على مستوى أمن الولايات.

وضمن مساعي المديرية العامة للأمن الوطني لمكافحة الجرائم الالكترونية ، قامت بإنشاء فرق مُتخصِصة في مكافحة الجريمة الالكترونية على مستوى 58 ولاية تتمحور مهامها في مايلي:[1]

- استقبال شكاوى المواطنين في مجال الجرائم المتواجدة في الفضاء السيبراني .
- البحث و التحري في الجرائم المعلوماتية تحت اشراف الجهات القضائية .
- توعية و تحسيس المواطنين بمخاطر الانترنيت وخصوصا على الأطفال .

ولتعزيز مهام المديرية العامة للأمن الوطني بخصوص محاربة الجريمة الالكترونية، وبالنظر للبُعد الدولي الذي عادة ما يتخذه هذا النوع من الاجرام ،فقد أكدت المديرية المعنية عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية INTERPOL والتي تُتيح مجالات للتبادُل المعلوماتي الدولي وتسهِّل الإجراءات القضائية المتعلقة بتسليم المجرمين،إضافة إلى مباشرة الإنابات القضائية الدولية ونشر أوامر بالقبض عن المبحوث عنهم دوليا .[2]

ثانيا : نيابة مديرية الشرطة العلمية والتقنية التابعة للمديرية العامة للأمن الوطني

أسندت المديرية العامة للأمن الوطني مهمة مكافحة الجريمة المعلوماتية لنيابة مديرية الشرطة العلمية والتقنية . تضع هذه الأخيرة لخدمة هذا الهدف مصالح علمية مُختصَّة بذلك ، تتولى أعمال البحث والتحري بشأن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال،وهذه الوحدات هي: المخبر المركزي للشرطة العلمية والكائن مقره بالجزائر العاصمة،المخبر الجهوي للشرطة العلمية،قسنطينة والمخبر الجهوي للشرطة العلمية وهران.

[1] سميحة بلقاسم و حميد بوشوشه ، المرجع السابق ، ، ص549 .

[2] فضيلة عاقلي ، **الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري** ، ضمن أعمال المؤتمر الدولي الرابع عشر حول الجريمة الالكترونية ، مركز جيل البحث العلمي ، طرابلس، ليبيا ، 2017 ، ص133.

ويتولى كل مخبر سواء المركزي أو الجهوي لولاية وهران أو قسنطينة،مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها،ومن جهة أخرى تؤدي الشرطة الجزائرية دورا هاما في مجابهة الإرهاب السيبراني ، وذلك من خلال : [1]

- الدوريات الالكترونية (خلال اليقظة الالكترونية) لرصد أي تصرُّف مشبوه .
- محاولة تتبُّع الأثر الالكتروني .
- العمل على تجفيف مصادر التمويل و التجنيد عبر الفضاء السيبراني.
- التعاون الدولي في مجال تبادل المعلومات و الخبرات .

الفرع الثالث : دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

نصت على إنشاء هذه الهيئة المادة **13 من القانون 09-04** المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، وقد اعتبرتها **المادة 2 من المرسوم الرئاسي 19-172** [2] المنشئ لها " " مؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية و الاستقلالية المالية توضع تحت سلطة وزارة الدفاع .

أمّا بخصوص مهامها، فقد حددتها **المادة 14 من القانون 09-04** السابق الذكر سابقا وتتمثل أساسا فيما يلي :

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته .
- مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الاعلام و الاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية .

---

[1] حسين ربيعي ، **آليات البحث و التحقيق في الجرائم المعلوماتية** ، أطروحة دكتوراه في الحقوق تخصص قانون العقوبات و العلوم الجنائية جامعة باتنة ، 2015-2016 ،ص177 .

[2] المؤرخ في 3 شوال 1440 الموافق لـ 6 يونيو 2019 **يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها** ، ج.ر عدد 37 صادر بتاريخ 9 يونيو 2019 .

- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و تحديد مكان تواجدهم.

وتعمل هذه الهيئة تحت إشراف ومراقبة لجنة يترأسها وزير.العدل،وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ، ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، وتضم الهيئة قضاة وضباطا وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية والدرك الوطني والأمن الوطني، وفقا لاحكام قانون الإجراءات الجزائية .[1]

تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون 09-04 المذكورة سابقا تحت رقابة السلطة القضائية عبر هيكلين هما :

أوّلا : مجلس التوجيه

ويتولى حسب **المادة 6 من المرسوم الرئاسي 19-172** ما يلي :

- التداول حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما .
- التداول حول وسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال .
- القيام دوريا بتقييم حصيلة التهديدات في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة .
- اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .
- الموافقة على برامج عمل الهيئة .
- إعداد النظام الداخلي للمجلس والمصادقة عليه خلال أول اجتماع .

[1] سمير بارة ، مرجع سابق، ص274.

- دراسة التقرير السنوي لنشاط الهيئة والمصادقة عليه .
- إبداء الرأي في كل مسألة تتصل بمهام الهيئة .
- تقديم كل اقتراح يتصل بمجال اختصاصها .
- المساهمة في ضبط المعايير القانونية في مجال اختصاصه .
- دراسة مشروع ميزانية الهيئة والموافقة عليه .

ثانيا : المديرية التقنية

تتولى هذه الأخيرة حسب **المادة 11 من المرسوم الرئاسي 19-172** ما يلي :

- مساعدة السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التي تتطلب اللجوء إلى أساليب التحري الخاصة للهيئة .
- جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبُّعها بغرض استعمالها في الإجراءات القضائية .

الفرع الرابع : القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

تم إنشاء هذا القطب بموجب الأمر رقم **21-11** المعدل والمتمم لقانون الإجراءات الجزائية والقاضي باستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ويتواجد على مستوى محكمة مقر مجلس قضاء الجزائر،وقد أُوكِلت لهذا القطب الجزائي الوطني مهمتين أساسيتين تتمثلان في:

- المتابعة و التحقيق في الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و الجرائم المرتبطة بها.
- الحكم في الجرائم المنصوص عليها في الباب السادس من **الأمر رقم 21-11** متى كانت تشكل جنحا.[1]

[1] سميحة بلقاسم و حميد بوشوشه ، مرجع سابق ،ص555

وقد فصَّلت **المادة 211 مكرر24** في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها،والتي يتعين على وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال وقاضي التحقيق ورئيس ذات القطب المختصين حصريا المتابعة والتحقيق و الحكم فيها، إذ تتمثل هذه الجرائم في:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شانها المساس بالأمن أو السكينة العامة أو استقرار المجتمع.
- جرائم نشر و ترويج أخبار مغرضة تمس بالنظام و الأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية .
- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين.
- جرائم التمييز و خطاب الكراهية.

المبحث الثاني: الأجهزة القضائية وآليات التحقيق والمتابعة في مكافحة الجرائم الالكترونية

تؤدي الأجهزة القضائية دورًا محوريًا في مواجهة الجريمة الإلكترونية، من خلال صلاحياتها في التحري والتحقيق ومتابعة الجناة. ويبرُز هذا الدور عبر تدخُّل النيابة العامة والمحاكم المختصة من خلال تطبيق النصوص القانونية والإجراءات الخاصة التي تراعي خصوصية هذا النوع من الجرائم المستحدثة.

المطلب الأول: دور النيابة العامة في مكافحة الجريمة الإلكترونية

تُعد النيابة العامة السلطة الوحيدة المخولة قانونًا بتحريك الدعوى العمومية ومباشرة إجراءاتها وهي بذلك تشكل حجر الأساس في مكافحة الجريمة الإلكترونية،لا سيما من خلال إشرافها المباشر على مراحل التحقيق والتنسيق مع الجهات المختصة تقنيًا وأمنيًا.

الفرع الأول: اختصاص النيابة العامة في تحريك الدعوى العمومية

يستند اختصاص النيابة العامة في تحريك الدعوى العمومية إلى مجموعة من النصوص القانونية، التي تمنحها صلاحية مباشرة الإجراءات الجزائية عند وقوع الجريمة، بما في ذلك الجرائم الإلكترونية التي تتميز بطابعها التقني المعقّد.

أولاً: الأساس القانوني لاختصاص النيابة العامة في تحريك الدعوى العمومية

تُعد النيابة العامة حجر الزاوية في النظام القضائي الجزائري، وهي الجهة المخولة قانوناً بتحريك الدعوى العمومية، ويستمد هذا الدور أساسه من مجموعة من النصوص القانونية، لاسيما **المادة 29** من قانون الإجراءات الجزائية : " تحرك الدعوى العمومية وتُباشَر باسم المجتمع من قبل النيابة العامة،وتقوم بممارستها السلطات القضائية المختصة طبقاً لأحكام هذا القانون ." وتطبيقا لهذا النص جاء في **المادة 36** من قانون الإجراءات الجزائية المعدل والمتمم ما يلي : " يمثل وكيل الجمهورية النيابة العامة لدى المحكمة، ويباشر بنفسه أو بواسطة مساعديه أعمال الضبط القضائي ويستقبل الشكاوى والبلاغات ويقرر ما يتعين اتخاذه بشأنها، ويقوم بإجراء أو يأمر باتخاذ جميع الإجراءات اللازمة للبحث والتحري عن الجرائم ومتابعة مرتكبيها."

ويُفهم من هذه النصوص أن النيابة العامة هي صاحبة الاختصاص الحصري في تحريك الدعوى العمومية، سواء تعلق الأمر بالجرائم التقليدية أو الجرائم ذات الطبيعة الحديثة، كالجريمة الإلكترونية. هذا الاختصاص يشمل دراسة الشكاوى أو البلاغات،التكييف القانوني للوقائع، الأمر بالتحقيق، المتابعة القضائية، وتقديم المتهمين أمام جهات الحكم المختصة.

وبالعودة إلى **الأمر رقم 15-02** [1] **المعدل والمتمم لقانون الإجراءات الجزائية** فإن النيابة العامة تتمتع أيضاً بصلاحية الإشراف على الضبطية القضائية، وهو ما يعزز دورها في المراحل الأولية من الإجراءات،خاصة فيما يتعلق بالجرائم الإلكترونية التي تتطلب سرعة وفعالية في التعامل مع الأدلة الرقمية .

وتجدر الإشارة إلى أن **المادة 10 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**،قد ألزمت مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتي يمكنها بدورها إصدار الأوامر اللازمة للولوج إلى الأنظمة المعلوماتية والتحقيق فيها، وهو ما يوسع من أُفق تدخُّلها في هذا النوع من الجرائم .

إجمالاً، فإن الأساس القانوني لاختصاص النيابة العامة في تحريك الدعوى العمومية يستند إلى منظومة قانونية متكاملة تكرّس هذا الدور،وتمنحه القوة القانونية والتنظيمية اللازمة لمواجهة كل أشكال الجريمة، بما فيها الجرائم الإلكترونية ذات الطبيعة المعقدة والتقنية.

ثانياً: نطاق اختصاص النيابة في مجال الجرائم الإلكترونية

تُمارس النيابة العامة اختصاصاتها في ميدان مكافحة الجريمة الإلكترونية وفق إطار قانوني دقيق،يأخذ بعين الاعتبار خصوصية هذا النوع من الجرائم التي تُرتكب غالبًا عن بُعد، وبوسائل تقنية متطورة، مما يفرض تدخلًا سريعًا وفعالًا من قبل أجهزة النيابة، مدعومًا بنصوص قانونية مرنة وملائمة للبيئة الرقمية.

[1] المؤرخ في 7 شوال 1436 الموافق لـ 23 يوليو 2015 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 08 يونيو 1966 **يتضمن قانون الإجراءات الجزائية** ، ج.ر عدد 40 صادر بتاريخ 23 يوليو 23 يوليو 2015

ومن أبرز صور هذا التطبيق ما نص عليه **القانون رقم 09-04** الذي منح للنيابة العامة سلطات موسعة لمباشرة المتابعات والتحقيقات. حيث خولت **المادة 6** من هذا القانون لوكيل الجمهورية أو النائب العام أن يأمر بأي وسيلة تقنية بحفظ أو تسجيل أو نسخ المعطيات المعلوماتية الضرورية للكشف عن الحقيقة، وله أن يأمر بالدخول إلى الأنظمة المعلوماتية وتفتيشها .

ممَّا سبق يُلاحظ أنَّ للنيابة العامة صلاحيات مباشِرة في الإذن باستخدام وسائل التحري الإلكتروني سواء من خلال تتبع الاتصالات أو حجز البيانات الرقمية، أو حتى الدخول القسري إلى الأنظمة المعلوماتية المشتبه فيها ، وكذا إعطاء الأوامر القضائية التي تتيح للضبطية القضائية تنفيذ إجراءات المراقبة والاعتراض،وهو ما يُعد من صميم التحقيقات في الجرائم السيبرانية مثلالاختراق الاحتيال الإلكتروني،أو الابتزاز المعلوماتي .

الفـــرع الثـــاني: الإشـــراف علـــى التحقيقـــات الخاصـــة بـــالجرائم الإلكترونيـــة

لا يقتصِـرُ دور النيابـة العامـة علـى تحريـك الـدعوى العموميـة فحسـب، بـل يمتـد أيضًـا إلـى الإشـراف الفعلـي علـى سـير التحقيقـات فـي الجـرائم الإلكترونيـة. ويشـمل هـذا الإشـراف توجيـه أعمـال الضـبطية القضـائية، والتنسـيق مـع الجهـات التقنيـة المختصـة، بمـا يضـمن قانونيـة الإجـراءات وكفاءتهـا فـي جمـع الأدلـة الرقميـة المعقـدة.

أولاً: دور النيابة العامة في توجيه الضبطية القضائية

تضطلع النيابة العامة بدور محوري في توجيه أعمال الضبطية القضائية،لا سيما في قضايا الجرائم الإلكترونية التي تتميز بتعقيداتها التقنية وسرعة وقوعها وانتشارها عبر الحدود. ويستند هذا الدور إلى أحكام قانون الإجراءات الجزائية الجزائري لاسيما المادة **36** [1] منه والتي تمنح وكيل الجمهورية صلاحية توجيه الضبطية القضائية وتلقي محاضرها وإصدار التعليمات بشأنها، وهو ما يُعزِّز من دور النيابة العامة في قيادة عملية البحث والتحري عن هذا النوع من القضايا .

وتزداد أهمية هذا الدور بالنظر إلى خصوصية هذه الجرائم،إذ غالبًا ما تستلزم وسائل إثبات رقمية وتقنيات متقدمة في التحري. كما أن النيابة العامة تُصدر تعليماتها لقضاة التحقيق أو الضبطية القضائية حول الإجراءات المستعجلة التي يجب اتخاذها، مثل حجز الأجهزة الرقمية، طلب تتبع مصدر الهجمات الإلكترونية، أو استصدار أوامر بالتحفظ على البيانات الرقمية.

[1] المعدلة بالمادة 6 من الأمر 15-02 ، المصدر السابق .

ثانياً: التنسيق مع الهيئات التقنية المختصَّة

في إطار التحقيق في الجرائم الإلكترونية، يبرُز التنسيق بين النيابة العامة والهيئات التقنية المختصة كأحد الأعمدة الأساسية لضمان فعالية الإجراءات التحقيقية والوصول إلى الجناة، بالنظر إلى الطبيعة التقنية المعقدة لهذه الجرائم. ويُستند هذا التنسيق إلى جملة من الأسس القانونية والتنظيمية أبرزها:

1- الإطار العام للتنسيق القضائي والتقني:

يُجيز قانون الإجراءات الجزائية للنيابة العامة الاستعانة بكل من ترى ضرورة مشاركته أو طلب خبرته في كشف الجريمة، لاسيما في الحالات التي تتطلب خبرات فنية عالية كما في الجرائم المعلوماتية وهو ما يُستشف من المادة **25 مكرر** [1] من نفس القانون، والتي تنص على أنه : " يمكن للنيابة العامة الاستعانة في مسائل فنية بمساعدين متخصصين ... " هؤلاء المساعدون يساهمون في مختلف مراحل الإجراءات تحت مسؤولية النيابة العامة التي يمكن أن تطلعهم على ملف الإجراءات لإنجاز المهام المسندة إليهم .

2. الاستعانة بالهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي:

هي سلطة إدارية مُستقلة تعمل تحت رئاسة رئيس الجمهورية،مقرُّها الجزائر العاصمة ، تُعد من أبرز الهيئات المُستحدثة الفاعلة في مجال مكافحة الجريمة الإلكترونية والمساعِدة لأجهزة العدالة حيث ألزمها المشرع بتقديم المساعدة للجهات القضائية من خلال إخطارها في حالة معاينة وقائع تحتمِلُ الوصف الجزائي حسب ما نصت عليه **الفقرة 13 من المادة 22 من القانون 18-07** المنشئ لها :" ... في إطار ممارسة مهامها تُعلِم السلطة الوطنية النائب العام المختص في حالة معاينة وقائع تحتمل الوصف الجزائي ... " علاوة على تخويلها حق توقيع عقوبات إدارية في حق المسؤول عن معالجة المعطيات تتمثل حسب ما نصت **عليه المادة 46 من القانون** أعلاه في الإنذار ، الإعذار ، السحب المؤقت للترخيص ، فرض غرامة مالية قدرُها 500.000 دينار جزائري .

[1] المضافة بالمادة 5 من الأمر 15-02 ، المصدر السابق .

المطلب الثاني: اختصاص المحاكم والإجراءات القانونية لمتابعة الجرائم الإلكترونية

تتطلب الجرائم الإلكترونية . بحكم طبيعتها التقنية واللامادية . معالجة قضائية دقيقة، سواء من حيث تحديد الجهة القضائية المختصة بالنظر فيها، أو من حيث اتباع إجراءات قانونية تواكب تطور الجريمة وخصوصية وسائل إثباتها. ومن هنا برزت أهمية تأطير مسألة الاختصاص القضائي بشكل واضح، إضافة إلى ضبط الإجراءات المتبعة عند متابعة مرتكبي هذه الجرائم أمام القضاء الجزائري.

الفرع الأول: اختصاص المحاكم الوطنية في نظر القضايا الإلكترونية

نظراً لخصوصية الجرائم الإلكترونية من حيث وقوعها في الفضاء الرقمي، فإن تحديد المحكمة المختصة بالنظر فيها يثير إشكالات قانونية وعملية متعددة، خاصة فيما يتعلق بالمكان الذي وقعت فيه الجريمة أو الأثر الناجم عنها. لذلك، اهتم المشرع بتنظيم هذا الاختصاص بما يضمن عدالة المتابعة وفعالية الإجراءات القضائية.

أولاً: تحديد المحكمة المختصة مكانياً ونوعياً

نظرًا لطبيعة الجرائم الإلكترونية التي تتم في بيئة افتراضية وقد تنطلق من مكان وتُستكمل أو تُؤثر في مكان آخر، فإن تحديد **الاختصاص المكاني والنوعي** للمحاكم في هذه القضايا يُشكّل إشكالًا قانونيًا دقيقًا يتطلب تأصيلًا على ضوء القوانين الجزائرية.

1-الاختصاص النوعي: المحاكم المختصة بالنظر في الجرائم الإلكترونية

يُحدد قانون الإجراءات الجزائية الاختصاص النوعي استنادًا إلى نوع الجريمة والعقوبة المقررة لها. وبالرجوع إلى **المواد المستحدثة من قانون العقوبات**، وتحديدًا من المادة **394مكرر إلى 394 مكرر 7**، نجد أن أغلب الجرائم الإلكترونية تُعد من **الجنح**، وبعضها من **الجنايات** (مثل اختراق أنظمة المعلومات ذات الطابع الأمني أو السيادي)، وبالتالي فإن الاختصاص النوعي يكون كما يلي :

- **محكمة الجنح (قسم الجنح على مستوى المحكمة)** :تنظر في أغلب الجرائم الإلكترونية مثل الدخول غير المشروع، التشويش على الأنظمة، نشر محتويات ضارة، الاحتيال الإلكتروني وغيرها مما يُصنف كجنحة.

- **محكمة الجنايات (على مستوى مجلس القضاء)** :في حال ارتكبت الجريمة في إطار منظم أو مست الأمن الوطني أو الدفاع، فإنها تُحال على محكمة الجنايات المختصة.

2-الاختصاص المكاني: تحديد مكان وقوع الجريمة الإلكترونية

تُطرح صعوبة كبيرة في تحديد المحكمة المختصة مكانياً بالنظر إلى أن الجريمة الإلكترونية لا ترتبط بمكان مادي محدد كما هو الحال في الجرائم التقليدية، بل قد يقع الفعل من منطقة،ويؤثر في منطقة أخرى أو عدة مناطق .

وبالرجوع لقانون الإجراءات الجزائية لاسيما في مادته **37** [1] فقد وضع المشرع قاعدة عامة وهي اختصاص المحكمة التي وقعت في دائرة اختصاصها الجريمة كليًا أو جزئيًا، أو تم العثور فيها على أحد عناصر الجريمة، أو تم فيها القبض على المتهم

وفي الجرائم الإلكترونية، غالبًا ما يُعتمد على:

- مكان تواجد **الخادم الإلكتروني (السيرفر)** المستهدف أو مصدر الجريمة.
- مكان إقامة المتهم عند الكشف عنه.
- مكان تواجد الضحية عند ارتكاب الجريمة.

ثانياً: إشكالات الاختصاص في الجرائم الإلكترونية

تُواجِه السلطة القضائية الجزائرية صعوبات حقيقية في تحديد الاختصاص النوعي والمكاني للنظر في الجرائم الإلكترونية، بسبب طبيعتها غير الملموسة وامتدادها خارج الحدود الإقليمية. وقد سعى المشرع إلى تنظيم هذا المجال من خلال جملة من المواد القانونية، لا سيما في قانون الإجراءات الجزائية.

1- **الجرائم الإلكترونية المرتكبة داخل الإقليم الوطني**

ويختص بنظرها حسب **المادة 37 من قانون الإجراءات الجزائية** المحكمة التي وقع في دائرة اختصاصها أحد عناصر الجريمة أو التي تم فيها القبض على المتهم أو التي يقيم فيها المتهم أو المجني

[1] المعدلة بالمادة 3 من القانون 04-14 ، المصدر السابق .

عليه ، كما يجوز تمديد هذا الاختصاص إلى دارة اختصاص محاكم أخرى في عدة جرائم ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، وبهذه الكيفية يكون المشرع قد أخذ بمنظور مُوسَّع للاختصاص المكاني، حيث يكفي تحقق عنصر واحد من عناصر الجريمة في دائرة معينة حتى تنعقِد لها ولاية النظر. وهذا مُفيد في الجرائم الإلكترونية، حيث قد يحدُث الاعتداء في مكان، وتظهر نتائجه في مكان آخر، ويُضبط المتهم في منطقة ثالثة.

2- **الجرائم الإلكترونية المرتكبة خارج الإقليم الوطني**

في إطار التعاوُن والمساعدة القضائية الدولية،منحت **المادة 15 من القانون 09-04** للمحاكم الجزائرية اختصاص النظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والمرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وكانت تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني. فهذا النص من شأنه أن يعزز دور القضاء الجزائري في متابعة مرتكبي الجرائم الإلكترونية الماسة بمصالحها الحيوية ، كل ذلك في إطار الاتفاقيات الدولية أو مبدأ المعاملة بالمثل بما يفتح المجال للتعاون الدولي بشأن الجرائم الإلكترونية التي تشمل عدة دول.

الفرع الثاني: الإجراءات الخاصَّة بمحاكمة مرتكبي الجرائم الإلكترونية

تختلف الإجراءات القضائية المتبعة في محاكمة مرتكبي الجرائم الإلكترونية عن مثيلاتها في الجرائم التقليدية، من حيث الأدوات التقنية المستعملة، وآليات جمع الأدلة، وطبيعة الخبرات المطلوبة ولهذا السبب، كان من الضروري ضبط إجراءات التحقيق والمحاكمة بما يتلاءم مع هذه الخصوصيات لضمان فاعلية العدالة.

أولاً: إجراءات التحقيق والتحري في الجرائم الإلكترونية

تتميز الجرائم الإلكترونية بطابعها التقني المعقد، مما يتطلب إجراءات تحرٍّ وتحقيق خاصة تختلف في بعض جوانبها عن الإجراءات التقليدية، وهو ما استدعى تدخل المشرع الجزائري لإفرادها بتنظيم قانوني خاص، لاسيما بمقتضى القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بالإضافة إلى الأحكام العامة الواردة في قانون الإجراءات الجزائية .

1- أوامر التفتيش الإلكتروني

خولت المادة 5 من القانون 09-04 المتعلق بالوقاية من الجرائم المُتصلة بتكنولوجيات الإعلام والاتصال لضباط الشرطة القضائية ما يلي : " يجوز ... وكذا ضبّاط الشرطة القضائية في إطار **قانون الإجراءات الجزائية** الدخول بغرض التفتيش ولو عن بُعد إلى :

أ. منظومة معلوماتية أو جزء منها ، وكذا المُعطيات المعلوماتية المُخزَّنة فيها .

ب. منظومة تخزين معلوماتية .

في الحالة المنصوص عليها في الفقرة **-أ-** من هذه المادّة ، إذا كانت هناك أسباب تدعو للاعتقاد بأنّ المُعطيات المبحوث عنها مُخزّنة في منظومة معلوماتية أخرى أو أنّ هذه المُعطيات يمكن الدّخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسُرعة إلى هذه المنظومة أو جزءٍ منها بعد إعلام السّلطة القضائية المُختصّة مُسبقا بذلك . "

كما أجاز ذات القانون لضباط الشرطة القضائية اتخاذ تدابير في غاية التقنية تتلاءمُ وطبيعة هذا النّوع من الجرائم آخذا بعين الاعتبار الحق المكفول دستوريا للأشخاص الطبيعيين في هذا الإطار : "... حماية الأشخاص الطبيعيين في مجال مُعالجة المُعطيات ذات الطابع الشّخصي حقٌ أساسي يضمنُهُ القانون ويُعاقِبُ على انتهاكه . "[1] مُخوّلا السُّلطة المُكلّفة بالتفتيش صلاحية تسخير كلِّ شخص له دراية بعمل المنظومة المعلوماتية محل البحث بالتدابير المُتّخذة لحمايتها قصد تزويدها بكلّ المعلومات الضّرورية لإنجاز مهامها .

2. أوامر الحجز الإلكتروني

كما خوّل المشرع بموجب **المواد من 6 إلى 9 من القانون 09-04** لضباط وأعوان الشرطة القضائية حق حجز المُعطيات المخزُّنة متى كانت مُفيدة في الكشف عنها ، وإذا لم يكُن من الضروري حجز كلّ المعومات بل جزءٍ منها فقط ، فقد فأجاز لها نسخ المُعطيات محل البحث والمُعطيات اللاّزمة لفهمِها على دعامة تخزين إلكترونية تكون قابلة للحجز والوَّضع في أحراز مختومة بالكيفيات المعمول بها

1 المادة **47** من المرسوم الرئاسي 20-442 ، المصدر السّابق .

طبقا للقواعد العامّة،مع وجوب السّهر على سلامة المُعطيات،واستعمال الوَّسائل التقنية الضرورية لتشكِيلها أو إعادة تشكِيلها، قصد جعلِها قابلة لأغراض التحقيق ، شرط ألاّ يؤدي ذلك إلى المساسِ بمحتواها .

كما قد يتّخذُ الحجز في هذا الصّنف من الجرائم طابعا آخر،هو منعُ الوصول إلى المُعطيات التي تحتويها المنظومة المعلوماتية أو نسخِها باستعمال التقنيات المُناسبة لمنع الوصول إليها أو الاطلاع عليها

3. اللجوء إلى الخبرة التقنية

تطبيقا لأحكام المادة **المادة 143** [1]

من قانون الإجراءات الجزائية التي تنص على ما يلي : " إذا رأى قاضي التحقيق أن إجراءات التحقيق تقتضي الاستعانة برأي أهل الخبرة، أمر بإجراء الخبرة من طرف خبير أو أكثر." فإنه يمكن للسلطات المختصة تعيين خبير تقني لفحص الأدلة الرقمية وتحليلها، بطلب من قاضي التحقيق أو بناءً على طلب النيابة العامة ، على أن يكونوا خبراء تقنيين مختصين في الأمن السيبراني أو تحليل الأنظمة المعلوماتية في إطار التحقيق في الجرائم الإلكترونية .

ثانياً: الضمانات القانونية للمتهم في القضايا الإلكترونية

الاستعانة بمحامٍ يعد حقًّا من حقوق الدفاع، بحيث يتمكن المتهم بواسطة محاميه من أن يدفع التهمة عن نفسه، وهذا يؤكد عدالة القضاء وقدسيته، حيث يجسد المحامي دور الضامن لسلامة الإجراءات بدءًا من التحقيق وانتهاءً بالمحاكمة، بحيث يؤدي دوره في الدفاع عن المتهم بهدف إثبات براءته ضمن الحدود التي قررها المشرع.

وفي هذا نصّت المادة 64 من قانون المحاماة المصري رقم (17) لسنة 1983 على أنه: **"على المحامي تقديم المساعدات القضائية للمواطنين غير القادرين وغيرهم في الحالات التي ينص عليها هذا القانون، وعليه أن يؤدي واجبه عمّن يُندب بنفس العناية التي يبذلها إذا كان موكَّلًا، ولا يجوز للمحامي المنتدب للدفاع أن يتنحى عن مواصلة الدفاع إلا بعد استئذان المحكمة التي يتولى الدفاع أمامها، وعليه أن يستمر في الحضور حتى تقبل تنحيه وتعيين غيره[2]".**

[1] المعدلة بالمادة 15 من القانون 06-22 ، المصدر السابق .

[2] المادة 64 من قانون المحاماة المصري رقم (17) لسنة 1983.

فتوجيه تهمة لمتهم معيّن من شأنه أن يُوقع الاضطراب في نفسه، حتى لو كان بريئًا، لأن موقف الاتهام في ذاته له نوع من الرهبة قد يُسيء معها المتهم حسن دفاعه عن نفسه، ولهذا فمن الطبيعي اللجوء إلى محامٍ يُعينه في الدفاع عن نفسه[1].

فقد يتقدم المحامي في الدفاع عن المتهم عن طريق إبداء الطلبات و الدفوع وتدوينها في المحضر أو طلب سماع الشهود وطلب ندب الخبراء لإجراء المعاينة، لكن لا يحق له مناقشة الشهود، بل له الحق في إبداء ملاحظاته على شهاداتهم. كما أنه مقيد في الكلام إلا بإذن المحقق، الذي يسمح له بذلك أو يمنعه إذا وجد أسبابًا هامة لهذا المنع.

وقد أكدت محكمة النقض المصرية على هذه الضمانة في كثير من أحكامها، فقضت[2]: **"لما كانت المادة 124 من قانون الإجراءات الجنائية، المستبدلة بالقانونين رقمي 145 لسنة 2006 و74 لسنة 2008، قد جرى نصها على أنه: لا يجوز للمحقق في الجنايات وفي الجنح المعاقب عليها بالحبس وجوبًا أن يستجوب المتهم أو يواجهه بغيره من المتهمين أو الشهود إلا بعد دعوة محاميه للحضور، عدا حالة التلبس وحالة السرعة بسبب الخوف من ضياع الأدلة، على النحو الذي يثبته المحقق في المحضر. وعلى المتهم أن يعلن اسم محاميه بتقرير لدى قلم كتاب المحكمة أو إلى مأمور السجن، أو يُخطر به المحقق، كما يجوز لمحاميه أن يتولى هذا الإعلان أو الإخطار. وإذا لم يكن للمتهم محامٍ أو لم يحضر محاميه بعد دعوته، وجب على المحقق من تلقاء نفسه أن يندب له محاميًا."...**

ومفاد ذلك أن المشرع وضع ضمانة خاصة لكل متهم في جناية أو جنحة معاقب عليها بالحبس وجوبًا، وهي وجوب دعوة محاميه إن وُجد قبل استجوابه أو مواجهته بغيره من المتهمين أو الشهود وأعطى للمتهم الحق في اختيار محاميه، فإذا لم يكن له محامٍ وجب على المحقق أن يندب له محاميًا من تلقاء نفسه. واستثنى المشرع من ذلك حالتين توخى فيهما الحفاظ على أدلة الدعوى، وهما حالة التلبس

[1] حسن صادق المرصفاوي، **المرصفاوي في المحقق الجنائي** ، منشأة دار المعارف بالاسكندرية، 1977، صص44-45

[2] خالد علي نزال الشعار ، **التحقيق الجنائي في الجرائم الالكترونية** ، بحث مقدم لاستيفتاء متطلبات الحصول على درجة الدكتوراه في الحقوق،جامعة المنصورة ،2020،ص21 .

وحالة السرعة لشبهة الخوف من ضياع الأدلة، واستلزم أن يثبت المحقق حالة السرعة التي دعته إلى التحقيق مع المتهم دون دعوة أو انتظار محاميه تطمينًا للمتهم وصونًا لحقه في الدفاع[1].

لما كان ذلك، وكان الحكم قد أطرح دفاع الطاعن في هذا الشأن بما مفاده أنه لما تبيّن عدم وجود محامٍ له، أرسل المحقق إلى نقابة المحامين ليندب له أحد المحامين، إلا أنه لم يجد أحدًا منهم، فلم يجد بدًّا من إجراء التحقيق وقام باستجوابه، فإن هذا الذي أورده الحكم يكون كافيًا وسائغًا في إطراح ذلك الدفع، ولا تثريب على النيابة إن هي باشرت التحقيق مع المتهم في غيبة أحد المحامين، ما دام أصبح ندبه أمرًا غير ممكن – كما هو الحال في هذه الدعوى – وإلا تعطلت عن أداء وظيفتها، فضلًا عن أن هذا الطاعن قد أنكر بتحقيقات النيابة، ولم يستند الحكم في إدانته إلى دليل من أقواله فيها، ومن ثم يكون منعه في هذا الصدد غير مقبول[2].

ومن هنا تظهر أهمية الاستعانة بمحامٍ في مجال الجرائم الإلكترونية. ففي قضية تتلخص وقائعها في قيام طالب بكلية الهندسة بإنشاء موقع له على شبكة الإنترنت، نشر فيه صورًا منافية للآداب وألفاظًا تمس بسمعة وعِرض فتاة وعائلتها. فقامت الفتاة بتحرير محضر بالإدارة العامة للمعلومات والتوثيق، التي أجرت على إثره التحريات، وكانت نتيجتها أن الموقع أُنشئ عن طريق جهاز كمبيوتر مربوط على أحد الهواتف برقم معين، وتم تحديد وجهة منزل المتهم، وأُلقي القبض عليه، وجرى إحالته من قبل النيابة العامة بتهم السب والقذف وإساءة استعمال أجهزة الاتصالات.

فتقدم الدفاع عن المتهم بطلب إعادة الدعوى، وكان من الأسباب أن مسألة إثبات الـ IP المرتبط بالهاتف مدار الشك لا يمكن التحقق منها دون الاستعانة بخبير فني متخصص من الخبراء المعتمدين لدى وزارة العدل. كما أن محرر التحريات لا يُعد خبيرًا، لأنه لم يُندب من النيابة العامة، وبالتالي لا يُعد دليلًا فنيًا، لأن المشرع حدد جهات الخبرة بالقانون رقم 59 لسنة 1952[3].

[1] خالد علي نزال الشعار ، المرجع السابق ، ص 21 .

[2] المرجع نفسه ، الصفحة نفسها .

[3] المرجع نفسه ، الصفحة نفسها .

خلاصة الفصل الثاني:

في ختام هذا الفصل، يتبين أن مكافحة الجريمة الإلكترونية ليست مسؤولية جهاز واحد فقط، بل هي عملية متكاملة تتطلب تعاونًا وثيقًا بين مختلف الفاعلين في المنظومة الأمنية والقضائية. فقد أبرزنا الدور الأساسي الذي تضطلع به **الشرطة** و**الدرك الوطني** في البحث والتحري وجمع المعلومات، من خلال وحدات تقنية متخصصة تعتمد على أدوات التحقيق الرقمي، مع انخراطها في تعاون وطني ودولي مستمر لتعقب النشاط الإجرامي الإلكتروني.

ومن جهة أخرى، تلعب **النيابة العامة** دورًا محوريًا في توجيه أعمال الضبطية القضائية، وتحريك الدعوى العمومية، والإشراف على التحقيقات،في حين تتكفل **المحاكم الوطنية** بالنظر في هذه القضايا ضمن اختصاصات مكانية ونوعية محددة، مع تطبيق إجراءات تضمن المحاكمة العادلة وفق القوانين الوطنية والدولية.

إن التصدي للجريمة الإلكترونية لا يقتصر فقط على الجانب التقني، بل يستلزم كذلك تحديث الإطار التشريعي، وتكوين القضاة والمحققين في المجال الرقمي، وتوفير الإمكانيات المادية والتقنية الكفيلة بتسهيل عملية الإثبات والردع.كما تبرز ضرورة تطوير التعاون الدولي وتبادل الخبرات، نظرًا للطبيعة العابرة للحدود لهذه الجرائم،ما يجعل التنسيق القضائي والأمني ركيزة أساسية في مكافحة التهديدات السيبرانية الحديثة.

الخاتمة

لقد أصبح من المسلم به اليوم أن الجريمة الإلكترونية لم تعد مجرد تهديد محتمل، بل أصبحت واقعًا يوميًا يفرض نفسه بقوة على مختلف الأصعدة، ويهدد الأمن القومي، والاقتصاد الوطني، وحقوق الأفراد، وحرمة الحياة الخاصة. وقد أظهرت هذه الدراسة أن الجزائر، إدراكًا منها لخطورة الظاهرة، قد قامت بخطوات تشريعية وتنظيمية معتبرة من أجل التصدي لهذا النوع من الجرائم، سواء من خلال إصدار قوانين خاصة، أو عبر تمكين الأجهزة الأمنية والقضائية من آليات قانونية وتقنية لملاحقة الجناة.

غير أن طبيعة الجريمة الإلكترونية، المعقدة والمتطورة باستمرار، تفرض تحديات كبيرة على مختلف الفاعلين، الأمر الذي يتطلب مراجعة مستمرة للمنظومة القانونية والمؤسساتية، وتطوير وسائل التحري الرقمي، وتعزيز التنسيق بين الجهات المعنية، والانفتاح على التجارب الدولية الناجحة إلى جانب تكثيف جهود التوعية والتكوين المتخصص في المجال الرقمي.

نتائج الدراسة

1. **تميز الجريمة الإلكترونية بخصائص فريدة** مثل الطابع غير المادي، والانتشار السريع، والصعوبة في تعقب الجناة، مما يجعل مواجهتها تختلف عن الجريمة التقليدية.
2. **المنظومة القانونية الجزائرية تحتوي على نصوص واضحة** لتجريم عدد من الأفعال الإلكترونية وتُدرجها ضمن القانون الجزائي المعدل بالقانون 09-04، لكنها تظل بحاجة إلى مزيد من التحديث لمواكبة التطورات التقنية المتسارعة.
3. **الأجهزة الأمنية كلفت بمهام التحري والبحث الرقمي**، إلا أن محدودية التكوين المتخصص ونقص التجهيزات التقنية يمثلان تحديًا فعليًا.
4. **الجهاز القضائي، بما فيه النيابة العامة والمحاكم، يضطلع بدور مهم** في التحقيق والمتابعة لكن الإجراءات لا تزال تقليدية في كثير من جوانبها، ولا تتماشى دائمًا مع تعقيد الجريمة الإلكترونية.
5. **ضعف التنسيق بين مختلف الجهات المعنية** (أمنية، قضائية، تقنية) يحد من فعالية التدخل في الوقت المناسب ومن تقديم الأدلة الرقمية بشكل قانوني سليم.

التوصيات والمقترحات

1. **تحديث وتطوير النصوص القانونية باستمرار** لمواكبة المستجدات التقنية، مع صياغة قانون خاص ومتكامل للجريمة الإلكترونية يتضمن أنواع الجرائم، آليات إثباتها، وتحديد اختصاص الجهات المتدخلة.
2. **إنشاء وحدات متخصصة في التحقيق الرقمي داخل أجهزة الأمن والنيابة العامة**، تكون مدربة على أعلى مستوى في تحليل الأدلة الرقمية.
3. **تعزيز التعاون الدولي في مجال مكافحة الجريمة الإلكترونية**، لا سيما في تتبع الجناة العابرين للحدود، وتبادل المعلومات القضائية والأمنية بشكل سريع وآمن.
4. **توفير تكوين أكاديمي ومهني في الجرائم المعلوماتية** لفائدة القضاة، ضباط الشرطة، الدرك ومساعدي القضاء، لضمان التعامل السليم مع الأدلة الرقمية.
5. **إطلاق حملات توعية رقمية للمواطنين**، خاصة لفائدة الفئات الهشة مثل الأطفال والمراهقين حول مخاطر الإنترنت وسبل الحماية القانونية المتاحة.
6. **تعزيز البحث العلمي في مجال الجرائم الإلكترونية**، عبر دعم الدراسات الجامعية، وإشراك الخبراء في القانون والمعلوماتية لتقديم حلول مبتكرة.
7. **تشجيع الشراكة بين القطاع العام والخاص**، لا سيما شركات الاتصالات والمعلوماتية، لتطوير أدوات رصد وتحليل الجرائم الرقمية.

قائمة المصادر و المراجع

أولا : القرآن الكريم

- سورة المائدة ، الآية 08.
- سورة الأنعام، الآية 124.

ثانيا : المعاجم وكتب اللغة

- ابن منظور، لسان العرب، دار إحياء التراث العربي، بيروت، 1999.
- محب الدين الفيروزآبادي، القاموس المحيط، دار الكتب العلمية، بيروت، 2007.
- إسماعيل بن حماد الجوهري، الصحاح في اللغة، دار العلم للملايين، الطبعة الرابعة، مجلد 1 بدون تاريخ.

ثالثا : النصوص القانونية

– القانون 04–09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 غشت 2009 **المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتهما** ، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية (ج.ر) عدد 47 صادر بتاريخ 16 غشت 2009 ؛

– القانون **15/04** المؤرخ في **4** ربيع الثانية **1435** الموافق لـ **4** فبراير **2014** يعدل ويتمم الأمر 66–166 المؤرخ في 08 صفر 1386 الموافق لـ 8 يونيو 1966 المتضمن **قانون العقوبات** ،ج.ر عدد **71** صادر بتاريخ **10** نوفمبر **2004** ؛

– القانون 06–22 المؤرخ في 29 ذي القعدة 1427 الموافق لـ 20 ديسمبر 2006 يعدل ويتمم الأمر 66–155 المؤرخ في 18 صفر 1386 الموافق لـ 8يونيو 1966 **المتضمن قانون الإجراءات الجزائية** ، ج.ر عدد 84 صادر بتاريخ 30 ديسمبر 2006 ؛

– **القانون 06–23** المؤرخ في **29** ذي القعدة **1427** الموافق لـ **20** ديسمبر **2006** يعدل ويتمم الأمر 66–165 المؤرخ في 18 صفر 1386 الموافق لـ 8يونيو 1966**المتضمن قانون العقوبات** ، ج.ر عدد **84** صادر بتاريخ 24 ديسمبر 2006 ؛

– القانون رقم 15–02 المؤرخ في 7 شوال 1436 الموافق لـ 23 يوليو 2015 يعدل ويتمم الأمر 66–155 المؤرخ في 18 صفر 1386 الموافق لـ 08 يونيو 1966 **يتضمن قانون الإجراءات الجزائية** ، ج.ر عدد 40 صادر بتاريخ 23 يوليو 23 يوليو 2015 ؛

– الفانون رقم 15–04 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ أول فبراير 2015 **يتعلق بالتصديق والتوقيع الإلكترونيين** ، ج.ر عدد 6 صادر بتاريخ 10 فبراير 2015 ؛

– القانون رقم 18–04 المؤرخ في 24 شعبان 1439 الموافق لـ 10 مايو 2018 **المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية** ، ج.ر عدد 27 صادر بتاريخ 13 ماي 2018 ؛

– القانون 18–05 المؤرخ في 24 شعبان 1439 الموافق لـ 10 يونيو 2018 **يتعلق بالتجارة الإلكترونية** ، ج.ر عدد 28 صادر بتاريخ 16 يونيو 2018 .

– القانون رقم 18–07 المؤرخ في 25 رمضان 1439 الموافق لـ 10 يونيو 2018 **المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي** ، ج.ر عدد 34 صادر بتاريخ 10 يونيو 2018 ؛

– المرسوم الرئاسي 19–172 المؤرخ في 3 شوال 1440 الموافق لـ 6 يونيو 2019 **يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها** ، ج.ر عدد 37 صادر بتاريخ 9 يونيو 2019 ؛

– المرسوم الرئاسي 20–05 المؤرخ في 24 جمادى الأول 1441 الموافق لـ 20 جانفي 2020 **المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية** ، ج.ر عدد 4 صادر بتاريخ 26 جانفي 2020 ؛

– المرسوم الرئاسي 20–442 المؤرخ في 15 جمادى الأولى 1442 الموافق لـ 30 ديسمبر 2020 **يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020 في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية** ، ج.ر عدد 82 صادر بتاريخ 30 ديسمبر 2020 ؛

– القانون 21–11 المؤرخ في 16 محرم 1443 الموافق لـ 25 غشت 2021 يتمم الأمر 66–156 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 **يتضمن قانون الإجراءات الجزائية** ، ج.ر عدد 65 صادر بتاريخ 26 غشت 2021 .

رابعا : الكتب الفقهية والقانونية

الإمام محمد أبو زهرة، **الجريمة والعقوبة في الفقه الإسلامي**، دار الفكر العربي، القاهرة، 1998 .

– محمود إبراهيم غازي، **الحماية الجنائية للخصوصية والتجارة الالكترونية**، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2014م .

– عبد الفتاح بيومي حجازي ، **مكافحة جرائم الكومبيوتر والأنترنيت في القانون العربي النموذجي** ، دار الكتب القانونية مصر ، الطبعة (ط)1 2007 .

– عبابنه محمد احمد ، **جرائم الحاسوب و أبعادها الدولية**، دار الثقافة ، عمان ، الأردن ، ط1، 2005 .

– عياد سامي علي حامد، **الجريمة المعلوماتية وإجرام الإنترنت**، دار الفكر الجامعي، مصر ، 2007، ص40

– الكعبي محمد عبيد ، **الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الانترنيت** ، دار النهضة العربية ، القاهرة طبعة2، 2009 .

– الصغير جميل عبد الباقي، **الأنترنيت و القانون الجنائي الأحكام الموضوعية للجرائم المتعلقة بالانترنيت**، دار النهضة العربية ، القاهرة ، مصر 2001، طبعة1 .

– يوسف أمير فرج ، **الإثبات الجنائي للجريمة الالكترونية و الاختصاص القضائي بها – دراسة مقارنة للتشريعات العربية و الأجنبية** – مكتبة الوفاء القانونية ، الإسكندرية ، طبعة 1، 2016 .

– النادي محمد إبراهيم سعد ، **جرائم الانترنيت بين الشريعة الإسلامية و القوانين الوضعية – دراسة مقارنة** – مكتبة الوفاء القانونية ، الإسكندرية ط1، 2017 .

– الشوايكة محمد أمين ، **جرائم الحاسوب و الانترنيت الجريمة المعلوماتية** ، دار الثقافة للنشر و التوزيع ، عمان ، الأردن 2011 .

– الدسوقي محمد كمال محمد ، **الحماية الجنائية لسرية المعلومات الإلكترونية – دراسة مقارنة –** ، دار الفكر و القانون للنشر و التوزيع ، القاهرة ، 2015 .

- عرب يونس خالد ، **دليل أمن المعلومات و الخصوصية جرائم الكمبيوتر و الأنترنيت** ، منشورات اتحاد المصارف العربية طبعة1، 2002 .

- أحمد عبد الظاهر الطيب ، **الجديد في الموسوعة الجنائية – دراسة لأهم جرائم قانون العقوبات والتشريعات الجنائية الخاصة** – دار النهضة العربية ، القاهرة ، مصر ، **1997** .

- محمود نجيب حسني ، **شرح قانون العقوبات – القسم العام** – دار النهضة العربية ، القاهرة ، مصر ، ط**5** **1982**

- المضحكي، حنان ريحان مبارك، **الجرائم المعلوماتية–دراسة مقارنة**– منشورات الحلبي الحقوقية، ط 1 .

- محمود مصطفى، **شرح قانون العقوبات** –**القسم العام** –دار النهضة العربية ، القاهرة ، مصر، **1974** .

- محمود محمود مصطفى ، **قانون العقوبات – القسم العام –** دار الفكر العربي ، القاهرة ، **1979** .

- علي عبد القادر القهوجي ، **قانون العقوبات – القسم العام –** الدار الجامعية ، بيروت ، لبنان ، **1994**

- هروال نبيلة هبة، **الجوانب الإجرائية لجرائم الأنترنت**، دار الفكر الجامعي، طبعة 1، 2007 .

- محمد عوض ، **قانون العقوبات – القسم العام –** دار الجامعة الجديدة للنشر ، الإسكندرية ، مصر ، **2000** .

- سميـــر عالية ، **شرح قانون العقوبات – القسم العام –** المؤسسة الجامعية للدراسات والنشر والتوزيع ، بيروت ، لبنان **1998** ، **ص 208** / نبيل صقر ، عز الدين قمراوي ، **الجريمة المنظّمة–التهريب والمخدرات وتبييض الأموال في التشريع الجزائري** ، دار الهدى ، عين مليلة، الجزائر **2008** .

- قشقوش، هدى حامد، **جرائم الحاسب الالكتروني في التشريع المقارن**، دار النهضة العربية، القاهرة، مصر ، 1992

- محمود نجيب حسني ، **النظرية العامّة للقصد الجنائي** ، دار النهضة العربية ، القاهرة ، مصر، ط**2** ، **1986**.

- الطائي، جعفر حسن جاسم، **جرائم تكنولوجيا المعلومات**، دار البداية، الطبعة الأولى، 2007 .

- سليمان عبد الله ، **شرح قانون العقوبات الجزائري–القسم العام–ج1**، ديوان المطبوعات الجامعية ، الجزائر، **1998** .

- سلاطنية بلقاسم، **الجرائم الإلكترونية في التشريع الجزائري**، دار هومة، الجزائر، 2018 .

- زيان عبد العزيز، **الجرائم المعلوماتية بين القانون الجزائري والاتفاقيات الدولية**، دار الخلدونية، الجزائر، 2021 .

[1] المرسوم الرئاسي رقم 20–05 المؤرخ في 24 جمادى الأول 1441 الموافق لـ 20 جانفي 2020 **المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية** ، ج.ر عدد 4 صادرة بتاريخ 26 جانفي 2020 .

- حسين بن سعيد الغافري، **التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت** ، دار النهضة العربية، القاهرة 2009 .

- حسن جوخدار ،**التحقيق الابتدائي في قانون أصول المحاكمات الجزائية– دراسة مقارنة** – دار الثقافة للنشر والتوزيع عمان، ،2008 .

- عبد الرحمن خلفي، **محاضرات في قانون الإجراءات الجزائية** ، دار الهدى عين مليلة ، الجزائر ، 2010 .

- شهاوي قدري عبد الفتاح ، **مناط و تحريات – الاستدلالات و الاستخبارات** – منشاة المعارف ، مصر ،1998 .

- حسن صادق المرصفاوي،"المرصفاوي في المحقق الجنائي"، منشأة دار المعارف بالاسكندرية، ،1977 .

– حسن صادق المرصفاوي، **المرصفاوي في التحقيق الجنائي**، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر 1990 .

– كمال كمال الرخاوي، **إذن التفتيش فقها وقضاء**، الطبعة ألأولى، دار الفكر والقانون، المنصورة، مصر، ،2000 .

– محمد حزيط ، **قاضي التحقيق في النظام القضائي الجزائري** ، ط2، دار هومة ، الجزائر ، 2009 .

– بن حريقة محمد الأمين، **وسائل و أساليب التحري في مجال مكافحة الجرائم الالكترونية** ، مذكرة مقدمة لنيل شهادة الماستر في القانون القضائي كلية الحقوق و العلوم السياسية ، جامعة عبد الحميد بن باديس ، مستغانم ، 2019 2020– .

– أيمن بن ناصر بن جماد العباد ، **المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي – دراسة مقارنة –** مكتبة القانون والاقتصاد الرياض ، 2015 .

– ديباجة ، **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.الموافق عليها من طرف مجلس وزراء الداخلية والعدل بالقاهرة** بتاريخ 2010.12.21 .

– عبد الله جعفر كوفلي ، **العمل الأمني الناجح "دراسة نظرية تحليلية** ، دار الحليج للنشر و الطباعة ، عمان ، الأردن 2019 .

خامسا : المقالات والمجلات العلمية

– زينب ياقوت ،" **واقع الجريمة عبر الفايسبوك وسبل الحد من انتشارها: دراسة حالة الجزائر**" مجلة الدراسات و البحوث القانونية ، جامعة محمد بوضياف ، المسيلة ، الجزائر ، المجلد 7، العدد 2، 2022 .

– عون فاطمة الزهراء ، **الإجراءات التشريعية المستحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري – القطب الجزائي الوطني نموذجا –** مجلة حقوق الإنسان والحريات ، جامعة ابن باديس ، مستغانم ، الجزائر ، المجلد 7 ، العدد 2 2022 .

– وسام الدين محمد العلكة ، **التعاون الدولي في مواجهة جرائم الانترنيت**، مجلة آداب البصرة ، مجلة علمية فصلية محكمة تصدر عن كلية الآداب ، جامعة الصرة ، العراق ، العدد 66 ، 2013 .

– خالد الشرقوني السموني ، **مكافحة الجريمة الالكترونية على المستويين الوطني و الدولي** ، المجلة المغربية للإدارة والتنمية ، الرباط ، المغرب العدد112 2012 .

– بارة سمير ، " **الدفاع الوطني والسياسات الوطنية للامن السيبراني في الجزائر ، الدور و التحديات** " المجلة الجزائرية للأمن الإنساني جامعة باتنة 1 ، الجزائر ، المجلد2، العدد2، 2017 .

– ادريس عطية ، **مكانة الأمن السيبراني في منظومة الأمن الوطني** ، مجلة مصداقية ، المدرسة العليا العسكرية للإعلام والاتصال ، الجزائر المجلد 1، العدد1 .

– سفيان حديدان ، **الدخول أو البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات** ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية جامعة محمد بوضياف ، المسيلة ، الجزائر ، المجلد2، العدد8 ، 2017 .

– لوكال مريم ، **الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي في ضوء قانون حماية المعطيات** ، مجلة العلوم القانونية و السياسية ، جامعة الوادي ، الجزائر ، المجلد 10، العدد1، 2019 .

– رابح سعاد ، **ضوابط مكافحة الجريمة المعلوماتية** ، مجلة القانون العام الجزائري و المقارن ، جامعة جيلالي اليابس سيدي بلعباس ، الجزائر المجلد 7 ، العدد1 ، 2021 .

– سميحة بلقاسم و حميد بوشوشه ، **الجريمة الالكترونية بعد الاجرام في الجزائر "واقعها و اليات مجابهتها** " ، مجلة العلوم الإنسانية لجامعة جامعة العربي بن مهيدي ، أم البواقي، الجزائر ، المجلد 10، العدد1، 2023 .

– عرب، يونس ،**إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات**، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – أبو ظبي 10–12 /2/ 2002 .

– بن عميور آمنة ، بوحلايس إلهام ، " **القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال** " عدد خاص بفعاليات الملتقى الدولي حول " **القانوني الجنائي للأعمال نحو توجه جديد للتجريم المعقد يوم 14 أكتوبر 2021** " مجلة البحوث في العقود وقانون الأعمال ، جامعة قسنطينة ، الجزائر ، المجلد 7 ، العدد 1 ، 2022 .

– فضيلة عاقلي ، **الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري** ، ضمن أعمال المؤتمر الدولي الرابع عشر حول الجريمة الالكترونية ، مركز جيل البحث العلمي ، طرابلس، ليبيا ، 2017 .

الأطروحات والرسائل الجامعية :

– شنتير خضيرة ، **الآليات القانونية لمكافحة الجريمة الالكترونية – دراسة مقارنة** – أطروحة دكتوراه ، كلية الحقوق والعلوم السياسية ، جامعة أحمد دراية ، ادرار2020–2021 .

– خالد علي نزال الشعار ، **التحقيق الجنائي في الجرائم الالكترونية** ، بحث مقدم لاستيفاء متطلبات الحصول على درجة الدكتوراه في الحقوق،جامعة المنصورة ،2020 .

سادسا : الأطروحات والرسائل الجامعية :

– شنتير خضيرة ، **الآليات القانونية لمكافحة الجريمة الالكترونية – دراسة مقارنة** – أطروحة دكتوراه ، كلية الحقوق والعلوم السياسية ، جامعة أحمد دراية ، ادرار2020–2021 .

– خالد علي نزال الشعار ، **التحقيق الجنائي في الجرائم الالكترونية** ، بحث مقدم لاستيفاء متطلبات الحصول على درجة الدكتوراه في الحقوق،جامعة المنصورة ،2020 .

– فيصل بدري ، **مكافحة الجريمة الالكترونية في القانون الدولي و الداخلي** ، رسالة دكنوراه ، جامعة الجزائر 01 2017–2018 .

– مجاهدي خديجة صافية ، **اليات التعاون الدولي لمكافحة الجريمة المنظمة** ، أطروحة دكتوراه ، كلية الحقوق و العلوم السياسية ، جامعة مولود معمري ، تيزي وزو ، 2018 .

– حمزة بن عقون، **السلوك الإجرامي للمجرم المعلوماتي**، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية تخصص علم الإجرام و العقاب جامعة باتنة، ،2011/2012 .

- سهيلة بوزبرة، **مواجهة الصفقات العمومية المشبوهة**، مذكرة ماجستير في القانون الخاص، كلية الحقوق جامعة جيجل الجزائر ، 2008 .

- عمار حشمان ، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة تخرج لنيل شهادة ماستر تخصص إدارة التحقيقات الاقتصادية و المالية،جامعة قاصدي مرباح ورقلة ،2018-2019 .

سابعا : دراسات أجنبية

- Leukfeldt, R., Veenstra, S., &Stol, W. (2013). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. International Journal of Cyber Criminology, Vol. 7 (1).
- Salvage Ph , **droit pénal général** , **3**éme **édition , 1994** .

فهرس الموضوعات

ملخص

تتناول هذه الدراسة الإطار المفاهيمي والقانوني للجريمة الإلكترونية، مع التركيز على التشريع الجزائري والآليات المعتمدة في مكافحتها. وقد تم تحليل المفهوم اللغوي والاصطلاحي للجريمة الإلكترونية، مع إبراز خصائصها المميزة مثل الطابع غير المادي، والصعوبة في تعقب مرتكبيها. كما استعرضت الدراسة مختلف النصوص القانونية الجزائرية ذات الصلة، والعقوبات المقررة، إلى جانب الإجراءات المعتمدة من قبل الأجهزة الأمنية (الشرطة، الدرك الوطني) والسلطة القضائية (النيابة العامة، المحاكم).

وخلصت الدراسة إلى أن الإطار القانوني الجزائري لا يزال في حاجة إلى مزيد من التحديث والتكييف مع التطورات الرقمية، وأن التنسيق بين الفاعلين في مكافحة هذا النوع من الجرائم يتطلب تدعيمًا تشريعيًا وتقنيًا. وقد قُدمت مجموعة من التوصيات لتقوية الردع القانوني، وتطوير قدرات البحث والتحقيق الرقمي، وتعزيز التوعية المجتمعية بمخاطر الجريمة الإلكترونية.

الكلمات المفتاحية

الجريمة الإلكترونية ، القانون الجزائري، الأمن الرقمي، الأدلة الرقمية، الشرطة القضائية، الدرك الوطني

النيابة العامة، المحاكم الجزائية، التشريعات الحديثة، التحقيق الرقمي، الأمن السيبراني

Summary: This study explores the conceptual and legal framework of cybercrime, with a focus on Algerian legislation and the mechanisms adopted to combat it. It analyzes the linguistic and terminological definitions of cybercrime, highlighting its distinctive features such as its intangible nature and the difficulty of tracking perpetrators. The study also reviews relevant Algerian legal texts and prescribed penalties, as well as the procedures implemented by security agencies (police, national gendarmerie) and the judiciary (public prosecution, courts).The study concludes that the Algerian legal framework still requires further updates and adaptations to keep pace with digital developments. It also stresses the need for stronger legislative and technical coordination among actors involved in combating cybercrime. A set of recommendations is proposed to enhance legal deterrence, improve digital investigation capacities, and raise public awareness of the risks associated with cybercrime

KeywordsCybercrime, Algerian law, digital security, digital evidence, judicial police, national gendarmerie,public prosecution, criminal courts, modern legislation, digital investigation, cybersecurity.