

مذكرة

لنيل شهادة الماستر

تحت عنوان

المستحدث في الجريمة الالكترونية في ظل قانون الإجراءات الجزائية رقم 14-25 وقانون العقوبات

الشعبة: الحقوق

التخصص: علم الجريمة

تحت إشراف الأستاذ:

أ. بن شنات صالح

من إعداد الطالبين:

ميراوي عبد القادر

موفق طارق

أعضاء لجنة المناقشة

المؤسسة	الصفة	الاسم واللقب
جامعة وهران-1	رئيساً	أ/ عز الدين قمراري
جامعة وهران-1	مشرف	أ/ صالح بن شنات
جامعة وهران-1	مناقشا	أ / محمد سعيد

السنة الجامعية 2026/2025

بسم الله الرحمن الرحيم

إهداء:

باسم الله والحمد لله والصلاة على أشرف خلق الله، اللهم صلى على سيدنا محمد
وعلى اهله وأصحابه الى يوم الدين أما بعد:

نهدي هذا العمل المتواضع الى:

- عائلتنا الكريمتين

- والى كل من ساهم في هذا البحث من قريب او بعيد

شكر وتقدير

حتى لا نكون ممن قال فيهم رسول الله صل الله عليه وسلم:

"من لا يشكر الناس لم يشكر الله"

نشكر الله عز وجل الذي منحنا القوة والإرادة لإكمال دراستنا، ومنحنا القدرة على انجاز هذا البحث

نتقدم بالشكر الخالص لأستاذنا " د. صالح بن شنات " على قبوله الاشراف

على هذا العمل، كما نتقدم بالشكر لأعضاء لجنة المناقشة الاستاذين: د/

قمراري عز الدين و د/ محمد سعيد لتفضلهم بمناقشة هذا البحث،

كما لا يفوتنا تقديم الشكر الخاص للأستاذ " د. بوهدة محمد الأمين " مدير

معهد علم الاجرام لمنحنا هذه الفرصة وتوفيره رفقة الطاقم الإداري

الظروف المواتية للدراسة والتحصيل العلمي.

والى كل اساتذتنا الكرام كل باسمه وصفته

في

" معهد علم الاجرام بوهران "

شكرا الى كل من ساندنا من قريب أو بعيد

مقدمة:

لقد أفرزت الثورة التكنولوجية المعاصرة تحولاً جذرياً في بنية الحضارة الإنسانية، فلم تعد التقنيات الرقمية مجرد وسائل مساعدة أو أدوات ثانوية، بل أضحت الإطار المركزي الذي تُعاد ضمنه صياغة أنماط التفاعل الاجتماعي، وتُدار من خلاله المبادلات الاقتصادية، وتُرسَم في نطاقه ملامح السياسات الدولية، فقد غدا الفضاء الرقمي بيئة متكاملة للحياة المعاصرة، تتداخل فيها المصالح والوظائف بشكل غير مسبوق، الأمر الذي جعله ركيزة أساسية في استقرار الدول واستمرارية مؤسساتها.

غير أن هذا التطور المتسارع، وعلى الرغم مما حمله من إمكانيات هائلة وآفاق واعدة، قد أفرز في المقابل تحديات عميقة ومعقدة، لعل أخطرها بروز نمط جديد من الإجرام يُعرف بالجريمة الإلكترونية. فهذا النوع من الجرائم لم يعد مجرد امتداد للجريمة التقليدية في ثوب رقمي، بل يمثل تحولاً نوعياً في المفهوم الإجرامي ذاته من حيث مرتكبيه والوسائل المستعملة والخصائص والآثار المترتبة عنها.

إذ تتسم الجريمة الإلكترونية بكونها لا مادية، عابرة للحدود ومن أي مكان في العالم دون الحاجة إلى حضور مادي لمسرح الجريمة، وسريعة التنفيذ يمكن ارتكابها في لحظات وهو ما يجعلها أكثر تعقيداً وصعوبة الإثبات وأخطر من الجرائم التقليدية.

وتتبع خطورة هذه الجرائم من طبيعة البيئة التي تنشأ فيها، حيث تتجسد العلاقة الجدلية بين الابتكار البشري والتطور التقني في أوضح صورها. فقد أتاح التقدم التكنولوجي أدوات متطورة يمكن توظيفها إيجابياً في خدمة الإنسان، غير أن بعض الأفراد استغلوا هذه الأدوات ذاتها لارتكاب أفعال غير مشروعة، مستفيدين من الثغرات التقنية والقصور التشريعي.

وهكذا أصبح الجاني يعتمد فقط على مهارات تقنية ومعرفة معلوماتية تمكنه من الولوج إلى الأنظمة الآلية، والاستحواذ على البيانات، والتلاعب بها، بل وحتى تخريب البنى التحتية الحيوية للمساس بالأمن العام.

مقدمة:

كما تتميز الجريمة الإلكترونية بخصوصية الدليل المرتبط بها، وهو ما يُعرف بالدليل الرقمي، الذي يتسم بطبيعته الهشة وسرعة قابليته للتلف أو التغيير أو الحذف، فضلاً عن صعوبة تعقبه وإثباته. وهذا ما يطرح إشكالات جوهرية أمام منظومة العدالة الجزائية، التي بُنيت في الأصل على الدليل الملموس. ومن ثم، وجدت القواعد القانونية الموضوعية منها والإجرائية، نفسها أمام تحدٍ حقيقي يستدعي تكيفها بما يتلاءم مع خصوصية الفضاء الرقمي. ولم تقف خطورة الجريمة الإلكترونية عند حدود الاعتداء على الأفراد أو المساس بخصوصياتهم، بل امتدت لتطال الأمن القومي والسيادة الرقمية للدول، حيث باتت الهجمات السيبرانية قادرة على استهداف المنظومات المالية والمعلوماتية وتعطيلها، بما يهدد بشل الاقتصاد الوطني ويقوض الثقة في البيئة الرقمية. كما أن لهذه الجرائم آثاراً نفسية واجتماعية عميقة، إذ تساهم في نشر القلق وانعدام الأمن الرقمي، وتؤثر على تماسك المجتمع في ظل تزايد الاعتماد على الوسائط التكنولوجية.

وفي خضم هذه التحولات، تبرز أهمية هذا البحث من كونه يتناول موضوعاً تتقاطع فيه التكنولوجيا مع القانون، حيث لم يعد دور التكنولوجيا مقتصرًا على تسهيل الحياة اليومية، بل أصبح عنصراً محورياً في استقرار الدول وحماية مصالحها الحيوية. وتكمن الأهمية القانونية لهذا الموضوع في تسليط الضوء على الآليات الإجرائية المستحدثة التي أقرها المشرع لضبط الدليل الرقمي، وتحديد المسؤولية الجزائية في بيئة افتراضية، بما يسهم في إرساء دعائم عدالة جنائية رقمية قادرة على مواجهة هذا النمط المستجد من الإجرام.

كما أن اختيار هذا الموضوع لم يكن صدفة، بل جاء استجابة لجملة من الاعتبارات الموضوعية والعلمية، من أبرزها الرغبة في استكشاف التحول التشريعي الذي عرفتته المنظومة القانونية من خلال النصوص الموضوعية المستحدثة في قانون العقوبات والاجرائية في قانون الإجراءات الجزائية، والتي هدفت إلى سد الفراغ القانوني في مواجهة الإجرام المعلوماتي. إضافة إلى ذلك، فإن خطورة الآثار الناجمة عن هذه الجرائم، سواء على المستوى الاقتصادي أو

مقدمة:

الأمني أو الاجتماعي، تفرض ضرورة دراستها وتحليل أبعادها المختلفة. ويُضاف إلى ذلك وجود فراغ نسبي يربط بين الجوانب التقنية البحتة والنصوص القانونية، خاصة في ظل ما يثيره إثبات هذه الجرائم من صعوبات عملية وتعقيدات إجرائية مرتبطة بسرعة زوال الأدلة الرقمية.

وانطلاقاً من ذلك، يسعى هذا البحث إلى تحقيق جملة من الأهداف العلمية، تتمثل أساساً في تحديد المفاهيم القانونية الحديثة المرتبطة بالجريمة الإلكترونية في ظل التشريع الراهن، وتحليل الإجراءات المستحدثة التي أقرها المشرع، كآليات التفتيش عن بعد والحجز الرقمي للبيانات، وتقييم مدى فعاليتها في كشف الجناة وضبط الأدلة. كما يهدف إلى إبراز العلاقة التفاعلية بين التطور التكنولوجي وتطور السلوك الإجرامي، مع الوقوف على مدى قدرة القانون على تحقيق التوازن بين متطلبات مكافحة الجريمة وضمان حماية الحقوق والحريات الأساسية.

وفي ضوء ما سبق، يمكن إبراز إشكالية هذه الدراسة في السؤال الرئيسي التالي:

إلى أي مدى وفقت التعديلات المستحدثة في قانون العقوبات وقانون الإجراءات الجزائية الجديد في إرساء نظام قانوني وإجرائي متكامل يكفل مواجهة الجريمة الإلكترونية وضبط أدلتها الرقمية بفعالية؟

وللإجابة عن هذه التساؤلات، تم الاعتماد على المنهج التحليلي من خلال دراسة النصوص القانونية المستحدثة وتحليل مضامينها، إلى جانب المنهج الوصفي الذي يهدف إلى توصيف ظاهرة الجريمة الإلكترونية واستجلاء أبعادها المختلفة.

وقد قسمنا هذه الدراسة إلى فصلين رئيسيين؛ خُصص الفصل الأول للإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري، حيث تناولنا فيه ماهية هذه الجرائم وخصائصها المستحدثة، إلى جانب السياسة العقابية التي أقرها المشرع لمواجهتها في ظل التعديلات الحديثة.

مقدمة:

أما الفصل الثاني، فقد تناولنا فيه الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية، من خلال دراسة الإطار المؤسسي المتخصص، وكذا مختلف وسائل التحري والتحقيق الرقمي، وصولاً إلى بيان حجية الدليل الرقمي والضمانات القانونية المرتبطة به.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

أصبح الفضاء الرقمي مجالاً جديداً لارتكاب الجرائم، إذ لم تعد الأفعال الإجرامية محصورة في صورها المادية التقليدية، بل اتسعت لتشمل اعتداءات سيبرانية عابرة للحدود الوطنية تمس بالأنظمة والبيانات والخصوصية. وقد تنبه المشرع الجزائري إلى خطورة هذه التحولات، فعمل على وضع إطار قانوني يجمع بين القواعد الموضوعية والإجرائية لمواجهة ما نتج عن التطور التكنولوجي المتسارع الذي أدى إلى إساءة استخدام الأنظمة المعلوماتية. ويهدف هذا الفصل إلى تحديد ماهية الجرائم الإلكترونية، وتبيان أركانها الأساسية وخصائصها في المبحث الأول، مع التطرق إلى السياسة الجزائية التي اعتمدها المشرع الجزائري للتصدي لهذه الجريمة المتغيرة والياتها التقنية المعقدة في المبحث الثاني.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

المبحث الأول: ماهية الجرائم الإلكترونية المستحدثة وخصائصها

تعد الجريمة الإلكترونية ظاهرة ذات طبيعة قانونية وتقنية مركبة، إذ لا تقتصر على كونها امتداداً للجريمة التقليدية، بل تمثل كياناً مستقلاً يتميز بخصائص ووسائل خاصة تستدعي وضع تعريفات دقيقة تتجاوز الإطار المادي التقليدي. فهي، إلى جانب طابعها العابر للحدود وكونها غير ملموسة، تتسم بصعوبة الكشف عنها وسرعة زوال أدلتها الرقمية، الأمر الذي يفرض تحديات مستمرة أمام جهات التحقيق من الناحيتين التقنية والقانونية. ومن خلال هذا المبحث، سيتم السعي إلى تحديد المفهومين الاصطلاحي والتشريعي للجريمة الإلكترونية وتطورها في المطلب الأول، مع إبراز الخصائص الأساسية التي تجعل منها جريمة "ذكية" تستهدف الأنظمة المعلوماتية وبياناتها والحقوق والحريات الشخصية في البيئة الرقمية في المطلب الثاني.

المطلب الأول: مفهوم الجريمة الإلكترونية وتطورها

يُعد مفهوم الجريمة الإلكترونية من المفاهيم الحديثة نسبياً، إذ ارتبط ظهوره بالتطور المتسارع في مجال تكنولوجيا المعلومات والاتصال. وعلى الرغم من انتشار هذا النوع من الجرائم، فإنه لا يوجد تعريف دولي موحد وشامل لها، نظراً لتعدد صورها وتنوع وسائل ارتكابها. وقد اختلف هذا المفهوم قدر من الغموض، نتيجة اختلاف الجهود الفقهية الرامية إلى صياغة تعريف دقيق جامع مانع، حيث لم يتوصل الفقه إلى اتفاق نهائي بشأنه، بل ذهب بعض الباحثين إلى عدم جدوى وضع تعريف خاص، على أساس أن هذه الجرائم ليست سوى جرائم تقليدية تُرتكب بوسائل إلكترونية¹.

وعليه، سيتم في هذا المطلب عرض مختلف التعاريف التي قُدمت للجريمة الإلكترونية، مع بيان تطورها القانوني، وذلك وفق التقسيم التالي:

¹ - حفيظ نقادي معالم الجريمة المعلوماتية في القانون الجزائري مجلة الحقوق و العلوم الانسانية ، العدد 20 ، جامعة زيان عاشور، بالجلفة 2014، ص 170.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

الفرع الأول: تعريف الجريمة الإلكترونية

لا يوجد مصطلح موحد للدلالة على هذه الظاهرة، فهناك من يطلق عليها ظاهرة الغش المعلوماتي أو الاختلاس المعلوماتي أو الجريمة السيبرانية أو الإلكترونية وعلة هذه الاختلافات هو خشية حصر هذه الجريمة في مجال ضيق¹، ومرد ذلك الى أنه ليس لها جانب قانوني فقط بل تتداخل مع جوانب تقنية والتي بطبيعتها متطورة بتطور التكنولوجيا. لذلك سيتم تناول هذا المفهوم من خلال التعريف اللغوي، ثم الفقهي، وأخيراً التعريف الذي تبناه المشرع الجزائري.

أولاً: التعريف اللغوي والفقهي للجريمة الإلكترونية

1- التعريف اللغوي

قبل الخوض في التعريف الفقهي، يجدر التوقف عند المعنى اللغوي للمصطلح، نظراً لتأثير اللغة في تحديد المفاهيم الاصطلاحية. ويتكون مصطلح "الجريمة الإلكترونية" من كلمتين:

الجريمة: لغة كلمة مشتقة من الجرم وهو التعدي أو الذنب وجمع الكلمة اجرام وجروم وهو الجريمة وقد جرم يجرم واجترم وأجرم فهو مجرم جريم، وهي طبقاً للمفهوم الاجتماعي كل سلوك إرادي غير مشروع يصدر عن شخص مسؤول جنائياً في غير حالات الإباحة عدواناً على مال أو مصلحة أو حق محمي بجزاء جنائي²، والإلكترونية: تستخدم لوصف فكرة أو جزء من الحاسب أو علم المعلومات³.

¹ - محمد علي العريان، الجرائم المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، مصر، 2004، ص 43.

² - هبة نبيلة هروال، جرائم الانترنت دراسة مقارنة، أطروحة دكتوراه، جامعة تلمسان، الجزائر، 2013/2014، ص 12.

³ بoudisse بجاد عبد الرؤوف، أليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة ماستر، جامعة محمد

البشير الابراهيمي برج بوعرييج، الجزائر، 2021/2022، ص 9.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

2- التعريف الفقهي للجريمة الإلكترونية

اختلف الفقهاء في وضع تعريف موحد للجريمة الإلكترونية، حيث اعتمد كل اتجاه على زاوية معينة، سواء من حيث الوسيلة أو الفاعل أو موضوع الجريمة. والتي يمكن عرضها كما يلي:

أ- المفهوم الضيق:

يعتمد هذا الاتجاه على تحديد الجريمة الإلكترونية وفق معيار معين، وقد تعددت هذه المعايير¹:

1- وفق معيار وسيلة ارتكاب الجريمة:

يُنظر إلى الجريمة الإلكترونية على أنها كل فعل غير مشروع يُرتكب باستخدام الحاسوب أو إحدى الوسائل التقنية كالهواتف الذكية. وقد عرّفها الأستاذ MASS بأنها: "الاعتداءات التي يمكن ارتكابها بواسطة الوسائل المعلوماتية بهدف تحقيق ربح".

كما عرفها الفقيه الألماني TIEDMANN بأنها: "كل سلوك غير مشروع أو ضار بالمجتمع يتم بواسطة الحاسوب".

في حين اعتبرها MAWRE: "كل فعل غير مشروع يتدخل فيه الحاسوب كوسيلة".

2- وفق معيار المعرفة التقنية:

يركز هذا الاتجاه على شخص الجاني، حيث يشترط توفر معرفة تقنية لديه. وقد عرفها THOMSON DAVID بأنها: "كل جريمة يتطلب ارتكابها توفر معرفة بتكنولوجيا الحاسوب لدى الفاعل".

¹ - غنية باطلي، الجريمة الإلكترونية- دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015، ص 16، 17.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

3- وفق معيار موضوع الجريمة:

يرى هذا الاتجاه أن الجريمة الإلكترونية تتحدد بموضوعها، أي عندما يكون محل الاعتداء هو المعلومات أو البيانات، بغض النظر عن الوسيلة المستخدمة.

ب- المفهوم الواسع:

جاء هذا الاتجاه كرد فعل على ضيق المفهوم السابق، حيث وسّع نطاق الجريمة الإلكترونية ليشمل كل فعل غير مشروع له صلة بالتكنولوجيا، سواء من حيث الوسيلة أو الموضوع أو النتيجة.

فقد عرفها PARKER بأنها: "كل فعل إجرامي متعمد، له علاقة بالمعلوماتية، ويترتب عليه ضرر للمجني عليه أو منفعة للجاني"¹.

كما عرّفها الفقيهان MIEL و CREDO بأنها تشمل استخدام الحاسوب كأداة لارتكاب الجريمة، وكذلك حالات الولوج غير المشروع إلى الأنظمة والبيانات.

أما منظمة التعاون والتنمية الاقتصادية فقد اعتبرتها: "كل فعل أو امتناع من شأنه الإضرار بالمكونات المادية أو المعنوية للحاسوب وشبكات الاتصال، باعتبارها من المصالح التي يحميها القانون الجنائي".

كما عرّفها مؤتمر الأمم المتحدة العاشر لمنع الجريمة (فيينا 2000) بأنها: "كل جريمة يمكن ارتكابها داخل نظام حاسوبي أو عبر شبكة معلوماتية".

¹ -جدي نسيم، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مذكرة ماجستير، جامعة وهران، 2014، ص 9.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

ج- الاتجاه الفقهي المختلط (الجامع)

نتيجة للانتقادات الموجهة لكل من الاتجاهين السابقين، ظهر اتجاه ثالث يجمع بينهما، ويعتمد على معيار المصلحة محل الحماية.

ويُعرف هذا الاتجاه الجريمة الإلكترونية بأنها: "كل سلوك غير مشروع يمس المعالجة الآلية للمعطيات أو نقلها، سواء بشكل مباشر أو غير مباشر، وبما يخالف القواعد القانونية". وقد تبني هذا التوجه كل من ALTERMAN و BALOCH، كما ينسجم مع تعريف منظمة التعاون والتنمية الاقتصادية للغش المعلوماتي، الذي يعتبر الجريمة الإلكترونية كل فعل يمس الأموال أو المصالح المادية والمعنوية نتيجة استخدام التكنولوجيا¹.

ثانياً: تعريف الجريمة الإلكترونية في التشريع الجزائري

اعتمد المشرع الجزائري مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، خلافاً لما هو شائع من تسميات مثل الجرائم الإلكترونية أو السيبرانية، وذلك بهدف توسيع نطاق التجريم ليشمل مختلف الأفعال المرتبطة بالتكنولوجيا.

وورد تعريف هذه الجرائم في القانون رقم 09-04، حيث نصت المادة 2 على أنها: "الجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات، وكل جريمة تُرتكب أو يُسهّل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

وهذا التعريف يجمع بين:

الجرائم الإلكترونية بالطبيعة التي تستهدف الأنظمة المعلوماتية وبياناتها،

والجرائم التقليدية التي تُرتكب أو يسهل استخدام الوسائل الإلكترونية ارتكابها.

كما عرف القانون رقم 21-11 المعدل والمتمم لقانون الإجراءات الجزائية بموجب نص المادة 211 مكرر 22 في الفقرة 3 منه الجريمة الإلكترونية وهو نفس التعريف الذي ورد في

¹ -خالد داودي، الجريمة المعلوماتية، دار الاصدار العلمي للنشر والتوزيع الجزائر، ط1، 2008، ص 25.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

نص المادة 2 من القانون رقم 04-09 مع توسيع من مفهوم الوسيلة المستخدمة في ارتكاب هذا النوع من الجرائم بإضافة أي وسيلة أخرى أو الية ذات صلة بتكنولوجيات الاعلام والاتصال ويرجع ذلك الى خصوصية هذه الجريمة المستحدثة والتي ترتبط ارتباطا مطردا بالتطور التكنولوجي المتسارع وهو نفس التعريف الذي تم الإبقاء عليه في نص المادة 335 الفقرة 3 من قانون الإجراءات الجزائية الجديد، وتم كذلك تعريف المقصود بالجريمة الالكترونية الأكثر تعقيدا في قانون العقوبات بموجب نص المادة 338 الفقرة من قانون الإجراءات الجزائية.

الفرع الثاني: التطور التاريخي للجريمة الالكترونية

إن مفهوم الجريمة الإلكترونية قد عرف تطورا تاريخيا متدرجا مع التطور العلمي والتقني واستحداث وسائل تكنولوجية جديدة، خاصة بعد أن أصبحت المجتمعات الحديثة تعتمد بشكل أساسي على الكمبيوتر.

وقد مرت الجريمة الإلكترونية بمراحل متعددة في تطورها، حيث تم رصدها لأول مرة في الإحصائيات خلال الفترة الممتدة بين (1971-1990)، إذ كانت الجرائم المسجلة آنذاك محدودة جدا، حيث لم يتجاوز عددها جريمة إلى ثلاث جرائم على مستوى العالم. ومن أبرز هذه الجرائم ما وقع سنة 1988، عندما تم استخدام الحاسوب لسرقة مبلغ 70 مليون دولار من بنك شيكاغو الوطني الأول. وفي نفس السنة، تم إنشاء أول فريق لطوارئ الحاسوب (CERT) بمعهد هندسة البرمجيات بجامعة كارنيجي ميلون الأمريكية، لمواجهة مختلف أشكال الجريمة الإلكترونية. كما تبنت اللجنة الوزارية لمجلس أوروبا سنة 1989 التوصية رقم 9 (89) المتعلقة بمكافحة جرائم الحاسوب¹.

أما خلال عقد التسعينيات، فقد شهدت الجرائم الإلكترونية تزايدا ملحوظا، ومن أبرزها حادثة سنة 1994، حيث كان عدد مستخدمي الإنترنت عالميا حوالي 25.454.590، وتمكن

¹ . عفاف بعون، نسيم أولاد سالم، الجريمة الالكترونية- قراءة سوسيوتاريخية في النشأة والاثار، مجلة القبس للدراسات النفسية والاجتماعية- المجلد 5 العدد 20 جامعة يحي فارس المدية الجزائر، 2023، ص 72.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

طالب أمريكي يبلغ من العمر 16 سنة، يُعرف باسم Data Stream (نمر البيانات)، من اختراق أنظمة حاسوبية تابعة لمعهد أبحاث الطاقة الكوري ووكالة ناسا وجهات حكومية أمريكية أخرى، قبل أن يتم توقيفه في إنجلترا. وفي سنة 1995، تمكنت عصابة روسية محترفة من الاستيلاء على 10 ملايين دولار من بنك سيتي بنك باستخدام الحاسوب وتحويلها إلى حسابات في فنلندا وإسرائيل. ومنذ ذلك الحين، تزايدت الجرائم الإلكترونية بشكل مستمر في مختلف دول العالم، بالتوازي مع تنامي الجهود الدولية والإقليمية لوضع استراتيجيات فعالة لمكافحتها¹. وبناءً على ذلك، فإن الجريمة الإلكترونية مرت بمراحل تاريخية متعاقبة تبعاً للتطورات التكنولوجية، ويمكن تلخيصها كما يلي²:

أولاً: مرحلة الخمسينيات من القرن الماضي

تمثل هذه المرحلة بداية ظهور الحواسيب وانطلاق ثورة تكنولوجيا المعلومات، التي كانت في البداية منفصلة عن وسائل الاتصال التي ظهرت في الأربعينيات. ويرتبط ظهور الجرائم الإلكترونية تاريخياً بظهور الحاسوب وانتشاره، حيث بدأ ذلك سنة 1954 في الولايات المتحدة الأمريكية مع طرح أول جهاز حاسوب للبيع وبدء استخدامه تجارياً. ومنذ ذلك الوقت، بدأت ظاهرة جرائم الحاسوب في الظهور، لكنها كانت تقتصر في بدايتها على سوء استخدام الحاسوب من الناحية الأخلاقية. وقد سُجلت أول جريمة إلكترونية سنة 1957 في الولايات المتحدة، ثم تلتها تقارير متعددة ترصد حالات سوء استخدام الحاسوب، وتم تصنيفها ضمن جرائم العبث والتخريب وسرقة المعلومات أو الاستعمال غير المشروع. وخلال هذه الفترة، لم يكن هناك تمييز واضح بين الجرائم التي تستهدف المكونات المادية للحاسوب وتلك التي تستهدف

¹ -مجمع البحوث والدراسات: (2016)، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، سلطة عمان، مجلس التعاون لدول الخليج العربية، ص 9.

² -ميرفت محمد حبابية، مكافحة الجريمة الإلكترونية، ط1، عمان، دار اليازوري العلمية للنشر والتوزيع، 2022، ص 25.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

معطياته، كما أن التكييف القانوني لهذه الجرائم كان يتم وفق نفس المفاهيم المطبقة على الجرائم التقليدية¹.

ثانيا: مرحلة الستينيات والسبعينيات من القرن الماضي

شهدت هذه المرحلة انتشاراً أوسع لاستخدام الحاسوب، وبرز خلالها مفهوم إساءة استعماله والعبث بالبيانات، خاصة مع بداية الستينيات. كما بدأت الصحف لأول مرة في نشر مقالات تتناول هذه الظاهرة، حيث ركزت على التلاعب بالبيانات المخزنة وتخریب أنظمة الحاسوب².

ثالثا: مرحلة الثمانينيات من القرن الماضي

تميزت هذه المرحلة بظهور مفهوم جديد لجرائم الحاسوب المرتبطة باختراق الأنظمة عن بعد، كما ظهرت الفيروسات الإلكترونية التي تستهدف تدمير الملفات والبرامج. وخلال هذه الفترة، شاع مصطلح "الهاكرز" للدلالة على الأشخاص الذين يقومون باختراق الأنظمة الحاسوبية³.

رابعا: مرحلة التسعينيات من القرن الماضي والقرن الحالي

شهدت هذه المرحلة ظهور أشكال جديدة ومتطورة من جرائم الحاسوب، تزامناً مع انتشار الإنترنت، من بينها الدخول غير المصرح به إلى الأنظمة، والتلاعب بمحتوياتها أو تدميرها، إضافة إلى الهجمات على المواقع الإلكترونية. كما امتدت هذه الجرائم لتشمل التجسس الصناعي والأمني، والاستيلاء على بيانات بطاقات الائتمان واستغلالها بشكل غير مشروع، فضلاً عن الاعتداء على سمعة الأفراد من خلال الرسائل الإلكترونية.

¹ - عفاف بعون، نسيم أولاد سالم، المرجع السابق، ص 72 - 73.

² - المرجع نفسه، ص 73.

³ - المرجع نفسه والموضع نفسه.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

أما في الألفية الجديدة، فقد عرفت الجرائم الإلكترونية تصاعداً ملحوظاً من حيث الحجم والخطورة، مما يبرز أن لهذه الجرائم جذوراً تاريخية تعود إلى الأربعينيات والخمسينيات، إلا أنها لم تكن معروفة آنذاك بالشكل الذي هي عليه اليوم. وهو ما دفع الدول إلى التسابق نحو وضع تشريعات تهدف إلى الوقاية منها ومكافحتها.

ونتيجة لهذا التطور في مجال المعلوماتية، ظهرت أنواع جديدة من الجرائم لم يكن لها وجود لولا ظهور الحاسوب، حيث شهدت فترة التسعينيات والقرن الحالي أنماطاً متقدمة من جرائم الحاسوب تزامنت مع انتشار الإنترنت، وبرزت أنشطة القراصنة (الهاكرز) الذين يقومون باختراق الأنظمة والمواقع المعلوماتية، والدخول إليها دون ترخيص، والتلاعب بالبيانات المخزنة أو تدميرها، مستفيدين من الإمكانات التي يوفرها الإنترنت. كما شملت هذه الجرائم تعطيل الأنظمة باستخدام البرمجيات الخبيثة، أو إتلافها مادياً، أو استغلالها دون إذن، إلى جانب الهجمات الإلكترونية التي تستهدف تعطيل المواقع. وامتدت كذلك إلى أنشطة التجسس الصناعي والأمني، والاستيلاء على البيانات ذات القيمة الاقتصادية، وسرقة بيانات بطاقات الائتمان واستعمالها بطرق غير مشروعة للاستيلاء على الأموال، فضلاً عن الإساءة إلى سمعة الأفراد عبر الرسائل الإلكترونية أو استغلال مواقع الإنترنت للترويج لمحتوى غير قانوني¹.

¹ -يونس عرب (2002)، موسوعة القانون وتقنية المعلومات دليل أمن المعلومات والخصوصية)، الجزء الأول، منشورات اتحاد المصارف العربية، ص 306.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

المطلب الثاني: خصائص الجريمة الإلكترونية وأركانها القانونية

إن الجريمة الإلكترونية تختلف عن الجرائم التقليدية، ليس فقط من حيث التعريف والوسائل والتقنيات المستعملة وطرق مكافحتها، بل يمكن تمييز هذا النوع من الجرائم من خلال تحديد خصائصه المميزة وبيان أركانه القانونية. وعليه سيتم تناول هذا المطلب من خلال فرعين كما يلي:

الفرع الأول: خصائص الجريمة الإلكترونية

أضفى ارتباط الجريمة الإلكترونية بالحاسوب وشبكة الإنترنت مجموعة من الخصائص التي تنفرد بها عن غيرها من الجرائم التقليدية، وهو ما أكسبها طابعاً قانونياً خاصاً.

أولاً: الطابع العابر للحدود

إن الجريمة الإلكترونية بطبيعتها من الجرائم التي لا تعترف بالحدود الجغرافية للدول، مما قد يمنحها بعداً دولياً. فساهمت شبكة المعلومات في توسيع عملية تبادل المعلومات بين الدول رغم بعد المسافة آلاف الأميال وفي نفس الوقت استفاد المجرمون من هذه الخصوصية لارتكاب جرائمهم عن بعد أو في أماكن متعددة من العالم وفي وقت واحد، كما يمكن أن يكون المجني عليه في غير الدولة التي يقيم فيها الجاني¹.

ثانياً: صعوبة اكتشافها وإثباتها

وتعد هذه الخاصية من أبرز خصائصها، إذ إن الدليل الرقمي دليل سهل النقل والتعديل والازالة في ثواني معدودة من طرف الجاني، ومما يصعب عملية الإثبات عدم وجود أي اثر مادي لها يستخدم كدليل، لا عنف فيه فهو مجرد ارقام وبيانات تحذف أو تعدل من سجلات ذاكرة الحاسوب حيث تصبح غير موجودة.

¹ - خالد ممدوح ابراهيم، أمن الجريمة الالكترونية، الدار الجامعية للطباعة والنشر والتوزيع، 2008، ص 82.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

ويزداد الأمر تعقيداً، بنقص الخبرة الفنية لدى المحققين الذي يقف عائقاً امام اثباتها، لأن هذا النوع من الجرائم يتطلب خبرة فنية عالية، والمأما واسعاً باستخدام الحاسوب أو جهاز بإمكانه المعالجة الآلية للمعطيات المعلوماتية¹.

ثالثاً: عدم التبليغ عن الجرائم الإلكترونية

يعد عدم التبليغ من العوائق الأساسية في كشف الجرائم الإلكترونية، فالعديد منها لا يتم التبليغ عنه، مما يفسر قلة القضايا المسجلة. ومرد ذلك أن اكتشافها يكون غالباً بعد مدة طويلة من ارتكابها وبالصدفة ويؤدي الى محو الأدلة فيجعل الضحية يعتقد انه لا طائلة من التبليغ أو خوفاً من التبعات النفسية والاجتماعية، ولا يقف عند هذا الحد وإنما يمتد الأمر الى أنه يمتنع عن تقديم أي مساعدة لجهات التحقيق إن وقعت وعلمت بها السلطات الامر الذي يصعب من التحقيق ليس من ناحية الكشف عنها فحسب بل وفي اثباتها².

رابعاً: صعوبة الاكتشاف لخصوصية الوسيلة

تتميز الجريمة الإلكترونية بأنها جريمة هادئة وسريعة التنفيذ، إذ يمكن ارتكابها في ثوانٍ معدودة بمجرد الضغط على لوحة المفاتيح، دون أن تترك أثراً أو ضجيجاً، وغالباً ما يكون الجاني بعيداً عن مسرح الجريمة، وقد يتواجد في دولة أو قارة أخرى. كما أنها لا تُكتشف إلا بعد فترة من الزمن من خلال ملاحظة آثارها فقط. وتزداد صعوبة إثباتها بسبب عدة عوامل، منها غياب الاعتراف من الجاني، وعدم وجود شهود، وسرعة التنفيذ، وغياب الأدلة المادية. فالجريمة الإلكترونية لا تترك أثراً مادياً ملموساً يمكن فحصه، بل تتعلق ببيانات رقمية يمكن حذفها أو التلاعب بها بسهولة. وحتى عند ضبط الدليل الإلكتروني، فإن التعامل معه يتطلب مهارات تقنية عالية، وقد يؤدي سوء التعامل معه إلى إتلافه. كما أن بعض الدول لا تزال تعتمد على أساليب تقليدية في التحقيق، مع نقص في تكوين رجال الضبطية القضائية وعدم

¹ - بوحزمة نصيرة، التحقيق الجنائي في الجرائم الإلكترونية رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، جامعة جيلالي ليايس سيدي بلعباس، 2022، ص 35.

² - بوحزمة نصيرة، المرجع السابق، ص 33.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

توفر الوسائل التقنية اللازمة، مما يزيد من صعوبة الحصول على الأدلة. ويواجه المحققون صعوبات في تقدير أهمية الدليل الإلكتروني، وقد يتسببون في إتلافه أو تجاهله، كما قد لا يقومون بمصادرة أدوات الجريمة كالحاسوب وملحقاته. وقد يرفض القاضي أحياناً الدليل الإلكتروني لعدم اقتناعه به¹، وقد يتعرض للتلف أثناء استعماله. ويرى بعض رجال القانون أن اكتشاف هذه الجرائم غالباً ما يكون نتيجة أخطاء الجاني وسوء تخطيطه.

خامساً: الاعتماد على الخداع والتضليل

يعتمد مرتكبو الجرائم الإلكترونية على الذكاء والمهارات التقنية، حيث يستخدمون أساليب الخداع والتضليل لاختراق الأنظمة والوصول إلى المعلومات. ولذلك يُعتبر هذا النوع من الجرائم "إجرام الأذكى"، وغالباً ما يكون الدافع وراءه إثبات القدرة على تجاوز الأنظمة، إلى جانب تحقيق مكاسب مادية أو معنوية.²

الفرع الثاني: الأركان القانونية للجريمة الإلكترونية

رغم أن الجريمة الإلكترونية تُرتكب في بيئة افتراضية، إلا أنها لا تختلف عن الجريمة التقليدية من حيث ضرورة توافر أركانها القانونية، والمتمثلة في الركن الشرعي، والركن المادي، والركن المعنوي، مع خصوصية تميز كل ركن من أركان هذه الجريمة.

¹ - عبد الصديق الشيخ، الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم. المتصلة بتكنولوجيات الإعلام والاتصال، مجلة معالم للدراسات القانونية والسياسية، المجلد 4 العدد 1 لسنة 2020، ص 196.

² - صورية بورباب، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد 01، جامعة طاهري محمد بشار، 2019، ص 94.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

أولاً: الركن الشرعي

يقصد بالركن الشرعي انه لا يمكن أن توجد جريمة ولا عقوبة دون ان تكون مقررة بواسطة نص قانوني صادر من السلطات العامة، مع تنبيه المواطنين بما يجب عليهم القيام به او عدم القيام به تحت طائلة التعرض لعقوبة جزائية¹. وقد اتجهت بعض التشريعات إلى تعديل نصوص الجرائم التقليدية لتتكيف مع الجرائم الالكترونية المستحدثة، في حين فضلت تشريعات أخرى سنّ قوانين خاصة للوقاية منها ومكافحتها.

ثانياً: الركن المادي

يتمثل الركن المادي في الأفعال والسلوكيات الصادرة عن الإنسان، والتي تتجسد في نشاط إجرامي يؤدي إلى نتيجة ضارة. ويتميز هذا الركن في الجريمة الإلكترونية بخصوصية، حيث قد تُعد بعض الأفعال التحضيرية جرائم قائمة بذاتها، مثل شراء برامج الاختراق أو حيازة وسائل فك التشفير أو المواد غير المشروعة.

كما يتطلب الركن المادي توفر عناصر أساسية، تتمثل في:

السلوك المادي:

لا يُعاقب القانون على النوايا أو الأفكار المجردة بل يجب أن يجب أن تتجسد في سلوك مادي سواء بالفعل او الامتناع، كالدخول غير المشروع إلى منظومة المعالجة الآلية للمعطيات أو البقاء فيها أو التلاعب ببياناتها وتتم كل تلك الافعال في بيئة رقمية.

¹ -لحسين بن شيخ آث ملويا، المنتقى في القضاء العقابي، دار الخلدونية، الجزائر، 2012، ص 27.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

مباشرة النشاط المجرم:

السلوك المادي في هذه الجريمة الإلكترونية هو عمل تقني يقوم به المجرم الإلكتروني، بالدخول غير المرخص إلى نظام معلوماتي أو المساس بقاعدة بياناته بجمع بيانات شخصية كالبريد الإلكتروني من منظومة معلوماتية لاستغلالها في مراسلتهم الكترونياً¹، ولا يشترط دوماً حدوث الضرر في هذا الفعل. وقد يتمثل في استغلال التقنية التكنولوجية لارتكابها أو تسهيل ذلك.

ثالثاً: الركن المعنوي

يمثل الركن المعنوي الجانب النفسي للجاني، أي توافر الإرادة الإجرامية والوعي بعدم مشروعية الفعل، ويختلف حسب نوع الجريمة الإلكترونية المرتكبة وطبيعتها الافتراضية.

ويأتي القصد الجنائي كتجسيد عملي لهذا الركن، حيث يظهر في سلوك الجاني وعمله وفق نية واضحة لإحداث فعل يعاقب عليه القانون مع إدراكه بعدم مشروعيته، مثل الدخول غير المصرح به إلى نظام معلوماتي محمي. كما يشمل القصد حالات إحداث الضرر عمداً أو تجاوز النتائج المتوقعة للفعل.

وبذلك، يمكن فهم القصد الجنائي كأداة لتحديد مدى توافر الركن المعنوي في الجريمة الإلكترونية، فهو يوضح نية الجاني ووعيه بالأثر الذي يمكن أن يحدثه، مما يسهل على القانون تقييم المسؤولية الجنائية وبيان حدود العقوبة.

ويُفترض القصد الجنائي إذا أدى سلوك الجاني إلى نتيجة ضارة، حتى وإن لم يقصدها مباشرة، طالما كانت نتيجة نشاطه. كما يُعد الاستمرار في البقاء داخل النظام بعد الدخول غير المقصود سلوكاً إجرامياً إذا تم عن علم وإرادة، ويُستدل على ذلك من خلال تصرفاته داخل النظام.

¹. Myriam Quémener, les données personnelles à l'ère numérique Quelle protection sur le plan pénal, REVUE DU DROIT, n°1 – 2016, p74.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

كما يشمل الركن المعنوي حالات الاعتداء العمدي على أنظمة المعالجة، مثل تعطيلها أو نشر الفيروسات أو التلاعب بالبيانات. وقد تتحقق الجريمة كذلك في بعض الحالات حتى مع حسن النية، مثل استخدام الموظف للحاسوب لأغراض شخصية مما يؤدي إلى إلحاق ضرر بالنظام، كإدخال وسائط تخزين مصابة بفيروسات.

المبحث الثاني: السياسة الجزائية للجرائم المتصلة بتكنولوجيات الاعلام والاتصال

لم يعد السلوك الإجرامي في البيئة الرقمية مجرد مخالفة عارضة للقواعد التقليدية، بل تحول إلى ظاهرة معقدة تستهدف البنى التحتية للدول وتمس بالكيان المعنوي للأفراد، الأمر الذي فرض تبني سياسة جزائية تتسم في الوقت ذاته بالمرونة والصرامة. وتسعى هذه السياسة من جهة إلى تحقيق توازن بين حماية المجتمع من الأنشطة الاجرامية التي تستخدم تكنولوجيات الاعلام والاتصال كوسيلة أو تستهدفها، وبين ضمان حماية الحقوق والحريات الأساسية للأشخاص من جهة أخرى. ويهدف هذا المبحث إلى دراسة توجه السياسة الجزائية التي انتهجها المشرع الجزائري من خلال التعديلات الحديثة، وبيان آليات إرساء الحماية الجزائية للفضاء الرقمي، من خلال تحليل الإطار القانوني لجرائم الاعتداء على الأنظمة وبياناتها وجرائم المحتوى في المطلب الأول، والسياسة العقابية المستحدثة في المطلب الثاني.

المطلب الأول: الجرائم الإلكترونية المستحدثة في قانون العقوبات

تُعد جرائم الاعتداء على المنظومات المعلوماتية من أخطر صور الإجرام المعاصر، بالنظر إلى طبيعة المصلحة المحمية فيها، والتي تتمثل في سلامة وأمن النظم الرقمية التي أصبحت تشكل أساسا لمختلف الأنشطة الحيوية في الدولة الحديثة. فهذه الجرائم لا تستهدف مجرد مكونات تقنية معزولة، بل تمس بشكل مباشر البنية التحتية الرقمية، بما تحمله من معطيات استراتيجية واقتصادية وأمنية. ويقصد بها تلك الأفعال التي تنال من السلامة المنطقية للأنظمة، كالتلاعب بالبرمجيات والبيانات، أو السلامة المادية من خلال تعطيل الأجهزة أو إتلافها، الأمر الذي قد يؤدي إلى شلل كامل في الخدمات العامة أو الخاصة. وعليه فإن

الفصل الأول: الإطار المفاهيمي والتجري للجرائم الإلكترونية في التشريع الجزائري

الطابع التقني البحت لهذه الجرائم يتطلب فهماً دقيقاً لآلياتها وكفاءة عالية لدى أجهزة الضبط القضائي في التعامل معها.

الفرع الأول: جرائم الاعتداء على المنظومات المعلوماتية

أولاً: جريمة الدخول أو البقاء غير المشروع في منظومة للمعالجة الآلية للمعطيات

تُشكل جريمة الدخول أو البقاء غير المشروع في نظام معلوماتي الأساس الذي تتبني عليه باقي الجرائم المعلوماتية، إذ تمثل نقطة الانطلاق نحو ارتكاب أفعال أكثر تعقيداً وخطورة، كالتجسس الرقمي أو سرقة البيانات أو تخريبها. وقد أحاطها المشرع الجزائري بعناية خاصة من خلال المادة 394 مكرر من قانون العقوبات المعدل والمتمم، واضعاً بذلك إطاراً قانونياً يهدف إلى حماية الأنظمة المعلوماتية من أي تسلسل غير مشروع¹.

ويتحقق الركن المادي لهذه الجريمة بمجرد تحقق فعل الولوج غير المصرح به، دون اشتراط حدوث نتيجة ضارة، وهو ما يعكس الطبيعة الوقائية للنص الجنائي. ويشمل هذا الولوج مختلف الوسائل التقنية، سواء عبر كسر الحواجز الأمنية كجدران الحماية، أو استغلال الثغرات البرمجية، أو حتى استخدام بيانات اعتماد تم الحصول عليها بطرق غير مشروعة. ويكفي أن يتم هذا الفعل بطريق الغش أو الاحتيال التقني لقيام الجريمة، مما يبرز توجه المشرع نحو تجريم الخطر قبل تحققه فعلياً.

أما البقاء غير المشروع، فيتجسد في استمرار الشخص داخل النظام المعلوماتي رغم زوال السند القانوني الذي كان يبرر هذا التواجد، وهو ما يُعد صورة سلبية للسلوك الإجرامي، تعكس استغلالاً غير مشروع للصلاحيات الممنوحة. وغالباً ما يرتبط هذا الفعل بما يعرف

¹ -قانون العقوبات الجزائري، المادة 394 مكرر المعدلة بالقانون 06-24 المؤرخ في 24 افريل 2024 ، جريدة رسمية عدد

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

بتجاوز الصلاحيات، حيث يتمكن الجاني من النفاذ إلى مستويات أعلى من التحكم داخل النظام، بما يتيح له الوصول إلى بيانات أو وظائف محظورة.

وقد اتجه المشرع في إطار تعزيز الحماية الجزائية، إلى تشديد العقوبات في الحالات التي تستهدف فيها الأنظمة الخاصة المتعلقة بالدفاع الوطني أو المؤسسات الخاضعة للقانون العام، حيث تصل العقوبة إلى 10 سنوات حبسا طبقا لنص المادة 394 مكرر 3 من قانون العقوبات المعدل والمتمم، وهذا بالنظر إلى خطورة هذه الأفعال المرتكبة في إطار الحروب الهجينة، والتي تعد أكثر تهديدا لاستقرار الامن القومي للدول من الحروب التقليدية.

ثانيا: جرائم ادخال والازالة والتعديل الغير مشروعين للمعطيات

إذا كان الدخول عن طريق الغش الى منظومة معالجة الية للمعطيات يمثل مرحلة الاختراق ويعتبر من جرائم الخطر، فإن جرائم الادخال والازالة والتعديل الغير مشروعين تمثل مرحلة التنفيذ المادي للإضرار بالنظام المعلوماتي أو المعطيات التي يتضمنها، وهي بذلك أخطر من الجريمة الأولى لما تنطوي عليه من آثار مادية ومباشرة على عمل النظام المعلوماتي وسلامة بياناته. وقد جرم المشرع هذه الأفعال صراحة بموجب نص المادة 394 مكرر 1 من قانون العقوبات المعدل والمتمم، والتي تعاقب على كل فعل يؤدي إلى عرقلة سير النظام المعلوماتي.

ويقصد بالإدخال غير المشروع إضافة معطيات جديدة لم تكن موجودة من قبل على الدعامة الخاصة سواء كانت خالية أو كان يوجد بها معطيات من قبل، وذلك قد يتم بهدف التشويش على صحة البيانات والمعلومات القائمة¹، ومثال ذلك ادخال بيانات مصطنعة لموظفين وعمال في قاعدة معطيات مؤسسة معينة للحصول على أجور ومرتببات.

¹ - د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، ط1، منشورات زين الحقوقية،

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

أما فعل الازالة، فيقصد به إزالة جزء من المعطيات المسجلة في نظام المعالجة الآلية أو إضافة جزء من المعطيات الى المنطقة الخاصة بالذاكرة، وقد أوصى التقرير الصادر عن المجلس الأوروبي بخصوص جرائم تقنية المعلومات بتجريم الأفعال التي تؤدي الى محو المعلومات¹. وقد يتم ذلك يدويا أو عن طريق الاستعانة ببرامج فيروسات خاصة يتم وضعها داخل النظام بعد الدخول اليه للقيام بذلك² أو بقبائل منطقية Logic Bomb تظل كامنة حتى ينشطها حدث معين، أما فعل التعديل غير المشروع فهو تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى³.

الفرع الثاني: الجرائم المستحدثة المرتبطة بالمحتوى الرقمي

شهدت الجريمة المعلوماتية تحولا نوعيا، حيث لم تعد تقتصر على الاعتداء على الأنظمة، بل امتدت لتشمل استغلال الفضاء الرقمي كوسيلة لنشر محتوى غير مشروع يمس بالنظام العام أو الحقوق الفردية. ويعكس هذا التحول انتقال الإجرام من البعد التقني إلى البعد الاجتماعي، حيث أصبحت المنصات الرقمية فضاءً لارتكاب أفعال تمس القيم الأساسية للمجتمع.

أولا: جريمة نشر وترويج الأخبار الكاذبة والمغرضة

في إطار محاربة نشر الأخبار والأنباء التي تهدف الى المساس بالنظام والأمن العموميين، جرم المشرع من خلال نص المادة 196 مكرر من قانون العقوبات المعدل والمتمم نشر وترويج الاخبار المضللة والمغلوطة أو التي يراد بها التلاعب بالرأي العام أو تشويه الحقائق وليس الاعلام.

¹ - المرجع نفسه، ص 536.

² - كفيروس LOTUS الذي استهدف قطاع الطاقة والخدمات في فينيزولا سنة 2025 وتم الكشف عنه في سنة 2026 موقع bleepingcomputer.com تاريخ الزيارة 2026/05/10.

³ - علي جعفر، المرجع السابق، ص 538.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

من بين الوسائل التي يتم الاستعانة بها لارتكابها تكنولوجيات الاعلام والاتصال وهنا تكمن خطورة هذه الجريمة في السرعة الفائقة في الانتشار وعلى نطاق واسع والفورية وعدم التحكم في نتائجها وإعادة النشر والمشاركة ويحدث بما يعرف بأثر الدومينو: Domino Effect أو Chain Reaction¹.

وقد سمحت المادة 114 من القانون رقم 25-14 في إطار التحري والتحقيق في هذا النوع من الجرائم إمكانية اللجوء الى وسائل التحري الخاصة، باعتراض المراسلات ووضع الترتيبات التقنية بما يسمح بتعقب المجرمين الذين يقفون وراء هذه الجرائم وتتبع هذه الشبكات الالكترونية وجمع الأدلة الالكترونية وضبطها وبالنتيجة توقيف الفاعلين.

ثانياً: التحرش الإلكتروني والمساس بالحرمة الخاصة للأفراد

شملت الحماية الجزائية مختلف صور المساس بالخصوصية والحياة الخاصة، من خلال تجريم التقاط أو تسجيل أو نشر أو إذاعة المعطيات الشخصية من صور أو فيديوهات أو رسائل الكترونية دون رضا صاحبها طبقاً لنص المادة 333 مكرر 4 من قانون العقوبات المعدل والمتمم²، وهو ما يعكس إدراكاً متزايداً لأهمية حماية الحياة الخاصة في البيئة الرقمية. وغالباً ما تتداخل هذه الأفعال مع جريمة الابتزاز الإلكتروني، حيث يتم استغلال المحتوى الشخصي للضغط على الضحية للحصول على منفعة مادية أو خدمة أو أي مقابل آخر.

ولتعزيز حماية الضحايا، أقر المشرع آليات إجرائية وقائية جديدة بموجب نص المادة 12 من القانون رقم 09-04 والتي تتمثل في الزام مقدمي خدمات الانترنت بالتدخل الفوري لسحب المحتويات المخالفة للقانون أو جعل الدخول اليها غير ممكن، إلى جانب اعتماد وسائل تقنية تسمح بحصر إمكانية الدخول الى الموزعات التي تحتوي على المحتوى المجرم³.

¹ - hbrarabic.com تاريخ زيارة الموقع 2026/05/10.

² - معدلة بموجب القانون رقم 24-06 المؤرخ في 28 افريل 2024 جريدة رسمية عدد 30.

³ - هذه الإجراءات إدارية وقائية لوقف الجريمة والتي تليها فتح تحقيقات ومتابعات جزائية عن تلك الأفعال بعد اخطار الجهات المحققة أو الجهات القضائية المختصة.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

ثالثا: الجرائم ذات الصلة بمواد اباحية عن الأطفال

هي تلك الأفعال المتمثلة في القيام بتوزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة لمواد اباحية متعلقة بالقصر المنصوص عليها في المادة 333 مكرر 1 من قانون العقوبات والتي أصبح في وقتنا الحاضر الانترنت والهواتف الذكية ومواقع التواصل الاجتماعي أهم وسيلة ترتكب بها تلك الجرائم وهذا يحولها الى جريمة الكترونية، وبذلك لم تعد جريمة أخلاقية تقليدية بل جريمة بمستويات متعددة لما لها من عواقب اجتماعية ونفسية ومستقبلية على الضحايا.

المطلب الثاني: السياسة العقابية المستحدثة

سيتم التطرق للمسؤولية الجزائية عن الجريمة الإلكترونية في التشريع الجزائري، حيث يركز الفرع الأول على دراسة المسؤولية الجزائية للشخص الطبيعي، بينما يعالج الفرع الثاني المسؤولية الجزائية للشخص المعنوي.

الفرع الأول: المسؤولية الجزائية للشخص الطبيعي

نص المشرع الجزائري على مجموعة من العقوبات الأصلية والتكميلية المقررة للشخص الطبيعي، وتشمل ما يلي:

أولاً: العقوبات الأصلية

إن العقوبات الأصلية المطبقة على الشخص الطبيعي في الجريمة الإلكترونية متعددة بتعدد تلك الجرائم¹، وقد أقرها المشرع على الأفعال المجرمة في قانون العقوبات والاحكام الجزائية في القوانين الخاصة، وهي كالتالي:

1- العقوبات المقررة لجريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي

¹ - د. عباس كريمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مجلة البيان للدراسات القانونية والسياسية، العدد الرابع، جامعة برج بوعرييج، الجزائر 2017، ص 129.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

تعتبر هذه الجريمة من أبرز الجرائم الإلكترونية وأخطرها على المؤسسات والأفراد، لأنها تشكل انتهاكاً مباشراً للحقوق والحريات. ويختلف الفقه في طبيعة هذه الجريمة، فمنهم من يعتبرها جريمة واحدة تؤدي إلى نفس النتيجة، ومنهم من يفرق بين جريمتين:

الدخول إلى النظام المعلوماتي: يقصد به تحقيق فعل الدخول إلى النظام، ويشمل كل الأفعال التي تمكن من الوصول إلى النظام المعلوماتي والسيطرة على بياناته أو المعلومات التي يحتويها. كما يشمل الدخول إلى محتويات جهاز الكمبيوتر أو إجراء أي اتصال بالنظام المحمي دون ترخيص أو وجه حق¹.

البقاء غير المشروع داخل النظام المعلوماتي: تُعد من الجرائم المستمرة، حيث تبقى قائمة طالما أن الجاني متصل بالنظام بطريقة غير قانونية ودون ترخيص. ويقصد بالبقاء التواجد داخل نظام المعالجة الآلية للبيانات ضد إرادة من له الحق في السيطرة على النظام والتصرف فيه.

غالباً ما تقتزن الجريمتان معاً، وهو ما دفع أغلب التشريعات وجزء من الفقه المقارن إلى جمع الصورتين في جريمة واحدة تحت مسمى "الدخول والبقاء غير المشروع في النظام المعلوماتي". وقد نص المشرع في المادة 394 مكرر على عقوبتين أصليتين لهذه الجريمة.

أ. العقوبة في صورتها البسيطة:

الحبس من 6 أشهر إلى سنتين وبغرامة مالية من 60.000 دج إلى 200.000 دج،

ب. العقوبة في صورتها المشددة:

تضاعف العقوبة إذا نتج عن الفعل حذف أو تعديل المعطيات في المنظومة،

¹ - دمان ذبيح وعماد بهلول سمية الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، 2020، ص 146

الفصل الأول: الإطار المفاهيمي والتجريم للجرائم الإلكترونية في التشريع الجزائري

وإذا ترتب عن الفعل تخريب نظام تشغيل المنظومة، فتكون العقوبة الحبس من سنة إلى 3 سنوات، والغرامة من 100.000 دج إلى 300.000 دج.

2- العقوبات المقررة لجريمة الاعتداء العمدي على المعطيات

يقصد بالاعتداء على المعطيات أي تجاوز يهدف للإضرار بمعلومات الكمبيوتر أو وظائفه، سواء بالمساس بسريتها، أو سلامة محتواها، أو تعطيل قدرة وكفاءة النظام على أداء وظائفه. ويتحقق هذا الاعتداء عادة بعد مرحلة الدخول أو البقاء غير المشروع في النظام، ويأخذ صورتين: الاعتداء على المعطيات الداخلية والاعتداء على المعطيات الخارجية للنظام. تنص المادة 394 مكرر 1 من قانون العقوبات على ما يلي:

"يعاقب بالحبس من سنة إلى 3 سنوات، وبغرامة مالية من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."

وعقوبة الاعتداء العمدي على المعطيات مشددة على عقوبة الدخول أو البقاء غير المشروع، سواء في صورته البسيطة، لأن هذه الأخيرة قد لا تؤدي إلى أضرار ملموسة، أما العقوبة مشددة فلأنها أكبر لأنها أكثر خطرا وضرا منها.

الفصل الأول: الإطار المفاهيمي والتجريم للجرائم الإلكترونية في التشريع الجزائري

ثانياً: العقوبات التكميلية

يرى المشرع أن العقوبة الأصلية قد لا تكون كافية لردع الجاني أو حماية المصلحة، لذا أضاف عقوبات تكميلية وفق المادة 09 المعدلة بالقانون 06/23، وهي مرتبطة بالعقوبة الأصلية، وتطبق بالنطق بها فقط، وتشمل:¹

1- المصادرة:

هي عقوبة تكميلية يحكم بها الى جانب العقوبات الاصلية ففي الجنايات تأمر المحكمة بمصادرة الأشياء التي استعملت او كانت ستستعمل في تنفيذ الجريمة او التي حصلت منها، أما بالنسبة للجنح يؤمر بها وجوباً اذا كان القانون ينص صراحة عليها مع مراعاة حقوق الغير حسن النية، وهذا طبقاً للقواعد العامة المادة 15 مكرر 1 من قانون العقوبات، مع الإشارة الى انه يمكن الأمر بها كتدبير أمن طبقاً لنص المادة 16 من قانون العقوبات.

هذه القواعد تتصرف كذلك على المصادرة في الجرائم الالكترونية فنص عليها قانون العقوبات في جرائم المساس بأنظمة المعالجة الآلية للمعطيات في نص المادة 394 مكرر 6 فيحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة.

2- الغلق

يشمل إغلاق المواقع أو الأماكن التي ارتكبت فيها الجريمة، بما في ذلك المحل أو مكان الاستغلال إذا ارتكبت الجريمة بعلم المالك². ولم تحدد المادة مدة الغلق، فيتم تطبيق القواعد العامة لقانون العقوبات وفق لنص المادة 16 مكرر 1 منه:

¹ -رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه جامعة ابو بكر بلقايد، تلمسان، 2017-2018، ص 246.

² - رابحي عزيزة، المرجع السابق، ص 246.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

في الجنايات: تصل حتى 10 سنوات.

في الجنح: تصل حتى 5 سنوات.

الفرع الثاني: المسؤولية الجزائية للشخص المعنوي

نص قانون العقوبات الجزائري على المسؤولية الجزائية للأشخاص المعنوية في الجرائم المتعلقة بالمساس بالأنظمة الآلية للمعطيات في نص المادة 394 مكرر 4 منه وقررت العقوبات في بموجب نص المادتين 18 مكرر و18 مكرر 1 من نفس القانون والتي تتمثل فيما يلي:

1- الغرامة التي تعادل مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

2- واحدة أو أكثر من العقوبات التكميلية الآتية:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.
- المنع من مزاولة نشاط أو أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائياً أو لمدة لا تتجاوز خمس سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر وتعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات، وتتصب الحراسة على ممارسة النشاط الذي أدى إلى جريمة أو الذي ارتكبت الجريمة بمناسبته.

الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري

ويشترط ليكون الشخص المعنوي مسؤولاً جزائياً طبقاً لنص المادة 51 مكرر من قانون العقوبات أن ترتكب الجريمة لحسابه من طرف أجهزته أو ممثليه القانونيين أو الحائزين على تفويض سلطات عندما ينص القانون على ذلك.

وتجدر الإشارة في هذا السياق أن هذه المسؤولية الجزائية ليست مقتصرة على جرائم الاعتداء على نظم المعالجة الآلية فحسب، بل تشمل كل الجرائم التي يرتكبها الشخص المعنوي، بينما فيما يتعلق بالجرائم ضد الأنظمة المعلوماتية المحددة في المواد 394 مكرر وما بعدها، فإن الغرامة المقررة على الشخص المعنوي تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وذلك تطبيقاً للمادة 394 مكرر 4 من قانون العقوبات الجزائري.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

نظرا لخصائص الجرائم الإلكترونية المستحدثة، من حيث حدوثها خفية وسرعة إزالة آثارها ونطاق ارتكابها، نتج عن ذلك ظهور قصور بيّن في القواعد الموضوعية والإجرائية التقليدية التي وُضعت أساسًا للتعامل مع الجرائم المادية. وبناء على ذلك، تدخل المشرع الجزائري إضافة الى القواعد الموضوعية المتعلقة بالتجريم والعقاب، امتد ليشمل وضع قواعد إجرائية تعيد ضبط التفتيش والمراقبة والحجز والتحري بما يتكيف مع خصوصيات البيئة الرقمية. ويهدف هذا الفصل إلى إبراز المقاربة الإجرائية المستحدثة التي اعتمدها المشرع في ظل التعديلات الأخيرة، والتي تقوم على محورين رئيسيين، أولها وضع آليات مؤسسية متخصصة تتمتع بالكفاءة والتي سيتم التطرق إليها في المبحث الأول، وثانيها اعتماد أساليب تحري وتحقيق رقمية مستحدثة لتحقيق التوازن بين جمع الأدلة الرقمية وحماية الحقوق والحريات داخل الفضاء الرقمي في المبحث الثاني.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

المبحث الأول: الهيئات الوطنية المتخصصة في مكافحة الجرائم الإلكترونية

تقتضي مكافحة الجرائم الإلكترونية إنشاء جهات قضائية متخصصة وفي نفس الوقت مصالح للتحري والتحقيق متخصصة تتجاوز إمكانيات أجهزة الضبطية القضائية التقليدية، وهو ما دفع بالمشروع إلى استحداث قطب جزائي وطني متخصص ومصالح متخصصة للشرطة القضائية.

وعليه، يتناول هذا المبحث الدور الأساسي الذي يختص به القطب الجزائي الوطني في بسط الاختصاص القضائي على الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال في المطلب الأول، إلى جانب عرض الوظائف الوقائية والعملياتية للمصالح الإدارية والأمنية المستحدثة للتصدي لهذا النوع من الاجرام في المطلب الثاني.

المطلب الأول: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

استجابةً لمتطلبات الواقع العملي، وإدراكاً من المشرع لعدم كفاية توسيع الاختصاص المحلي لبعض الجهات القضائية أو الاكتفاء بإنشاء أجهزة إدارية، مثل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹، لمواجهة الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات، تم تخصيص هذا المطلب لبيان الإطار القانوني المنظم للقطب الجزائي الوطني. وذلك من خلال التعريف به وبيان أساسه القانوني في الفرع الأول، ثم عرض اختصاصاته في الفرع الثاني.

¹ - استحدثت لأول مرة بموجب المرسوم الرئاسي رقم 15-261 لسنة 2015، وتم إعادة تنظيمها بالمرسوم الرئاسي

19-172 لسنة 2019، الملغى بموجب المرسوم الرئاسي رقم 20-183 والملغى من جديد بالمرسوم الرئاسي رقم

21-439 المتمم بالمرسوم الرئاسي رقم 24-381 والذي أعاد تنظيمها من جديد.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

الفرع الأول: تعريف القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وأساسه التشريعي

نظرًا لما تتطوي عليه الجرائم الإلكترونية من اعتداءات خطيرة على الخصوصية الرقمية، واتساع مجال ارتكابها في رقعة جغرافية غير محدودة وفي إطار تدعيم الحماية الإجرائية تدخل المشرع من خلال تعديل قانون الإجراءات الجزائية، واستحدث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب الأمر رقم 21-11 المعدل للأمر 66-155 المتضمن قانون الإجراءات الجزائية، وخصص له بابًا كاملاً، ومنحه اختصاصًا وطنيًا¹.

وبذلك تم تعزيز السلطة القضائية بإنشاء هذا القطب القضائي المتخصص بموجب تعديل قانون الإجراءات الجزائية لسنة 2021. وتم الحفاظ على هذا المكسب القضائي في قانون الإجراءات الجزائية الجديد رقم 25-14 وتم النص عليه في المادة 335 منه.

وتعرف الأقطاب الجزائية بوجه عام بأنها جهات قضائية متخصصة تختص بالنظر في فئة معينة من الجرائم المحددة قانونًا، دون أن تكون جهات قضائية استثنائية، إذ لا تعمل بإجراءات مغايرة للنظام القضائي العام، بل تخضع لنفس القواعد الإجرائية المعمول بها أمام الجهات القضائية العادية. كما أنها تعتبر محاكم ذات اختصاص إقليمي موسع، تمارس اختصاصها العادي إلى جانب اختصاص إضافي منح لها في جرائم محددة على سبيل الحصر². ومن هذا المنطلق، يظهر القطب الجزائي كآلية لتعزيز فعالية الأداء القضائي ورفع جاهزية العدالة لمواجهة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال³.

¹ - الأمر 21 - 11 المؤرخ في 25 أوت 2021، المعدل والمتمم للأمر 66 - 155 المتضمن قانون الإجراءات الجزائية، الصادر في الجريدة الرسمية عدد 65 الصادرة في 26 أوت 2021.

² - عميور خديجة، قواعد اختصاص الأقطاب الجزائية للنظر في جرائم الفساد، مجلة دراسات في الوظيفة العامة، العدد الثاني، ديسمبر سنة 2014، ص 133.

³ - بن عميور أمينة، بوحلايس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 07 العدد 01 2022، ص 72.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

ويوجد هذا القطب في دائرة اختصاص مجلس قضاء الجزائر، متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وهي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية والجرائم المرتبطة بها¹، والحكم فيها إذا كانت هذه الجرائم تشكل جناحاً.

ويمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وقاضي التحقيق ورئيس ذات القطب، صلاحياتهم في كامل الإقليم الوطني، ويختصون حصرياً في الجرائم الالكترونية الأكثر خطورة وتعقيداً².

الفرع الثاني: الاختصاصات النوعية للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

ولفهم دور القطب الجزائي نحدد نطاق اختصاصاته والمهام المسندة إليه وهذا طبقاً لقانون الإجراءات الجزائية رقم 14-25 على النحو التالي:

أولاً: الاختصاص النوعي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

حددت المادة 337 من قانون الإجراءات الجزائية، اختصاص هذا القطب في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والجرائم المرتبة بها والحكم فيها كذلك إذا كانت تشكل جناحاً، ويختص كذلك حصرياً طبقاً لنص المادة 337 من قانون

¹ - ورد هذا التعريف في نص المادة 2 من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، وأضافت الى هذا التعريف الفقرة 3 من نص المادة 335 من ق إ ج: أو أي وسيلة أخرى أو البية ذات صلة بتكنولوجيات الاعلام والاتصال.

² - أنظر المادة 336 من ق إ ج مع الإشارة ان الجرائم الالكترونية المعقدة حددت في نص المادة 337 من ق إ ج على سبيل الحصر.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

الإجراءات الجزائية بالنظر في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، وكذا الجرائم المرتبطة وتشمل هذه الجرائم¹:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها الإخلال بالأمن العام أو السكينة العامة أو استقرار المجتمع.
- جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين، سواء كانت ذات طابع منظم أو عابر للحدود الوطنية.
- الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات الخاصة بالإدارات والمؤسسات العمومية.
- جرائم الاتجار بالبشر أو العابر للحدود الوطنية.
- جرائم التمييز وخطاب الكراهية.

كما وسع المشرع نطاق اختصاص القطب ليشمل الجرائم الأكثر تعقيداً أو المرتبطة بهذه الجرائم، خاصة في حالات تعدد الفاعلين أو الشركاء، أو تعدد الضحايا، أو امتداد الجريمة على نطاق جغرافي واسع، أو اتسامها بطابع منظم عابر للحدود، أو مساسها بالنظام والأمن العموميين، أو استلزامها التعاون القضائي الدولي²، ويختص في هذه الحالة كذلك حصرياً طبقاً لنص المادة 338 الفقرة 1 من قانون الإجراءات الجزائية.

¹ - هي نفس الجرائم التي تضمنها نص المادة 211 مكرر 24 من قانون الإجراءات الجزائية القديم.

² - سلمى عبد النبي، دور القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في مواجهة الاعتداءات الواقعة على المعطيات المعلوماتية مجلة الحقوق والعلوم السياسية، المجلد 11، العدد 02، سنة 2024، ص 23.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

ثانيا: الاختصاص المشترك

طبقا لنص المادة 340 من قانون الإجراءات الجزائية، يتضح أن القطب الجزائي له اختصاصا مشتركا الناتج عن تطبيق المواد 58 و 70 و 468 بالنسبة للجرائم المتصلة بتكنولوجيات الاعلام والاتصال والجرائم المرتبطة بها، وذلك عندما يتعلق الأمر ببعض الجرائم المحددة كالتالي:

- الجرائم المنصوص عليها في المواد 119 مكررة 389 مكرر و 389 مكرر 1 و 389 مكرر 2 و 389 مكرر 3 من قانون العقوبات،
- في الجرائم المتعلقة بالفساد القانون رقم 06-01،
- الجرائم المنصوص عليها في الامر رقم 96-22 المعدل والمتمم والمتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج،
- الجرائم المنصوص عليها في المواد 11 و 12 و 13 و 14 و 15 من الامر رقم 05-06 والمتعلق بمكافحة التهريب،
- الجرائم المتعلقة بالنقد والقرض،
- الجرائم المتعلقة ببورصة القيم المنقولة،
- جرائم التهريب والغش الضريبيين.

وفي هذه الحالة يرسل وكلاء الجمهورية لدى الجهات القضائية المختصة إقليميا وفقا لنص المادة 58 من قانون الإجراءات الجزائية فورا وبكل الطرق نسخا من التقارير الإخبارية الواردة إليهم من ضباط الشرطة القضائية الذين يقومون بالتحريات وكذلك إجراءات التحقيق المنجزة من طرفهم الى وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، كما يمكنه التدخل تلقائيا في القضايا التي تدخل في اختصاصه ما لم يخطر قاضي التحقيق.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

ويختص وكيل الجمهورية على مستوى هذا القطب بالقضية بالمطالبة بها سواء كانت على مستوى التحريات أو التحقيق القضائي بعد أخذ رأي النائب العام على مستوى مجلس قضاء الجزائر، ويصدر مقررًا بالتخلي لصالحه، أما إذا أخطر قاضي التحقيق فيصدر هذا الأخير أمرًا بالتخلي عن الملف لصالح قاضي التحقيق على مستوى القطب المتخصص.

كما أن وكيل الجمهورية وقاضي التحقيق على مستوى هذا القطب يختصان بالمتابعة والتحقيق في جميع الجرائم الداخلة ضمن اختصاصه، بينما يقتصر اختصاص قاضي الحكم على الجرائم ذات الوصف الجنحي، وفقًا لما نصت عليه المادة 335 من قانون الإجراءات الجزائية، أما الجرائم الموصوفة بالجنايات فتظل من اختصاص محكمة الجنايات الابتدائية طبقًا للمادة 385 من قانون الإجراءات الجزائية.

ثالثًا: مسألة تزامن الاختصاص

عالج المشرع مسألة تداخل الاختصاصات في هذا المجال، وميز بين حالتين:

حالة تزامن الاختصاص مع القطب الجزائي الوطني الاقتصادي والمالي، حيث يؤول الاختصاص لهذا الأخير وفقًا لنص المادة 341 من قانون الإجراءات الجزائية.

وفي حالة تزامن الاختصاص مع القطب الجزائي الوطني لمكافحة الإرهاب والجريمة المنظمة عبر الوطنية، حيث ينعقد الاختصاص لهذا الأخير وجوبًا طبقًا لنص المادة 342 من قانون الإجراءات الجزائية.

وفي هذا السياق، فإن تخلي القطب الجزائي عن الاختصاص لفائدة هذه الجهات يعد أمرًا منطقيًا، باعتبار أن الوسائل التكنولوجية في هذه الحالات تشكل مجرد وسيلة لارتكاب الجريمة، بينما يبقى الفعل الإجرامي الأصلي من اختصاص الجهات القضائية الأخرى المختصة¹.

¹ - سلمى عبد النبي، المرجع السابق، ص 23، 24.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

رابعاً: الاختصاص الإقليمي

طبقاً لنص المادة 336 من قانون الإجراءات الجزائية، منح المشرع القطب الجزائي الوطني اختصاصاً يمتد إلى كامل الإقليم الوطني، حيث يمارس كل من وكيل الجمهورية وقاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني.

وذلك يعكس إدراك المشرع بخطورة الجرائم الإلكترونية واتساع نطاقها الجغرافي، سواء من حيث تعدد أماكن ارتكابها أو تعدد المساهمين فيها، أو المتضررين بها أو لطابعها المنظم والعابر للحدود يتطلب تدخلاً قضائياً نوعياً متركزاً في جهة واحدة عليا لمواجهتها.

المطلب الثاني: الهيئات الإدارية والأمنية المكلفة بمكافحة الجرائم الإلكترونية

قامت معظم الدول باستحداث أجهزة متخصصة لمكافحة هذا النوع من الأجرام المستحدث، وتختلف هذه الأجهزة عن الأجهزة المختصة بضبط الجرائم التقليدية من حيث طريقة التكوين، فهي تعتمد على البناء العلمي والتقني لأفرادها¹.

الفرع الأول: الهيئات الإدارية المكلفة بالوقاية والتحقيق في الجرائم الإلكترونية

أولاً: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

استحدثت المشرع الجزائري هذه الهيئة بموجب قانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، كما نظم عملها في البداية المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015².

¹ -صهيب سهيل غازي زامل، البحث والتحري عن الدليل الإلكتروني في المسائل الجزائية، أطروحة دكتوراه، جامعة وهران 2، 2022، ص 60.

² - طبقاً لنص المادة 13 من القانون رقم 09-04 تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب المرسوم الرئاسي رقم 15-261 لسنة 2015، وتم إعادة تنظيمها بالمرسوم الرئاسي 19-172 لسنة 2019، الملغى بموجب المرسوم الرئاسي رقم 20-183 والملغى من جديد بالمرسوم الرئاسي رقم

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

وتقوم هذه الهيئة بتقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال عن طريق جمع المعلومات والتزود بها وانجاز الخبرات القضائية، وتسهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي مع نظيراتها في الخارج في هذا الشأن، وفقا لأحكام المادتين 17 و18 من نفس القانون المشار اليه أعلاه.

ثانيا: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

دون إغفال أن قانون الإجراءات الجزائية يتطور بالتوازي مع العالم الرقمي ويتم اللجوء الى أدوات إجرائية جديدة كالتسرب الالكتروني أو اعتراض البيانات عن بعد ومن الضروري كذلك تطوير سياسات تهدف الى توقع المخاطر الرقمية¹ ومكافحتها، استحدثت المشرع بموجب نص المادة 22 من القانون رقم 18-07 المؤرخ في 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المعدل والمتمم²، هي سلطة إدارية مستقلة تهدف الى حماية المعطيات ذات الطابع الشخصي في اطار السهر على مطابقة معالجة المعطيات الشخصية لهذا القانون، وضمان عدم انطواء استعمال تكنولوجيات الاعلام والاتصال على أي اخطار تمس بحقوق الأشخاص والحريات العامة والحياة الخاصة.

439-21 المتمم بالمرسوم الرئاسي رقم 24-381 والذي أعاد تنظيمها من جديد ووضعت لدى رئيس الجمهورية وتمارس مهامها تحت رقابة السلطة القضائية وطبقا لأحكام قانون الإجراءات الجزائية.

1-Myriam Quémener, op. cit. , P86.

². صدر في الجريدة الرسمية عدد 34 المؤرخة في 10 يونيو 2018، والمعدل والمتمم بموجب القانون رقم 25-11 المؤرخ في 24 يوليو 2018 والصادر في الجريدة الرسمية عدد 48 المؤرخة في 24 يوليو سنة 2025.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

الفرع الثاني: الهيئات الأمنية المكلفة بالوقاية والتحقيق في الجرائم الإلكترونية

سعت كل من المديرية العامة للأمن الوطني وجهاز الدرك الوطني إلى إنشاء فرق متخصصة لمكافحة الجرائم المعلوماتية، وتكوين عناصر متخصصة في هذا المجال على المستويين الداخلي والخارجي، إضافة إلى توفير مخبرين علميين للشرطة العلمية والتقنية يمتلكون أحدث الأجهزة ذات التكنولوجيا المتطورة لكشف هذا النوع من الجرائم¹.

أولاً: المصالح التابعة للأمن الوطني

تعمل المديرية العامة للأمن الوطني على تحديد سياسة أمنية فعالة، مستثمرة كل الإمكانيات البشرية والتقنية المتاحة للتصدي لكل أنواع الجرائم، لا سيما الجرائم الإلكترونية، بهدف حماية المصالح العامة والخاصة المرتبطة باستخدام تكنولوجيات الاعلام والاتصال، وعليه تم انشاء مصالح وهيئات مركزية لمكافحة هذا النوع من الاجرام وكذلك فرق متخصصة لمكافحة الجرائم السيبرانية تابعة للمصالح الولائية للشرطة القضائية على مستوى أمن الولايات.

1- المصلحة المركزية لمكافحة الجريمة السيبرانية SCLC:

لضرورة الامن المعلوماتي قامت المديرية العامة للأمن الوطني سنة 2011 بإنشاء خلية لمحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني، ليتم بعدها انشاء المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال بمديرية الشرطة القضائية بالمديرية العامة للأمن الوطني سنة 2015، والتي تتمثل مهامها في

¹ -محمد السعيد زناتي الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات العدد الثاني، ديسمبر 2017 المركز الجامعي إليزي الجزائر، ص 34.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

مساعدة مصالح الشرطة القضائية في مجال التحريات التقنية والتعاون والمشاركة في التحقيقات ذات البعد الوطني والدولي في مجال مكافحة الجرائم الإلكترونية¹.

وفي سبيل تدعيم مصالح الولايات للشرطة القضائية، قامت المديرية العامة للأمن الوطني سنة 2010 بإنشاء نحو 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط والشرق والغرب والجنوب، لتتم لاحقاً تغطية جميع مصالح الأمن عبر الولايات المختلفة².

2-مخبر الشرطة العلمية:

وتوجد على مستوى جهاز الأمن الوطني ثلاث مخابر مكلفة بالبحث عن الأدلة في الجرائم المعلوماتية، وهي:

●المخبر المركزي للشرطة العلمية بالجزائر العاصمة.

●المخبر الجهوي للشرطة العلمية بوهران.

●المخبر الجهوي للشرطة العلمية بقسنطينة.

ولتدعيم وتسهيل عمل المحققين في التحريات والحصول على الأدلة الرقمية على المستوى المحلي وسرعة انجاز الخبرات التقنية يوجد مشروع لإنشاء 3 مخابر أخرى جهوية بورقلة، وبشار، وتمنراست.

وفي إطار التحقيق في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وجمع الأدلة الإلكترونية، أنشأت دائرة تقنية على مستوى تلك المخابر متخصصة في استغلال الأدلة الرقمية وتحليلها واعداد الخبرات بشأنها.

¹- سميحة بلقاسم، حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر.. واقعها وآليات مجابقتها، مجلة العلوم الإنسانية، المجلد 10 العدد 1، جامعة ام البواقي، 2023، ص 548.

² -سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد 30، عدد 3، ديسمبر 2019، ص 53.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

ثانيا: المصالح التابعة للدرك الوطني

يكافح الدرك الوطني في مجال الشرطة القضائية الاجرام والجريمة المنظمة ويستعمل في هذا الإطار وسائل تحريات الشرطة العلمية والتقنية وخبرة الأدلة الجنائية، ويتضمن لتنفيذ مهامه هياكل علمية وتقنية¹.

1- مصلحة الوقاية من جرائم الاعلام الالي للدرك الوطني CPLCIC:

هي هيئة أمنية متخصصة تابعة للدرك الوطني المعروفة بمركز مكافحة الجرائم الالكترونية أنشأت سنة 2008 تتولى معالجة قضايا الجرائم المعلوماتية والسيبرانية، وتهدف الى تأمين منظومة المعلومات لخدمة الامن العمومي، وتعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا افراد أو منظمات أو دول، والوقاية ومكافحة الجريمة السيبرانية².

2- المصلحة المركزية العملياتية لمكافحة الجريمة المنظمة تابعة للدرك الوطني:

أنشأت هذه المصلحة بموجب المرسوم الرئاسي رقم 24-231 المؤرخ في 8 يوليو سنة 2024³، وضعت تحت السلطة المباشرة لقائد الدرك الوطني يمتد اختصاصها الى كامل التراب الوطني وتمارس صلاحياتها وفقا لقانون الإجراءات الجزائية والتي يمكنها التحقيق في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المعقدة وذات الامتداد الجغرافي الوطني.

¹ - المادتين 8 و 13 من المرسوم الرئاسي رقم 23-313 المعدل والمتمم مؤرخ في 3 سبتمبر سنة 2023 والمتضمن مهام الدرك الوطني وتنظيمه، جريدة رسمية عدد 59 مؤرخة في 10 سبتمبر سنة 2023.

² - د. ادريس عطية، مكانة الامن السيبراني في منظومة الامن الوطني الجزائري، مجلة مصداقية المدرسة العليا العسكرية للإعلام والاتصال، المجلد 1، العدد 1، 2019، ص 112-113.

³ - صدر في الجريدة الرسمية عدد 48 المؤرخة في 14 يوليو سنة 2024.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

3- المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني:

أنشأ المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني بموجب المرسوم الرئاسي رقم 04-183 المعدل والمتمم المؤرخ في 26 يونيو سنة 2004¹، وهو مؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية والاستقلال المالي مقره بالجزائر موضوع تحت وصاية وزير الدفاع الوطني ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه، من مهامه القيام بإجراء الخبرات والفحوص العلمية بناء على طلب من القضاة والمحققين والسلطات المؤهلة وهذا في إطار التحريات الأولية والتحقيقات القضائية، بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنگ.

ويضم ضمنه دائرة متخصصة في الاعلام الالي، تقوم بإنجاز الخبرات المرتبطة بالتكنولوجيات الحديثة في مجال الاتصالات والرقميات فيقوم خبراءها بالولوج واستخراج ومعالجة المحتوى الرقمي المخزن على مختلف أنواع الدعامات الالكترونية.

وتتمثل الوظيفة الأساسية لهذه المصالح في خدمة العدالة ودعم وحدات التحري في مهام الشرطة القضائية، خصوصاً في مجال مكافحة جميع أنواع الجرائم بما فيها الجريمة المعلوماتية حيث يختص قسم الاعلام الالي والإلكترونيك بالتحقيق في الجرائم المعلوماتية².

المبحث الثاني: آليات التحري والتحقيق الرقمي المستحدثة

الدليل الرقمي بطبيعته لا مادي Intangible وقابل للتغيير والتلف بسهولة، مما استدعى اعتماد أساليب تحري خاصة تدعيماً للإجراءات التقليدية المعروفة، كالتفتيش عن بعد، والمراقبة الإلكترونية، واعتراض المراسلات. والتي أصبحت تتعدى كونها إجراءات تقنية بحتة بل إجراءات قانونية مستحدثة تهدف الى وضع آليات تقنية للتبليغ عن الجرائم الالكترونية واتخاذ

¹ - صدر في الجريدة الرسمية عدد 41 مؤرخة في 27 يونيو 2004 وعدل بموجب المرسوم الرئاسي رقم 09-118

المؤرخ في 14 افريل 2009 جريدة رسمية رقم 24 مؤرخة في 22 أفريل 2009.

² - سعيدة بوزنون، المرجع السابق، ص 53 - 54.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

الإجراءات التحفظية في الوقت الحقيقي. ويتناول هذا المبحث تحليل الأساليب الخاصة للتحري والتحقيق التي كرسها قانون الإجراءات الجزائية الجديد والقوانين الإجرائية الخاصة في المطلب الأول، مع إبراز الإجراءات المعتمدة في جمع الأدلة الرقمية وضمان سلامتها بما يكفل حجيتها أمام القضاء، مع بيان الضمانات القانونية الكفيلة بمنع إساءة استعمالها في المطلب الثاني.

المطلب الأول: الأساليب الخاصة للتحري والتحقيق

نظرًا للتطور الكبير الذي شهده العالم في مجال التكنولوجيا الرقمية، وما ترتب عنه من آثار سلبية خطيرة تمس بالنظام العام، برز نوع جديد من الجرائم بات يهدد استقرار المجتمعات. وهو ما دفع المشرع الجزائري إلى تبني أساليب مستحدثة للبحث والتحري عن الجريمة، من خلال تعديل قانون الإجراءات الجزائية بموجب القانون رقم 22/06 المؤرخ في 2006/07/20، وذلك باعتماد ما يُعرف بأساليب البحث والتحري الخاصة.

الفرع الأول: اعتراض المراسلات الإلكترونية ومراقبة الاتصالات

أن التطور المتسارع في وسائل الاتصال الإلكترونية أفرز أنماطًا جديدة من الجرائم التي يصعب كشفها بالوسائل التقليدية، الأمر الذي استدعى تدخل المشرع لاعتماد تقنيات حديثة في مجال البحث والتحري. ومن بين أبرز هذه الوسائل اعتراض المراسلات الإلكترونية ومراقبة الاتصالات، باعتبارهما من الإجراءات الخاصة التي تهدف إلى تتبع النشاط الإجرامي في بيئته الرقمية، مع ما يثيرانه من إشكالات تتعلق بالتوازن بين فعالية التحري وحماية الحقوق والحريات الفردية.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

أولاً: اعتراض المراسلات

يُعد اعتراض المراسلات من أساليب التحري الخاصة المستحدثة في مجال التحري والتحقيق، ويُقصد به تتبع المراسلات الخاصة بالمشتبهِ فيهم والمتهمين بشكل خفي دون علمهم، باعتباره إجراءً تحري يتم بسرية، وبما أنه قد يترتب عنه المساس بالحياة الخاصة للأشخاص وسرية محادثاتهم. فاضع هذا الإجراء الى وجوب الحصول على إذن مسبق ومكتوب من الجهة القضائية المختصة ووفق الاجراءات المحددة قانوناً، بهدف الحصول على دليل رقمي يُستعمل في اثبات الجريمة الالكترونية.

ووفقاً لنص المادة 114 من قانون الإجراءات الجزائية، فإن اعتراض المراسلات في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال لا يقتصر على المكالمات الهاتفية فقط، بل يشمل مختلف أنواع الاتصالات السلكية واللاسلكية¹. أما بخصوص وسيلة الاعتراض، فإن المشرع لم يُحدد أداة معينة، فيتم بوضع ترتيبات تقنية ويجوز تسخير أي عون مؤهل للقيام بذلك.

ثانياً: مراقبة الاتصالات الإلكترونية

لم يعرف المشرع الجزائري شأنه شأن العديد من التشريعات المقارنة إجراء مراقبة الاتصالات الإلكترونية، وإنما اكتفى بالنص عليه في المادة 3 من القانون رقم 09-04 حيث جاء فيها: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو ضرورات التحريات أو التحقيقات القضائية الجارية، ووفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية وهذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وتجميع وتسجيل محتواها في حينها، والقيام بعمليات التفتيش والحجز داخل منظومة معلوماتية".

¹ - سبق ادراج هذا الاجراء في نص المادة 65 مكرر 5 من قانون الاجراءات الجزائية القديم الأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون الإجراءات الجزائية بموجب القانون رقم 06-22، ج ر، عدد 84 المعدل والمتمم.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

وتحديد الحالات التي تسمح باللجوء اليه في نص المادة 4 من نفس القانون¹، وبذلك، فإن مراقبة الاتصالات الإلكترونية تُعد إجراءً استثنائيًا لا يُلجأ إليه إلا في الحالات المحددة على سبيل الحصر.

وتقرر التشريعات المعاصرة أن ضابط فائدة المراقبة في ظهور الحقيقة يعتبر السند الشرعي المبرر للاعتراض، فيباح استثناء وفي حدود ضيقة².

الفرع الثاني: أسلوب التسرب

أولاً: أسلوب التسرب في قانون الإجراءات الجزائية

تطرق المشرع الجزائري إلى تعريف أسلوب التسرب من خلال نص المادة 121 من قانون الإجراءات الجزائية حيث نصت على ما يلي:

يقصد بالتسرب قيام ضابط أو عون شرطة قضائية، تحت إشراف ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة، من خلال إيهامهم بأنه فاعل معهم أو شريك لهم أو متواطئ معهم.

ويسمح لضابط أو عون الشرطة القضائية، لهذا الغرض، باستعمال هوية مستعارة، كما يمكنه عند الاقتضاء ارتكاب الأفعال المنصوص عليها في المادة 121 الفقرة 2، ولا يجوز تحت طائلة البطالان أن تشكل هذه الأفعال تحريضاً على ارتكاب الجرائم.

¹ - نصت المادة 04 من القانون رقم 09-04 على أنه يجوز لضابط الشرطة القضائية اللجوء الى هذا الاجراء لمقتضيات التحريات والتحقيقات القضائية في الجرائم الالكترونية وفي حالات محددة على سبيل الحصر (في الوقاية من جرائم الإرهاب والتخريب وجرائم أمن الدولة ، حالة توفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام وللمساعدة في التحقيقات والمعلومات القضائية في حالة ما اذا كان من الصعب الوصول الى نتيجة للأبحاث دون اللجوء للمراقبة الالكترونية ، وفي اطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة)، وبعد الحصول على إذن قضائي مكتوب من الجهة المختصة.

² - د. أشرف عبد القادر قنديل، الاثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2015، ص

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

ومن خلال هذا النص، يُستفاد أن التسرب يتمثل في قيام ضابط أو عون الشرطة القضائية بمراقبة المشتبه فيهم في ارتكاب جناية أو جنحة، من خلال التظاهر بأنه فاعل أصلي أو شريك، وذلك بهدف كشف الحقيقة.

ثانيا: أسلوب التسرب في القوانين الخاصة

كما أشار المشرع الجزائري إلى أسلوب التسرب في قانون مكافحة الفساد¹، غير أنه لم يضع له تعريفاً صريحاً، بل استعمل مصطلح "الاختراق" للإشارة إليه، باعتباره أحد إجراءات التحري.

التسرب الإلكتروني:

يمكن لضابط الشرطة القضائية بالتسرب الكترونيا الى منظومة معلوماتية او نظام للاتصالات الالكترونية لمراقبة الأشخاص المشتبه في ارتكابهم الجرائم المنصوص عليها في هذه القوانين وهذا بعد الحصول على إذن قضائي من وكيل الجمهورية أو قاضي التحقيق حسب كل حالة المادة 26 من القانون رقم 20-05 المؤرخ في 28 افريل سنة 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها .

تم النص كذلك على هذا الاجراء في المادة 16 من القانون رقم 20-15 المؤرخ في 30 ديسمبر سنة 2020 المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها، والمادة 32 من القانون رقم 23-04 المؤرخ في 7 مايو سنة 2023 المتعلق بالوقاية من الاتجار بالبشر ومكافحته.

¹ - القانون رقم 06-01 مؤرخ في 20 فيفري 2006 يتعلق بالوقاية من الفساد ومكافحته ج ر عند 14 صادر في 08 مارس 2006، المتمم بالأمر رقم 10-2005 مؤرخ في 26 اوت 2010، ج و عند 50 صادر في 1 سبتمبر 2010 معدل ومتمم بالقانون رقم 11-15 مؤرخ في 02 أوت 2011، ج ر عند 44 صادر في 10 أكتوبر 2011.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

المطلب الثاني: إجراءات ضبط الأدلة المستحدثة وحجبتها وضماناتها

أضحى التعامل مع الجريمة المعلوماتية يفرض تجاوز الأطر التقليدية لإجراءات البحث والتحري، لاسيما تلك المرتبطة بالتفتيش والحجز في نطاقه المادي الضيق، إذ لم يعد مسرح الجريمة مقتصرًا على مكان جغرافي محدد، بل امتد إلى فضاءات رقمية عابرة للحدود. ومن ثم، برزت الحاجة إلى تبني آليات إجرائية حديثة تتسم بالمرونة والسرعة والقدرة على التكيف مع الطبيعة اللامادية للدليل الرقمي، وهو ما تجسد في اعتماد أساليب التفتيش الإلكتروني العابر للحدود، إلى جانب الحجز المعلوماتي الوقائي الذي يهدف إلى تأمين الأدلة قبل تعرضها للإتلاف أو التغيير، بما يضمن الحفاظ على حجبتها القانونية وسلامتها التقنية.

الفرع الأول: إجراءات ضبط الأدلة الرقمية المستحدثة

أولاً: التفتيش الإلكتروني عن بعد

يعتبر التفتيش الإلكتروني عن بعد (Remote Search) في الفضاء الرقمي من أهم الإجراءات الحديثة التي تبناها المشرع الجزائري على خلاف ما هو متعارف عليه في التفتيش المادي التقليدي في قانون الإجراءات الجزائية الذي يتطلب التنقل إلى الأماكن للتفتيش والمعاينة والحجز، وتم النص عليه صراحة في المادة 5 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، حيث خولت لضابط الشرطة القضائية، بناءً على إذن مكتوب من السلطة القضائية المختصة، صلاحية الدخول إلى منظومة معلوماتية أو جزء منها بغرض البحث عن المعطيات المخزنة واستغلالها في التحقيق. ولم يقف النص عند هذا الحد، بل سمحت بإمكانية توسيع نطاق التفتيش ليشمل منظومات أخرى مرتبطة بها تقنياً.

وعلى خلاف مقتضيات القواعد العامة للتفتيش باعتباره من إجراءات التحقيق يبادر به عند ارتكاب الجريمة لجمع الأدلة والقرائن من غير الممكن القيام به دون وقوع الجريمة هذا هو المبدأ المتعارف عليه، لكن المشرع الجزائري خرج هذه القاعدة بحيث استبق الأحداث

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

وجعل من التفتيش كذلك مهمة وقائية من خلال عمليات المراقبة المسبقة كما نصت عليه المادة 3 من القانون رقم 09-04¹.

وتبرز الأهمية التطبيقية لهذا الإجراء بشكل خاص في مجال الحوسبة السحابية (Cloud Computing)، حيث تُخزن البيانات في خوادم قد تكون موزعة عبر عدة دول، وهو ما يثير إشكاليات قانونية دقيقة تتعلق بمبدأ السيادة الوطنية وحدود الاختصاص القضائي. وفي هذا الإطار، جاءت اتفاقية بودابست لتؤسس لنوع من التنسيق الدولي، خاصة من خلال مادتها التاسعة عشرة، التي ترمي إلى تسهيل الوصول إلى الأدلة الرقمية في إطار من التعاون واحترام القوانين الوطنية لكل دولة².

ولا يقتصر الولوج القانوني على مجرد التفتيش في صورته التقليدية، بل يتسع ليشمل تقنيات أكثر مرونة وفعالية، من بينها مراقبة الاتصالات الإلكترونية، الذي نظمته المشرع في المادة 4 من القانون رقم 09-04، والتي تسمح لضابط الشرطة القضائية بوضع الترتيبات التقنية قصد التغلغل داخل الشبكات الإجرامية المغلقة، لاسيما تلك الناشطة عبر ما يُعرف بالشبكة المظلمة (Dark Web)، بهدف جمع أدلة مباشرة حول الأنشطة غير المشروعة وتسجيلها. ويُعد هذا الأسلوب من الوسائل المتقدمة التي تتيح اختراق البيئات الإجرامية الرقمية التي يصعب الوصول إليها بالوسائل التقليدية دون اللجوء إلى هذه التقنية.

غير أن خطورة هذا الإجراء تكمن في احتمالية مساسه بالحياة الخاصة للغير، الأمر الذي دفع بالمشرع وضع قيود دقيقة لتنظيمه. فقد اشترطت المادة 4 المشار إليها اعلاه بوجوب أن تتم بإذن مكتوب من السلطة القضائية المختصة، مع قصر اللجوء إلى هذا الأسلوب على فئات معينة من الجرائم الخطيرة، متمثلة في جرائم الإرهاب والاعتداءات على أمن الدولة.

¹ - زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة - الجزائر، 2011، ص 138.

² - اتفاقية بودابست: تعتبر قفزة نوعية هائلة في مجال التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، والتي تم

التوقيع عليها ببودابست بتاريخ 2001/11/23 وهذا لمواكبة إساءة استخدام التطور التكنولوجي المتسارع في مجال

المعلوماتية لارتكاب الجرائم الإلكترونية وصادقت عليها إلى حد الآن 81 دول. لاطلاع عليها في موقع : [مجلس أوروبا](#)

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

ويعكس هذا التقييد محاولة تحقيق التوازن بين متطلبات الفعالية في مكافحة الجريمة من جهة، وضمان احترام حقوق الإنسان في البيئة الرقمية من جهة أخرى.

وعليه، فإن التفتيش الإلكتروني عن بعد، بما ينطوي عليه من إمكانيات تقنية متطورة كالتوسع الشبكي والتسرب الرقمي، يشكل أداة أساسية في مواجهة الجريمة المعلوماتية، غير أن مشروعيتها وفعاليتها تظلان مرهونتين بمدى احترام الضوابط القانونية والإجرائية التي تكفل حماية الحقوق الأساسية وتكرس مبدأ الشرعية في المجال الرقمي.

ثانياً: الحفظ الإلكتروني للمعطيات وحجزها

1- حفظ المعطيات المتعلقة بحركة السير

طبيعة الدليل الرقمي بسهولة محوه أو تعديله أو العبث به في وقت وجيز للغاية، فرضت على سلطات التحقيق إيجاد إجراءات فورية وفعالة لضمان الحفاظ عليه بحالته الأصلية، كون أن قانون الإجراءات الجزائية لم يتضمن إجراءات خاصة بحجز هذا النوع من الأدلة سواء في حالة التلبس طبقاً لنص المادة 75 أو في حالة التحقيق الابتدائي بموجب نص المادة 97 منه. فاستحدث المشرع الجزائري إجراءات خاصة وقاية أولاً بموجب نص المادة 11 من القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إذ أوجب على مزودي خدمات الاتصال الالتزام بحفظ بيانات حركة السير (Traffic Data)، لمدة لا تقل عن سنة من تاريخ التسجيل¹. ويُفهم من هذا الالتزام أنه يشكل ضماناً وقائية تحول دون ضياع الأدلة أو إتلافها، لتقديمها مستقبلاً كأدلة ووضعها تحت تصرف الجهات القضائية المختصة، خاصة في ظل إمكانية تدخل الفاعلين عن بعد لمحو آثار نشاطهم الإجرامي.

¹ - انظر: المادة 11 من القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47.

2- حجز المحتويات المجرمة

إن الأصل في البحث والتحري في الوقائع المجرمة هو الحجز المادي لجسم الجريمة، ولكن يصدم ذلك مع خصوصية الجريمة الإلكترونية بالطبيعة اللامادية للبيانات أولاً وثانياً قد يتعذر ذلك تقنياً لعدة أسباب، فعندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية لمعطيات تكون مفيدة في الكشف عن الجرائم أو مرتكبيها فليس من الضروري حجز كل المنظومة فيتم نسخها على دعامات الكترونية تكون قابلة للحجز والوضع في أحرار طبقاً لنص المادة 6 من القانون رقم 04-09.

أما إذا تعذر ذلك لأسباب تقنية فتستعمل التقنيات المناسبة لمنع الوصول إليها أو إلى نسخها وهذا طبقاً لنص المادة 7 من القانون رقم 04-09.

3- الالتزامات الخاصة بمقدمي الانترنت

ألزمت المادة 12 من القانون رقم 04-09 مقدمي خدمة الانترنت وبمجرد علمهم بوجود محتوى مخالف للقانون بالتدخل الفوري بسحب المحتوى المجرم بعد تخزينه أو حظر الدخول إليه أو حصر ذلك إذا كان السحب غير ممكناً وتتم هذه الإجراءات¹.

وتتم هذه الإجراءات التي هي في الأصل التزامات قانونية لمقدمي خدمة الانترنت فيقوم بوضع ترتيبات تقنية تسمح بذلك². وقد يعُتبر الامتناع غير المبرر عن تنفيذها فعلاً مجرماً، لما ينطوي عليه من عرقلة حسن سير التحريات القضائية لكشف الحقيقة.

¹ - انظر: المادة 12 من القانون رقم 04-09.

² - بعض الآليات التقنية المعتمدة في هذه الحالة: الموقع www.esafety.gov.au

* تصفية العناوين URL Filtering بمنع الوصول لروابط محددة تحتوي على المحتوى المجرم.

* حجب بروتوكول الانترنت IP Blocking بمنع الوصول للخوادم المستضيفة لهذا المحتوى.

* البصمة الرقمية Hashing باستخدام خوارزميات للتعرف على المحتوى المجرم ومنع إعادة رفعها مرة أخرى

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

الفرع الثاني: حجية الدليل الرقمي وحماية الحقوق والحريات

أضحت مسألة التوفيق بين فعالية الدليل الرقمي، المستمد من تقنيات التحري الحديثة، وبين ضرورة حماية الحقوق والحريات الأساسية، من أبرز الإشكالات التي تصدى لها المشرع في إطار القانون رقم 25-14. فالتطور التكنولوجي المتسارع لم يفرز فقط أنماطاً جديدة من الجرائم، بل أوجد كذلك وسائل متقدمة لاكتشافها وإثباتها، الأمر الذي فرض على التشريع مواكبة هذا التحول من خلال إقرار قواعد إجرائية تضمن فعالية المتابعة الجزائية دون المساس بجوهر الحقوق الدستورية. ومن هذا المنطلق، سعى المشرع إلى إرساء توازن دقيق بين متطلبات الأمن الرقمي وضمانات الحرية الفردية، عبر منظومة قانونية تقوم على الشرعية، والرقابة القضائية، واحترام الخصوصية.

أولاً: تقدير حجية الدليل الرقمي

أجازت المادة 349 من قانون الإجراءات الجزائية إمكانية اثبات الجرائم بأي طريق من طرق الاثبات بما فيها الإلكترونية، وللقاضي اصدار حكمه وفقاً لاقتناعه الشخصي ولكن أصبح أكثر من ضرورة مراعاة النزاهة الرقمية للأدلة الرقمية Digital Integrity in Cybercrime كون انه أصبح مع التطور الإلكتروني يمكن توليد ادلة رقمية مزيفة لا يمكن تمييزها عن الادلة الحقيقية وأصبحت تحدياً للخبراء، وهذا لاستخدام المجرم الإلكتروني لتقنيات عالية جداً تكشفها فقط فحوصات معقدة مثل تحليل البيانات الوصفية Metadata ، الأمر الذي يستدعي تطوير تقنيات كشف التزوير، ووضع أنظمة سلسلة الكتل Blockchain لتوثيق الادلة ومنع التلاعب بها، وكذلك التنظيم القانوني الدقيق للتعامل مع الدليل الرقمي.

وبما ان الدليل الإلكتروني تطبيق من تطبيقات الدليل العلمي، وذلك بما يتميز به من موضوعية وحياد وكفاءة مما يجعل اقناع القاضي الجنائي أكثر جزماً و يقيناً، حيث يساعده

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

على التقليل من الأخطاء القضائية، والاقتراب الى العدالة بخطوات أوسع والتوصل الى درجة أكبر نحو الحقيقة¹.

وتقدير القاضي للدليل الرقمي يتم من خلال التأكد من توافر العناصر التالية:

- **سلامة الدليل وموثوقيته (Integrity)&(Reliability)** : إن احتمال حدوث الخطأ الفني في جمع وتحليل الدليل الرقمي ممكن جدا، بالنظر الى الأجهزة المعقدة التي تستعمل في الجريمة²، فيتم التأكد من أن البيانات لم تتعرض للتعديل أو التغيير أو الحذف بعد جمعها، ويتم فحص الجهاز والجهة التي صدر منها الدليل مع الاعتماد على تقارير الخبراء بعد تقييمها للتحقق من ذلك.

- **مشروعية الحصول عليه (Legality)**: تخضع قواعد الاثبات الجنائي لمبدأ المشروعية ومقتضاه أن الدليل الجنائي بما يتضمنه من ادلة مستخرجة من وسائل الكترونية كالمبيوتر مثلا، لا يكون مشروعاً ومن ثم مقبولا في الاثبات الا اذا جرت عملية البحث عنه والحصول عليه واقامته امام القضاء في اطار احكام القانون واحترام قيم العدالة واخلاقيتها التي يحرص على حمايتها³، ويتم بالتحقق من وجود إذن قضائي وأنه تم وفق الإجراءات القانونية المعمول بها، ويتم استبعاد الأدلة التي تم الحصول عليها بطريقة غير مشروعة⁴.

- **علاقة الدليل بالقضية (Relevance)** : يتم التأكد من أن الدليل مرتبط مباشرة بالوقائع، مع استبعاد التي لا علاقة لها بالقضية وخصوصا التي تنتهك الخصوصية.

¹ - د. أشرف عبد القادر قنديل، المرجع السابق، ص 224.

² - هلالى عبد الله أحمد، حجية المخرجات الكمبيوترية، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997، ص 22.

³ - أشرف عبد القادر قنديل، المرجع نفسه، ص 206.

⁴ - الراجح أنه يتم استبعاد أدلة الإدانة التي تم الحصول عليها بطريقة غير مشروعة، في حين أدلة البراءة المتحصل عليها بطريقة غير مشروعة فالراجح أنه لا يتم استبعادها طبقاً لمبدأ المصلحة الأولى بالحماية إضافة الى حماية مبدأ قرينة البراءة باعتبارها الأصل في الانسان انظر المرجع نفسه، ص 211.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

- قابلية الفحص والمراجعة (Verifiability) : إذ يتوجب على القاضي أن يبرزها مهما كانت طبيعتها صورة أو فيديو أو تسجيل أو شرائط أو نسخ ورقية من مقتطفات الكترونية للمتهم ومناقشتها في حضوره والسماح له بإبداء رايه في هذا الموضوع وتسجيله، كما يجب ان يحضر الخبير جلسة الاستماع ويقدم جميع استنتاجاته في تقرير الخبرة ومناقشتها أمام القاضي والمتهم والحضور¹.

- مساندة الدليل الرقمي بأدلة أخرى (Corroboration): يتم تدعيمه بالأدلة الأخرى كالشهادة، القرائن، الوثائق بعد الموازنة بينها والتأكد من مطابقتها.

ثانيا: حماية الحقوق والحريات خلال التحريات

نظراً لما تتطوي عليه وسائل التحري الرقمية من قدرة فائقة على التغلغل في أدق تفاصيل الحياة الخاصة للأفراد، فقد أولى المشرع في القانون رقم 04-09 عناية خاصة لمسألة حماية الخصوصية، باعتبارها من الحقوق الأساسية المكفولة دستورياً. فالتفتيش الرقمي، بخلاف نظيره التقليدي، قد يمتد ليشمل كمّاً هائلاً من البيانات الشخصية، بما في ذلك المراسلات والاتصالات الخاصة، والصور الشخصية الأمر الذي يستوجب إخضاعه لرقابة قانونية صارمة².

وفي هذا الإطار، أوجب القانون ضرورة الحصول على إذن قضائي مسبق، مكتوب ومسبب، قبل مباشرة أي إجراء من شأنه المساس بسرية الاتصالات أو البيانات الشخصية، مع اشتراط تحديد نطاق هذا الإذن بدقة، سواء من حيث الموضوع أو المدة أو الأشخاص المعنيين، بما يمنع التوسع غير المشروع في الإجراءات التحقيقية.

¹ . صابرين يوسف عبد الله، دور الأدلة المرئية في الإثبات الجزائي، مجلة كلية الحقوق، المجلد الثالث عشر، المجلد الثالث عشر، العدد الثاني، جامعة النهرين، 2017، ص 265.

² -انظر: المادة 47 من الدستور الجزائري (المعدل 2020)، الجريدة الرسمية رقم 82.

الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية

كما يقوم هذا التنظيم على مبدأي الضرورة، بحيث لا يجوز اللجوء إلى الوسائل التقنية المتقدمة إلا إذا كانت ضرورية لكشف الحقيقة، ومتناسبة مع خطورة الجريمة المرتكبة. وعليه، فإن اللجوء إلى هذه الإجراءات يكون لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية، مما يحد من مخاطر التعسف في استعمال السلطة، ويمنع تحويل هذه الوسائل إلى أدوات لانتهاك الحريات الفردية.

ومن جهة أخرى، لا يجوز استعمال المعلومات المتحصل عليها إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية وفي هذا الإطار حرص المشرع على جعل المعلومات محل البحث في مأمن وذلك في حالة استحالة حجزها لأسباب تقنية وباستخدام التقنيات اللازمة لمنع الوصول إليها وهو ما نصت عليه المادة 7 من القانون رقم 09-104¹.

¹ - زبيحة زيدان، المرجع السابق، ص 152.

خاتمة:

إن التطور المتسارع للجريمة الالكترونية مستغلة في ذلك الطفرة التكنولوجية وخصوصا تلك المتعلقة بتكنولوجيات الاعلام والاتصال جعل القواعد القانونية الموضوعية والاجرائية الكلاسيكية في مفترق طرق في مواكبتها المستمرة بسبب البطيء الواضح إن لم نقل الجمود بينما هي تتطور وتصبح أكثر خطرا وضررا، يضاف الى ذلك صعوبة ضبطها وإثباتها كون انها تعتمد على نوع جديد من الأدلة الغير مادية التي يسهل تغييرها وإزالتها وكذلك تزويرها وقد يتم ذلك بعيدا عن مسرح الجريمة.

كل ذلك دفع بالمشعر الجزائري الى تجريم تلك الأفعال تدريجيا في قانون العقوبات بدءا بموجب القانون رقم 04-15 والمتعلقة بالمساس بأنظمة المعالجة الالية للمعطيات والذي تلاه صدور القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها تدعيما للقواعد الإجرائية الكلاسيكية بقواعد مستحدثة كالتفتيش الالكتروني والتفتيش عن بعد والمراقبة الالكترونية والحجز الالكتروني، وصدر كذلك قانون الإجراءات الجزائية الجديد رقم 14-25 والذي أجاز الاستعانة بالتقنيات التكنولوجية والاثبات بالطرق الالكترونية وفي نفس الوقت استمرت التعديلات المتممة لقانون العقوبات بتجريم أفعال كانت في الأصل جرائم تقليدية وارتكبت بوسائل تكنولوجيات الاعلام والاتصال فأصبحت أكثر ضررا عن سابقتها فتم تشديد عقوبتها مع إقرار مسؤولية الشخص المعنوي عن تلك الجرائم، وتجدر الاشارة أن المشعر جرم بعض الأفعال التي تشكل جرائم الكترونية في القوانين الخاصة باعتبارها مكملة لقانون العقوبات، ولم يغفل كذلك توفير ضمانات لحماية الحقوق والحريات الأساسية للأشخاص، وتم تعزيز فعالية الجهات القضائية والضبطية القضائية والهيئات المكلفة بالوقاية في مواجهة الجرائم المعلوماتية العابرة للحدود.

وقد أسفرت الدراسة عن مجموعة من النتائج الرئيسية التي توضح مدى التغيير والتحول الذي أحدثته تلك التعديلات التي مست قانون العقوبات وقانون الإجراءات الجزائية الجديد:

➤ استعمال تكنولوجيات الاعلام والاتصال يمكن ان يكون ظرفا مشددا في معظم الجرائم التقليدية وهي الحالة الأكثر شيوعا وهذا كما سبق الإشارة اليه فهو لا يغير جوهر الجريمة بل مجرد أداة، وقد يكون جريمة مستقلة بذاتها في حالات معينة في الحقيقة هي جرائم مستحدثة بسبب التطور التكنولوجي فلم تكن موجودة في العالم المادي كالقرصنة الالكترونية.

➤ حافظ قانون الإجراءات الجزائية رقم 14-25 على مبدأ حرية الإثبات في المادة 349 منه، مع توسيع نطاقه ليشمل الإثبات بالطرق الالكترونية، مع الإبقاء على مبدأ الاقناع الشخصي للقاضي الجزائي.

استناداً إلى هذه النتائج، يمكن تقديم مجموعة من التوصيات العملية لتعزيز فاعلية قانون العقوبات والقانون رقم 14-25 وضمان تطبيقه بشكل فعال:

➤ تطوير برامج تكوينية مستمرة للقضاة وأعاون الضبطية القضائية: للاطلاع على الآليات الجديدة مثل التحفظ على الأملاك الرقمية وحجزها، وإدارة الأدلة الرقمية بكفاءة عالية.

➤ تفعيل التعاون الدولي: بإبرام اتفاقيات دولية بما يسمح بتنفيذ الإنابات القضائية الإلكترونية عبر الحدود، لتجاوز التحديات القانونية والتقنية المرتبطة بالطبيعة العابرة للحدود للجريمة المعلوماتية.

➤ ضرورة التخصص للمحققين في الجرائم الالكترونية لما له من فائدة للتعامل مع هذا النوع من الجرائم للحصول على الأدلة الرقمية وتقديمها على ماهية عليه.

➤ ضرورة جمع جميع النصوص التشريعية في قانون واحد كما هو الحال في قانون مكافحة التزوير واستعمال المزور لسنة 2024، مع وضع نصوص تفاعلية تسمح بمواكبة

التطور السريع لهذه الجريمة ولما لا السماح بالتفويض التشريعي كما هو معمول به في الجرائم الاقتصادية والمالية بالإحالة الى التنظيم.

➤ وجوب اخضاع مقدمي الخدمات بمفهوم القانون رقم 09-04 في إطار تنفيذهم للالتزامات الخاصة بهذا القانون الى الرقابة القضائية قبل اتخاذها، لما لها من مساس بالحقوق والحريات الفردية.

➤ تعزيز التوعية بالحقوق والضمانات: توعية المجتمع المدني والمؤسسات الاقتصادية بالضمانات القانونية لحماية الخصوصية أثناء عمليات التفتيش الرقمي، بما يعزز الثقة في العدالة الإلكترونية ويقلل مخاطر المساس بالخصوصية.

قائمة المصادر والمراجع:

أولاً: النصوص القانونية والتنظيمية

- الدستور الجزائري المعدل سنة 2020.
- قانون العقوبات الجزائري، المعدل والمتمم، خاصة بموجب القانون رقم 06-24 لسنة 2024.
- القانون رقم 04-09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- القانون رقم 14-25 المؤرخ في 03 أوت 2025، المتضمن قانون الإجراءات الجزائية.
- الأمر رقم 66-156 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.
- الأمر رقم 11-21 المؤرخ في 25 أوت 2021، المعدل والمتمم لقانون الإجراءات الجزائية.
- القانون رقم 01-06 المؤرخ في 20 فيفري 2006، المتعلق بالوقاية من الفساد ومكافحته، المعدل والمتمم.
- المرسوم الرئاسي رقم 15-261 لسنة 2015 المتعلق بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- المرسوم التنفيذي رقم 19-172 لسنة 2019 المتعلق بتنظيم الهيئة الوطنية.
- المرسوم التنفيذي رقم 21-439 المتعلق بإعادة تنظيم الهيئة الوطنية.

ثانياً: الكتب

- خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي، الجزائر، 2008.

- هلاي عبد الله أحمد، حجية المخرجات الكمبيوترية، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997.
- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة - الجزائر، 2011.
- صابرين يوسف عبد الله، دور الأدلة المرئية في الإثبات الجزائي، مجلة كلية الحقوق، المجلد الثالث عشر، العدد الثاني، جامعة النهرين، 2017.
- محمد علي العريان، الجرائم المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، مصر، 2004.
- غنية باطلي، الجريمة الإلكترونية: دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015.
- المستشار خالد القاضي، قانون مكافحة جرائم تقنية المعلومات، عالم الكتب، القاهرة، 2022.
- حسين بن آث ملويا، المنتقى في القضاء العقابي، دار الخلدونية، الجزائر، 2012.
- مرفت محمد حبابية، مكافحة الجريمة الإلكترونية، دار اليازوري العلمية، عمان، 2022.
- يونس عرب، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، 2002.

ثالثاً: المقالات والدراسات العلمية

- عباس كريمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مجلة البيان للدراسات القانونية والسياسية، العدد الرابع، جامعة برج بوعرييج، الجزائر 2017.
- حفيظ نقادي، "معالم الجريمة المعلوماتية في القانون الجزائري"، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، 2014.

-
- *ادريس عطية، مكانة الامن السيبراني في منظومة الامن الوطني الجزائري، مجلة مصداقية المدرسة العليا العسكرية للإعلام والاتصال، المجلد 1، العدد 1، 2019.
- محمد السعيد زناتي، "الجريمة المعلوماتية في ظل التشريع الجزائري"، مجلة إيليزا، 2017.
- سميحة بلقاسم، حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر.. واقعها واليات مجابقتها، مجلة العلوم الإنسانية، المجلد 10، العدد 1، جامعة ام البواقي، 2023.
- صورية بوربابة، "التعاون الدولي في مكافحة الجرائم المعلوماتية"، مجلة القانون الدولي، 2019.
- سعيدة بوزنون، "مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة العلوم الإنسانية، 2019.
- دمان ذبيح، عماد بهلول سمية، "الآليات العقابية لمكافحة الجريمة الإلكترونية في الجزائر"، مجلة الحقوق والعلوم السياسية، 2020.
- عبد الصديق الشيخ، "الوقاية من الجرائم الإلكترونية في ظل القانون 09-04"، مجلة معالم للدراسات القانونية والسياسية، 2020.
- عميور خديجة، قواعد اختصاص الأقطاب الجزائية للنظر في جرائم الفساد، مجلة دراسات في الوظيفة العامة، العدد الثاني، ديسمبر سنة 2014.
- بن عميور أمينة، بوحلايس إلهام، "القطب الجزائي الوطني لمكافحة الجرائم المعلوماتية"، مجلة البحوث في العقود وقانون الأعمال، 2022.
- شريفة سوماتي، "القطب الجزائي الوطني كآلية جديدة"، مجلة الدراسات القانونية، 2022.

■ عفاف بعون، نسيمة أولاد سالم، الجريمة الالكترونية- قراءة سوسيو تاريخية في النشأة والاثار، مجلة القبس للدراسات النفسية والاجتماعية- المجلد 5 العدد 20 جامعة يحي فارس المدية الجزائر، 2023.

■ سلمى عبد النبي، "دور القطب الجزائري في مكافحة الجرائم المعلوماتية"، مجلة الحقوق والعلوم السياسية، 2024.

رابعاً: الرسائل الجامعية

■ بوحزمة نصيرة، التحقيق الجنائي في الجرائم الالكترونية رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، جامعة جيلالي ليايس سيدي بلعباس، 2022.

■ ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، جامعة باتنة، 2016.

■ رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، جامعة تلمسان، 2018.

■ جدي نسيم، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة ماجستير، جامعة وهران، 2014.

■ هبة نبيلة هروال، جرائم الانترنت دراسة مقارنة، أطروحة دكتوراه، جامعة تلمسان، الجزائر، 2014.

■ بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة ماستر، جامعة محمد البشير الابراهيمي برج بوعريج، الجزائر، 2022.

خامساً: الملتقيات والتقارير

○ مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس، 2016.

○ بوزيدي مختارية، "ماهية الجريمة الإلكترونية"، مداخلة في ملتقى آليات مكافحة الجرائم الإلكترونية، الجزائر، 2017.

المراجع باللغة الأجنبية:

Myriam Quéméner, les données personnelles à l'ère numérique Quelle protection sur le plan pénal, REVUE DU DROIT, n°1 – 2016.

سادسا: المواقع الالكترونية

الجريدة الرسمية

–www.joradp.dz/HAR/Index.htm

اتفاقية بودابست

–<https://rm.coe.int/budapest-convention-in-arabic/1680739173>

–bleepingcomputer.com

– www.esafety.gov.au

أ	مقدمة:
1	الفصل الأول: الإطار المفاهيمي والتجريبي للجرائم الإلكترونية في التشريع الجزائري
2	المبحث الأول: ماهية الجرائم الإلكترونية المستحدثة وخصائصها
2	المطلب الأول: مفهوم الجريمة الإلكترونية وتطورها
3	الفرع الأول: تعريف الجريمة الإلكترونية
7	الفرع الثاني: التطور التاريخي للجريمة الإلكترونية
11	المطلب الثاني: خصائص الجريمة الإلكترونية وأركانها القانونية
11	الفرع الأول: خصائص الجريمة الإلكترونية
13	الفرع الثاني: الأركان القانونية للجريمة الإلكترونية
16	المبحث الثاني: السياسة الجزائية للجرائم المتصلة بتكنولوجيات الاعلام والاتصال
16	المطلب الأول: الجرائم الإلكترونية المستحدثة في قانون العقوبات
17	الفرع الأول: جرائم الاعتداء على المنظومات المعلوماتية
19	الفرع الثاني: الجرائم المستحدثة المرتبطة بالمحتوى الرقمي
21	المطلب الثاني: السياسة العقابية المستحدثة
21	الفرع الأول: المسؤولية الجزائية للشخص الطبيعي
25	الفرع الثاني: المسؤولية الجزائية للشخص المعنوي

26	الفصل الثاني: الآليات القانونية المستحدثة لمكافحة الجرائم الإلكترونية.....
27	المبحث الأول: الهيئات الوطنية المتخصصة في مكافحة الجرائم الإلكترونية.....
27	المطلب الأول: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.....
	الفرع الأول: تعريف القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وأساسه
28	التشريعي.....
	الفرع الثاني: الاختصاصات النوعية للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام
29	والاتصال.....
33	المطلب الثاني: الهيئات الإدارية والأمنية المكلفة بمكافحة الجرائم الإلكترونية.....
33	الفرع الأول: الهيئات الإدارية المكلفة بالوقاية والتحقيق في الجرائم الإلكترونية.....
35	الفرع الثاني: الهيئات الأمنية المكلفة بالوقاية والتحقيق في الجرائم الإلكترونية.....
38	المبحث الثاني: آليات التحري والتحقيق الرقمي المستحدثة.....
39	المطلب الأول: الأساليب الخاصة للتحري والتحقيق.....
39	الفرع الأول: اعتراض المراسلات الإلكترونية ومراقبة الاتصالات.....
41	الفرع الثاني: أسلوب التسرب.....
43	المطلب الثاني: إجراءات ضبط الأدلة المستحدثة وحجيتها وضماناتها.....
43	الفرع الأول: إجراءات ضبط الأدلة الرقمية المستحدثة.....
47	الفرع الثاني: حجية الدليل الرقمي وحماية الحقوق والحريات.....
50	خاتمة:.....

53	قائمة المصادر والمراجع:
58	الفهرس:

الملخص:

تتناول هذه الدراسة الجرائم الإلكترونية المستحدثة في التشريع الجزائري، على ضوء قانون العقوبات رقم 24-06 وقانون الإجراءات الجزائية الجديد رقم 25-14. وتهدف الدراسة إلى تحليل الأشكال الجديدة للإجرام المعلوماتي وطرق تكييفها قانونيًا، مع إبراز دور المشرع في تنظيم إجراءات التفتيش الإلكتروني عن بعد والمراقبة الإلكترونية وطرق حجز الأدلة الرقمية. كما توضح الدراسة الجهات القضائية المستحدثة وكذا الهيئات الإدارية للوقاية ومكافحة هذه الجريمة. وأبرزت الدراسة أهمية المسؤولية الجزائية للشخص المعنوي في حماية الأنظمة المعلوماتية. وأخيرًا، تقدّم الدراسة توصيات لتعزيز العدالة الرقمية، وتطوير التكوين القضائي، وتنشيط التعاون الدولي لمكافحة الجريمة المعلوماتية. يُظهر البحث أن التشريع الجزائري يسعى إلى موازنة حماية الحريات مع فعالية مكافحة الجرائم الإلكترونية.

الكلمات المفتاحية: الجريمة الإلكترونية – القواعد الإجرائية المستحدثة – القواعد الموضوعية المستحدثة.

Abstract:

This study addresses the newly emerging cybercrimes in Algerian legislation, in light of the Penal Code and the new Code of Criminal Procedure No. 25-14. The study aims to analyze the new forms of cybercrime and their legal classification, highlighting the legislator's role in regulating remote electronic search procedures, electronic surveillance, and methods for seizing digital evidence. It also details the newly established judicial authorities as well as the administrative bodies responsible for the prevention and combating of these crimes. The study underscores the importance of criminal liability for legal entities in protecting information systems. Finally, the study offers recommendations to enhance digital justice, develop judicial training, and promote international cooperation to combat cybercrime. The research demonstrates that Algerian legislation seeks to balance the protection of freedoms with the effectiveness of combating cybercrime.

Keywords: Cybercrime – Newly introduced procedural rules – Newly introduced substantive rules

