الجمهورية الجزائرية الديمقراطية الشعبية
جامعة المجاهد عبد الحفيظ بوالصوف ميلة
كلية الحقوق

قسم: الحقوق
التخصص: ماستر قانون جنائي

الرقم التسلسلي:
الرمز:

الأجهزة الفاعلة في مجال البحث والتحري عن الجرائم المعلوماتية

مذكرة ضمن متطلبات نيل شهادة _ ماستر_

إعداد الطلبة:
- لشهب فيصل
- رزايقي رحمة

الأستاذ المشرف:
- عديد أمينة

أعضاء لجنة المناقشة:

اسم ولقب الأستاذ(ة)	الجامعة	الرتبة	الصفة
بوعزة نضيرة	جامعة المجاهد عبد الحفيظ بوالصوف ميلة	أستاذ محاضر _أ_	رئيسا
عديد أمينة	جامعة المجاهد عبد الحفيظ بوالصوف ميلة	أستاذ محاضر _أ_	مشرفا ومقررا
مقورة مفيدة	جامعة المجاهد عبد الحفيظ بوالصوف ميلة	أستاذ محاضر_ب_	ممتحنا

السنة الجامعية:2026/2025

الجمهورية الجزائرية الديمقراطية الشعبية
جامعة المجاهد عبد الحفيظ بوالصوف ميلة
كلية الحقوق

قسم: الحقوق
التخصص: ماستر قانون جنائي

الرقم التسلسلي:
الرمز:

الأجهزة الفاعلة في مجال البحث والتحري عن الجرائم المعلوماتية

مذكرة ضمن متطلبات نيل شهادة _ ماستر_

إعداد الطلبة:
- لشهب فيصل
- رزايقي رحمة

الأستاذ المشرف:
- عديد أمينة

السنة الجامعية: 2026/2025

بسم الله الرحمن الرحيم

الملخص:

لقد نتج عن الثورة الرقمية والطفرة التكنولوجية المعاصرة ظهور نمط إجرامي مستحدث يعرف بـ "الجريمة المعلوماتية"؛ وهي الجريمة التي فرضت واقعاً قانونياً وإجرائياً جديداً يختلف جذرياً عن الأنماط التقليدية للجريمة. وقد جاءت هذه الدراسة المعنونة "آليات البحث والتحري عن الجرائم المعلوماتية" لتسليط الضوء على الإطار المفاهيمي والمؤسساتي والإجرائي الذي تبناه المشرع الجزائري لمواجهة هذا التحدي السيبراني المتسارع. فمن خلال هذه الدراسة نجد أن الجريمة المعلوماتية بطبيعتها اللامادية والعابرة للحدود فرضت على المشرع الجزائري تبني مقاربة مرنة تجمع بين آليات الوقاية (الهيئة الوطنية وسلطة حماية المعطيات) وآليات الردع (الضبطية القضائية المتخصصة وآليات البحث والتحري)، مع الاعتماد على وسائل تقنية مستحدثة كبرامج التتبع لإثبات الدليل الرقمي؛ إلا أن فعالية هذه المنظومة تظل مرهونة بمواجهة صعوبات إخفاء الأدلة ونقص التكوين الفني والتشريع القانوني الخاص بهذا النوع من الجرائم، مما يستدعي حتمياً تكثيف التأهيل التقني للمحققين وتدويل التعاون القضائي لمواكبة الطفرة الرقمية.

Summary:

The digital revolution and the contemporary technological boom have given rise to a new criminal pattern known as "cybercrime." This crime has imposed a new legal and procedural reality that differs radically from traditional forms of crime. This study, entitled "Mechanisms for Investigating and Combating Cybercrime," aims to shed light on the conceptual, institutional, and procedural framework adopted by the Algerian legislator to confront this rapidly evolving cyber challenge.

The study reveals that the intangible and transnational nature of cybercrime has compelled the Algerian legislator to adopt a flexible approach that combines preventative mechanisms (the National Authority and the Data Protection Authority) with deterrent mechanisms (specialized judicial police and investigative mechanisms), while relying on modern technological means such as tracking software to establish digital evidence. However, the effectiveness of this system remains contingent on overcoming the difficulties of concealing evidence and the lack of technical training and specific legislation for this type of crime. This necessitates, inevitably, intensifying the technical training of investigators and internationalizing judicial cooperation to keep pace with the digital revolution.

شكروتقدير

الحمد لله الذي بنعمته تتمّ الصالحات، نحمده سبحانه وتعالى على توفيقه وإعانته لإتمام هذا العمل المتواضع.

أتقدم بخالص الشكر والتقدير إلى الأستاذة عديد أمينة لإشرافها على هذه المذكرة، وعلى كل ما قدّمته من توجيهات علمية قيمة ونصائح سديدة، وعلى صبرها ومتابعتها المستمرة طوال فترة إنجاز هذا البحث.

كما أتوجه بالشكر إلى أعضاء لجنة المناقشة الموقرة على تفضلهم بقبول قراءة هذه المذكرة وتقييمها، وإثرائها بملاحظاتهم العلمية القيّمة.

ولا يفوتني أن أتقدم بجزيل الشكر إلى كافة أساتذتي الذين أشرفوا على تكويني العلمي طوال مشواري الجامعي، وإلى كل من ساهم من قريب أو بعيد في إنجاز هذا العمل.

كما أخصّ بالشكر عائلتي الكريمة على دعمها المتواصل وتشجيعها الدائم، سائلًا الله أن يوفق الجميع لما فيه الخير والنجاح.

الإهداء

إلى من علمتني معنى الصبر والعزيمة والكفاح

أمي الغالية

إلى من علمني أن القاع مزدحم وعليَ أن أجد لي مكانا في القمة، إلى من لا يرضى إلا أن يراني شامخة

والدي الكريم

إلى أستاذي في الحياة، من علمني أن الطموح لا سقف له

أخي العزيز عادل

إلى كل فرد من أفراد أسرتي هم البلسم والدواء والدافع

إخوتي دون استثناء

إلى من سرنا سويا ونحن نشق الطريق نحو النجاح والإبداع إلى من تكاتفنا يد بيد لنتغلب معا مرارة الأيام

إلى رفيقات كل الدروب تقوى، سارة، إيمان

وقبل كل هؤلاء، إلى نفسي التي تأبى الاستسلام قبل الوصول، والهزيمة قبل الإنجاز، والرضوخ قبل الطموح

"رحمة"

الإهداء

الحمد لله الذي بنعمته تتم الصالحات، وبتوفيقه تنجز الأعمال وتبلغ الغايات.

أهدي هذا العمل المتواضع الى نفسي، ثمرة سنوات من السعي والاجتهاد، وما رافقها من صبر وتحديات ومحاولات مستمرة في سبيل التطور.

كما أحمد الله تعالى وأشكره على فضله وتوفيقه اللذان كانا سببا في تيسير هذا الإنجاز واتمامه وأسأله ان يبارك فيه ويجعله نافعا.

"فيصل"

المقدمة

مقدمة:

نشأت الجريمة كظاهرة اجتماعية منذ بداية وجود الإنسان في إطار الجماعة، حيث كان غياب القواعد المنظمة في المجتمعات البدائية يؤدي إلى ظهور سلوكيات عدوانية مرتبطة أساسًا بالغريزة، مثل الاعتداء على الغير أو الاستيلاء على الممتلكات. وفي تلك المرحلة، لم يكن هناك مفهوم قانوني واضح للجريمة، بل كانت تُعالج وفق مبدأ الانتقام الفردي أو العائلي.

ومع تطور المجتمعات وظهور التنظيمات القبلية ثم الدول، بدأت تتشكل قواعد عرفية تضبط سلوك الأفراد وتحدد الأفعال المرفوضة، فتحول التعامل مع الجريمة تدريجيًا من الانتقام الشخصي إلى نوع من العدالة الاجتماعية.

ففي العصور القديمة، خصوصًا مع نشوء الحضارات الكبرى، بدأ تقنين الجريمة بشكل أوضح، مما ساهم في ترسيخ مبدأ الشرعية. ثم تواصل التطور في العصور الحديثة مع بروز الدولة الحديثة، حيث أصبح القانون الجنائي أكثر تنظيمًا، وتم التأكيد على حماية الحقوق والحريات وضرورة تناسب العقوبة مع الجريمة وغيرها من المبادئ القانونية.

أما في العصر الحديث والمعاصر، فلم يعد يُنظر إلى الجريمة فقط باعتبارها فعلًا مخالفًا للقانون، بل أصبحت تُعد ظاهرة معقدة لها أسباب متعددة ومتداخلة، وهو ما دفع إلى تطوير السياسات الجنائية لتشمل، إلى جانب العقاب، وسائل الوقاية والعلاج. وفي هذا السياق، أنشأت الدول منظومات ومؤسسات وأجهزة قضائية أكثر احترافية وتنظيمًا، تكفل حماية المجتمع وتضمن استقراره.

غير أنه، وفي ظل التطور التكنولوجي الذي شهده العالم في الوقت الراهن، تحولت الحياة من كل ما هو تقليدي ومادي إلى ما هو حديث ورقمي، حيث تم كسر الحدود بين الدول والشعوب، وأصبح من الشائع، بل ومن الضروري، استعمال الحاسوب وشبكات الاتصال بشكل يومي، سواء بالنسبة للحكومات أو الشركات أو الأفراد، وهو ما حقق قفزة حضارية كبيرة للبشرية.

لكن، وعلى الرغم من الانعكاسات الإيجابية لهذه الثورة المعلوماتية، فقد ترتبت عنها أيضًا آثار سلبية، كالإدمان والأضرار الصحية وغيرها، غير أن أخطرها يتمثل في ظهور نوع من الجرائم المستحدثة التي ترتكز على استغلال الأنظمة المعلوماتية بطريقة غير مشروعة، بقصد إحداث ضرر يمس حقوق وسلامة وخصوصية الآخرين في الفضاء الرقمي، وقد تتطور في بعض الحالات لتهدد أمن الدول واقتصادها، وهي ما يُعرف بالجرائم المعلوماتية.

وتستمد هذه الجرائم خطورتها من سهولة ارتكابها، إضافة إلى أن آثارها لا تقتصر على نطاق إقليمي محدد، فضلًا عن أن مرتكبيها يتميزون بالذكاء والخبرة التقنية العالية في التعامل مع الأنظمة المعلوماتية، وهو ما أثار تحديات قانونية وعملية أمام الأجهزة الأمنية في مختلف الدول، باعتبار أنها كانت معتادة على التعامل مع الجرائم التقليدية التي يمكن رصدها وتتبع مرتكبيها من خلال الأدلة المادية.

ومن بين المشكلات الإجرائية التي تواجه هذه الأجهزة عند تعاملها مع هذا النوع من الجرائم، أنها تُرتكب في بيئة افتراضية وتقنية بحتة، فضلًا عن أنها تُرتكب في الخفاء عن طريق التلاعب بالبيانات وتزييفها وتمويه الهويات باستعمال خوارزميات وبرامج معقدة. أضف إلى ذلك أن النصوص الخاصة بالبحث والتحري في مجال الجرائم التقليدية لا تصلح دائمًا للتطبيق على الجرائم المعلوماتية، بسبب عائق مبدأ إقليمية النصوص الجنائية، وهو ما تسبب في صعوبة ملاحقة مرتكبيها وتحقيق العدالة. وعليه، فرضت هذه الجرائم على مختلف دول العالم ضرورة تكييف قوانينها واستحداث أجهزة متخصصة مدعمة بخبراء ذوي كفاءة تقنية عالية، من أجل الحد من انتشار هذه الجرائم ورصد مرتكبيها.

ولم يكن المشرع الجزائري بمنأى عن هذه التحديات التي فرضتها الجرائم المعلوماتية، حيث اتخذ جملة من الإجراءات التنظيمية والمؤسساتية، إضافة إلى تدعيم المنظومة القانونية بنصوص خاصة تهدف إلى رفع فعالية التصدي لهذا النوع من الجرائم، وذلك من خلال استحداث أجهزة وهياكل متخصصة مكلفة بالبحث والتحري فيها من جهة، وتطوير قدرات المصالح الأمنية بما يتناسب مع طبيعتها من جهة أخرى. ويعكس ذلك وعي الدولة الجزائرية بضرورة التكيف مع التحولات الرقمية المتسارعة والعمل على حماية الفضاء السيبراني الوطني من مختلف أشكال الاعتداءات، في إطار رؤية تهدف إلى تعزيز الأمن المعلوماتي وترسيخ سيادة القانون في المجال الرقمي.

وتكتسي دراسة موضوع الجريمة المعلوماتية والأجهزة المعنية بالبحث والتحري على المستويين العلمي والعملي أهمية بالغة تتمثل في اندراج الجرائم المعلوماتية ضمن الجرائم المستحدثة التي فرضت إعادة النظر في المفاهيم التقليدية للقانون الجنائي، حيث تساهم في تطوير الإطار النظري للجريمة من خلال تحليل خصائصها غير المادية وطابعها التقني وصعوبة التعرف على مرتكبيها وضبطهم. كما تبرز أهمية هذا الموضوع في كونه مجالًا متعدد التخصصات، يجمع بين القانون وتقنيات الإعلام الآلي وعلم الإجرام، مما يتيح فهمًا أعمق لآليات الإجرام الرقمي وأساليب مواجهته.

كما تبرز الأهمية العملية للدراسة في كون الجرائم المعلوماتية تمس الأمن المعلوماتي للدولة والأفراد على حد سواء، مما يستدعي تطوير آليات فعالة للكشف عنها ومكافحتها، خاصة في ظل ما تطرحه من صعوبات تقنية وإجرائية. كما تساعد هذه الدراسة على تقييم مدى نجاعة الأجهزة المختصة في مواجهتها، واقتراح سبل تعزيز قدراتها بما يواكب التحولات الرقمية المتسارعة، لا سيما مع انتشار تطبيقات الذكاء الاصطناعي واستعمالها المتزايد.

وتتعدد الأسباب التي دفعتنا لاختيار هذا الموضوع، حيث تتضافر العوامل الموضوعية مع الدوافع الشخصية لتشكل أهمية هذه الدراسة. فعلى الصعيد الموضوعي، يفرض الانتشار المتزايد للجرائم المعلوماتية في ظل التطور التكنولوجي المتسارع نفسه كضرورة ملحة للبحث، نظراً لما تشكله هذه الجرائم من خطورة بالغة على الأفراد والمؤسسات والدول على حد سواء. كما تكتسي هذه الدراسة أهميتها من حداثة الموضوع وراهنيته القانونية والعملية، مما جعله محط اهتمام فقهي وتشريعي متزايد، بالإضافة إلى رغبتنا في إبراز دور الأجهزة المختصة في مكافحة هذه الجرائم وتقييم مدى فعاليتها في التصدي لها.

أما على الصعيد الشخصي والذاتي، فقد جاء اختيارنا لهذا الموضوع نتيجة اهتمامنا الخاص بالمجال الرقمي والجرائم المرتبطة به، ورغبتنا الصادقة في التعمق في الجوانب القانونية والتقنية المعقدة التي تحيط به. كما نابع هذا الاختيار من ميلنا الدائم لدراسة المواضيع الحديثة التي تلامس الواقع العملي وتواكب التطورات الراهنة، وسعينا المستمر لإثراء رصيدنا العلمي والمعرفي في هذا الحقل المعرفي المتجدد.

بالإضافة إلى أن هذه الدراسة تهدف إلى تسليط الضوء على الجريمة المعلوماتية من خلال تعريفها وبيان خصائصها وصورها المختلفة، مع التركيز على تحليل الإطار القانوني الذي ينظم عمليات البحث والتحري عن هذه الجرائم في ظل التشريع الجزائري. كما تسعى الدراسة إلى إبراز أهم الصعوبات والتحديات التي تواجه الأجهزة المكلفة بالبحث والتحري في هذا المجال، والتعرف على الآليات المؤسساتية التي اعتمدها المشرع الجزائري لمكافحة هذه الظاهرة، وصولاً إلى تقييم مدى فعالية الأجهزة المختصة في التصدي للجرائم المعلوماتية واقتراح مجموعة من الحلول والتدابير الكفيلة بتعزيز أدائها وتطوير قدراتها في هذا السياق.

وبناءً على ذلك، برزت الحاجة إلى تسليط الضوء على هذا الموضوع محل الدراسة، من أجل البحث في مدى فعالية الأجهزة المكلفة بالبحث والتحري عن الجرائم المعلوماتية، وكذا النصوص القانونية التي تستند إليها، ومدى توفيق المشرع الجزائري في تنظيم هذا المجال. ومن هنا تبرز الإشكالية الرئيسية للدراسة والمتمثلة في:

ما مدى فعالية الأجهزة المكلفة بالبحث والتحري عن الجرائم المعلوماتية في القانون الجزائري؟

ومن هذه الإشكالية الرئيسية تتفرع مجموعة من التساؤلات الفرعية، تتمثل فيما يلي:

- ما المقصود بالجريمة المعلوماتية؟
- ما هي صور الجرائم المعلوماتية؟
- فيما يتمثل الإطار القانوني لعمليات البحث والتحري عن الجرائم المعلوماتية؟
- ما هي الصعوبات التي تعرقل إجراءات البحث والتحري عن الجرائم المعلوماتية؟
- ما هي الآليات المؤسساتية التي اعتمدها المشرع الجزائري في هذا المجال؟

وللإجابة على الإشكالية المطروحة والتساؤلات الفرعية المنبثقة عنها تم الاعتماد في هذه الدراسة على المنهج الوصفي التحليلي، وذلك من خلال وصف ظاهرة الجرائم المعلوماتية وتحليل النصوص القانونية المنظمة لها، إضافة إلى دراسة مختلف الآليات المؤسساتية المعتمدة في مجال البحث والتحري عنها، مع الاستعانة بالمنهج المقارن عند الضرورة لإبراز بعض الجوانب المتعلقة بالتشريعات المقارنة.

كما تتحدد نطاقات هذه الدراسة من خلال ثلاثة أبعاد رئيسية تضمن تركيز البحث وتحقيق أهدافه بدقة؛ فعلى الصعيد الموضوعي، تقتصر الدراسة على معالجة الجرائم المعلوماتية من حيث تأصيلها المفاهيمي، وتصنيف صورها المختلفة، مع تحليل الإطار القانوني والمؤسساتي الناظم لعمليات البحث والتحري عنها. أما مكانياً، فتُركز الدراسة نطاق بحثها على التشريع الجزائري، مسلطةً الضوء على الأجهزة المختصة المكلفة بمكافحة هذه الجرائم داخل الدولة الجزائرية. وأخيراً، تتحدد الدراسة زمنياً من خلال استقراء وتحليل النصوص القانونية والتنظيمية السارية والمعمول بها في التشريع الجزائري إلى غاية تاريخ إعداد هذه المذكرة.

وللإجابة على الإشكالية المطروحة والإحاطة بمختلف جوانب الموضوع، تم تقسيم هذه الدراسة إلى فصلين، حيث تعرضنا في الفصل الأول للإطار المفاهيمي والقانوني للبحث والتحري عن الجرائم المعلوماتية، من خلال تناول المفاهيم العامة المتعلقة بالجرائم المعلوماتية في المبحث الأول، وذلك عبر التطرق إلى مفهوم الجريمة المعلوماتية من حيث تعريفها وخصائصها وأركانها، ثم بيان أهم صور الجرائم المعلوماتية. أما المبحث الثاني، فقد خصصناه لدراسة الإطار القانوني لعمليات البحث والتحري عن الجرائم المعلوماتية، من خلال إبراز التكريس القانوني لسلطة البحث والتحري في ظل القوانين العامة والخاصة، بالإضافة إلى مختلف الصعوبات التي تعترض البحث والتحري في هذا النوع من الجرائم.

وخصصنا الفصل الثاني لدراسة الآليات المؤسساتية والإجرائية المتعلقة بالبحث والتحري عن الجرائم المعلوماتية، حيث تناولنا الأجهزة والهيئات المختصة بمكافحة الجرائم المعلوماتية في المبحث الأول، ثم تطرقنا في المبحث الثاني إلى الإجراءات القانونية والتقنية المعتمدة في مجال البحث والتحري، مع بيان أهم الضمانات والصعوبات المرتبطة بها. وأنهينا هذا البحث بخاتمة تضمنت أهم النتائج المتوصل إليها، مدعمة بجملة من الاقتراحات والتوصيات التي رأينا أنها قد تساهم في تعزيز فعالية مكافحة الجرائم المعلوماتية.

الفصل الأول: الإطار المفاهيمي والقانوني للبحث والتحري عن الجرائم المعلوماتية

شهد العالم خلال العقود الأخيرة تطورًا تكنولوجيًا متسارعًا شمل مختلف مجالات الحياة، الأمر الذي أدى إلى تغير أنماط التعامل والتواصل بين الأفراد والمؤسسات والدول. وقد ساهم هذا التطور في انتقال المجتمعات من البيئة التقليدية إلى البيئة الرقمية، حيث أصبحت التكنولوجيا الحديثة والأنظمة المعلوماتية جزءًا أساسيًا من الحياة اليومية. وبالموازاة مع هذه التحولات، لم تعد الجريمة تقتصر على صورتها التقليدية المعروفة كالسرقة والاحتيال والاعتداء المادي، بل ظهرت أنماط جديدة من الجرائم تعتمد على الوسائل التقنية الحديثة، مستفيدة من التطور الهائل في مجال الإعلام الآلي وشبكات الاتصال، وهو ما أدى إلى بروز ما يعرف بالجرائم المعلوماتية باعتبارها من أخطر الجرائم المستحدثة في العصر الحديث.

وقد ارتبط ظهور هذه الجرائم أساسًا بالوسيلة المستعملة في ارتكابها، والمتمثلة في الحاسوب والأنظمة المعلوماتية وشبكات الإنترنت، حيث أصبحت هذه الوسائل تشكل البيئة الأساسية التي تُرتكب من خلالها مختلف الأفعال الإجرامية. فبفضل التطور التقني، أصبح بإمكان الجناة اختراق الأنظمة المعلوماتية، والاستيلاء على البيانات، والتجسس الإلكتروني، ونشر الفيروسات، والاحتيال عبر الإنترنت، دون الحاجة إلى التواجد المادي في مكان الجريمة. كما ساعدت الطبيعة الافتراضية لهذه الوسائل على صعوبة اكتشاف الجناة وتحديد هوياتهم، خاصة في ظل اعتمادهم على تقنيات متطورة للتخفي وتمويه آثارهم الإلكترونية.

ولم تقتصر خطورة الجرائم المعلوماتية على مجرد المساس بالأفراد فقط، بل امتدت آثارها لتشمل المؤسسات والهيئات الحكومية والاقتصادات الوطنية، حيث أصبحت تهدد أمن المعلومات وخصوصية البيانات وسلامة المعاملات الإلكترونية. كما نتج عنها خسائر مالية كبيرة، إضافة إلى تأثيرها السلبي على الثقة في التعاملات الرقمية والتطور التكنولوجي. وقد ازدادت خطورة هذه الجرائم مع الطابع العابر للحدود الذي تتميز به، الأمر الذي جعل مكافحتها من أكبر التحديات التي تواجه مختلف الدول والأجهزة الأمنية والقضائية.

وأمام هذه الانعكاسات السلبية والخطيرة، أصبح من الضروري تسليط الضوء على الجريمة المعلوماتية من خلال دراسة مفهومها وخصائصها وصورها المختلفة، وهو ما سيتم التطرق إليه من خلال **(المبحث الأول)**، ثم دراسة الإطار القانوني والإجرائي المتعلق بالبحث والتحري عنها، وكذلك الصعوبات التي تثيرها وهو ما سيتم التطرق إليه من خلال **(المبحث الثاني)**.

المبحث الأول: مفاهيم عامة حول الجرائم المعلوماتية.

بعد ما شهده العامل من ثورة رقمية هائلة في العقود الأخيرة والتي مست مختلف المجالات، هذا ما صاحبه سعي الدول وفي نفس الوقت إلى حماية أنظمتها المعلوماتية من الهجمات والتهديدات السيبرانية أو ما يعرف بالجريمة المعلوماتية التي نمت وتطورت بشكل سريع، وهو ما يتطلب الوقوف على مفهوم هذه الجريمة الحديثة، أين سيتم إبراز مفهوم الجريمة المعلوماتية في هذا المبحث، من تعريف وخصائص وأركان **(المطلب الأول)**، ثم ستستعرض لبعض صور هذه الجريمة من خلال **(المطلب الثاني)**.

المطلب الأول: مفهوم الجريمة المعلوماتية

عند محاولة الكشف عن مفهوم مصطلح معين، فإنه يتم التطرق إلى إبراز كل ما من شأنه إزالة الغموض والإبهام عنه، وجعله في متناول كل من يهتم بالإلمام به، وبذلك سنقوم بتعريف الجريمة المعلوماتية من خلال **(الفرع الأول)**، من الناحية اللغوية والاصطلاحية وكذلك من الجانب الفقهي من خلال التطرق إلى مختلف الآراء الفقهية حول المقصود بهذه الجريمة، مع تسليط الضوء على التعريف القانوني لها في مختلف التشريعات والقوانين الوضعية، وللخوض فيها أكثر وأكثر يستلزم دراسة خصائصها من خلال **(الفرع الثاني)**، أما أركانها فستدرس من خلال**(الفرع الثالث)** من هذا المطلب.

الفرع الأول: تعريف الجريمة المعلوماتية

إن الجريمة المعلوماتية مصطلح مركب من كلمتي "الجريمة" و"المعلومات"، مما يستلزم توضيح مفهوم كل منهما على حدا قبل التطرق إلى مفهومها.

أولا: تعريف الجريمة

يتبين من خلال الدراسات التاريخية تضارب التعريفات الواردة بخصوص مفهوم الجريمة، فحسب المنظور الاجتماعي عرفت الجريمة على أنها انتهاك لحقوق وبادئ المجتمع وأعرافه، والذي يستلزم عقابا كرد فعل اجتماعي. أما من المنظور النفسي فترى الجريمة على أنها ثمرة الصراع بين الذات أوما يسمى بنزعة التفوق والشعور الاجتماعي[1].

[1]_ صلاح الدين عباسي، سلسلة العلوم الإجرامية: دراسات في علم الإجرام (Alpha Doc، 2015)، 47،48.

لم يتطرق المشرع صراحة للجريمة، فعمل فقهاء ودارسي القانون على تعريفها، إذ تعد الجريمة في الفقه القانوني كل فعل أو امتناع عن فعل يعاقب عليه القانون بنص قانوني صريح وفق ما جاءت به المادة 1 من قانون العقوبات الجزائري:" لا جريمة ولا عقوبة ولا تدبير أمن إلا بنص."[1]

ثانيا: تعريف المعلوماتية

ظهر مصطلح المعلوماتية لأول مرة في خمسينيات القرن الماضي من قبل مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفياتي A.I. Mikhailovكاسم لعلم المعلومات العلمية[2].

فهي كل البيانات أو الحقائق الرقمية أو البرمجيات التي تخزن، تعالج، أو تنقل عبر أنظمة الحاسوب والشبكات الإلكترونية، والتي يمكن استهدافها بالاختراق أو السرقة أو التلاعب أو التجسس.

وتشمل هذه المعلومات بيانات شخصية أو مالية أو تجارية أو حكومية، وتكتسب أهميتها القانونية والأمنية من كونها محورية في النشاط الرقمي وحماية لخصوصية وسلامة الأنظمة.

ثالثا: تعريف الجرائم المعلوماتية "Information Crimes"

رغم الانتشار الواسع للجرائم المعلوماتية إلا أن تعريفها لم يحظى بعد بإجماع عالمي، إذ تختلف التعريفات بحسب السياق القانوني أو التقني أو الأكاديمي أو الفقهي فبعض التعريفات تركز على النشاط الإجرامي في حد ذاته عبر الحواسيب والشبكات، بينما تركز أخرى على الأضرار الناتجة على الأفراد أو المؤسسات أو على الأمن العام. ومن بين هذه التعاريف نذكر:

1_ التعريف اللغوي

يقصد بالجريمة لغة الذنب، ونقول جرَم وأجرم واجترام بمعنى إدعى عليه بذنب لم يقترفه أما المعلوماتية فهي ترجمة للمصطلح الفرنسي information بمعنى المعالجة الآلية للمعطيات، ويعود هذا المصطلح إلى فيليب داريفوس، والذي قصد به العلم الذي يربط المعلومات والحاسوب والاتصالات.

[1] _ المادة1 من الأمر رقم 156/66 المتضمن قانون العقوبات/المعدل والمتمم، ع.30، ج ر ج ج.4.

[2] _ طاهر محمود أبو القاسم، *الجرائم المعلوماتية: صعوبات وسائل التحقيق فيها وكيفية مواجهتها* (المنظمة العربية للتنمية الإدارية، 2019)، 22،23.

كما ذهب البعض إلى القول إنه ليس من السهل وصف المعلومة بدقة فقط يمكن إدراك أثرها، والمعلومة عبارة عن مجموعة من المفاهيم والحقائق التي لا يجوز تأويلها أو تفسيرها لا عن الأفراد ولا عن طريق الأنظمة الإلكترونية[1].

2_ التعريف الفقهي

لم يتفق الفقه على إيراد تسمية موحدة للجريمة المعلوماتية، فهناك من يطلق عليها تسمية "الجرائم الإلكترونية" وآخرون يطلقون عليها تسمية "جرائم المعلوماتية" وأيضا مسمى "جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال" أو "جرائم الكومبيوتر والأنترنت" أو "الجرائم المستحدثة"؛ وأيا كان المسمى الذي يطلق على الجريمة المعلوماتية، وإزاء التصدي لهذه الظاهرة، اجتهد الفقهاء والباحثون في علم الإجرام المعلوماتي لتقديم تعريفات دقيقة ووجيهة لها تختلف وتتباين باختلاف التشريعات والمدارس والمعايير والمناهج؛ فهناك من عرفها من جانب تقني فني وهناك من ركز على الجانب القانوني.

ومن بين هذه التعريفات، تعريف الفقيه "David Thomson" الذي عرفها بأنها:" أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"، وحسب هذا التعريف فإنه يشترط أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة من العلم بتكنولوجيا الحاسبات الآلية[2].

أما الفقيه"Ven De Merwe" الذي ركز في تعريفه لها على وسيلة ارتكابها، فإنه يرى بأن الجريمة المعلوماتية هي:" الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي." فالفقيه اشترط وجود الحاسب الآلي كونه أداة أو وسيلة ارتكاب الجريمة سواء وقعت عليه أم بواسطته.

كما يرى الأستاذ Trédman أن الجريمة المعلوماتية تشمل أي "جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات"؛ وفي هذا التعريف ربط Trédman الفعل غير المشروع في الجريمة بالنتيجة الناجمة عنه أو الفائدة المالية المتعلقة به[3].

---

[1] _صونيا مقري ووليد بن بلعامر، "المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي رقم20-05"، *مجلة البحوث في العقود وقانون الأعمال*، 2(2025):131،092281/article/en/dz.cerist.asjp://https .

[2] _ رمزي حوحو، منيرة بلورغي، مواجهة الجريمة المعلوماتية في الجزائر، *مجلة الحقوق والحريات*، ع.2 (2014): 42، https://asjp.cerist.dz/en/article/139253.

[3] _ رمزي حوحو، منيرة بلورغي، نفس المرجع السابق، 43.

وذهب الفقيه Rosenblatt إلى تعريفها بقوله:" هي كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والتي تعطله." وفي هذا الاتجاه حصر مفهوم الجريمة في الاعتداءات الماسة بالأنظمة المعلوماتية وهذا ذهبت إليه منظمة التعاون الاقتصادي في تعريفها لهذا النوع من الجرائم مبينة على أنها "كل سلوك غير مشروع أو غير مصرح به يتعلق بالمعالجة الآلية للمعطيات أو نقلها[1]."

ويعرف جانب آخر من الفقه الجريمة المعلوماتية بالنظر إلى نتيجة الاعتداء، إذ يرى الأستاذ الأمريكي Mass أن المقصود بالجريمة المعلوماتية يتمثل في الاعتداءات القانونية التي ترتكب بواسطة أجهزة الاتصال والمعلومات بغرض تحقيق الربح.

ويرى الأستاذ Parker أن الجريمة المعلوماتية هي:" كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية تنشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل." فالجريمة المعلوماتية هي كل فعل غير مشروع تقع بواسطة الحاسب الآلي أو عليه وتلحق إما ضررا بالمجني عليه أو ربحا ماديا للجاني.

ولقد عرفها الدكتور عبد الفتاح مراد على أنها:" جميع الأفعال المخالفة للقانون والشريعة التي تستلزم معرفة تامة بتقنيات الحاسب الآلي ونظم المعلومات سواء لارتكابها أو للتحقيق فيها والتي تتطلب توفر شبكة الأنترنت[2]." فهي جريمة تقنية يتم فيها الاعتداء على معطيات الحاسب الآلي المخزنة وعلى المعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الأنترنت.

كما يعرفها الأستاذ الدكتور جاسم محمد جندل بأنها:" كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة عالية بتقنية الحاسب الآلي، نظاما حاسوبيا أو شبكة حاسوبية للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة.[3]" فهي جريمة تشمل أي انتهاك أو اعتداء يتم على البيانات والمعلومات الرقمية بغرض التلاعب بها أو إتلافها، إذ لا يستهدف هذا النوع من الجرائم المستحدثة إلا البيانات والمعطيات والمعلومات الرقمية الموجودة على الحاسب الآلي.

---

[1] _أمال حابت، "الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 04-15 و09-04"، *مجلة هيرودوت للعلوم الإنسانية والاجتماعية* 7، ع.25(2023):56، https://asjp.cerist.dz/en/article/218900.

[2] _ محمد الشبلي العتوم، *جرائم تكنولوجيا المعلومات: النظرية العامة للجرائم الإلكترونية* (دار الثقافة للنشر والتوزيع،2021)،19.

[3] _جام محمد جندل، *الجرائم الإلكترونية* (دار المعتز للنشر والتوزيع، 2022)، 28.

وذهب بعض الفقهاء إلى القول بأن الجريمة المعلوماتية هي كل عمل أو امتناع يأتيه الإنسان اضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها، وفي ذلك الاتجاه يرى كل من Michel وCredo أن الجريمة المعلوماتية تسهل استخدام الحاسب الآلي كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته كما تمتد لتشمل الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به[1].

3_ تعريف الجريمة المعلوماتية في التشريع الجزائري والتشريعات المقارنة

مع الانتشار الواسع للجريمة المعلوماتية وتخطيها للحدود الوطنية للدول، أصبح لزاما التصدي لهذه الظاهرة التي أصبحت تهدد الأمن المعلوماتي والوطني في نفس الوقت، الأمر الذي أدى إلى ادخال مثل هذه الجرائم قي نطاق الأفعال المجرمة وتخصيص عقوبات تحد من تفاقمها وتوسعها. وبالتالي اتجهت العديد من التشريعات القانونية الدولية والوطنية إلى تعديل وتكييف قوانينها لتتماشى مع هذا النوع من الجرائم. ومن أول التشريعات التي أبدت اهتمامها بالجريمة المعلوماتية السويد، من خلال سنها لقانون البيانات الآلية السويدي سنة1973 المتعلق بجرائم الحاسب الآلي والإنترنت، ثم تلتها الولايات المتحدة الأمريكية بتشريعها أول قانون خاص متعلق بالجرائم الإلكترونية سنة 1985، ثم حذت حذوها العديد من التشريعات سواء الغربية أو العربية مؤخرا[2].

ومن بين هذه التشريعات التي عرفتها نذكر:

أ. الجريمة المعلوماتية في التشريع الأمريكي

لقد استند المشرع الأمريكي في تعريفه للجريمة المعلوماتية إلى كيفية ارتكابها وتكييفها القانوني حسب ما نص عليه القانون رقم 12-13 لسنة 1986 الخاص بمواجهة جرائم الكومبيوتر، إذ قام بتعريفها على أنها:" الاستخدام غير المصرح به لأنظمة الحاسب الآلي المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لها، وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة."

[1] _رمزي حوحو، أمينة بلورغي، مرجع سابق، 43.

[2] _محمد بن أحمد، "الأحكام القانونية لأركان الجريمة المعلوماتية: دراسة في التشريع الجزائري والمقارن"، *مجلة البحوث في الحقوق والعلوم السياسية* 10، 2(2024):5، https://asjp.cerist.dz/en/article/258272.

وأيضا عرفها مكتب التقنية التابع لوزارة العدل بالولايات المتحدة الأمريكية على أنها:" الجرائم التي تلعب فيها البيانات المعالجة آليا والبرامج المعلوماتية دورا أساسيا[1]"؛ فهي الجرائم المرتبطة بالحاسبات الآلية والأنظمة المتعلقة بها.

ب. الجريمة المعلوماتية في التشريع السعودي:

اهتم المشرع السعودي كغيره من التشريعات بالجرائم المعلوماتية، ويظهر ذلك بإصداره لنظام مكافحة الجرائم المعلوماتية بموجب المرسوم ملكي رقم م/17 الصادر في 26 مارس 2007، والذي ينص في المادة الأولى منه على أن الجريمة المعلوماتية هي:" أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام[2]." أي أنها أي فعل غير مشروع يرتكب باستخدام الحاسب الآلي مع توافر شبكة الأنترنت؛ وحتى لا يبقى أي لبس في المصطلحات والمفاهيم المتعلقة بهذه الجريمة المستحدثة أعطى مفهوما واضحا وصريحا للحاسب الآلي في نفس المادة إذ اعتبر هذا الأخير بأنه" أي جهاز ثابت أو منقول سلكي منقول أو لاسلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له."

ج. الجريمة المعلوماتية في التشريع الأردني

لقد اهتم المشرع الأردني كغيره من التشريعات بالجريمة المعلوماتية، من خلال تعريفه للمفاهيم المتعلقة بالجريمة المعلوماتية وذلك في قانون الجرائم الإلكترونية الأردني رقم27 لسنة 2015، والذي تم تعديله سنة 2023، فيذكر في المادة الثانية منه بأن[3]:

نظام المعلومات هو:" مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية."

[1] _ طاهر محمود أبو القاسم، مرجع سابق، 24.

[2] _المادة1، نظام مكافحة الجرائم المعلوماتية، المرسوم الملكي السعودي 2007، رقم(م/17)، قرار مجلس الوزراء 79، المؤرخ في 8ربيع الأول 1428 الموافق ل 26 مارس 2007.

[3] _ المادة 2، قانون الجرائم الإلكترونية الأردني لسنة 2023، رقم 17، ع.4338، ج.ر5843.

وأن البيانات هي كل "الأرقام أو الحروف أو الرموز أو الأشكال أو الأصوات أو الرسومات التي ليس لها دلالة بذاتها."

أما المعلومات فقد عرفها بأنها:" البيانات التي تمت معالجتها وأصبح لها دلالة."

كما عرف الشبكة المعلوماتية على أنها:" ارتباط بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها."

أما الموقع الإلكتروني فقد عرفه بأنه:" حيز لإتاحة المعلومات عبر الشبكة المعلوماتية من خلال عنوان محدد."

وما يلاحظ على المشرع الأردني أنه أيضا أعطى تعريفات واضحة للمفاهيم والمصطلحات المتصلة بالجريمة المعلوماتية لكيلا يحدث أي لبس أو تلاعب فيما يتعلق بهذه الجرائم؛ وما يستشف من هذه التعريفات أن الجريمة المعلوماتية هي نوع الجرائم الذي يمس نظام المعلومات أو البيانات المرتبطة بالحاسب الآلي والتي تستلزم وجود شبكة الاتصالات.

د. الجريمة المعلوماتية في التشريع المصري

نص المشرع المصري على تجريم الأفعال غير المشروعة المرتبطة بالمعلوماتية والتقنيات الإلكترونية في القانون رقم 175 المتعلق بمكافحة جرائم تقنية المعلومات الصادر في 14 أوت سنة 2018، إذ عمل على تعريف وتوضيح المصطلحات المتعلقة بهذا النوع من الجرائم المستحدثة في الباب الأول من هذا القانون والمعنون بالأحكام العامة، إذ عرف في المادة الأولى منه تقنية المعلومات بأنها[1]:" أي وسيلة مترابطة أو غير مترابطة تستخدم لتخزين واستخدام واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيا أو لاسلكيا." فهي مجموعة الوسائل المستعملة من أجل تخزين وتنظيم واسترجاع وحتى تطوير ومعالجة المعلومات الموجودة بالحاسب الآلي.

أما النظام المعلوماتي، فعرفه بأن:" مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية."

[1]_المادة 1، قانون مكافحة جرائم تقنية المعلومات لسنة 2018، رقم 175، ع.32 مكرر، ج. ر. ج. م. ع.3.

كما وضح مفهوم البرنامج المعلوماتي بقوله:" مجموعة الأوامر والتعليمات المعبر عنها بأي لغة أو رمز أو إشارة والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة، سواء كانت هذه الأوامر والتعليمات في شكلها الأصلي أو في شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي."

وكذلك بين معنى الشبكة المعلوماتية، فهي:" مجموعة من الأجهزة أو نظم المعلومات التي تكون مرتبطة معا، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها[1]."

ومنه يمكن استخلاص مفهوم الجريمة المعلوماتية أو كما سماها المشرع المصري "جرائم تقنية المعلومات" بأنها كل الأفعال المجرمة وغير المشروعة التي تمس نظام وبرامج المعلومات من تغيير وتعديل واستخدام وتزوير وغيرها وذلك بواسطة استعمال الحاسب الآلي وشبكة الاعلام والاتصال.

هـ. الجريمة المعلوماتية في التشريع الجزائري:

بالنسبة للمشرع الجزائري، الذي حذا حذو المشرع الفرنسي في تسمية الجرائم المعلوماتية "بجرائم المساس بأنظمة المعالجة الآلية للمعطيات"، تبنى مفهوما ضيقا للجريمة المعلوماتية من خلال القانون رقم 04-15 ومن ثم انتقل للمفهوم الأوسع من خلال القانون رقم 09-04.

لقد نصّ القانون رقم 04-15، المعدِّل والمتمِّم للأمر 66-155 المتضمّن قانون العقوبات، على إدراج قسم سابع مكرر تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات. وفي سنة 2006، أُدخل تعديل آخر على قانون العقوبات بموجب القانون رقم 06-23، غير أنّ هذا التعديل لم يتناول النصوص التجريمية المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، وإنما اقتصر على تشديد العقوبات المقررة لهذه الأفعال. ويُستفاد من هذا التدخل التشريعي أنّ المشرّع اعتبر المعطيات جوهر المجال المعلوماتي، باعتبارها العنصر الذي يُغذّي الحاسب الآلي، حيث تُعالج وتُخزَّن لتتحول إلى معلومات، وهو ما يفسّر تبنّيه لمصطلح المساس بأنظمة المعالجة الآلية للمعطيات، مع الإشارة إلى أنه عاد واستعمل مصطلح تكنولوجيا الإعلام والاتصال في تعديل آخر لقانون العقوبات سنة 2016[2]، فالمشرع لم يقدّم تعريفًا صريحًا لمفهوم المساس بأنظمة المعالجة الآلية للمعطيات. وإذا كان المقصود

[1] _المادة 1، القانون رقم 175، المتضمن مكافحة جرائم تقنية المعلومات.

[2] _أمال حابت، مرجع سابق، 54.

بالمساس هو الاعتداء، فإن أنظمة المعالجة الآلية للمعطيات تُفهم على أنها منظومة متكاملة من الآليات والإجراءات المنظمة التي تتيح جمع البيانات وتصنيفها وفرزها ومعالجتها، ثم تحويلها إلى معلومات قابلة للاسترجاع عند الحاجة. وتُستخدم هذه المعلومات من قبل الإنسان لإنجاز مهام معينة، أو لاتخاذ قرارات، أو لأداء وظائف مختلفة استنادًا إلى المعرفة المستمدة من النظام[1].

أما في القانون رقم 09-04 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بين وحدد المشرع المفاهيم المتعلقة بهذا النوع من الجرائم، كالتالي:

عرف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في الفقرة الأولى على أنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية."

وأيضا عرف المنظومة المعلوماتية في الفقرة الثانية منها على أنها:" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين." وهنا يتضح بأنها مجموعة متكاملة من النظم والبرمجيات المستخدمة في جمع البيانات ومعالجتها وتخزينها بشكل آلي وفق برامج محددة ما يتيح التبادل الفعال للمعلومات بين الأجهزة المختلفة داخل المؤسسة أو المنظمة.

بالإضافة إلى تعريفه للمعطيات المعلوماتية على أنها:" أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها."

كما بين مفهوم مقدم الخدمات على أنه:" أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية وأو نظام الاتصالات. وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها."

[1] _ أمال حابت، مرجع سابق، 54.

زيادة على ذلك عرف الاتصالات الإلكترونية على أنها:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية[1]."

ومن التعريفات السابقة يمكن استخلاص تعريف للجريمة المعلوماتية على أنها كل نشاط غير قانوني يتم في فضاءات رقمية باستغلال الحواسيب الآلية أو استهدافها في وجود شبكة الأنترنت لتحقيق أهداف مختلفة بقصد الإضرار أو الاستعمال غير المشروع.

الفرع الثاني: خصائص الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية من بين الجرائم المستحدثة التي أتى بها التطور التكنولوجي في مجال المعلومات والاتصالات والتي تتم في الفضاءات الرقمية على غرار الجرائم التقليدية التي تكون في العالم المادي، الأمر الذي أكسبها خصائص وسمات من حيث نطاق وقوعها وصفاتها، وصفات مرتكبيها، وأيضا الإجراءات القانونية المتعلقة بها.

1_ جريمة عابرة للحدود الوطنية (Transnational):

أتاح انتشار شبكة الاتصالات العالمية وربط الحواسيب بهذه الشبكات تعدي الجريمة المعلوماتية للحدود الجغرافية للقارات والدول، فالعالم كله يمكن أن يكون مسرحا لارتكاب هذا النوع من الجرائم، كما لا يحدها زمان معين رغم الاختلاف في المواقيت بين الدول. وهذا ما يثير في كثير من الأحيان تحديات قانونية تقنية وسياسية وإدارية بشأن مواجهتها حول تحديث الدولة صاحبة الاختصاص القضائي لهذه الجريمة وكذلك تحديد الواجب تطبيقه، بالإضافة إلى الإشكاليات المتعلقة بإجراءات الملاحقة القضائية وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام، ويعد ذلك من بين الأسباب التي تستدعي تفعيل التعاون الدولي من أجل مكافحتها[2].

[1] _ المادة 2، من القانون المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، رقم09-04، ع. 47، ج. ر. ج. ج. 5.

[2] _الطاهر ياكر، *الجرائم الإلكترونية: الأحكام الموضوعية والإجرائية –دراسة مقارنة–* (دار بلقيس، 2024)، 31.

2_ جريمة ناعمة (White-collar Crime):

تستهدف الجريمة المعلوماتية المعنويات لا الماديات، فهي جريمة ناعمة تتطلب جهدا ذهنيا محكما وتفكيرا علميا دقيقا مدروسا قائما على المعرفة التقنية المتقدمة بالحاسب الآلي والتعامل السليم المحكم بشبكة الأنترنت لا جهدا عضليا أو عنفا أو أسلحة لارتكابها كالجرائم التقليدية[1].

فعلى سبيل المثال الدخول غير المشروع للأنظمة أو الحسابات أو ما يسمى بالاختراق "Hacking" لا يتطلب أخذ جهاز الشخص الآخر عنوة أو اقتحام منزله بل يقتضي المعرفة التقنية الكافية لكيفية استغلال الثغرات الأمنية والخوارزميات وتجاوز أنظمة الحماية.

وكذلك الاحتيال الإلكتروني"Online Fraud" الذي لا يستدعي مقابلة الشخص وجها لوجه ولا حتى سؤاله عن المعلومات الشخصية الخاصة به وإنما إرسال روابط إلكترونية وهمية عبر مختلف وسائل التواصل الاجتماعي ما يمكن الجاني من الولوج إلى المعلومات الشخصية المتعلقة بالضحية المحمولة على جهازه الخاص.

3_ صعوبة الإثبات (Difficulty of Proof):

الأصل في الجريمة إقامة الدليل وإسناده إلى المتهم ولكن نظرا إلى التطورات العلمية الحاصلة وظهور ما يسمى بالدليل الرقمي يجعل إثبات هذا النوع من الجرائم أكثر صعوبة، لأن الجاني مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي ملموس يمكن فحصه، فالآثار المترتبة عنها مجرد أرقام تتغير في السجلات وهذا يصعب من إجراءات اكتشاف الجريمة ومعرفة مرتكبيها، فمعظم الجرائم المعلوماتية يتم اكتشافها بالصدفة أو بعد وقت طويل من ارتكابها[2].

ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها على أساس أنها تفتقر إلى الدليل المادي التقليدي كالبصمات، كما يصعب الاحتفاظ الفني بآثارها وإن وجدت فهي تحتاج إلى خبرة تقنية خاصة يتعذر على المحقق التقليدي نيلها أو التعامل معها لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع والتضليل بدس برامج أو حقن برمجيات ضارة أو وضع كلمات سرية ورموز وشفرات تعيق الوصول إلى الدليل وقد يلجأ مرتكبوها لتشفير التعليمات بحيث يستحيل إيجاد أي دليل يدينه[3]. إضافة إلى ضعف القضاء ورجال الشرطة فيما يخص الأمور التقنية وقلة معرفتهم بالأمور وعدم كفاية القوانين والتشريعات القائمة.

---

[1] _محمد أحمد جندل، مرجع سابق، 53.

[2] _محمد الشبلي العتوم، مرجع سابق، 27.

[3] _ الطاهر ياكر، مرجع سابق، 33.

4_ جريمة متعددة الأشكال والأهداف والدوافع:

تتجسد الجريمة المعلوماتية في أشكال عدة مثل التجسس الإلكتروني، الإرهاب الإلكتروني، القرصنة، والمواقع المتخصصة في القذف وتشويه سمعة الأفراد فضلا عن انتحال الشخصية وسرقة أو تدمير أمن البيانات، وغالبا ما تكون أهدافها إما أفراد طبيعيين أو معنويين(بنوك، شركات، حكومات، جامعات، مؤسسات مالية، منشآت عسكرية، محطات الأخبار والبورصات) بالإضافة إلى المؤسسات غير الحكومية، وتكون غالبا دوافع هذه الجرائم مختلفة فمنها الشخصي(الانتقام، الفضول، الربح المادي)، الإرهاب السيبراني أو التنظيمي (التنظيمات الحكومية وغير الحكومية)[1].

5. الامتناع عن التبليغ في الجرائم المعلوماتية (Omission to Report):

تميز الجريمة المعلوماتية بعدم الإبلاغ عنها من طرف الضحية أو المجني عليه. وهذا راجع إلى أن هذه الجرائم تمس خصوصية الأفراد، كما تمس الأشخاص المعنوية كالشركات حيث أنها تتخوف من أن تؤدي أعمال التحقيق التي تقوم بها إلى احتجاز حواسيبها وهذا ما يؤدي إلى خسائر مادية جراء ذلك التحقيق[2].

6. خصوصية المجرم المعلوماتي (The Privacy of Cybercriminal):

يتميز المجرم المعلوماتي عن المجرم العادي بعدة خصائص وسمات على رأسها الاحترافية والذكاء والكفاءة التقنية العالية. فالجرائم المعلوماتية لا تتم إلا من قبل أشخاص ذوي الخلفية العلمية والفنية التقنية العالية، بالإضافة إلى اتسامهم بمعدل ذكاء يؤهلهم إلى الدخول والتطوير والتعديل في الأنظمة الأمنية والمعلوماتية والقدرة على التهرب من المتابعة القانونية لصعوبة الإثبات والتتبع. والغالب أن ينتمي المجرم المعلوماتي إلى فئة العابثين مثل الهاكرز "hackers" الذين تتراوح أعمارهم ما بين 16سنة إلى 30 سنة أو الكراكرز" Crackers" الذين تتراوح أعمارهم ما بين 25سنة إلى 45 سنة[3].

---

[1] _دليلة خينش، *الجريمة الإلكترونية والأمن الاجتماعي* (ديوان المطبوعات الجزائرية،2023)، 28،29.

[2] –مقري صونيا وبن بلعامر وليد، "المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي رقم20–05 ، *مجلة البحوث في العقود وقانون الأعمال*، 2(2025):134، https://asjp.cerist.dz/en/article/281092.

[3] _محمد أحمد جندل، مرجع سابق، 65،66.

الفرع الثالث: أركان الجريمة المعلوماتية

تُعدّ الجريمة المعلوماتية من الظواهر الإجرامية الحديثة التي باتت تمسّ بمصالح حيوية مرتبطة بالمعطيات والأنظمة الرقمية. ورغم خصوصية هذا النوع من الجرائم من حيث الوسيلة والمحل، إلا أنّها لا تخرج عن الإطار العام للنظرية العامة للجريمة، التي لا تقوم إلا بتوافر جميع أركانها الأساسية والتي تتمثل في الركن الشرعي إذ سيتم تسليط الضوء عليه، ومن ثم الركن المادي والركن المعنوي.

أولا: الركن الشرعي

يقصد بالركن الشرعي للجريمة نص التجريم الذي يضفي على فعل القيام أو الامتناع عن الفعل صفته غير المشروعة. فالجريمة لم تكتسب وصفها كجريمة إلا منذ تقرير تجريمها بنص قانوني، وبدون نص التجريم يصبح فعل القيام أو الامتناع عن الفعل مشروعا مهما بدا ملوما أو مستنكرا من وجهة نظر الدين أو الأخلاق أو الأعراف الاجتماعية[1].

فالركن الشرعي أو ما يعرف "بمبدأ الشرعية الجنائية" أول وأهم ركن لقيام الجريمة، حيث لا يمكن تصور جريمة أو الحديث عنها من دون وجود ركنها الشرعي الذي يمثل النموذج القانوني والصفة غير المشروعة لفعل القيام أو الامتناع، إذ لا تقوم المساءلة الجنائية عنها إلا بوجود نص تجريم وعقاب؛ وهذا استنادا إلى القاعدة الشرعية أوما يعرف بمبدأ مشروعية التجريم والعقاب الذي يوجب عدم جواز العقاب عند انتفاء النص التشريعي، وسندا إلى أن القياس محصور في ميدان النصوص التجريمية الموضوعية [2].

وطبقا لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على أنه" لا جريمة ولا عقوبة أو تدبير أمن بغير قانون[3]"، جرم القانون رقم 04-15 بعض صور الجريمة المعلوماتية ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان " المساس بأنظمة المعاجلة الآلية للمعطيات" من الفصل الثالث المعنون " الجنايات والجنح ضد الأموال" من الباب الثاني المتعلق "بالجنايات والجنح ضد الأفراد" وذلك في المواد من 394مكرر إلى المادة 394 مكرر 7 من قانون العقوبات المعدل والمتمم[4].

[1] _محمد بن أحمد، مرجع سابق، 2.

[2] _ المرجع نفسه.

[3] _ المادة 1، القانون المعدل والمتمم لقانون العقوبات، رقم 04-15، ع. 71، ج.ر.ج.ج. 8.

[4] _ المواد 394 مكرر إلى 394مكرر7 من القانون رقم 04/15 المتضمن قانون العقوبات الجزائري المعدل والمتمم.

في حين جاء القانون 09-04 متضمنا للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها كجانب وقائي يحد من وقوع الجرائم المعلوماتية، من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتسجيل وتجميع محتواها في حينها والقيام بإجراءات التفتيش داخل المنظومة المعلوماتية. ولجوء المشرع إلى تقنين أو النص على مثل هذه الجرائم المستحدثة وجعلها في نطاق مبدأ الشرعية يمنع القاضي من اللجوء إلى القياس، بمعنى عدم جواز لجوء القاضي الجنائي إلى قياس فعل لم يرد نص على تجريمه على فعل ورد نص تجريمه، فيقرر القاضي الجنائي للأول عقوبة الثاني بسبب التشابه بين الفعلين[1].

ثانيا: الركن المادي

يقصد بالركن المادي للجريمة وجود فعل خارجي له طبيعة ملموسة تحركها الحواس، والركن المادي يعني بصورة خاصة الواقعة الإجرامية التي يتكون منها السلوك المادي الخارجي الذي ينص القانون على تجريمه، أي كل ما يدخل في كيان الجريمة وتكون له طبيعة مادية فتلمسه الحواس، وهو ضروري لقيامها إذ لا يعرف القانون جرائم بدون ركن مادي، ولذلك سماه البعض بماديات الجريمة[2]. فهو المظهر الخارجي لها وكيانها الظاهر، وهو الماديات المحسوسة في العالم الخارجي كما حددتها نصوص التجريم، فالقاعدة أنه " لا جريمة دون ركن مادي" أو "لا جريمة فعل"[3].

والجريمة المعلوماتية كغيرها من الجرائم لا بد لإثبات قيامها توافر الركن المادي، الذي يقوم على ثلاثة عناصر أساسية تتمثل في السلوك الإجرامي والنتيجة الإجرامية والعلاقة السببية التي تربط بينهما. غير أنّ التطبيق العملي يثير إشكالات خاصة تتعلق بطبيعة هذا الركن في مجال الجرائم المعلوماتية، حيث تكمن خصوصية هذه الإشكالية في ارتباط هذه الجرائم بأنظمة إلكترونية تتعرض للاعتداء أو الاستغلال بطرق غير مشروعة. وغالبًا ما يترتب عن هذا الاعتداء أو الاختراق أضرار مادية أو معنوية، قد تتجلى في إتلاف النظام المعلوماتي أو التلاعب بالبيانات والمعلومات[4]. وتأسيسا على ما تم ذكره فإن العناصر الأساسية لتوافر الركن المادي في الجريمة المعلوماتية هي:

---

[1] _ حمزة خضري وحمزة عشاش، "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، *مجلة الدراسات القانونية والسياسية* 6، 2(2020): 173، https://asjp.cerist.dz/en/article/116332.

[2] _الطاهرياكر، مرجع سابق، 39.

[3] _ حمزة خضري وحمزة عشاش، مرجع سابق، 174.

[4] _محمد بن أحمد، مرجع سابق،8.

1_ السلوك الإجرامي:

يقصد بالسلوك الإجرامي ذلك النشاط الذي يصدر عن إرادة الإنسان والذي يظهر في العالم الخارجي، وهو يأتي إما في شكل سلوك إيجابي يتمثل في فعل ينهى عنه القانون وإما في شكل سلوك سلبي ويتمثل في الامتناع عن القيام فعل يأمر به القانون.

والسلوك المادي في الجريمة المعلوماتية يتطلب وجود بيئة رقمية وجهاز حاسب آلي واتصال بشبكة الأنترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته؛ فالسلوك المادي يرتبط دائما بالمعلومات المخزنة على الحاسب الآلي أو النظام المعلوماتي، أي أنه لا بد من ضرورة استخدام الحاسب الآلي وسيطا لارتكاب هذا النوع من جرائم الوسيلة، كما يجب توافر التقنية العالية والمعرفة الكافية بتقنيات الحاسب من طرف مرتكبي الجريمة المعلوماتية، فهذا الاستخدام يعتبر جزء من السلوك المادي للجريمة المعلوماتية[1].

لكن مع صعوبة الجريمة المعلوماتية وصعوبة إثبات الركن المادي فيها خاصة أن الجريمة ترتكب عن طريق تدفق معلومات عبر نظم الحاسب الآلي والتي لا يمكن الإمساك بها ماديا فصعوبة المشكلة أن السلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب فتقوم معه الجريمة كما هو الحال في جرائم الاعتداء على الأموال العامة أو الخاصة[2].

ويضاف إلى فلسفة السلوك الإجرامي في الجرائم المعلوماتية هو تدارك المشرع المقارن حينما نص على هذا النوع من الجرائم والتي ترتكب عبر الحاسوب نجد المشرع يقرر صراحة عبارات تدل على ذلك ومنها:" إذا ارتكب الجريمة باستخدام الحاسوب..." أو عبارة "... باستخدام المعالجة الآلية للبيانات" ويكون المشرع بهذه الحالة مدركا للقيمة في ارتكاب أو الشروع في ارتكاب جريمة عبر الإنترنت أو باستخدام الحاسوب المرتبط بالأنترنت

مما تقدم نرى أن النشاط المادي يبنى على العلاقة التقنية بين مرتكب الجريمة المعلوماتية وبين الجهاز أو الآلة، وفي كيفية تحديد حدوث السلوك الإجرامي باستخدام الإنترنت والحاسوب، فاستخدام هذين الأخرين ليس هدفا بحد ذاته وإنما السعي لتحقيق الربح والفائدة[3].

[1] _ الطاهر ياكر، مرجع سابق، 40.

[2] _ محمد بن أحمد، مرجع سابق، 9.

[3] _ المرجع نفسه.

2_ النتيجة الإجرامية:

كان الفقه التقليدي يشترط لقيام الركن المادي في الجريمة تحقق نتيجة إجرامية ملموسة. غير أنّ الاتجاهات الحديثة في السياسة الجنائية لم تعد تربط قيام الجريمة دائمًا بتحقق هذه النتيجة، خاصة في طائفة من الجرائم التي يُطلق عليها جرائم الخطر، حيث يكفي مجرد تعريض المصلحة المحمية للخطر. ويُعدّ هذا التوجه واضحًا في مجال الجريمة المنظمة، كما كرّسته اتفاقية الأمم المتحدة لسنة 2000، التي أقرت تجريم مجرد الاتفاق على ارتكاب إحدى الجرائم المنصوص عليها، حتى في غياب تحقق النتيجة الإجرامية[1].

والنتيجة الإجرامية في الجرائم المعلوماتية تثير إشكالات تتعلق بتحديد زمان ومكان تحققها، ومدى امتدادها من العالم الافتراضي الرقمي إلى العالم المادي المحسوس، خاصةً في ظل طابعها العابر للحدود وما قد ينجم عنه من ضرر أو خطر يتجاوز الإقليم الذي وقع فيه الفعل، حيث يأخذ هذا الامتداد شكل العدوان على حق أو مصلحة قائمة ومشروعة في دولة أخرى أو دول متعددة[2]. وذلك مع الأخذ بالاعتبار أيضا أن هناك من الجرائم التي يكون لها وجود سواء عبر الأنترنت أو عبر الحاسب أي كل الجرائم التقنية التي لا يمتد أثرها إلى العالم المادي ويشمل ذلك بالطبع صعوبة اكتشافها وإقامة الدليل على ارتكابها.

3_ العلاقة السببية:

لا يكتمل الركن المادي للجريمة إلا بتوافر علاقة سببية تربط بين السلوك الإجرامي والنتيجة المترتبة عليه، بحيث تُنسب هذه النتيجة إلى ذلك السلوك. وفي حال انتفاء هذه العلاقة، تنتفي المسؤولية الجنائية. وعندما يشترط القانون تحقق نتيجة جرمية، فإن قيام هذه العلاقة يصبح ضروريًا لاستكمال عناصر الركن المادي، إذ تُسهم في تحديد نطاق المسؤولية واستبعادها متى انقطعت الصلة السببية بين الفعل والنتيجة[3].

ففي المفهوم القانوني، تتباين صلة السببية عن فكرة النية الإجرامية، حيث تعتبر السببية عنصرا في الركن المادي للجريمة، بينما تعتبر النية الإجرامية عنصرا في الركن المعنوي. فصلة السببية تستند إلى الخواص المادية للسلوك وتفعيله للنتيجة المحظورة قانونا، وينبغي بالتالي أن يؤخذ هذا الاختلاف في الاعتبار عند تحديد معيار المسؤولية القانونية.

---

[1] _ الطاهر ياكر، مرجع سابق، 41.

[2] _ محمد بن أحمد، مرجع سابق، 10.

[3] _ الطاهر ياكر، مرجع سابق، 41.

في جرائم الاعتداء على الحق أو المصلحة المعلوماتية عبر الإنترنت أو الحاسوب، يتحقق الركن المادي من خلال سلوك يتمثل في الولوج إلى الشبكة باستعمال الحاسوب ثم التعدي على خصوصية النظام. وتقوم علاقة السببية متى ثبت حدوث الضرر أو حتى مجرد الخطر. ويتجلى ذلك، مثلًا، في جرائم حيازة مواد الاستغلال الجنسي للأطفال المخزنة على جهاز أو منشورة عبر موقع إلكتروني، حيث تقوم الصلة السببية على الربط بين فعل الحيازة وبين أفعال الترويج أو العرض أو التداول. وعليه، فإن تحقق هذه الجرائم—سواء في صورتها التامة أو في مرحلة الشروع—يقتضي وجود رابطة سببية بين النشاط المادي والنتيجة المترتبة عليه[1].

ثالثا: الركن المعنوي

لا تقتصر الجريمة على كونها سلوكًا ماديًا وما يترتب عليه من نتائج، بل تنطوي أيضًا على بعد نفسي يتمثل في الركن المعنوي، إذ لا تنهض المسؤولية الجنائية بمجرد تحقق الفعل المادي. وإنما يستلزم ذلك توافر إرادة آثمة تُوجّه سلوك الجاني المخالف للقانون، بحيث تُشكّل هذه الإرادة حلقة الوصل بين الواقعة الإجرامية في صورتها المادية والشخص الذي صدرت عنه، والذي يُنسب إليه الفعل ويُسأل عنه قانونًا[2]؛ فهو التعبير عن الحالة الذهنية والنفسية للجاني، ويشكّل أساس قيام المسؤولية الجنائية لما يتضمنه من إسناد يبرّر حق الدولة في العقاب. ويمكن تعريفه بأنه الرابطة التي تصل بين الوقائع المادية للجريمة وشخصية مرتكبها، وهي التي يُبنى عليها استحقاق اللوم والعقاب. كما يتمثل في إرادة إجرامية تتجه إلى تحقيق سلوك غير مشروع، يحدّد القانون صوره وكيفية تحققه، وتتكوّن هذه الإرادة أساسًا من عنصر يتمثل في إرادة النشاط[3] ، ولذلك فالركن المعنوي هو الإرادة الآثمة للنفسية الإجرامية التي دفعت الجاني إلى اقتراف الجريمة، سواء كان الفعل الضار الذي ارتكبه الجاني صدر عن قصد عمد معبرا عن سوء نية أم مجرد فعل ضار صادر عن خطأ أو عن إهمال بدون تعمد.

ويُعدّ توافر الركن المعنوي في الجرائم المعلوماتية عنصرًا أساسيًا لفهم طبيعة السلوك الإجرامي وتكييفه قانونًا، غير أنّ تقدير هذا الركن يثير صعوبات عملية قد تعيق الوصول إلى الإدانة. وقد أُثير جدل فقهي وقضائي حول ما إذا كانت جريمة الدخول غير المشروع إلى النظام المعلوماتي تتطلب قصدًا عامًا أو خاصًا، وهو ما يستلزم تحليل ظروف الواقعة والحالة الذهنية للجاني.

[1]_ محمد بن أحمد، مرجع سابق، 12.

[2] _أبو القاسم، الجرائم المعلوماتية، 100.

[3]_ الطاهر ياكر، مرجع سابق، 42.

وقد اتجه القضاء المقارن بدايةً إلى اشتراط العمد في جريمة الولوج فقط، مما أثار انتقادات لعدم التمييز بين هذه الجريمة وغيرها من صور الاعتداء المعلوماتي. غير أنّ القضاء الفرنسي استقر لاحقًا على اعتماد فكرة "سوء النية" كمعيار جامع لتجريم الأفعال المعلوماتية، باعتبارها تعبيرًا عن قصد الإضرار والعدوان على النظام المعلوماتي، وهو ما أكده أيضًا تقنين البريد والاتصالات من خلال اشتراط احترام سرية الاتصالات، بما في ذلك البريد الإلكتروني، وعدم تطبيق النصوص العقابية إلا بتوافر هذا العنصر[1].

وقد يتخذ الركن المعنوي في الجريمة المعلوماتية إحدى الصورتين:

1_ الجريمة المعلوماتية كجريمة عمدية:

كان هناك تصور قديم بأن المجرم يتميز بالغباء والانحطاط الفكري والثقافي، الأمر الذي يجعله إنسانا معاديا للمجتمع، لكن سرعان ما تغير هذا التصور بتطور الجريمة وظهور جرائم غسيل الأموال والجرائم المعلوماتية بكافة أشكالها، فأصبح الكثير منا ينظر إلى المجرم المعلوماتي على أنه يتمتع بذكاء وثقافة وفكر، فالجريمة المعلوماتية تتطلب نصيبا من المعرفة التخصصية بالكومبيوتر والأنترنت، الأمر الذي لا يتوافر للجميع في مجتمعنا.

وكون الجريمة عمدية في الأصل إلا ما استثنى المشرع بنص خاص، فتكون الجريمة غير عمدية والجريمة المعلوماتية حسب المتصور لا تقع إلا بصورة عمدية يسبقها التفكير والتأمل في الحصول على المعلومات واختراق الكومبيوتر من أجل تحقيق هدف الجاني[2].

2_ الجريمة المعلوماتية كجريمة غير عمدية:

قد تقع الجريمة المعلوماتية على غير وجه العمد نتيجة الإهمال أو قلة الاحتياط أو عدم مراعاة القوانين والأنظمة. ويتحقق ذلك عندما تتجه إرادة الفاعل إلى مباشرة السلوك دون أن تنصرف إلى إحداث النتيجة الإجرامية. ومن الأمثلة على ذلك قيام شخص باستخدام أقراص مرنة (Flop Disk) أو أقراص مدمجة (CD) أو وحدات تخزين محمولة (Flash Memory) خاصة به، دون التأكد من خلوها من الفيروسات، مما يؤدي إلى نقلها إلى أجهزة العمل أو الشبكة والتسبب في إتلافها أو تعطيلها[3].

---

[1]_محمد بن أحمد، مرجع سابق، 13.

[2]_ محمود أبو القاسم، مرجع سابق، 100.

[3]_ المرجع نفسه.

المطلب الثاني: صور الجرائم المعلوماتية

تُعدّ الجرائم المعلوماتية من أبرز صور الإجرام المستحدث المرتبط بتطور تكنولوجيا المعلومات والاتصال، حيث لم تعد تقتصر على أنماط تقليدية، بل امتدت لتطال مختلف عناصر البيئة الرقمية وما يرتبط بها من برامج وأشخاص وأموال. ويُلاحظ أن هذا النوع من الجرائم يتسم بتعدد صوره وتنوع أساليبه تبعًا للمحل الذي ينصب عليه الاعتداء.

وعليه، سيتم التطرق إلى الجرائم الواقعة على البرامج من خلال **(الفرع الأول)** ومن ثم التعرض إلى صور الجرائم الواقعة على الأموال من خلال **(الفرع الثاني)**، وأخيرا سنتناول صور الجرائم الواقعة على الأشخاص من خلال **(الفرع الثالث)**.

الفرع الأول: الجرائم الواقعة على البرامج

يُقصد بالبرنامج الحاسوبي مجموعة من التعليمات المكتوبة بإحدى لغات البرمجة مثل Python وJava وC++ وSQL، بهدف تنفيذها على الحاسوب لإنجاز مهام محددة. وتزداد خطورة الجرائم المعلوماتية عندما يكون محلّها البرامج بدلاً من المكونات المادية للنظام المعلوماتي، نظرًا لما تتضمنه هذه البرامج من بيانات ومعلومات ذات قيمة. كما يتطلب هذا النوع من الجرائم مستوى عاليًا من المعرفة التقنية والفنية في مجال البرمجة، ومن بين صور الجرائم الواقعة على البرامج نميز:

أولا: الجرائم الواقعة على البرامج التطبيقية

تعد البرامج التطبيقية مجموعة البرمجيات المطورة خصيصا لخدمة حاجات المستخدم النهائية، حيث تمكنه من تنفيذ وظائف عملية متنوعة نحو معالجة النصوص والاتصال وتصفح الأنترنت وإدارة البيانات ضمن بيئة نظام التشغيل مثل: Microsoft Word، Microsoft Excel، Google Chrome، ...

وغالبا يقوم المجرم المعلوماتي بتعديل هذه البرامج والتلاعب فيها إما من أجل الاستفادة المادية.

1_ تعديل البرنامج:

إن الهدف الرئيسي من تعديل البرنامج هو اختلاس الأموال وينتشر هذا النوع من الجرائم في مجال الحسابات في الشركات على سبيل المثال[1]، إذ يقوم المبرمج بتعديل البرنامج الذي بإدارة صحيحة لحسابات المنشأة، التي

[1]_محمود أبو القاسم، مرجع سابق، 74.

تتضخم في فترات زمنية ببعض النفقات، ثم يقوم باستقطاع مبلغ زهيد كل شهر من الإيرادات، وقد استطاع من خلال هذا أن يحقق فائدة كبيرة من خلال الكسور المحسوبة بدقة، وتمكن من خلال ذلك في ست سنوات من اختلاس مليون دولار. وأيضا قيام مبرمج بإحدى الشركات الأمريكية بكتابة برنامج وإدخاله إلى حاسب الشركة مضمنا إياه حصيلتها على حسابه، مع تعديل استمارة المحاسبة الضريبية الخاصة به، بحيث لا يظهر فيها دخله الحقيقي، وقد تم اكتشاف الواقعة بناء على شكوى قدمت إلى قسم المرتبات بالشركة لعدم صحة استمارة المبرمج[1].

2_ التلاعب في البرنامج:

إن ارتباط أنظمة المعالجة الآلية للمعطيات بميادين عديدة وتزايد الاعتماد عليهما في مختلف التعاملات جعل الحالات التي يمكن ارتكاب جريمة التلاعب فيها لا حصر لها، وإن كانت تتفاوت فيما بينها من حيث مقدار الخسائر الناجمة عنها وعدد الحالات المرتكبة.

قد يصل الأمر بأحد المبرمجين ذي النوايا السيئة إلى زرع برنامج فرعي غير مسموح به في البرنامج الأصلي ويسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي.

ويمكن دفن هذا البرنامج الصغير في مكونات البرمجيات الخاصة بالمنشأة ولصغيرها ودقتها لا يتم رصدها إلا بالصدفة[2]

ثانيا: الجرائم الواقعة على برامج التشغيل

برامج التشغيل هي البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بضبط وتنظيم التعليمات الخاصة بالنظام أي أنها تشكل حلقة وصل بين مكونات الحاسب الآلي المادية والبرمجيات الأخرى المستخدمة في معالجة البيانات. والجريمة في هذه الحالة تتحقق بتزويد البرنامج بمجموعة التعليمات إضافية يسهل الوصول إليها بواسطة شفرة تتيح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي والتلاعب في هذه البرامج يتم بطريقتين[3]:

[1] _ محمود أبو القاسم، مرجع سابق،74.

[2] _محمد أحمد جندل، مرجع سابق، 49.

[3] _ المرجع نفسه.

1_ طريقة المداخل المميزة:

عند إعداد وتصميم البرامج المعلوماتية، قد يترك المبرمجون بعض المنافذ أو "الممرات المميزة" التي تسمح بالولوج إلى البنية البرمجية، بهدف معالجة الأخطاء التي قد تظهر أثناء الاستخدام ولم تكن مكتشفة في مرحلة التطوير. ويُفترض أن تُغلق هذه المنافذ في النسخة النهائية من البرنامج. غير أنّ بعض المبرمجين ذوي النوايا السيئة قد يتعمدون الإبقاء على هذه الثغرات واستغلالها لاحقًا، باعتبارهم على دراية بها وبأهميتها التقنية، مما يتيح لهم في أي وقت استخدامها كوسيلة غير مشروعة للوصول إلى النظام. ومن خلال هذه المداخل يمكن الولوج إلى البيانات المخزنة والاطلاع على الشيفرة والتعليمات، الأمر الذي يمكّن الفاعل من التحكم في النظام المعلوماتي، بما يترتب عنه من آثار إيجابية لصالحه وسلبية على المستخدم أو مالك النظام.

2_ طريقة اصطناع برنامج وهمي

تتمثل هذه الطريقة في تصميم وإنشاء برنامج وهمي يكون الغرض الأساسي منه التخطيط للجريمة ومراقبتها وتنفيذها أي يتم تصميم البرنامج خصيصا لارتكاب الغش المعلوماتي.

الفرع الثاني: الجرائم الواقعة على الأشخاص

إن للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، ومثال ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الاطلاع على البيانات والمعلومات الخاصة لشخص ما أو تسجيل مكالمات أو فيديو أو مراقبته.[1]

وهي الجرائم التي يتم الوصول فيها إلى الهوية الإلكترونية للأفراد بطرق غير مشروعة، كحسابات البريد الإلكتروني وكلمات السر التي تخصهم، وقد تصل إلى حد انتحال شخصياتهم وأخذ الصور والملفات المهمة من أجهزتهم بهدف ابتزازهم ومساهمتهم، وتسمى أيضا بجرائم الأنترنت الشخصية، التي يقوم المجرم من خلالها بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته والذي قد يكون فردا أو مؤسسة تجارية، وتتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة هذه الوسائل إنشاء موقع على الشبكة يحتوي على المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين، ويضم لهذه الجرائم

[1] _أسمهان بوضياف، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، 11(2018): 357، https://asjp.cerist.dz/en/article/81720.

كذلك تشويه السمعة، الشائعات والأخبار الكاذبة لمحاربة الرموز السياسية والفكرية وحتى الدينية من أجل تشكيك الناس في مصداقية هؤلاء الأفراد، وقد يكون الهدف من ذلك هو الابتزاز[1].

الفرع الثالث: الجرائم الواقعة على الأموال

مثلت الآليات والتقنيات المتطورة والوسائل الإلكترونية الحديثة فرصة أمام راغبي تنفيذ الجرائم المالية وجرائم عمليات غسل الأموال في تنفيذ المعاملات المالية والمدفوعات والتسويات، وذلك من خلال القيام بأنشطة غير مشروعة باستخدام الوسائل التكنولوجية الحديثة أو تنظيماتها أو تطبيقاتها، خاصة بعد انتشار استخدام الأنترنت في شتى أنحاء العالم، وتنامى استخدام نظم وأساليب وأدوات تنفيذ المعاملات المالية والمصرفية ونظم الدفع الإلكتروني استنادا على تلك التطبيقات والنظم، حيث أنها تتغلب على أكبر مشكلة تواجههم ألا وهي النقل المادي للمبالغ النقدية الكبيرة وإمكانية التعرف على مصادر وأصحاب الأموال، لذا يقوم غاسلوا الأموال بنقل وتحويل الأموال المتحصلة من الأنشطة غير المشروعة، وهو ما نتج عنه تزايد ملحوظ في استخدام الوسائل الإلكترونية من قبل المجموعات الإجرامية المنظمة في عمليات غسل الأموال.

وتشمل تلك الجرائم على العموم الكثير من الممارسات منها: إدخال بيانات غير صحيحة أو تعليمات من غير المشروع التصريح بها، أو استعمال بيانات وعمليات غير مسموح الوصول إليها بغية السرقة من قبل موظفين فاسدين في الشركات والمؤسسات المالية والاقتصادية وحذف أو تعديل المعلومات المحفوظة، أو إساءة استعمال أدوات الأنظمة المتوافرة وحِزم البرامج.

والاحتيال الإلكتروني يتخذ أشكال عديدة إلا أنها تهدف جميعا إلى حصول الجناة على مبالغ مالية بطريقة غير مشروعة من الضحايا، والتي قد تكون عن سرقة أرقام البطاقات الائتمانية أو دفع الضحية لإرسال حوالات مالية أو شيكات رقمية لإجراء عمليات شراء لمنتجات وهمية على الأنترنت أو دفعهم إلى الكشف عن معلومات شخصية متعلقة بحساباتهم البنكية والبطاقات المرتبطة بها عن طريق الرسائل النصية أو البريد الإلكتروني أو المتاجر الإلكترونية المشبوهة، والتي تؤدي في النهاية إلى تمكن الجناة من خداع الضحايا عن طريق الاستخدام غير المصرح أو غير المشروع لبيانات البطاقات الائتمانية[2].

[1] _ الطاهر ياكر، مرجع سابق، 23.

[2] _المرجع نفسه، 22،23.

لقد صاحب ظهور شبكة الأنترنت تطورات كثيرة في شتى المجلات، حيث أصبحت معظم المعاملات التجارية تتم من خلالها، مما انجر عنه تطور وسائل الدفع والوفاء وأضحى جزء لا يتجزأ من هذه المعاملات، وفي خضم هذا التداول المالي عبر الأنترنت انتهز بعض المجرمين الفرصة من أجل السطو عليها، حيث ابتكرت عدة طرق من أجل ذلك، على غرار السطو والسرقة والتحويل الإلكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة، إلى جانب تزييف العملة وتزوير في محررات رسمية والاختلاس والدخول غير المشروع للبيانات والمعلومات المخزنة عن الحاسب والجرائم الواقع [1].

المبحث الثاني: الإطار القانوني لعميات البحث والتحري على الجرائم المعلوماتية

شهد العالم تطورا تكنولوجيا أدى إلى ظهور الجرائم المعلوماتية، التي تتميز بخصوصيتها التقنية وصعوبة اكتشافها مقارنة بالجرائم التقليدية، مما استدعى تكييف القواعد القانونية لمواجهتها، خاصة في مجال البحث والتحري.

وفي هذا السياق، برزت الحاجة إلى وضع إطار قانوني منظم لعمليات البحث والتحري عن الجرائم المعلوماتية بشكل يوازن بين فعالية السلطات المختصة في الكشف عنها، واحترام الحقوق والحريات الأساسية للأفراد، لاسيما الحق في الخصوصية وحماية المعطيات الشخصية. كما يتطلب هذا الإطار اعتماد وسائل إجرائية وتقنية حديثة، مثل المراقبة الإلكترونية واعتراض الاتصالات الرقمية، في حدود ما يسمح به القانون.

وعليه، يهدف هذا المبحث إلى تسليط الضوء على التكريس القانوني لسلطة البحث والتحري على الجرائم المعلوماتية وذلك من خلال **(المطلب الأول)** أين سيتم تناول سلطة البحث والتحري في ظل القوانين العامة والقوانين الخاصة؛ ومن ثم استعراض صعوبات البحث والتحري عن هذه الجرائم المستحدثة من خلال **(المطلب الثاني)** المرتبطة بالمنظومة القانونية والمادية وكذا الموارد البشرية.

المطلب الأول: التكريس القانوني لسلطة البحث والتحري عن الجرائم المعلوماتية

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام المعلوماتي وما يصاحبها من أضرار معتبرة على الأفراد ومؤسسات الدولة من جهة، ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد منذ الألفية الثانية إلى وضع نصوص قانونية تتعلق بمواجهة هذا النوع من الجرائم الخطيرة والمعقدة، وذلك من خلال تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع

[1] _ أسمهان بوضياف، مرجع سابق، 358.

التطورات الإجرامية في مجال تكنولوجية الإعلام والاتصال، وقام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات التي تتم عبر شبكة الأنترنت[1].

وعليه، سنتناول تكريس المشرع الجزائري لسلطة البحث والتحري عن الجرائم المعلوماتية في ظل القوانين العامة كقانون الإجراءات الجزائية وقانون العقوبات من خلال **(الفرع الأول)**، ومن ثم تكريسه لهذه السلطة في ظل القوانين الخاصة من خلال **(الفرع الثاني)**.

الفرع الأول: تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل القوانين العامة

حاول المشرع الجزائري إصدار قوانين عامة وخاصة وهياكل للتصدي للجرائم المستحدثة، فهناك جهود معتبرة قام بها المشرع الجزائري في محاربة قراصنة الأنترنت وإحالتهم قانونا على المحاكم، متأثرا بجل الدول العربية التي وضعت قوانين لمكافحة هذا النوع من الجرائم المستحدثة.

وعليه، سيتم التطرق إلى تكريس الجهود القانونية في ظل قانون الإجراءات الجزائري، ومن ثم سنتناول تكريسه للجهود القانونية في ظل قانون العقوبات.

أولا: تكريس سلطة البحث والتحري في ظل قانون الإجراءات الجزائية

قام المشرّع الجزائري بإخضاع قانون الإجراءات الجزائية لعدة تعديلات، من خلال إدراج آليات حديثة في مجال البحث والتحري والتحقيق، خاصة فيما يتعلق بالجرائم المستحدثة، وعلى وجه الخصوص الإجرام المعلوماتي، وذلك من خلال اعتماد وسائل تحقيق تتماشى مع البيئة الرقمية، مع الحفاظ على الضمانات القانونية. ورغم خصوصية هذا النوع من الجرائم، إلا أن متابعته تتم وفق الإجراءات التقليدية كالتفتيش والمعاينة والاستجواب، مع تكييفها بما يتلاءم مع طبيعة الدليل الرقمي[2].

وقد أوضح المشرّع خصوصية التفتيش في المجال المعلوماتي، مميزًا إياه عن التفتيش التقليدي من حيث إجراءاته وشروطه، بحيث لا تخضع هذه الجرائم لأحكام المادة 44، فأورد المشرع استثناءات تخص هذه الجرائم المستحدثة، فأجاز دخول المساكن وتفتيشها في أي وقت دون التقيد بالميقات القانوني في حالات التلبس. كما خفّف من بعض

[1] _أسمهان بوضياف، مرجع سابق، 360.

[2] _أحمد بن مالك، "خصوصية الجريمة المعلوماتية وسبل مكافحتها في التشريع الجزائري"، *المجلة الجزائرية للحقوق والعلوم السياسية* 8، 1(2023): 955، https://asjp.cerist.dz/en/article/222122.

الشروط الشكلية، إذ لا يُشترط رضا المعني بالتفتيش في الجرائم المعلوماتية، بل يكفي الإذن القضائي مع حضور شاهدين. وتمتد هذه الاستثناءات كذلك إلى مرحلة التحقيق الابتدائي، بإحالة النصوص القانونية ذات الصلة[1]. مع التنصيص على توقيف النظر في جريمة المساس بأنظمة المعالجة الآلية للمعطيات وفقًا للمادة 51 فقرة 06 من قانون الإجراءات الجزائية.

كما نص المشرّع الجزائري صراحة على تمديد الاختصاص المحلي لوكيل الجمهورية طبقًا للمادة 28 الفقرة 3 من قانون الإجراءات الجزائية رقم 25-14، إذ يهتم وكيل الجمهورية بالنظر في الجرائم الموصوفة في التشريع الجزائري على رأسها جرائم المساس بأنظمة المعالجة الآلية للمعطيات[2].

ورغم هذه الجهود التشريعية، إلا أن بعض الدراسات ترى أن هذه النصوص لا تزال غير كافية لمواكبة التطور السريع للجريمة المعلوماتية، الأمر الذي يستدعي تعزيز الإطار الإجرائي وتطوير وسائل التحري الحديثة فيما يتعلق بهذا النوع من الجرائم المستحدثة.

ثانيا: تكريس سلطة البحث والتحري في ظل قانون العقوبات الجزائري

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر 22-15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم 8 مواد من المادة 394 مكرر إلى المادة 394 مكرر 7.

وبغرض تدارك الفراغ القانوني، فقد قام المشرع الجزائري بموجب هذا القانون باستحداث جملة من النصوص التي تجرم الأفعال المتصلة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها ما يقابله من الجزاء، إذ قام المشرع بسن جملة من القواعد القانونية الموضوعية والتي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة[3].

---

[1] _ أحمد بن مالك، مرجع سابق، 955.

[2] _عائشة عبد الحميد، "الجرائم المعلوماتية وكيفية مكافحتها"، *مجلة الإناسة وعلوم المجتمع*، 7(جويلية 2020): 132، https://asjp.cerist.dz/en/article/165503.

[3] _أسمهان بوضياف، مرجع سابق، 363.

إذ نصت المادة 394 مكرر من القانون 04_15 على العقوبة بالحبس من 3 أشهر إلى سنة وبغرامة من 50000 إلى 100000دج لفعل الدخول أو البقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات، وإذا نتج عنها تخريب نظام اشتغال المنظومة تضاعف العقوبة بالحبس من 6أشهر إلى سنتين وبغرامة من 50000 إلى 150000دج، ولذلك مهما كانت طبيعة المعلوماتية يمكن أن تندرج ضمن هذه الاعتداءات التي تمس ببعض صور الحياة الخاصة للأفراد[1].

كما نصت المادة 394 مكرر 2 على تجريم بعض الأفعال وأقرت لها عقوبات خاصة بها منها:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المتعلقة بالمعالجة الآلية لمعطيات.

تُقرّ المادة 394 مكرر 6 بأنه، إضافةً إلى العقوبات الأصلية المتمثلة في الحبس والغرامة، ومع مراعاة حقوق الغير حسن النية، يجوز للقاضي الحكم بعقوبات تكميلية. وتشمل هذه العقوبات مصادرة الأجهزة والبرامج والوسائل المستعملة في ارتكاب الجريمة، فضلاً عن غلق المواقع الإلكترونية التي كانت محلاً لارتكاب الأفعال المجرّمة وفقاً لأحكام هذا القسم. كما يمكن الحكم بإغلاق المحل أو مكان الاستغلال إذا ثبت أن الجريمة قد ارتُكبت بعلم مالكه.[2].

الفرع الثاني: تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل القوانين الخاصة

إلى جانب الأحكام العامة التي جاء بها قانون الإجراءات الجزائية، لم يكتفِ المشرّع الجزائري بها لمواجهة خصوصية الجرائم المعلوماتية، بل عمد إلى تدعيمها بنصوص خاصة تُكرّس وتوسّع من سلطات البحث والتحري. ويأتي ذلك بالنظر إلى الطبيعة التقنية المعقدة لهذه الجرائم وصعوبة كشفها وإثباتها بالوسائل التقليدية، مما استوجب إقرار آليات إجرائية أكثر مرونة وفعالية.

وعليه، فإن القوانين الخاصة، من بينها قانون الإعلام رقم 12-05 والقانون رقم 03_05 المتعلق بحقوق المؤلف والحقوق المجاورة، وهو ما سيتم تناوله أولا، وكذلك قانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام

[1]_ المادة 394 مكرر، من القانون رقم 04_15 المتضمن قانون العقوبات الجزائري المعدل والمتمم.

[2]_أسمهان بوضياف، مرجع سابق، 363.

والاتصال الذي سيتم تسليط الضوء عليه ثانيا، تمثل إطارًا مكملًا يعزز من فعالية أجهزة الضبطية القضائية والسلطات المختصة في تتبع هذا النوع من الإجرام.

أولا: تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل قانون الإعلام والقانون رقم 03_05

1_ تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل قانون الإعلام رقم23-14:

تتجلى إرادة المشرع الجزائري في ضبط الحقل الإعلامي ضمن البيئة الرقمية من خلال إقرار منظومة ردعية بموجب القانون العضوي رقم 23-14 المتعلق بالإعلام، تهدف أساساً إلى إيجاد توازن موضوعي بين ممارسة حرية الصحافة الإلكترونية ومقتضيات حماية حرمة الحياة الخاصة وسير العدالة في ظل سرعة التداول المعلوماتي عبر الشبكات. وفي هذا السياق، نصت المادة 29 من هذا القانون على حظر نشر أو بث أي محتوى رقمي عبر الوسائط الإلكترونية والمواقع الإخبارية من شأنه الإضرار بسرية التحقيق الابتدائي أو الكشف عن فحوى المداولات القضائية، كما مدد نطاق التجريم ليشمل بث التقارير الإعلامية الرقمية المتعلقة بقضايا الحالة الشخصية أو الإجهاض لما تنطوي عليه من حساسية اجتماعية تستوجب الكتمان[1].

وعلاوة على ذلك، شدد المشرع على منع استخدام التقنيات الرقمية والصور والرسوم لإعادة تمثيل ظروف الجنايات والجنح المنصوص عليها في قانون العقوبات (المواد 255-263 مكرر، و333-342) تفادياً للمساس بوقار العدالة أو انتهاك حرمة الأشخاص، مع تكريس المسؤولية الجزائية لمديري النشر في الصحافة الإلكترونية عن كل محتوى يُبث بالمخالفة لهذه الضوابط، مما يجعل الفضاء الرقمي مجالاً تطبيقياً كاملاً لقواعد الحماية الجنائية[2].

2_ تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل القانون رقم 05-03:

كرّس المشرّع الجزائري الحماية القانونية للمصنفات الرقمية من خلال الاعتراف الصريح بوصف المصنف الفكري لمعطيات الحاسب الآلي، وذلك بموجب القانون رقم 05-03 المتعلق بحقوق المؤلف والحقوق المجاورة. وقد تجلّى هذا التوجه في توسيع نطاق المؤلفات المحمية ليشمل البرامج المعلوماتية وقواعد البيانات، باعتبارها نتاجًا ذهنيًا يستحق الحماية شأنه شأن المصنفات التقليدية[3].

---

[1]-القانون العضوي رقم 23-14، المتعلق بالإعلام، ع.56، ج ر ج ج.9.

[2]- القانون رقم 04/15 المتضمن قانون العقوبات الجزائري المعدل والمتمم.

[3]_أحمد بن مالك، مرجع سابق، 953.

وفي هذا الإطار، أقرّ المشرّع حماية مزدوجة لهذه المصنفات، تشمل الحقوق الأدبية المرتبطة بشخصية المؤلف، والحقوق المالية التي تخوّله استغلال مصنفه ومنع الغير من استعماله دون ترخيص. كما اعتبر أن كل اعتداء على هذه الحقوق، سواء عن طريق النسخ غير المشروع أو الاستغلال دون إذن، يندرج ضمن أفعال التقليد المنصوص عليها في المادة 151 من القانون المذكور.

ولم يكتف المشرّع بالتجريم فقط، بل دعم هذه الحماية بجزاءات ردعية، حيث أخضع هذه الأفعال للعقوبات المقرّرة في المواد 153 و154 و158 من نفس القانون، بما يعكس حرصه على توفير حماية جزائية فعالة للمصنفات الرقمية في مواجهة الاعتداءات المتزايدة في البيئة المعلوماتية[1].

ثانيا: تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل قانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال رقم09-04:

لم يخرج المشرع الجزائري عن الإطار العام للقواعد الإجرائية المنصوص عليها في قانون الإجراءات الجزائية، غير أنه سعى إلى تكييفها بما يتلاءم مع خصوصية الجريمة المعلوماتية، من خلال إقرار قواعد إجرائية ذات طابع خاص تستجيب للتطور التكنولوجي المتسارع الذي يشهده هذا النوع من الإجرام.

وفي هذا السياق، جاء القانون رقم 09-04 ليكرّس جملة من الآليات الحديثة في مجال البحث والتحري، حيث نصّت المادة 04 منه على اتخاذ تدابير تقنية تفرضها ضرورات التحريات والتحقيقات القضائية، والتي تتمثل أساسًا في مراقبة الاتصالات الإلكترونية، وجمعها وتسجيلها، إضافة إلى إجراء عمليات التفتيش والحجز داخل المنظومات المعلوماتية[2]. كما كرس بموجب نفس إطارًا إجرائيًا خاصًا لمراقبة الاتصالات الإلكترونية، حيث أجاز، استثناءً من مبدأ سرية المراسلات، اللجوء إلى ترتيبات تقنية لمراقبة الاتصالات متى اقتضت ذلك ضرورات حماية النظام العام أو متطلبات التحريات والتحقيقات القضائية. كما حدّد هذا القانون حالات اللجوء إلى هذه الوسائل، لاسيما في مجال مكافحة الجرائم الخطيرة كالإرهاب والاعتداءات الماسة بأمن الدولة، أو عند وجود تهديدات تستهدف المنظومات المعلوماتية[3].

---

[1] _فتحي بن جديد،" حماية برامج الحاسوب بين قانون حقوق المؤلف الجزائري والاتفاقات الدولية"، *مجلة صوت القانون*9، 2(2023):596، https://asjp.cerist.dz/en/article/221469.

[2] _ وهيبة رابح، مرجع سابق، 325.

[3] _وردة شرف الدين، " مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية – في التشريع الجزائري–"، *مجلة المفكر* 10، 2(2017):547، https://asjp.cerist.dz/en/article/62283.

وفي المقابل، لم يترك المشرّع هذه الصلاحيات دون قيود، إذ أخضعها لرقابة قضائية صارمة، من خلال اشتراط الإذن المسبق من الجهات القضائية المختصة، وتحديد مدة المراقبة، وكذا حصر استعمال المعطيات في الأغراض الأمنية المحددة قانونًا. وهو ما يعكس محاولة تحقيق التوازن بين فعالية البحث والتحري في الجرائم المعلوماتية وضمان حماية الحياة الخاصة للأفراد[1].

غير أن هذا التوازن يظل نسبيًا من الناحية التطبيقية، في ظل اتساع نطاق السلطة التقديرية للجهات المختصة وغموض بعض المفاهيم التقنية، مما قد يفتح المجال أمام تأويلات تمسّ بجوهر الحق في الخصوصية، الأمر الذي يستدعي إعادة ضبط هذه الآليات بضمانات أكثر دقة وصرامة تكفل رقابة فعلية على ممارستها.

المطلب الثاني: صعوبات البحث والتحري عن الجرائم المعلوماتية

رغم الجهود التي بذلها المشرّع الجزائري في تكريس سلطات البحث والتحري وتدعيمها بآليات قانونية وتقنية لمواجهة الجرائم المعلوماتية، إلا أن هذه الأخيرة تطرح جملة من الصعوبات والتحديات التي تعيق الكشف عنها وإثباتها. ويعود ذلك إلى خصائصها التي تجعل الإجراءات التقليدية في كثير من الأحيان غير كافية أو فعالة.

وعليه، سيتم الوقوف عند أبرز الصعوبات القانونية المتعلقة بالبحث والتحري عن الجرائم المعلوماتية من خلال **(الفرع الأول)**، ومن ثم تناول الصعوبات المادية من خلال **(الفرع الثاني)**، ثم ستوضح الصعوبات المتعلقة بالموارد البشرية في **(الفرع الثالث)**.

الفرع الأول: الصعوبات المرتبطة بالمنظومة القانونية

تطرح الجرائم المعلوماتية تحديات قانونية متزايدة، نتيجة التطور السريع للتكنولوجيا مقارنة بوتيرة تطور النصوص التشريعية. ورغم سعي المشرّع الجزائري إلى تكييف المنظومة القانونية مع هذا النوع من الإجرام، من خلال إدراج نصوص خاصة وتعديل قواعد الإجراءات الجزائية، إلا أن هذه الجهود لا تخلو من نقائص تؤثر على فعالية البحث والتحري. وعليه، سيتم الوقوف في هذا الفرع على أبرز الصعوبات المرتبطة بالمنظومة القانونية.

أولا: عدم ملاءمة القواعد الإجرائية التقليدية لطبيعة الجرائم المعلوماتية

[1]_وردة شرف الدين، نفس المرجع السابق، 448.

ومن بين أهم هذه الصعوبات، عدم ملاءمة القواعد الإجرائية التقليدية لطبيعة الجرائم المعلوماتية، حيث وُضعت هذه القواعد أساسًا لمعالجة الجرائم التقليدية ذات الطابع المادي، مما يجعل تطبيقها على الجرائم الرقمية التي تتم في بيئة افتراضية أمرًا معقدًا. فالإجراءات المتعلقة بالبحث والتحري كالتفتيش والمعاينة، رغم أهميتها، تحتاج إلى تكييف يتماشى مع خصوصية الدليل الرقمي، الذي يتميز بعدم ماديته وقابليته للتغيير أو الإتلاف بسهولة[1].

ومن جهة أخرى، تطرح الجرائم المعلوماتية إشكالية الاختصاص القضائي، بالنظر إلى طابعها العابر للحدود، حيث يمكن أن تُرتكب الجريمة في دولة، ويكون أثرها في دولة أخرى، بينما يتواجد الفاعل في مكان مختلف. وهذا ما يثير صعوبات في تحديد الجهة القضائية المختصة، ويستدعي تعزيز آليات التعاون الدولي لمواجهة هذا النوع من الإجرام[2].

ثانيا: إشكالات الإثبات بالدليل الرقمي

كما تبرز إشكالية الإثبات الجنائي كأحد أهم التحديات القانونية، إذ يطرح الدليل الرقمي صعوبات تتعلق بمدى حجيته وإمكانية الاعتماد عليه أمام الجهات القضائية. فغياب إطار قانوني دقيق ينظم طرق جمع هذا النوع من الأدلة وحفظها قد يؤدي إلى الطعن في مشروعيتها، مما يؤثر سلبًا على فعالية المتابعة الجزائية[3].

تعتبر إجراءات استخلاص الدليل الجزائي الرقمي في الجرائم المعلوماتية خاصة بطبيعتها، فهناك العديد من الصعوبات التي تعترض الجهات المختصة بالبحث والتحري والتحقيق ولعل أهم تلك الصعوبات ارتكاب هذه الجرائم في بيئة إلكترونية وأنظمة معلومات مرتبطة بشبكة الأنترنت، كما أن محلها هو معلومات أو جرائم تتعلق بأشخاص عبر عالم غير محدود وغير متناهي، الشيء الذي يضفي عليها طابع خاص في طريقة ووسيلة الإعداد لها وتنفيذها[4]، فطبيعته التقنية الهشة وقابليته للتغيير أو الإتلاف بفعل التدخلات آلية أو البشرية، تعيق عملية جمعه وحفظه في صورته الأصلية. فامتيازه بطابعه اللامادي والعابر للحدود يطرح تحديات إضافية، خاصة فيما يتعلق

---

[1] _بثينة حبيباتي، " معوقات مكافحة الجريمة المعلوماتية"، *مجلة العلوم الإنسانية*، 50(ديسمبر 2018):86، https://revue.umc.edu.dz/h/article/view/2827/2973.

[2] _مريم عراب، "الاختصاص القضائي في الجرائم المعلوماتية"، *حوليات كلية الحقوق والعلوم السياسية* 7، 3(2015): 285،286، https://asjp.cerist.dz/en/article/80969.

[3] _خالد ضو، "حجيّة الدليل الإلكتروني وشروط قبوله في الإثبات الجنائي"، *مجلة الباحث الأكاديمي في العلوم القانونية والسياسية*5، 8(2022): 206، https://asjp.cerist.dz/en/article/183140.

[4] _ الطاهر ياكر، مرجع سابق، 149.

بتحديد مكان وجوده وتتبع مساره، وهو ما يفرض على أجهزة البحث والتحري الاعتماد على وسائل تقنية متطورة وتعاون دولي فعال[1]

ثالثا: تحديات تحقيق التوازن بين متطلبات البحث والتحري والحق في الخصوصية

وأخيرا، تبرز صعوبة تحقيق التوازن بين متطلبات البحث والتحري من جهة، وضمان حماية الحقوق والحريات الأساسية من جهة أخرى، خاصة فيما يتعلق بالحق في الخصوصية وسرية الاتصالات. فاستعمال وسائل التحري الحديثة، كالمراقبة الإلكترونية واعتراض الاتصالات، يقتضي إخضاعها لضوابط قانونية دقيقة لتفادي أي تعسف في استعمال السلطة[2].

الفرع الثاني: الصعوبات المادية

إلى جانب الصعوبات القانونية التي تعترض البحث والتحري في الجرائم المعلوماتية، تبرز صعوبات مادية وتقنية لا تقل أهمية، ترتبط أساسًا بخصوصية البيئة الرقمية وتعقيدها. فطبيعة هذا النوع من الجرائم تستلزم وسائل تقنية متطورة وإمكانيات مادية كبيرة لمواكبة أساليب الإجرام الحديثة، وهو ما يشكّل تحديًا حقيقيًا أمام الجهات المختصة. وعليه، سيتم في هذا الفرع إبراز أهم الصعوبات المادية المرتبطة بعمليات البحث والتحري في الجرائم المعلوماتية.

- **نقص التجهيزات التقنية المتطورة:** حيث تتطلب عملية تتبع الجرائم المعلوماتية أدوات وبرمجيات حديثة لتحليل البيانات الرقمية واستخراج الأدلة، وهي غالبا مكلفة وغير متوفرة بالشكل الكافي.
- **اعتماد تقنيات التشفير المتقدمة:** مثل التشفير من طرف إلى طرف(End-to-End Encryption) ، الذي يحول دون اعتراض محتوى الاتصالات أو الاطلاع عليها حتى من قبل مزودي الخدمة. كما تساهم بعض الخصائص الحديثة في تطبيقات الاتصال، مثل وضع الاختفاء (Vanish Mode) والرسائل ذاتية التدمير(Self-Destructing Messages) ، في محو الآثار الرقمية بشكل تلقائي، مما يصعّب عملية التتبع والتحليل الجنائي الرقمي.

[1]_ صهيب سهيل غازي زامل، "البحث والتحري عن الدليل الإلكتروني في المسائل الجزائية _دراسة حالة_"، (أطروحة دكتوراه، جامعة وهران2،سنة 2020_2021):44.

[2]_ وردة شرف الدين، مرجع سابق، 548.

- **استخدام مختلف الأدوات والتقنيات:** مثل استخدام أدوات إخفاء الهوية (Anonymity tools) التي تتيح للمستخدمين إخفاء هوياتهم الحقيقية وعناوينهم الإلكترونية، إلى جانب التشفير على مستوى الجهاز (Device Encryption)الذي يمنع الوصول إلى البيانات المخزنة حتى في حالة حجز الأجهزة. كما يشكل التخزين السحابي المشفر (Encrypted Cloud Storage) عائقًا إضافيًا، خاصة عندما تكون البيانات موزعة عبر خوادم متعددة وخاضعة لسياسات قانونية مختلفة. ولا يقلّ تعقيدًا عن ذلك خاصية حذف الحساب أو البيانات عن بعد(Remote Wipe) ، التي تمكّن الجناة من طمس الأدلة بشكل نهائي قبل وصول الجهات المختصة إليها.

وعلاوة على ما سبق، تبرز صعوبات أخرى مرتبطة باستخدام المواقع والخدمات الرقمية المتاحة عبر الشبكة المظلمة أو ما يُعرف بالأنترنت المجهول، مثل Tor و I2PاوFreenet، إضافة إلى أنظمة التشغيل المتخصصة في إخفاء الهوية مثل Tails OS وWho nix، حيث توفر هذه التقنيات مستويات عالية من السرية وإخفاء الهوية، مما يزيد من تعقيد عمليات التتبع وجمع الأدلة الرقمية، ويشكّل تحديًا حقيقيًا أمام الأجهزة الأمنية والقضائية.

وعليه، يتضح أنّ الصعوبات المادية في الجرائم المعلوماتية، كالتشفير وإخفاء الهوية ومحو البيانات، تعيق بشكل كبير عملية جمع الأدلة الرقمية والتحقيق فيها. وعليه، فإن تجاوز هذه التحديات يتطلب تطوير الوسائل التقنية وتعزيز قدرات الجهات المختصة، مع دعم التعاون الدولي لمواكبة هذا النوع المعقّد من الجرائم.

الفرع الثالث: الصعوبات المتعلقة بالمورد البشري

إلى جانب الصعوبات القانونية والمادية التي تعترض البحث والتحري في الجرائم المعلوماتية، تبرز صعوبات أخرى ذات طابع بشري، ترتبط أساسًا بكفاءة وتأهيل العنصر البشري المكلف بتطبيق هذه الإجراءات. إذ يتطلب التعامل مع هذا النوع من الجرائم مهارات تقنية وقانونية متخصصة، وقدرة على مواكبة التطور التكنولوجي المتسارع، وهو ما يشكّل تحديًا حقيقيًا أمام أجهزة البحث والتحري.

وعليه، سيتم في هذا الفرع إبراز أهم الصعوبات المرتبطة بالموارد البشرية في مجال الجرائم المعلوماتية.

أولا: ضعف التكوين المتخصص

- نقص التكوين المتخصص لدى أفراد الضبطية القضائية في مجال تقنيات الإعلام الآلي والأدلة الرقمية، مما ينعكس سلبًا على قدرتهم في التعامل مع الجرائم المعلوماتية بكفاءة. إذ يتطلب هذا المجال إلمامًا بآليات عمل

الأنظمة المعلوماتية وطرق اختراقها، وكذا كيفية جمع الأدلة الرقمية وحفظها وفق المعايير القانونية، وهو ما لا يتوفر دائمًا بالشكل الكافي[1].

- إشكالية مواكبة التطور التكنولوجي المتسارع، فبتطور أساليب الجريمة المعلوماتية، بشكل يفوق في كثير من الأحيان قدرات التكوين والتدريب المتاحين، مما يؤدي إلى فجوة معرفية بين المجرم المعلوماتي وأجهزة التحري. ويزداد هذا التحدي تعقيدًا في ظل اعتماد الجناة على تقنيات متقدمة يصعب على غير المختصين فهمها أو التعامل معها[2].

ثانيا: قلة الخبراء المتخصصين في مجال الأدلة الرقمية

- معاناة أجهزة البحث والتحري من محدودية الخبراء المختصين في مجال الأدلة الرقمية، سواء على مستوى التحليل التقني أو الخبرة القضائية، وهو ما قد يؤدي إلى تأخر الإجراءات أو ضعف جودة التقارير الفنية المعتمدة في الإثبات. كما أن التنسيق بين مختلف الفاعلين، من ضباط الشرطة القضائية وخبراء وتقنيين، قد يواجه بعض الصعوبات التنظيمية التي تؤثر على فعالية العمل الميداني[3].

وعليه، فإن الصعوبات البشرية تمثل عائقًا حقيقيًا أمام فعالية البحث والتحري في الجرائم المعلوماتية، الأمر الذي يستدعي ضرورة الاستثمار في التكوين المتخصص، وتعزيز الكفاءات البشرية، وتكثيف برامج التدريب المستمر، بما يواكب التطورات التكنولوجية ويضمن تحسين أداء الأجهزة المختصة.

---

[1] _خالد ضو، مرجع سابق،209،210.

[2] _ وردة شرف الدين، مرجع سابق،546.

[3] _وهيبة رابح، " الجريمة المعلوماتية في التشريع الإجرائي الجزائري"، *مجلة الباحث للدراسات الأكاديمية*، 4(ديسمبر 2014): 321، https://asjp.cerist.dz/en/article/5724.

من خلال ما تم التطرق إليه في هذا الفصل، يتضح أن الجريمة المعلوماتية تُعد من أبرز الجرائم المستحدثة التي أفرزها التطور التكنولوجي والثورة الرقمية، حيث فرضت نفسها كواقع إجرامي جديد يختلف عن الجرائم التقليدية المعروفة. وعليه، فإن فهم الجريمة المعلوماتية يمر عبر استقراء التعريفات التي صاغها فقهاء القانون، والتي تتفق في مجملها على أن الجريمة المعلوماتية هي كل فعل غير مشروع يتم باستعمال الوسائل المعلوماتية الذي يستهدف الأنظمة والبيانات المعلوماتية بقصد تحقيق منفعة غير مشروعة أو إحداث ضرر بالغير. غير أن كثرة التعاريف الفقهية يرجع أساسًا إلى التطور المستمر لهذا النوع من الجرائم وتعدد صورها وأساليب ارتكابها. كما أن التشريع الجزائري، على غرار بعض التشريعات المقارنة، لم يضع تعريفًا صريحًا ودقيقًا للجريمة المعلوماتية، وإنما اكتفى بالنص على بعض صورها ضمن قوانين خاصة.

وانطلاقًا من هذه التعاريف، أمكن الوقوف على أهم خصائص الجريمة المعلوماتية، والتي تتمثل أساسًا في طابعها التقني، وسهولة ارتكابها، وصعوبة اكتشافها وإثباتها، فضلًا عن طابعها العابر للحدود واعتمادها على الذكاء والخبرة التقنية لمرتكبيها. كما أن الوسيلة المستعملة في ارتكاب هذه الجرائم أدت إلى ظهور صور متعددة لها، من بينها جرائم الاختراق غير المشروع للأنظمة المعلوماتية، وغيرها من الجرائم التي تم ذكرها.

ومن جهة أخرى، وحتى تقوم المسؤولية الجزائية عن الجرائم المعلوماتية، لا بد من توافر أركانها القانونية المتمثلة في الركن الشرعي الذي يقتضي وجود نص قانوني يجرم الفعل، والركن المادي الذي يتمثل في السلوك الإجرامي المرتكب باستعمال الوسائل المعلوماتية وما يترتب عنه من نتائج، إضافة إلى الركن المعنوي القائم على القصد الجنائي والعلم والإرادة لدى الجاني. ونظرًا لخطورة هذا النوع من الجرائم عمل المشرع الجزائري على تكريس آليات قانونية وإجرائية خاصة بالبحث والتحري عنها، من خلال تعديل واستحداث مختلف القوانين.

ورغم تكريس المشرع لسلطات البحث والتحري ومنح صلاحيات واسعة للأجهزة والهيئات المختصة في مكافحة الجرائم المعلوماتية، إلا أن هذه الأجهزة ما تزال تواجه عدة صعوبات تحد من فعالية مهامها، من بينها الطابع التقني المعقد لهذه الجرائم، وصعوبة تحديد هوية الجناة، وسهولة إخفاء الأدلة الرقمية أو إتلافها، فضلًا عن الطابع العابر للحدود الذي يميزها، بالإضافة إلى النقص في الخبرات التقنية المتخصصة والتطور المستمر لأساليب الإجرام الإلكتروني. وهو ما يستدعي مواصلة تطوير المنظومة القانونية والمؤسساتية، وتعزيز التكوين التقني للأجهزة المختصة بما يواكب التطورات الرقمية المتسارعة

الفصل الثاني: الآليات المؤسساتية في مجال البحث والتحري عن الجرائم المعلوماتي

يُعدّ البحث والتحري في الجرائم المعلوماتية من أبرز التحديات التي تواجه الأنظمة القانونية المعاصرة، نظرًا لخصوصية هذا النوع من الجرائم وتعقّد الوسائل المستعملة في ارتكابها. ولمواجهة ذلك، عملت التشريعات الحديثة على وضع آليات مؤسساتية متخصصة تجمع بين الهيئات الرقابية والأجهزة الأمنية والقضائية، بهدف الوقاية من هذه الجرائم وضمان فعالية ملاحقتها.

وانطلاقًا من ذلك، يهدف هذا الفصل إلى إبراز مختلف الآليات المؤسساتية المعتمدة في مجال البحث والتحري عن الجرائم المعلوماتية، من خلال التعرف على الأجهزة المكلفة بالوقاية والتحري في **المبحث الأول**، إضافة إلى الوسائل والإجراءات المعتمدة في هذا المجال في **المبحث الثاني**، بما يساهم في تحقيق حماية قانونية فعّالة في البيئة الرقمية.

المبحث الأول: الأجهزة المكلفة بالوقاية في الجرائم المعلوماتية والتحري عنها

يعتبر تحديد الأجهزة المكلفة بالوقاية من الجرائم المعلوماتية والتحري عنها أمرًا أساسيًا لفهم كيفية مواجهة هذا النوع من الجرائم. إذ تتكامل أدوار الهيئات الرقابية مع الأجهزة الأمنية والقضائية في إطار منظومة تهدف إلى الحدّ من هذه الجرائم وضمان متابعتها بفعالية.

وعليه، يتناول هذا المبحث مختلف الجهات المختصة بالوقاية والتحري، مع إبراز طبيعة مهامها وأدوارها في هذا المجال. إذ سنتناول أهم الهيئات الرقابية المختصة عن طريق **المطلب الأول،** ومن ثم سيتم التطرق إلى الأجهزة المكلفة بالبحث والتحري عن الجرائم المعلوماتية من خلال **المطلب الثاني.**

المطلب الأول: الهيئات الرقابية في مجال الجرائم المعلوماتية

أمام التحديات التي برزت للتشريعات القانونية في مكافحة الجرائم المعلوماتية وعدم نجاعة الآليات التقليدية في مكافحتها، برزت الحاجة إلى إرساء آليات ومنظومات رقابية متخصصة تتولى الوقاية من هذه الجرائم ورصدها ومتابعتها؛ وفي هذا الخصوص عمد المشرع الجزائري إلى استحداث هيئات رقابية مختصة تعمل على تعزيز الأمن المعلوماتي من خلال التنسيق مع مختلف الجهات الأمنية والقضائية واعتماد آليات وقائية مسبقة للحد من المخاطر الرقمية.

وعليه، يقتضي تناول هذا المطلب الوقوف على أهم الهيئات الرقابية في مجال الجرائم المعلوماتية، من خلال التطرق إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من خلال **الفرع الأول،** وكذا السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي من خلال **الفرع الثاني،** باعتبارهما نموذجين أساسيين في هذا المجال.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

في إطار تعزيز آليات التصدي للجرائم المعلوماتية، لم يكتف المشرع الجزائري بإقرار نصوص قانونية موضوعية، بل اتجه كذلك إلى تدعيمها بأجهزة مؤسساتية متخصصة تتولى رصد المخاطر المرتبطة باستعمال تكنولوجيات الإعلام والاتصال والحد منها. وتعتبر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من أبرز هذه الهيئات، حيث أُنشئت بهدف دعم جهود الدولة في مجال الوقاية وتعزيز التنسيق بين مختلف الفاعلين في هذا المجال، وعليه يقتضي الأمر الوقوف على الإطار القانوني والتنظيمي لهذه الهيئة وكذلك إبراز مهامها وصلاحياتها.

أولا: الإطار القانوني والتنظيمي للهيئة

في هذا الصدد سيتم تناول الإطار القانوني والتنظيمي للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

1- الإطار القانوني:

لقد استحدث المشرّع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث نصّت المادة 13 منه على إنشاء هذه الهيئة، إذ جاء في نص المادة:"تُنشأ هيئة وطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال، وتُحدَّد تشكيلة هذه الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم[1]".

مع إحالة تحديد تنظيمها وتشكيلتها وكيفيات سيرها إلى التنظيم. وقد تم تجسيد هذا الإطار القانوني من خلال صدور نصوص تنظيمية سنة 2019، حيث نصّ على أنه: تُنشأ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، والتي جاءت لتفصل الأحكام المتعلقة بالهيئة وتحدد معالم عملها. ويهدف إنشاء هذه الهيئة أساسًا إلى تعزيز المقاربة الوقائية في مواجهة الجرائم المعلوماتية، من خلال استباق المخاطر المرتبطة باستخدام تكنولوجيات الإعلام والاتصال والحدّ من انتشارها[2].

2- الإطار التنظيمي للهيئة:

تعتبر هذه الهيئة مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلال المالي، وهو ما يمنحها قدراً من الاستقلالية في ممارسة مهامها. كما توضع تحت وصاية وزارة الدفاع الوطني، في إطار ضمان التنسيق بين مختلف الأجهزة المتدخلة في مجال مكافحة الجرائم المعلوماتية. ويُحدّد التنظيم الخاص بها كيفية تشكيلها وسيرها، بما يضمن فعالية أدائها وتكيّفها مع مختلف الأجهزة المعنية بمكافحة الجرائم المعلوماتية[3].

---

[1]_ المادة 13، من القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال.

[2]_سهيلة بوزبورة،"الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية"، *المجلة النقدية للقانون والعلوم السياسية* 17، 2(2022): 562،https://asjp.cerist.dz/en/article/209229.

[3]_أمال حابت، "دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، *المجلة الدولية للبحوث القانونية والسياسية* 5، 3(2021): 466،https://asjp.cerist.dz/en/article/174814.

ويتضح جليًا من خلال النصوص القانونية المؤطر لها أن المشرّع الجزائري لم يتجه إلى اعتبار هذه الهيئة سلطة إدارية مستقلة، على غرار بعض الهيئات الأخرى مثل الهيئة الوطنية للوقاية من الفساد ومكافحته، بل أبقاها ضمن فئة المؤسسات العمومية ذات الطابع الإداري.

ورغم ذلك، يُلاحظ أن المشرع يستعمل في بعض الأحيان مصطلحات مختلفة، إذ يصف هذه الأجهزة تارة بـ"السلطة" وتارة أخرى بـ"الهيئة"، وهو ما قد يثير نوعا من الغموض في تحديد طبيعتها القانونية بدقة. غير أن هذا التباين الاصطلاحي لا يغيّر من حقيقتها القانونية، حيث لم يتم إدراجها ضمن فئة السلطات الإدارية المستقلة، وهو ما يؤكد خضوعها لنظام قانوني أقرب إلى الهيئات الإدارية التقليدية[1].

وسعيًا إلى تمكين الهيئة من الاضطلاع بمهامها بكفاءة وفعالية، يقتضي الأمر إسنادها بهيكل تنظيمي وإداري يتسم بالنجاعة والاحترافية، يضمن حسن تنفيذ الاختصاصات المخوّلة لها قانونًا. فتخضع الهيئة لسلطة وزارة الدفاع الوطني، والتي حُدِّد مقرّها بالجزائر العاصمة، مع إمكانية نقله إلى أي مكان آخر بموجب قرار من وزارة الدفاع الوطني. كما تضمّن المرسوم الرئاسي رقم 19-172 تعديلاً في الهيكل التنظيمي للهيئة، حيث أصبحت تتكوّن من مجلس توجيه ومديرية عامة، بما يعكس تبنّي تنظيم مزدوج يجمع بين التوجيه الاستراتيجي والتنفيذ الإداري[2].

أ. مجلس التوجيه:

بعد وضع الهيئة تحت إشراف وسلطة وزارة الدفاع الوطني، بعد أن كانت في ظل المرسوم الرئاسي 15-261 تخضع لسلطة وزارة العدل، أصبحت تشكيلة مجلس التوجيه، الذي حل محل اللجنة المديرة، كالآتي:

يترأس هذا المجلس وزير الدفاع الوطني، القائد الأعلى للقوات المسلحة، أي رئيس الجمهورية، ومن الناحية العملية فإن نائب وزير الدفاع هو من ينوبه في رئاسة المجلس، وهو ما نصت عليه المادة 5 من المرسوم الرئاسي

19-172، كما يتشكل من ممثلي الوزارات التالية: وزارة الدفاع الوطني، ووزارة الداخلية، ووزارة العدل، ووزارة المواصلات السلكية واللاسلكية، كما أُسندت مهمة أمانة المجلس للمديرية العامة[3].

---

[1]–سهيلة بوزبرة، مرجع سابق،564،563.

[2]–حكيمة بوكحيل وسامية بن عديد، "الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية"، *الدراسات القانونية المقارنة* 7، (2021):1545، https://asjp.cerist.dz/en/article/156755.

[3]– المرجع السابق نفسه.

ب. المديرية العامة:

بموجب المادة 9 من المرسوم الرئاسي 19-172 سالف الذكر، فإنه تُنشأ مديرية عامة يترأسها مدير عام يُعيَّن طبقًا للتنظيم المعمول به في وزارة الدفاع الوطني، وهو ما نصت عليه المادة 19 من ذات المرسوم. ويتضح لنا الطابع الأمني للهيئة من خلال التشكيلة التي يغلب عليها عنصر الانتماء للمؤسسة العسكرية، كما أن المديرية، من الناحية التنظيمية، تضم بموجب المادة 10 من ذات المرسوم مديريتين، هما المديرية التقنية ومديرية للإدارة والوسائل.

- **المديرية التقنية:** تتكفل المديرية التقنية، على وجه الخصوص، بمهمة المراقبة الوقائية للاتصالات الإلكترونية من أجل الوقاية من الجرائم الموصوفة بالأفعال الإرهابية وأي اعتداء على أمن الدولة، هذا بالإضافة إلى مساعدة السلطات القضائية ومصالح الشرطة، بما في ذلك في مجال الخبرة القضائية، في إطار مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- **مديرية الإدارة والوسائل:** تُعنى مديرية الإدارة والوسائل، على وجه الخصوص، بالقيام بمهمة التسيير الإداري والمالي اليومي لمختلف الموارد البشرية للهيئة، كما تتولى تسيير إنفاق ميزانية الهيئة، سواء في مجال التموين أو صيانة العتاد والوسائل والمنشآت القاعدية[1].

ثانيا: مهام وصلاحيات الهيئة

رغم أن القانون المتضمن القواعد الخاصة المتصلة بجرائم الإعلام والاتصال ومكافحتها قد نصّ في المادة 14 منه على مهام الهيئة بصفة واضحة، إلا أنه في المرسوم الرئاسي 19-172 تم تفصيل هذه المهام وتوزيعها بين مجلس التوجيه والمديرية العامة.

1_ مهام مجلس التوجيه:

لقد خول المشرع لمجلس التوجيه بالهيئة مهام وصلاحيات من بينها ما يلي:

- التداول بشأن الاستراتيجية الوطنية للوقاية من الجرائم المعلوماتية المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما يختص بدراسة ومناقشة سبل تطوير التعاون مع مختلف المؤسسات والهيئات الوطنية المعنية بهذا المجال.
- إجراء تقييم دوري لمستوى التهديدات المرتبطة بالجرائم المعلوماتية، ومدى تحقيق الأهداف المسطرة، فضلا عن اقتراح الأنشطة والتدابير التي من شأنها تعزيز البحث وتقييم الجهود المبذولة في مجال الوقاية من هذه الجرائم ومكافحتها.

[1]-حكيمة بوكحيل، سامية بن عديد، نفس المرجع السابق، 1545.

- كما يمارس المجلس دورًا اقتراحيًا من خلال تقديم التوصيات في نطاق اختصاص الهيئة، ويسهم في ضبط المعايير القانونية ذات الصلة، إلى جانب دراسته لميزانية الهيئة والمصادقة عليها[1].

أما من حيث التسيير، فيجتمع مجلس التوجيه في دورتين عاديتين سنويًا بناءً على استدعاء من رئيسه، كما يمكن أن ينعقد في دورات غير عادية كلما دعت الضرورة إلى ذلك، سواء بمبادرة من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة، وفقًا لما نصّت عليه المادة 6 من المرسوم الرئاسي المنظم للهيئة، في حين حدّدت المادة 8 من نفس المرسوم القواعد والإجراءات المتعلقة بكيفيات سير المجلس، وذلك بموجب قرار يصدر عن وزير الدفاع الوطني[2].

2_ مهام المديرية العامة:

تتمثل مهام المديرية العامة فيما يلي:

- ضمان حسن سير الهيئة من خلال تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بما يحقق الانسجام والفعالية في الأداء.
- الاضطلاع على تبادل المعلومات مع الهيئات الأجنبية الناشطة في نفس المجال، في إطار التعاون الأمني، بغرض جمع وتحليل المعطيات المتعلقة بمرتكبي الجرائم المعلوماتية والتعرّف عليهم وتحديد أماكن تواجدهم.[3]

كما تمارس المديرية مهاما إدارية بحتة، طبقا لما نصت عليه المادة 17 من نفس المرسوم، والتي تتمثل أساسًا في:

- إعداد مشروع ميزانية الهيئة.
- إعداد وتنفيذ برامج عمل الهيئة.
- تسهر على تنسيق ومتابعة ومراقبة أنشطة مختلف هياكل الهيئة، بما يضمن حسن سيرها وتحقيق أهدافها.
- تتكفل بتحضير اجتماعات مجلس التوجيه، وتتولى مهام الأمانة العامة له.
- تقوم بإعداد التقرير السنوي لنشاطات الهيئة، بما يسمح بتقييم أدائها.
- تضمن مسك محاسبة الهيئة وفق قواعد المحاسبة العمومية[4].

[1]– المادة 6، المرسوم الرئاسي 19–172، المتعلق بتحديد تشكيلة الهيئة الوطنية لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، ع.37، ج. ر. ج. ج. 5.

[2]–حكيمة بوكحيل، سامية بن عديد، مرجع سابق، 1546.

[3]– حكيمة بوكيحل وسامية بن عديد، نفس المرجع السابق.

[4]– المادة 17، من المرسوم الرئاسي 19–172، المتعلق بتحديد تشكيلة الهيئة الوطنية لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال.

الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

بالإضافة إلىالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال كجهاز وطني لمكافحة الجرائم المعلوماتية، تبرز السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كهيئة رقابية استحدثها المشرع الجزائري لإرساء الآليات القانونية التي تكفل حماية الحقوق واحترام الأحكام القانونية المرتبطة بالبيانات الشخصية في إطار من الشرعية والشفافية، ضف إلى ذلك ضمان التوازن بين متطلبات الأمن المعلوماتي وحقوق الأفراد في الخصوصية.

وعليه، سيتم التطرق إلى هذه السلطة من خلال بيان إطارها القانوني، ثم تبيان مهامها وصلاحياتها، وكذا دورها في مجال حماية المعطيات الشخصية.

أولا: الإطار القانوني والتنظيمي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

1- الإطار القانوني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وخصائصها:

أ. الإطار القانوني:

تعد السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي حجر الزاوية في المنظومة الحمائية التي كرسها المشرع الجزائري، حيث جاء استقرارها تجسيداً للدستورية الرقمية والحق في الخصوصية، إذ استمدت هذه السلطة وجودها القانوني من صلب الدستور الجزائري لسنة 2016، وتحديداً المادة 46 منه، والتي أصبحت حاليا المادة 47 منه بعد تعديل الدستور سنة 2020، وتمثل هذه السلطة آلية توازن مؤسساتي تهدف إلى التوفيق بين مقتضيات الحفاظ على النظام العام والأمن الوطني من جهة، وبين صون الحقوق والحريات اللصيقة بالشخصية من جهة أخرى[1].

وعليه، استحدث المشرع الجزائري السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب القانون رقم 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعي ينفي مجال معالجة المعطيات ذات الطابع الشخصي مبينا الإطار القانوني العام لحماية البيانات الشخصية ومشددا على احترام الحياة الخاصة للأفراد وضمان عدم المساس بحقوقهم أو شرفهم أو سمعتهم. كما يخول المشرع لهذه السلطة مجموعة من الصلاحيات محددا كيفية تنظيمها وسيرها وقواعد عملها لضمان أداء مهامها في مجال حماية المعطيات الشخصية بفعالية[2].الأمر الذي يعكس رغبته في توفير الحماية القانونية والمؤسساتية الكافية للمعطيات الشخصية.

---

[1]-عبد الهادي كحلاوي وعبد الهاديين زيطة، "آليات حماية المعطيات ذات الطابع الشخصي، في ظل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"، *مجلة القانون والعلوم السياسية* 7، 2(2021):119، https://asjp.cerist.dz/en/article/163125.

[2]-عادل قرانة وفارس بوحديد، " مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري"، *مجلة العلوم القانونية والاجتماعية* 7، 2(2021):1057، https://asjp.cerist.dz/en/article/152268.

ب. خصائصها:

من ناحية التكييف، تُنشأ هذه الأخيرة لدى رئيس الجمهورية وتتمتع بالشخصية المعنوية والاستقلال المالي والإداري، إذ صنفها المشرع كـ "سلطة إدارية مستقلة"، وهو تكييف يمنحها مركزاً قانونياً متميزاً يتمثل في:

1. **الاستقلال العضوي والوظيفي:** من خلال تمتعها بالشخصية المعنوية والاستقلال المالي والإداري.
2. **الاستقلال المالي:** عبر إدراج ميزانيتها ضمن ميزانية الدولة، مما يمنحها أريحية في تنفيذ مهامها الرقابية.
3. **التنظيم الذاتي:** حيث خول لها القانون صلاحية إعداد نظامها الداخلي والمصادقة عليه بما يتلاءم مع خصوصية نشاطها[1].

2- الإطار التنظيمي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

أ. تشكيلة السلطة:

بناءً على ما جاء به نص المادة 23 من القانون رقم 18-07، فإن تشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ذات طبيعة جماعية تعتمد على التعددية والمؤسساتية لضمان الحياد والخبرة التقنية، حيث تتألف من 13 عضواً يتم تعيينهم بموجب مرسوم رئاسي لمدة عهدة محددة بخمس سنوات قابلة للتجديد[2]، وتتوزع هذه التشكيلة وفق ما يلي:

- **ثلاث (03) شخصيات** :من بينهم الرئيس يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية.
- **ثلاث (03) قضاة** :يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة.
- **عضو من كل غرفة من البرلمان** :يتم اختياره من قبل رئيس كل غرفة (المجلس الشعبي الوطني ومجلس الأمة)، بعد التشاور مع رؤساء المجموعات البرلمانية.
- **ممثل واحد** عن المجلس الوطني لحقوق الإنسان.
- **ممثل واحد** عن وزير الدفاع الوطني.

[1]- عبد الهادي كحلاوي، عبد الهادي بن زيطة، مرجع سابق، 119.

[2]- المادة 23 من القانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ع.34، ج. ر. ج. ج. 11.

- **ممثل واحد** عن وزير الشؤون الخارجية.

- **ممثل واحد** عن الوزير المكلف بالداخلية.

- **ممثل واحد** عن وزير العدل، حافظ الأختام.

- **ممثل واحد** عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة.

- **ممثل واحد** عن الوزير المكلف بالصحة.

إن حرص المشرع على إرساء هذا الهيكل التنظيمي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي يعكس إدراكاً عميقاً لضرورة تفعيل الرقابة على معالجة المعطيات الشخصية. وفي هذا الإطار، يبرز التوجه نحو الاسترشاد بالنماذج الدولية الرائدة، وفي مقدمتها تجربة مجلس أوروبا؛ الذي لم يكتفِ بوضع الأطر النظرية، بل عمد إلى إنشاء لجنة خبرة متخصصة تولت إصدار حزمة من الأدلة التوجيهية التفصيلية. وقد شملت هذه المرجعية الاسترشادية قطاعات ذات حساسية قانونية وتقنية عالية، لاسيما في مجالات الأنشطة الطبية، المعطيات الشخصية خاصة لدى الأجهزة الأمنية، وصولاً إلى البيانات المتعلقة بالمجال الجنائي، مما يوفر خريطة طريق موضوعية يمكن للسلطة الوطنية الاستئناس بها في ممارسة مهامها[1].

ب. ضوابط نظام عمل سير السلطة:

أخضع المشرع الجزائري السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي لمنظومة من الضوابط القانونية الصارمة، الهادفة إلى ضمان الحياد والنزاهة في أداء مهامها، مع توفير الآليات الهيكلية اللازمة لتعزيز فعاليتها الميدانية، من بينها نذكر:

- **الالتزامات المهنية وضوابط عدم التعارض (حالات التنافي):**

فرض القانون على رئيس وأعضاء السلطة الوطنية حزمة من القيود لضمان استقلاليتهم وشفافية قراراتهم، وتتمثل أبرز هذه الضوابط في:

- الالتزام بالسر المهني :يلتزم الأعضاء بالحفاظ على سرية المعلومات والبيانات التي يطلعون عليها بمناسبة ممارسة مهامهم، ويمتد هذا الالتزام كواجب قانوني حتى بعد انتهاء عهدتهم.

[1]–عبد الهادي كحلاوي وعبد الهادي بن زيطة، مرجع سابق، 120.

- حظر تضارب المصالح (حالات التنافي) :منَعَ المشرع الأعضاء من امتلاك أي مصالح مباشرة أو غير مباشرة في المؤسسات والكيانات التي تنشط في مجال معالجة المعطيات، وذلك تجنباً لأي انحياز قد يؤثر على الطبيعة الرقابية للسلطة.

- **الهياكل المساعدة والوسائل التقنية (الأمانة التنفيذية والسجل الوطني):**

لتمكين السلطة من تجسيد صلاحياتها، استحدث المشرع آليات دعم إداري وتقني تمثلت في:

- الأمانة التنفيذية :وهي الهيكل الإداري المشرف على تسيير الشؤون اليومية للسلطة، تحت إشراف أمين تنفيذي وبالاستعانة بطاقم إداري متخصص.
- السجل الوطني لحماية المعطيات :يعد أداة تقنية وقانونية جوهرية تشرف السلطة على مسكه، وتكمن وظيفته في توثيق كافة عمليات المعالجة، سواء الصادرة عن الهيئات العمومية أو القطاع الخاص، كما يتضمن مراجع النصوص القانونية المتعلقة بالملفات العمومية، وتدوين كافة التراخيص والتصريحات، مع كفالة حق الأشخاص في الاطلاع عليه وفق الضوابط المعمول بها[1].

ثانيا: مهام وصلاحيات السلطة

باعتبار السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي جهازًا رقابيًا وتنظيميًا محوريًا، خول لها المشرع الجزائري جملة من المهام والصلاحيات التي تهدف إلى ضمان حماية المعطيات الشخصية في إطار المادة 25 من القانون رقم 18-07 والمتمثلة في[2]:

أ. **مهام الرقابة**

تتولى السلطة مهمة مراقبة مدى مطابقة عمليات معالجة المعطيات الشخصية لأحكام القانون رقم 18-07، وذلك من خلال:

- السهر على احترام المبادئ القانونية المتعلقة بشرعية وشفافية معالجة البيانات.
- متابعة مدى التزام المسؤولين عن المعالجة بقواعد حماية الحياة الخاصة.
- القيام بعمليات التفتيش والتحقيق عند وجود أي إخلال أو انتهاك.

[1]- عبد الهادي كحلاوي وعبد الهادي بن زيطة، نفس المرجع سابق، 121.

[2]- المادة 25، القانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ب. مهام الترخيص والإخطار

تضطلع السلطة بدور أساسي في تنظيم عمليات معالجة المعطيات الشخصية، من خلال:

- منح التراخيص المسبقة في الحالات التي يوجب فيها القانون ذلك .
- تلقي التصريحات المتعلقة بعمليات معالجة البيانات .
- رفض أو تعليق أي معالجة غير مطابقة للضوابط القانونية[1] .

ج. المهام الاستشارية

تقوم السلطة بدور استشاري هام لفائدة السلطات العمومية والهيئات الخاصة، حيث:

- تبدي رأيها في مشاريع النصوص التشريعية والتنظيمية المتعلقة بحماية المعطيات .
- تقدم توصيات تقنية وقانونية لتحسين آليات حماية البيانات .
- تساهم في توجيه السياسات العامة في مجال الأمن الرقمي .

د. المهام التوعوية والتحسيسية

تهدف هذه المهام إلى نشر ثقافة حماية البيانات الشخصية، وتشمل:

- تنظيم حملات توعوية لفائدة الأفراد والمؤسسات حول حقوقهم وواجباتهم .
- نشر الإرشادات المتعلقة بالوقاية من مخاطر المساس بالمعطيات الشخصية .
- تشجيع اعتماد ممارسات سليمة في معالجة البيانات .

هـ. المهام الرقابية الجزائية والإدارية

تتمتع السلطة بصلاحيات ردعية عند وقوع مخالفات، حيث يمكنها:

- إصدار إعذار وتنبيه للمسؤولين عن المعالجة .

[1]– سهام بن دعاس وفادية بن عثمان، "ضمانات حماية المعطيات الشخصية في البيئة الرقمية في التشريع الجزائري"، *مجلة الحقوق والعلوم الإنسانية* 15، (2022):1685، https://asjp.cerist.dz/en/downArticle/315/15/1/186266.

- اتخاذ تدابير إدارية مثل تعليق أو وقف المعالجة غير المشروعة .
- إحالة المخالفات الخطيرة على الجهات القضائية المختصة[1] .

ومما سبق ذكره، يتضح أن مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي تعكس مقاربة شاملة تجمع بين الوقاية والرقابة والردع، بما يضمن حماية فعّالة للبيانات الشخصية. كما أن تعدد اختصاصاتها يعكس أهمية دورها في تحقيق التوازن بين حماية الخصوصية ومتطلبات التعامل مع المعطيات في البيئة الرقمية، غير أن فعالية هذه المهام تبقى مرتبطة بمدى توفر الإمكانيات البشرية والتقنية اللازمة لتطبيقها ميدانياً.

المطلب الثاني: الأجهزة المكلفة بالبحث والتحري عن الجرائم المعلوماتية

في امتداد لما تم تناوله في المطلب الأول من عرضٍ للهيئات الرقابية ذات الطابع الوقائي، يبرز الدور الحيوي للأجهزة المكلفة بالبحث والتحري عن الجرائم المعلوماتية، باعتبارها تمثل الجانب الإجرائي والزجري في مواجهة هذا النوع من الجرائم. فالطبيعة التقنية المعقدة لها، وما تتسم به من سرعة الانتشار وصعوبة التتبع، تفرض ضرورة وجود أجهزة متخصصة تمتلك الكفاءة التقنية والوسائل القانونية اللازمة للكشف عن هذه الجرائم وإثباتها.

وفي هذا الإطار، اجتهد المشرع الجزائري على تدعيم المنظومة الأمنية والقضائية بهياكل متخصصة، تتولى مهام البحث والتحري وجمع الأدلة الرقمية، مع مراعاة الخصوصيات التي تميّز هذا النوع من الجرائم. وعلى هذا الأساس وجب الوقوف عند أهم أجهزة الضبطية القضائية المتخصصة في مجال البحث والتحري عن هذه لجرائم من خلال **الفرع الأول**، ومن ثم بيان دور النيابة العامة في التوجيه والمتابعة من خلال **الفرع الثاني**.

الفرع الأول: الضبطية القضائية المتخصصة في مجال البحث والتحري عن الجرائم المعلوماتية

أمام التطور المتسارع للجرائم المعلوماتية، اتجهت التشريعات الحديثة إلى استحداث أجهزة قضائية وأمنية متخصصة تتولى مهمة البحث والتحري عن الدليل الإلكتروني، بالنظر إلى خصوصية هذا النوع من الجرائم وما يتطلبه من كفاءة تقنية وخبرة معلوماتية. ومن أهم هذه الأجهزة ما يلي:

أولا: جهات الضبطية القضائية:

1- وحدات مكافحة الجرائم الإلكترونية

تعد وحدات مكافحة الجرائم الإلكترونية من أهم الأجهزة المتخصصة في مجال البحث والتحري عن الدليل الإلكتروني، حيث تتولى مباشرة التحريات المتعلقة بالجرائم المرتكبة عبر الأنظمة المعلوماتية وشبكات الإنترنت.

[1]– سهام بن دعاس وفادية بن عثمان، نفس المرجع السابق،1686.

وتختص هذه الوحدات بتتبع عناوين بروتوكول الإنترنت(IP) ، وفحص الأجهزة الإلكترونية، وتحليل البرمجيات والفيروسات المستخدمة في ارتكاب الجريمة، بالإضافة إلى جمع الأدلة الرقمية وحفظها وفق الطرق القانونية والتقنية المعتمدة.

كما تعتمد هذه الوحدات على تقنيات حديثة وبرامج متطورة تمكنها من كشف الجرائم الإلكترونية والوصول إلى مرتكبيها، خاصة في ظل سهولة إخفاء الآثار الرقمية وسرعة انتقال البيانات عبر الشبكات[1].

2- مصالح الشرطة القضائية

تضطلع مصالح الشرطة القضائية بدور أساسي في مجال البحث والتحري عن الجرائم المعلوماتية، باعتبارها

الجهة المكلفة قانونا بجمع الاستدلالات والتحقيق الأولي في الجرائم. وقد عملت العديد من الدول على تدعيم هذه المصالح بعناصر متخصصة في الإعلام الآلي والتقنيات الرقمية، قصد تمكينها من التعامل مع الأدلة الإلكترونية وفهم طبيعتها التقنية[2].

إذ يُعتبر أعضاء الشرطة القضائية موظفين منحهم القانون صفة الضبطية القضائية من خلال ما جاءت به المادة20 من قانون الإجراءات الجزائري الجديد رقم 25-14 إذ تنص المادة على: " يقوم بمهمة الشرطة القضائية، القضاة والضباط والأعوان والموظفون المبينون في هذا الفصل"[3].

ويتمتع بصفة الضبطية القضائية كل من:

- رؤساء المجالس الشعبية البلدية
- ضباط الدرك الوطني وضباط الشرطة للأمن الوطني .
- بعض ضباط الصف الذين تتوفر فيهم شروط الأقدمية المهنية والتعيين القانوني.
- الموظفون التابعون للأسلاك الخاصة للمفتشين ومحققي وحفاظ وأعوان الشرطة للأمن الوطني.
- أعوان الشرطة والدرك الذين تتوفر فيهم شروط الأقدمية المهنية والتعيين القانوني[4].

كما خول لهم القانون بموجبها حقوقًا وفرض عليهم واجبات في إطار البحث عن الجرائم ومرتكبيها وجمع الاستدلالات عنها، فيبدأ دورهم بعد وقوع الجريمة وينتهي عند فتح التحقيق القضائي أو إحالة المتهم إلى جهة الحكم.

---

[1]- صهيب سهيل غازي زامل، مرجع سابق،61.

[2]- صهيب سهيل غازي، نفس المرجع السابق، 61.

[3]- المادة 20، قانون الإجراءات الجزائي الجزائري رقم 25-14، ع. 54، ج. ر. ج. ج. 7.

[4]- المادة 23 من القانون رقم 14/25 المتضمن قانون الإجراءات الجزائية.

وتتميز الشرطة القضائية عن الشرطة الإدارية في أن المهمة الرئيسية لهذه الأخيرة تتمثل في تنفيذ تدابير الشرطة العامة الصادرة عن السلطات المختصة، ومراقبة نشاط الأفراد والجماعات قبل وقوع الجريمة قصد المحافظة على الأمن العمومي ومنع أسباب الاضطرابات وإزالتها إذا وقعت، فأعمال الشرطة الإدارية إجراءات وقائية ومانعة، في حين أن أعمال الشرطة القضائية عبارة عن إجراءات رادعة.

كما تقوم الشرطة القضائية باتخاذ مختلف الإجراءات اللازمة للكشف عن الجريمة، مثل حجز الأجهزة الإلكترونية، ومعاينة الأنظمة المعلوماتية، والاستعانة بالخبراء المختصين لتحليل البيانات الرقمية واستخراج الأدلة منها[1].

3- الجهات التقنية ومزودو خدمات الاتصالات

تؤدي الجهات التقنية، وعلى رأسها مزودو خدمات الاتصالات والإنترنت، دوراً محورياً في إسناد السلطات القضائية خلال مراحل البحث والتحري عن الأدلة الإلكترونية. وتستمد هذه العملية إطارها التنظيمي من أحكام القانون رقم 02/26، الذي يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية والتعريف الإلكتروني، إذ نصت المادة الأولى منه على تعريف كل المفاهيم المتعلقة بالمعاملات الإلكترونية وتحديدها، كما تلتزم الجهات المختصة بتقديم الدعم التقني اللازم لجهات التحقيق[2].

وتتجسد هذه المهمة في تزويد الضبطية القضائية أو جهات التحقيق بالمعطيات التقنية الدقيقة، مثل تحديد هوية أصحاب الحسابات الإلكترونية، وعناوين بروتوكول الإنترنت (IP Addresses)، وبيانات الاتصال والربط. تساهم هذه المعلومات بشكل مباشر في تعقب المشتبه فيهم وتحديد نطاق نشاطهم الرقمي، مما يسهل الوصول إلى الأدلة الإلكترونية وربطها بالأشخاص المعنيين، الأمر الذي يعزز من فعالية التحقيقات الجزائية في مواجهة الجرائم المعلوماتية[3].

4- الخبراء والمختصون في الأدلة الرقمية

نظرًا للطبيعة الفنية المعقدة للدليل الرقمي، تستعين الجهات القضائية بخبراء مختصين في مجال الأدلة الرقمية، وعليه، بادرت المديرية العامة للأمن الوطني إلى استحداث مصالح مختصة، تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها، فقامت المديرية العامة للشرطة القضائية باستحداث أربع نيابات مديرية، وهي: نيابة مديرية

---

[1]- عز الدين عثماني، "إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية"، مجلة دائرة البحوث والدراسات القانونية والسياسية2، 4(2018):53، https://asjp.cerist.dz/en/article/132110.

[2] - المادة1 من القانون رقم 06/26، الذي يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، ع. 14، ج. ر. ج. ج. 6.

[3] -عز الدين عثماني، مرجع سابق، 53.

الشرطة العلمية والتقنية، ونيابة مديرية الاقتصاد والمالية، ونيابة القضايا الإجرامية، والمصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

كما تستعين الجهات القضائية بخبراء مختصين في مجال الأدلة الرقمية، تكون لهم القدرة على تحليل البيانات الإلكترونية وفك تشفيرها واستخراج المعلومات التقنية المرتبطة بالجريمة. ويقوم هؤلاء الخبراء بفحص الأجهزة والبرمجيات وتحليل محتوياتها، مع إعداد تقارير فنية تساعد القاضي وجهات التحقيق على فهم الوقائع التقنية للقضية. وتبرز أهمية الخبرة الفنية خاصة في الجرائم التي تتطلب تحليلًا دقيقًا للأنظمة المعلوماتية أو استرجاع البيانات المحذوفة أو تتبع العمليات الإلكترونية المعقدة[1].

ثانيا: مهام الضبطية القضائية المتخصصة في الجرائم المعلوماتية

وفقاً لأحكام قانون الإجراءات الجزائية، تضطلع الضبطية القضائية بعدة مهام أساسية، أهمها:

- تطبيق المادة **19 من قانون الإجراءات الجزائية** التي تخول لها البحث والتحري عن الجرائم وجمع الأدلة.
- معاينة الجرائم المعلوماتية فور وقوعها.
- حجز الأجهزة والوسائط الرقمية المستعملة في ارتكاب الجريمة.
- جمع الأدلة الإلكترونية وحفظها وفق معايير تقنية دقيقة.
- تتبع مصدر الهجمات الإلكترونية وتحديد هوية الفاعلين.
- تنفيذ أوامر النيابة العامة وقاضي التحقيق في إطار التحقيق الابتدائي.

كما يخول لها القانون، استعمال الوسائل التقنية الحديثة في المعاينة والإثبات، بما يتماشى مع طبيعة الجريمة المعلوماتية[2].

كما تخضع الضبطية القضائية لرقابة النيابة العامة وفقاً للمادة20من قانون الإجراءات الجزائية رقم 25-14، حيث يتولى وكيل الجمهورية إدارة نشاطها على مستوى المحكمة، بينما يمارس النائب العام الإشراف العام على عملها على مستوى المجلس القضائي. كما تخضع أيضاً لرقابة غرفة الاتهام، وهو ما يضمن احترام الشرعية الإجرائية ومنع أي تجاوز في استعمال السلطة أثناء البحث والتحري[3].

[1]– صهيب سهيل غازي زامل، مرجع سابق، 61

[2]– المادة 119، القانون رقم 14/25، المتضمن قانون الإجراءات الجزائية.

[3]– المادة 119، من نفس القانون.

الفرع الثاني: دور النيابة العامة في التوجيه والمتابعة

تؤدي النيابة العامة دورًا أساسيًا في توجيه ومتابعة أعمال الضبطية القضائية، باعتبارها الجهة المشرفة على تحريك الدعوى العمومية والساهرة على حسن تطبيق القانون. وقد حرص المشرّع الجزائري بموجب قانون الإجراءات الجزائية المعدل بالقانون رقم 25-14 على تكريس هذا الدور من خلال مجموعة من النصوص القانونية التي منحت للنيابة العامة صلاحيات الإشراف والرقابة والتوجيه، خاصة في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

أولًا: دور النيابة العامة في توجيه أعمال الضبطية القضائية

يتجلى الدور التوجيهي للنيابة العامة من خلال إشرافها على سير التحريات والتحقيقات الابتدائية التي يباشرها ضباط الشرطة القضائية. فقد نصت المادة 24 من قانون الإجراءات الجزائية على أن ضباط الشرطة القضائية الذين يباشرون البحث والتحري في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يعملون تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميًا، مع إلزامهم بإعلام وكيل الجمهورية المختص في جميع الحالات[1].

كما خوّلت المادة 25 لضباط الشرطة القضائية إمكانية تمديد عمليات مراقبة الأشخاص والأموال والمتحصلات المرتبطة بالجرائم المعلوماتية عبر كامل الإقليم الوطني، غير أن ذلك يتم تحت رقابة النيابة العامة وبعد إخطار وكيل الجمهورية المختص، مما يعكس سلطة النيابة العامة في توجيه إجراءات البحث والتحري وضمان مشروعيتها[2].

ويظهر الدور التوجيهي للنيابة العامة كذلك من خلال ما نصت عليه المادة 26، التي أجازت لضباط الشرطة القضائية اتخاذ بعض الإجراءات بناءً على إذن مكتوب من وكيل الجمهورية المختص إقليميًا، ومن ذلك طلب نشر الإشعارات أو الصور الخاصة بالأشخاص محل البحث أو المتابعة، الأمر الذي يؤكد خضوع بعض إجراءات التحري لرقابة وتوجيه السلطة القضائية[3].

ثانيًا: دور النيابة العامة في متابعة أعمال الضبطية القضائية

تمارس النيابة العامة دورًا رقابيًا ومتابعًا لأعمال الضبطية القضائية منذ بداية التحريات إلى غاية انتهاء الإجراءات. فقد ألزمت المادة 27 ضباط الشرطة القضائية بإخطار وكيل الجمهورية المختص إقليميًا دون تأخير بالجنايات والجنح التي تصل إلى علمهم، مع موافاته بأصول المحاضر والمستندات والأشياء المضبوطة فور الانتهاء من أعمالهم.

---

[1]– المادة 24، من القانون رقم 14/25 المتضمن قانون الإجراءات الجزائية.

[2]– المادة 25، من نفس القانون.

[3]– المادة 26، من نفس القانون.

كما تتولى النيابة العامة مراقبة مدى احترام ضباط الشرطة القضائية للإجراءات القانونية أثناء تحرير المحاضر، خاصة ما تعلق بتضمين البيانات المتعلقة بالأطراف والعناوين الإلكترونية وأرقام الهواتف، والحصول على موافقتهم الصريحة بشأن التبليغ الإلكتروني، وهو ما يعكس مواكبة المشرّع للتطورات الرقمية في مجال الإجراءات الجزائية[1].

ومن جهة أخرى، منح المشرّع للنيابة العامة سلطة متابعة وتقييم أداء ضباط الشرطة القضائية، حيث نصت المادة 28 على أن النائب العام يمسك ملفًا فرديًا لكل ضابط شرطة قضائية، كما يتولى وكيل الجمهورية، تحت سلطة النائب العام، تنقيط ضباط الشرطة القضائية العاملين بدائرة اختصاص المحكمة. ويُؤخذ هذا التنقيط بعين الاعتبار عند الترقية، مما يكرّس الرقابة الإدارية والقضائية للنيابة العامة على أعمال الضبطية القضائية[2].

وعليه، يتضح أن النيابة العامة تمارس دورًا محوريًا في توجيه ومتابعة أعمال الضبطية القضائية، من خلال الإشراف على التحريات، ومراقبة شرعية الإجراءات، وضمان احترام أحكام قانون الإجراءات الجزائية، بما يحقق فعالية مكافحة الجرائم المعلوماتية وحماية الحقوق والحريات.

المبحث الثاني: وسائل وإجراءات التحري عن الجرائم المعلوماتية

في ظلّ التطور المتسارع لتكنولوجيات الإعلام والاتصال، وما أفرزه من أنماط إجرامية مستحدثة تتسم بالتعقيد والخفاء، لم يعد من الممكن الاعتماد على الأساليب التقليدية في البحث والتحري، الأمر الذي استدعى تبنّي وسائل تقنية متطورة وإجراءات قانونية خاصة تتلاءم مع طبيعة الجرائم المعلوماتية. فهذه الجرائم، بحكم طابعها اللامادي وسرعة ارتكابها وصعوبة تتبعها، تفرض اعتماد آليات دقيقة تمكّن من كشفها وإثباتها بكفاءة.

وفي هذا السياق، عمل المشرّع على تكريس مجموعة من الوسائل التقنية، كدور الخبرة الفنية وبرامج التتبع ومراقبة الاتصالات الإلكترونية، إلى جانب تنظيم إجراءات التفتيش وفق ضوابط شكلية وموضوعية تضمن فعالية التحري من جهة، وحماية الحقوق والحريات من جهة أخرى.

وعليه، سيتم تناول هذا المبحث من خلال التطرق إلى الوسائل المستخدمة في البحث والتحري عن الجرائم المعلوماتية من خلال **(المطلب الأول)**، ثم إلى الإجراءات القانونية المنظمة للتفتيش في هذا المجال من خلال **(المطلب الثاني)**.

المطلب الأول: الوسائل المستخدمة في مجال البحث والتحري عن الجرائم المعلوماتية

نظرًا لخصوصية الجرائم المعلوماتية وما تتسم به من طابع تقني معقّد، أصبح الاعتماد على الوسائل التقليدية في البحث والتحري غير كافٍ للكشف عنها وإثباتها، الأمر الذي استوجب تبنّي وسائل تقنية حديثة تتلاءم مع طبيعة البيئة الرقمية. ونظرا لخصائص هذه البيئة الصعبة، اعتمدت الجهات المختصة على جملة من الوسائل التقنية

[1]– المادة 27، من القانون 14/25 المتضمن قانون الإجراءات الجزائية.

[2]– المادة 28، قانون الإجراءات الجزائية.

للبحث والتحري عن هذه الجرائم، من بينها الخبرة الفنية وبرامج التتبع وكشف الاختراق ومراقبة الاتصالات الإلكترونية، باعتبارها أدوات فعّالة تساهم في جمع الأدلة الرقمية وتحليلها، وتعزيز فعالية عمليات البحث والتحري.

وعليه، سيتم التطرق في هذا المطلب إلى مختلف هذه الوسائل من خلال دراسة دور الخبرة التقنية من خلال **(الفرع الأول)**، ثم برامج التتبع من خلال **(الفرع الثاني)**، وأخيرًا مراقبة الاتصالات الإلكترونية من خلال **(الفرع الثالث)**.

الفرع الأول: دور الخبرة التقنية في عملية البحث والتحري عن الجرائم المعلوماتية

تُعتبر الخبرة من بين أهم الإجراءات التي ينبغي الاهتمام بها في إطار التحقيق في الجريمة المعلوماتية، وذلك راجع إلى صعوبة التعامل مع هذا النوع من الجرائم، وعدم الإلمام الكافي بجوانبها التقنية والمعرفية والفنية. إذ تقتضي عمليات البحث الجنائي والتحقيق في جرائم الإنترنت الاستعانة بخبرات متعددة ومتنوعة، ويتم اعتماد الخبراء بالارتكاز على نوعية الأساليب المستخدمة في ارتكاب الجريمة، كالتلاعب بالبيانات، والتلاعب بالبرامج الأساسية أو برامج التطبيقات، والغش أثناء نقل وبث البيانات، وتزوير المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة بعد المعالجة[1].

أولاً: مفهوم الخبرة التقنية في الجرائم المعلوماتية

يقصد بالخبرة التقنية في مجال الجرائم المعلوماتية الاستعانة بخبير مختص يمتلك معارف فنية وتقنية في مجال الإعلام الآلي، قصد مساعدة جهات التحقيق والقضاء في فهم المسائل التقنية المرتبطة بالجريمة الإلكترونية، والكشف عن الأدلة الرقمية وتحليلها واستخلاص النتائج الفنية المتعلقة بها.

وتُعد الخبرة في هذا المجال نوعاً من وسائل الإثبات الحديثة التي فرضتها خصوصية الجريمة المعلوماتية، باعتبار أن هذه الأخيرة ترتكب في بيئة رقمية تعتمد على الأنظمة المعلوماتية وقواعد البيانات والشبكات الإلكترونية، وهو ما يتطلب معرفة تقنية دقيقة لفهم طبيعة الاعتداء وكيفية وقوعه[2].

ثانياً: الأساس القانوني للخبرة التقنية في التشريع الجزائري

نظم المشرع الجزائري الخبرة القضائية ضمن أحكام قانون الإجراءات الجزائية الجزائري الجديد رقم 25-14 في القسم العاشر من الباب الثالث في الفصل الأول، حيث منح لجهات التحقيق والقضاء إمكانية الاستعانة بالخبراء كلما تعلق الأمر بمسائل فنية تستوجب معرفة خاصة وذلك بما نصت عليه المادة 239 منه. حيث جاء هذا التعديل ليكرس بشكل أوضح الاعتماد على الوسائل الإلكترونية والأدلة الرقمية في مجال الإثبات والتحري، مع تدعيم دور

[1]-وهيبة رابح، " الجريمة المعلوماتية في التشريع الإجرائي الجزائري"، مجلة الباحث للدراسات الأكاديمية، (ديسمبر 2014): 329، https://asjp.cerist.dz/en/article/5724.

[2]– مختار تابري، "الخبرة في الجريمة المعلوماتية"، *الحوار المتوسطي* 11، 3(2020): 382، https://asjp.cerist.dz/en/article/142535.

الخبرة التقنية في فحص الأنظمة المعلوماتية وتحليل المعطيات الإلكترونية، بما يتلاءم مع التطور الذي تشهده الجرائم المعلوماتية.

وبما يوليه المشرع من أهمية للخبرة التقنية للخبراء المختصين، أقر حماية قانونية إذا كانت حياتهم أو حياة أحد أفراد عائلاتهم مهددة بسبب المعلومات المقدمة من طرفهم للقضاء والتي من شأنها إظهار الحقيقة في الجرائم المذكورة في المادة 129 من قانون الإجراءات الجزائية من بينها جرائم تكنولوجيا الإعلام والاتصال[1].

كما عزز القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها من أهمية الوسائل التقنية في جمع الأدلة الرقمية والكشف عن الجرائم الإلكترونية.

ثالثاً: أهمية الخبرة التقنية في مجال البحث والتحري

تظهر أهمية الخبرة التقنية في كونها تساعد جهات التحقيق على كشف الحقيقة في الجرائم المعلوماتية، خاصة أن الدليل الإلكتروني يتميز بخصوصية تجعله قابلاً للتعديل أو الإتلاف أو الإخفاء بسهولة. ولهذا، يساهم الخبير التقني في استخراج الأدلة الرقمية بطريقة علمية تحافظ على سلامتها القانونية والتقنية.

كما تساعد الخبرة التقنية في:

- تحليل الأنظمة المعلوماتية المخترقة.
- تتبع مصدر الهجمات الإلكترونية وتحديد هوية الفاعلين.
- استرجاع البيانات المحذوفة أو المشفرة.
- فحص الأجهزة والدعائم الرقمية المستعملة في ارتكاب الجريمة.
- تفسير المعطيات التقنية التي يصعب على القاضي أو المحقق فهمها دون مساعدة فنية[2].

رابعاً: دور الخبير التقني في المحافظة على الدليل الإلكتروني

يلعب الخبير التقني دوراً أساسياً في حماية الدليل الإلكتروني من التلف أو التغيير، وذلك من خلال اتباع إجراءات تقنية دقيقة أثناء عملية الفحص والحجز الإلكتروني، لأن أي خطأ تقني قد يؤدي إلى ضياع الدليل أو التشكيك في مصداقيته أمام القضاء.

[1]– المادة 129، القانون رقم 14/25، المتضمن قانون الإجراءات الجزائية.

[2]–أحسن بوسقيعة، *التحقيق في الجرائم المعلوماتية*، (دار هومة للطباعة والنشر والتوزيع، 2021)، 115.

ولهذا، يتعين على الخبير احترام المعايير الفنية المعتمدة أثناء استخراج البيانات وتحليلها، مع توثيق جميع العمليات المنجزة ضمن تقارير فنية رسمية يمكن الاستناد إليها خلال مختلف مراحل الدعوى الجزائية.

وبناء على ما سبق، يتضح أن الخبرة التقنية أصبحت ضرورة حتمية في مجال البحث والتحري عن الجرائم المعلوماتية، بالنظر إلى الطابع الفني والتقني الذي يميز هذا النوع من الجرائم، حيث لم يعد بالإمكان الاعتماد على الوسائل التقليدية وحدها في كشف الحقيقة، بل أصبح اللجوء إلى الخبراء التقنيين أمراً أساسياً لضمان فعالية الإثبات وحماية الدليل الإلكتروني .

الفرع الثاني: مراقبة الاتصالات الإلكترونية

تُعد مراقبة الاتصالات الإلكترونية من بين إجراءات التحقيق الحديثة التي لجأت إليها جهات التحقيق في سعيها لجمع الأدلة الإلكترونية، وذلك من خلال تقنيات حديثة تتماشى مع طبيعة وخصوصية الجريمة الإلكترونية.

كما تعتبر من بين الوسائل الفعالة التي اعتمدها المشرع الجزائري في مجال البحث والتحري عن الجرائم المعلوماتية، نظراً لما توفره من إمكانية تتبع الأنشطة الإجرامية المرتكبة عبر الشبكات والوسائط الرقمية، وكشف هوية الفاعلين وأساليب تنفيذ الجرائم الإلكترونية..

أولاً: الاتصالات الإلكترونية

1- مفهوم الاتصالات الإلكترونية:

لقد عرفت المادة 2 من القانون 09-04 " الاتصالات الإلكترونية بأنها: "كل تراسل أو إرسال أو استقبال لعلامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية[1]"

كما عرفها بموجب المادة 05 من المرسوم الرئاسي رقم 261-15 بأنها " كل تراسل أو إرسال أو استقبال عالمات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال." مما يلاحظ أن المشرع استبدل كلمة "مختلفة" بـ"أيا كانت طبيعتها"، و"بواسطة" بـ"عن طريق"، وأضاف عبارة "بما في ذلك وسائل الهاتف الثابت والنقال"، في محاولة منه لتدارك الثغرة الموجودة في نص المادة 2 من القانون09-04 [2].

[1]- المادة 2 من القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[2]-إسماعيل بن يحيى، "التعريف بمراقبة الاتصالات الإلكترونية كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية"، *مجلة صوت القانون* 8، 2(2022): 1068، https://asjp.cerist.dz/en/downArticle/268/8/3/194283.

2- صور الاتصالات الإلكترونية:

لقد بينت المادة 05 من المرسوم الرئاسي 261-15، صور الاتصالات الإلكترونية المتمثلة في المراسلات السلكية واللاسلكية وكذا البريد الإلكتروني.

أ. المراسلات السلكية واللاسلكية:

يقصد بالمراسلات كافة الرسائل المكتوبة، أياً كانت الوسيلة المستخدمة في إرسالها، سواء وُضعت داخل مظروف مغلق أو مفتوح، أو كانت في شكل بطاقة مكشوفة، متى كان قصد المرسل حجب مضمونها عن غير المرسل إليه. فقد عرف المشرع الجزائري المراسلات السلكية واللاسلكية بموجب المادة 08 الفقرة 02 من القانون 2000-03 بأنها: "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية."

ومن خلال ما جاء به نص المادة، يتبين أن المشرّع عند تنظيمه لمفهوم الاتصالات الإلكترونية قد انصرف إلى المراسلات ذات الطابع السلكي واللاسلكي، مستبعداً بذلك المراسلات التقليدية كالمراسلات الورقية عبر البريد العادي، لعدم إدراجها ضمن مفهوم الاتصالات الإلكترونية[1].

ب. البريد الإلكتروني:

لم يقدّم المشرّع الجزائري تعريفًا للبريد الإلكتروني، غير أنّ الفقه يستأنس بالتعريف الوارد في التشريع الفرنسي ضمن القانون 2000/575، والذي يعتبره كل رسالة نصية أو صوتية أو مرفقة بصور أو أصوات، تُرسل عبر شبكة اتصالات عامة وتُخزّن في خوادم الشبكة أو في أجهزة المرسل إليه ليتمكّن من استرجاعها. في حين اعتمد المشرّع الفرنسي مصطلح Courriel رسميًا، واعتبره مرادفًا لمصطلح Courrier électronique وفق ما ورد في الجريدة الرسمية الفرنسية لسنة 2003[2].

ثانيا: مراقبة الاتصالات الإلكترونية:

1- مفهوم مراقبة الاتصالات الإلكترونية:

لم يضع المشرّع الجزائري تعريفًا لمراقبة الاتصالات الإلكترونية، بل اكتفى بتنظيمها كإجراء قانوني في المادة 03 من القانون 09-04، التي تجيز وضع ترتيبات تقنية لمراقبة الاتصالات وتجميع وتسجيل محتواها داخل منظومة معلوماتية في إطار حماية النظام العام أو مقتضيات التحري والتحقيق[3].

[1]- إسماعيل بن يحيى، نفس المرجع السابق، 1069.

[2]- نفس المرجع.

[3]- نفس المرجع، 1070.

في حين عرفها المشرع الأمريكي، بموجب قانون المراقبة السلكية (Intercept) بأنها: "الاكتساب السمعي أو الالتقاط السمعي، أو أي التقاط لمحتويات أي اتصال سلكي أو إلكتروني أو شفوي باستخدام أي جهاز إلكتروني أو ميكانيكي أو أي جهاز آخر."

كما يعرف الفقه المراقبة الإلكترونية بأنها العمل الذي يقوم به المراقِب باستخدام التقنية الإلكترونية لجمع البيانات والمعلومات والتقصي عن الجرائم والمشتبه فيهم، سواء كان الخاضع للمراقبة شخصًا أو مكانًا أو شيئًا، حسب طبيعته، لتحقيق غرض أمني أو أي غرض آخر[1].

2- أشكال المراقبة الإلكترونية:

أ. اعتراض المراسلات السلكية واللاسلكية:

لقد خول المشرع الجزائري للجهات القضائية المختصة، والمتمثلين في ضباط وأعوان الشرطة القضائية، عملية اعتراض المراسلات السلكية واللاسلكية كما جاء في نص المادة 114 من قانون الإجراءات الجزائية الجزائري رقم 25-14 بأن: " .... يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي: اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ..." لكن المشرع لم يعطي تعريفا صريحا وواضحا لهذه العملية بل اكتفى بذكرها[2].

ب. اعتراض البريد الإلكتروني:

يُعتبر اعتراض البريد الإلكتروني من صور مراقبة الاتصالات الإلكترونية، ونظرًا لكونه يعتمد على شبكة الإنترنت كوسيلة للتواصل، فإن الطرق التقليدية لا تصلح لمراقبة البريد الإلكتروني. لهذا ظهرت برامج متطورة قادرة على مراقبته، ومن بينها نظام كارنيفور (CARNIVORE)، الذي كانت تستخدمه وكالة المباحث الفيدرالية الأمريكية للتجسس[3] .

3- حالات اللجوء إلى مراقبة الاتصالات الإلكترونية

لقد حددت المادة 04 من القانون 09-04 الحالات التي تسمح باللجوء إلى إجراء مراقبة الاتصالات الإلكترونية، والتي تشمل:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

[1]- إسماعيل بن يحيى، نفس المرجع السابق، 1070.

[2]- المادة 114، القانون رقم 14/25، المتضمن قانون الإجراءات الجزائية.

[3]- إسماعيل بن يحيى، مرجع سابق، 1073.

- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية[1].

كما يتم اللجوء إلى عمليات المراقبة في هذه الحالات بناءً على إذن مكتوب من السلطات المختصة، غير أنه في الحالة (2) يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنصوص عليها في المادة 13 من نفس القانون، إذنًا لمدة ستة (6) أشهر قابلة للتجديد، وذلك على أساس تقرير يبيّن طبيعة الترتيبات التقنية المستعملة والأغراض المؤدية لها[2].

ثالثا: ضمانات إجراء المراقبة الإلكترونية

ينبغي اللجوء إلى إجراء مراقبة الاتصالات الإلكترونية إلا إذا كان له مقتضى مبرر، أي أنه يستلزم القيام بالإجراء لعدم وجود بديل، وغالبًا ما يتعلق الأمر بمكافحة الجرائم التي يتم ارتكابها عبر الوسائط الإلكترونية أو أن تكون هذه الأخيرة هدفًا لها، سواء للوقاية منها أو لردع مرتكبيها في حال وقوعها أو الشروع فيها، متى كان الشروع معاقبًا عليه طبقًا لأحكام قانون العقوبات والقوانين العقابية الخاصة.فالجرائم التي يجوز التحقيق فيها بالاستعانة بإجراء مراقبة الاتصالات الإلكترونية، بالنظر إلى موضوعها، محددة على سبيل الحصر في المادة 114 من قانون الإجراءات الجزائية رقم 25-14[3].

أ- مبرر اللجوء لإجراء مراقبة الاتصالات الإلكترونية:

تجيز المادة 3 من القانون رقم 20-23 المتعلق بضبط السمعي البصري، مراقبة الاتصالات الإلكترونية مع مراعاة سرية المراسلات، وذلك لحماية النظام العام أو لمقتضيات التحريات والتحقيقات القضائية. غير أن هذا الإجراء لا يُلجأ إليه بصورة آلية، بل يُقيَّد بالضرورة وغياب البدائل، وفق ما تؤكده المادة 20 من القانون نفسه.

[1]- المادة 4، القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[2]- أحمد بن مالك، مرجع سابق، 959.

[3]-لحسن ناني وبغشام زقاي، " ضوابط وإجراءات مراقبة الاتصالات الإلكترونية في التشريع الجزائري"، الدراسات القانونية المقارنة 9، (جوان 2023):119، https://asjp.cerist.dz/en/article/225601.

ويُستند في طلب الإذن إلى تقرير مفصل يبيّن ظروف القضية، والقرائن المبررة للمراقبة، والوقائع السابقة، مع إثبات عدم جدوى الوسائل الأخرى، إضافة إلى الإشارة إلى المساعدة القضائية الدولية عند الاقتضاء. كما يتضمن التقرير الوسائل التكنولوجية المقترحة لتنفيذ المراقبة بحسب طبيعة الاتصال، مع تحديد حدود استعمالها، وجدول زمني أولي للعملية

ب-تحقيق أغراض إجراء مراقبة الاتصالات الإلكترونية:

لقد أقر المشرّع الجزائري إجراء اللجوء إلى مراقبة الاتصالات الإلكترونية وتفتيش المنظومة المعلوماتية في حالات استثنائية فقط، لما لها من اعتداء على حق الإنسان في سرية حياته الخاصة واتصالاته الشخصية، لغرض معين وهو الوصول إلى حقيقة الجريمة والكشف عن مرتكبيها خلال مرحلتي جمع الاستدلالات والتحقيق الابتدائي، ولم يتم التوصل إلى ذلك عن طريق اللجوء إلى الإجراءات التقليدية، إذ تنص المادة 3من القانون 09-04 على أنه يتم اللجوء إلى هذا الإجراء متى تطلبت مستلزمات التحريات أو التحقيقات القضائية الجارية.

إذ لا يتم إجراء المراقبة إلا بعد ارتكاب الجريمة وأثناء مرحلة جمع الاستدلالات أو التحقيق القضائي، ويكون الغرض من ذلك هو التوصل إلى معرفة مرتكبي الجريمة، وذلك في حالة عدم جدوى الإجراءات التقليدية في الوصول إلى الحقيقة المنشودة[1].

المطلب الثاني: الإجراءات المتبعة للتفتيش في الجرائم المعلوماتية

يصنف التفتيش من بين أهم الإجراءات الجزائية التي تُعتمد في إطار البحث والتحري عن الجرائم المعلوماتية، غير أنّ خصوصية هذا النوع من الجرائم، وما يرتبط به من أدلة رقمية غير مادية وسريعة الزوال، تفرض إخضاع هذا الإجراء لضوابط قانونية دقيقة تختلف في بعض جوانبها عن التفتيش التقليدي. فالتعامل مع الأنظمة المعلوماتية والبيانات الإلكترونية يقتضي مراعاة طبيعتها الخاصة، سواء من حيث كيفية الوصول إليها أو طرق حفظها وضمان سلامتها.

وفي هذا السياق، حرص المشرع على تنظيم التفتيش في الجرائم المعلوماتية من خلال تحديد شروطه الشكلية وهو ما سيتم التطرق إليه في **الفرع الأول** والموضوعية من خلال **الفرع الثاني**، إلى جانب إقرار مجموعة من الضمانات القانونية التي تكفل حماية الحقوق والحريات، لاسيما حرمة الحياة الخاصة وسرية المعطيات الشخصية.

[1]- لحسن ناني وبغشام زقاي، نفس المرجع السابق، 122.

الفرع الأول: الشروط الشكلية للتفتيش في الجرائم المعلوماتية

لقد نص القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، في المادة 5 أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها
- منظومة معلوماتية [1]

ويختلف التفتيش في مجال المعلوماتية عن التفتيش العادي، فالأول يستهدف جهاز الحاسب الآلي بمكوناته المادية والمعنوية، ولمباشرة إجراء التفتيش وفق أحكام المادة 78 من قانون الإجراءات الجزائية يشترط:

1- **وجود الإذن بالتفتيش:** يتوجب وجود إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق. إلى جانب استظهاره قبل دخول المنزل المراد تفتيشه، بالإضافة إلى أن يتضمن البيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش[2].

2- **وقت إجراء التفتيش:** الأصل في التفتيش أنه لا يتم قبل الخامسة صباحا ولا بعد الثامنة مساء، إلا أنه فيما يخص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص[3] مع احترام تدابير السر المهني.

3- **حضور الأشخاص المعنيين أثناء التفتيش:**

حسب ما جاءت به المواد 76، 78، 158 من قانون الإجراءات الجزائري، يشترط أن يتم التفتيش في حضور المتهم، أما في حالة ما إذا تعذر عليه الحضور وقت الإجراء، يتوجب على ضابط الشرطة القضائية تعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربًا كان من الواجب أن ينيب عنه شاهدين من غير المعنيين بالإجراء[4].

4- **محضر التفتيش في الجرائم المعلوماتية:**

تسمى محاضر الشرطة القضائية محاضر البحث الابتدائي وتكمن أهميتها في قيمتها الممنوحة لها كوسيلة إثبات على وقوع الجريمة ونسبتها إلى فاعلها من جهة، ومن جهة أخرى في خطورة الصلاحيات الواسعة الممنوحة بموجبها لضابط الشرطة القضائية، لذلك عرّف المشرع الجزائري محاضر الشرطة القضائية بأنها الوثائق المكتوبة التي يحررها ضابط الشرطة القضائية أثناء ممارسته لمهامه ويضمنها ما عاينه أو تلقاه من

---

[1]- وهيبة رابح، مرجع سابق، 327.

[2]- المرجع السابق نفسه.

[3]- عز الدين عثماني، مرجع سابق، 57.

[4]- المرجع السابق نفسه.

معلومات أو قام به من عمليات تدخل في اختصاصه[1]، وتتمثل هذه الأدلة المادية في الورق، جهاز الحاسب الآلي وملحقاته، الأقراص الصلبة، أقراص الليزر، ...وغيرها باعتبار أن الأشياء المعنوية لا تصلح بطبيعتها لأن تكون محلا للضبط في مجال الجرائم المعلوماتية[2].

الفرع الثاني: الشروط الموضوعية للتفتيش في الجرائم المعلوماتية

إلى جانب الشروط الشكلية، ولكي يكتسب إجراء التفتيش في الجرائم المعلوماتية صفة المشروعية والصحة القانونية، لا بد من توافر مجموعة من الشروط الموضوعية العامة والأساسية التي تتمحور حول وجود سبب نظامي مشروع، ومحل مادي أو افتراضي يقع عليه التفتيش، بالإضافة إلى صدور الأمر من سلطة ذات اختصاص.

وتتمثل هذه الشروط الموضوعية في الآتي:

1- شرط المشروعية والسبب (وقوع جريمة معلوماتية)

يُعد وجود "السبب" الركيزة الأساسية والمشروعية القانونية التي تمنح السلطة المختصة الحق في إصدار إذن التفتيش. فلا يجوز بأي حال من الأحوال انتهاك حرمة النظم المعلوماتية أو مكوّنات الحاسوب والبيانات المتصلة بها إلا إذا تحقق وقوع جريمة فعلية. وينبثق عن هذا الشرط جزئيتان هما:

- **أن تحمل الجريمة وصف جناية أو جنحة:** لا يجوز مباشرة التفتيش المعلوماتي إلا إذا كانت الجريمة الإلكترونية المرتكبة تُصنف قانوناً بأنها جناية أو جنحة، وتُستثنى المخالفات تماماً من نطاق التفتيش نظراً لقلة خطورتها، وحمايةً لحرمة الحياة الخاصة للأشخاص وسرية اتصالاتهم التي لا تتناسب مع ضآلة المخالفة.

- **حتمية وقوع الجريمة:** يجب أن يكون التفتيش مبنياً على جريمة وقعت بالفعل ويجري التحقيق فيها، فلا يجوز التفتيش بناءً على افتراضات أو توقعات لجريمة محتملة الوقوع في المستقبل[3].

- **اتهام شخص أو أكثر بمساهمتهم في ارتكاب الجريمة:** يجب أن تتوافر ضد الشخص المراد تفتيشه أو تفتيش حاسوبه أو منزله دلائل كافية للاعتقاد بأنه ساهم في ارتكاب الجريمة، سواء كانت بصفة فاعل أصلي أو شريك يستوجب اتهامه بها، وكذا خبرة القائم بالتفتيش والتي يمكن بها تأكيد نسبة الجريمة لفاعلها،

[1]-عز الدين عثماني، مرجع سابق، 57.
[2]- رابح وهيبة، مرجع سابق، 328.
[3]– سهيلة طمين، "إشكالية التفتيش في الجريمة المعلوماتية"، المجلة النقدية للقانون والعلوم السياسية 20، (2025): 471، https://asjp.cerist.dz/en/article/271847.

ويعتبر عدم اكتشاف قاضي التحقيق لهوية المتهم في الشكاوى ضد مجهولين، سببا لحفظ الملف وإصدار أمر ألا وجه للمتابعة[1].

- **توافر إشارات ودلائل قوية توحي إلى تواجد أدلة تفيد في كشف الجريمة:** قبل أن يقوم المحقق بعملية التفتيش أو يأذن بها لا بد من توافر دلائل كافية، ويقصد بها الإشارات التي تقوم عادة على المضمون العقلي والمنطقي لوقائع وملابسات الجريمة، على أن المحل المراد تفتيشه تتواجد فيهم وسائل أو برامج استعملت في اقتراف الجريمة أو فيه مستندات معلوماتية تساعد على الكشف عن الجريمة[2].

2- محل التفتيش المعلوماتي:

المحل في الجريمة المعلوماتية لا يقوم بذاته، بل يرتبط بمكان تواجد المتهم والأجهزة التي بحوزته (كالحاسوب والهاتف). ويُشترط في هذا المحل موضوعياً ما يلي:

- **أن يكون معيناً تعييناً نافياً للجهالة:** حمايةً للحريات، يجب تحديد الأجهزة والأنظمة المراد تفتيشها بدقة. فلا يجوز تفتيش جميع حواسب شركةٍ ما بشكل عشوائي، ولا تفتيش هواتف أفراد عائلة المتهم دون مبرر قانوني يربطهم بالجريمة.
- **ألا يكون المحل متمتعاً بالحصانة:** استثنى القانون بعض الأماكن والأشخاص من التفتيش المباشر (مثل: المقار الدبلوماسية، مكاتب المحامين، والمجالس النيابية). فلا يجوز تفتيش وسائلهم الإلكترونية إلا من قِبل القاضي المختص ووفق إجراءات استثنائية صارمة، وإلا عُدَّ الإجراء باطلاً[3].

3- يجب أن تكون السلطة مختصة بالتفتيش: يعتبر قاضي التحقيق صاحب الاختصاص الأصيل في

إصدار إذن التفتيش ومباشرته وفقاً لقواعد الاختصاص المحلي والنوعي التي نصت عليها المادة 69 من قانون الإجراءات الجزائية المعدل والمتمم رقم 25-04. في حين يمارس رجال الضبط القضائي (الشرطة والدرك) التفتيش إما بناءً على ندب قضائي (إذن مكتوب) من قاضي التحقيق، أو في حالة التلبس بالشرط القانوني الذي يبيح تفتيش ما بحوزة المقبوض عليه من هواتف وحواسب. بينما تتولى الجهات المستحدثة المراقبة المستمرة للشبكات والوقاية من الجرائم الإلكترونية وتتبعها وفق القانون رقم 9-04[4].

[1]- سهيلة طمين، نفس المرجع السابق، 471.

[2]- المرجع السابق نفسه، 472.

[3]- المرجع نفسه.

[4]- المرجع نفسه.

يتضح من خلال ما تم التطرق إليه في هذا الفصل المتعلق بالآليات المؤسساتية في مجال البحث والتحري عن الجرائم المعلوماتية أن المشرع الجزائري قد سعى إلى بناء منظومة متكاملة تجمع بين الوقاية من هذا النوع المستحدث من الإجرام وبين مكافحته بوسائل قانونية وتقنية متطورة، تتماشى مع التحولات الرقمية المتسارعة.

فمن جهة أولى، أُسندت مهمة الوقاية والحماية إلى هيئات رقابية متخصصة، على غرار الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، باعتبارهما آليتين مؤسساتيتين تعملان على تعزيز الأمن الرقمي وحماية الحقوق والحريات، خاصة الحق في الخصوصية وحماية البيانات الشخصية.

ومن جهة ثانية، أوكلت مهمة البحث والتحري إلى أجهزة الضبطية القضائية المتخصصة والنيابة العامة، التي تمثل العمود الفقري في كشف الجرائم المعلوماتية وجمع الأدلة الرقمية وتوجيه مجريات التحقيق، في إطار احترام مبدأ المشروعية والرقابة القضائية.

كما أبرز هذا الفصل أهمية الوسائل التقنية الحديثة في دعم العمل التحقيقي، حيث أصبحت الخبرة التقنية، وبرامج التتبع وكشف الاختراق، ومراقبة الاتصالات الإلكترونية أدوات أساسية لا غنى عنها في مواجهة الجرائم السيبرانية، لما توفره من قدرة على تحليل المعطيات الرقمية وتتبع الجناة وكشف أساليبهم الإجرامية.

وفي السياق ذاته، تبين أن إجراءات التفتيش في الجرائم المعلوماتية قد خضعت لضوابط دقيقة من حيث الشروط الشكلية والموضوعية، إلى جانب إقرار ضمانات قانونية صارمة، بهدف تحقيق التوازن بين فعالية البحث والتحري من جهة، وصون الحقوق والحريات الفردية وحماية الحياة الخاصة من جهة أخرى، خصوصاً في ظل حساسية الدليل الرقمي وسهولة التلاعب به.

وعليه، يمكن القول إن المنظومة القانونية والمؤسساتية الجزائرية في مجال مكافحة الجرائم المعلوماتية تشكل إطاراً متكاملاً نسبياً، إلا أنها تبقى في حاجة مستمرة إلى التطوير والتحديث، لمواكبة التطور المتسارع لوسائل الإجرام الإلكتروني وتعزيز فعالية آليات المكافحة والتحري على المستويين الوطني والدولي.

خاتمة

خاتمة:

في الختام، يتبين أن الجرائم المعلوماتية أصبحت من أخطر التحديات التي تواجه المنظومة القانونية والأمنية الحديثة، نظرا للتطور المتسارع لتكنولوجيات الإعلام والاتصال واتساع استخدام الوسائط الرقمية في مختلف مجالات الحياة. ولأجل التصدي لهذه الجرائم، عمل المشرّع الجزائري على وضع منظومة قانونية وأمنية تعتمد على أجهزة مختصة في البحث والتحري، تتولى كشف الجرائم المعلوماتية وتتبع مرتكبيها باستعمال وسائل تقنية وقانونية تتماشى مع طبيعة هذا النوع المستحدث من الجرائم. وقد تجسد ذلك من خلال إرساء قواعد إجرائية خاصة، وسنّ نصوص قانونية متعلقة بحماية الأنظمة المعلوماتية والمعطيات الشخصية، إلى جانب إنشاء هيئات وأجهزة متخصصة موجهة لمكافحة الجرائم المعلوماتية وتعزيز الأمن السيبراني.

غير أنّ فعالية هذه المنظومة تبقى مرتبطة بمدى تطوير الوسائل التقنية، وتحسين مستوى تكوين الموارد البشرية المتخصصة، وتعزيز التعاون الوطني والدولي في مجال تبادل الخبرات والمعلومات، بالنظر إلى الطابع التقني والعابر للحدود الذي يميز هذا النوع من الجرائم. لذلك، فإن مكافحة الجرائم المعلوماتية تقتضي مواصلة تحديث التشريع الجزائري وتدعيم آليات التنسيق بين مختلف الجهات المعنية، بما يضمن تحقيق التوازن بين حماية الأمن الرقمي والمعلوماتي للأفراد واحترام الحقوق والحريات الأساسية.

ومن خلال دراستنا لهذا الموضوع، توصلنا إلى جملة من النتائج، من أهمها:

- أن المشرّع الجزائري لم يستقر على تسمية موحدة للجرائم المعلوماتية، إذ استخدم في بعض النصوص مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، وفي نصوص أخرى مصطلح "جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، الأمر الذي يعكس نوعا من عدم التوحيد الاصطلاحي في السياسة التشريعية الجزائرية.

- رغم تعدد صور الجرائم المعلوماتية وتباين درجة خطورتها، وما تتميز به من طبيعة تقنية خاصة وآثار اقتصادية وأمنية بالغة، إلا أن المشرّع الجزائري اتجه في معالجتها إلى تبني ذات السياسة العقابية المقررة للجرائم التقليدية، من خلال التركيز على الجزاءات المادية والجزائية دون إرساء منظومة قانونية متكاملة تتلاءم مع خصوصية هذا النوع من الجرائم.

- أن الطابع العابر للحدود لهذه الجرائم وسهولة ارتكابها وتحقيق عوائد مالية ضخمة منها، يقتضي اعتماد نصوص قانونية أكثر تخصصا ومرونة، قادرة على مواكبة التطور التكنولوجي وأساليب الإجرام الرقمي الحديثة.

- مواكبة الجزائر نسبيا للتطورات الدولية المتعلقة بمكافحة الجرائم المعلوماتية، من خلال تبني بعض الآليات الحديثة المرتبطة بحماية الأنظمة المعلوماتية وحماية المعطيات ذات الطابع الشخصي.

- أن المشرّع الجزائري أولى أهمية خاصة للدليل الإلكتروني، من خلال تكريس حجيته القانونية في الإثبات، بما ساهم في تسهيل عملية الإثبات أمام الجهات القضائية في الجرائم المعلوماتية.

- اعتماد المشرّع على أجهزة وهيئات متخصصة في مجال الوقاية والبحث والتحري، على غرار الضبطية القضائية المتخصصة والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

- محدودية الإمكانيات التقنية والوسائل الحديثة اللازمة لكشف بعض الجرائم المرتكبة عبر الخوارزميات والتطبيقات المتطورة وتقنيات إخفاء الهوية وتمويه عنوان الحاسب الآلي الخاص بالمجرم.

- وجود بطء إجرائي أحيانا في التعامل مع بعض القضايا المعلوماتية مقارنة بسرعة ارتكاب الجريمة وانتشار آثارها في البيئة الرقمية.

- وجود فراغ تشريعي نسبي فيما يتعلق ببعض الجوانب المستحدثة للجرائم المعلوماتية، وعدم تحيين بعض النصوص القانونية بما يواكب التطورات التقنية الحديثة، الأمر الذي ينعكس سلبا على فعالية أجهزة البحث والتحري.

- محدودية الخبرة التقنية الوطنية في بعض المجالات الدقيقة، خاصة ما يتعلق بالأمن السيبراني والتحليل الجنائي الرقمي المتقدم واسترجاع الأدلة الرقمية.

وبناء على هذه النتائج، يمكن تقديم جملة من التوصيات، تتمثل فيما يلي:

- مراجعة وتحيين القوانين المتعلقة بالجرائم المعلوماتية بشكل دوري، مع توسيع نطاق الحماية القانونية بما ينسجم مع التطور المستمر للتكنولوجيا، ولِمَ لا إصدار قانون خاص ومستقل بالجرائم المعلوماتية.

- تعزيز التكوين المتخصص لفائدة القضاة وأعوان الضبطية القضائية والخبراء التقنيين، بما يسمح برفع كفاءتهم في التعامل مع الأدلة الرقمية والجرائم الإلكترونية الحديثة.

- تدعيم الأجهزة المختصة بالوسائل التقنية الحديثة والبرمجيات المتطورة اللازمة لكشف الجرائم المعلوماتية وتتبع مرتكبيها.

- إطلاق حملات تحسيسية وتوعوية لفائدة الأفراد والمؤسسات حول مخاطر الجرائم المعلوماتية وطرق الوقاية منها.

- تطوير منصات إلكترونية خاصة بالجهات الأمنية والقضائية من أجل تسهيل وسرعة التبليغ عن الجرائم المعلوماتية، وتفادي الإجراءات التقليدية والورقية.

- تعزيز التعاون الدولي والإقليمي في مجال مكافحة الجرائم المعلوماتية، خاصة فيما يتعلق بتبادل المعلومات والخبرات وتسليم المجرمين.

- تشجيع البحث العلمي وإقامة شراكات بين الجامعات ومراكز البحث والهيئات الأمنية، قصد تطوير آليات مبتكرة لمواجهة الجرائم المعلوماتية.

- دعم التخصصات الجامعية المتعلقة بالأمن السيبراني والتحقيق الرقمي، بما يساهم في تكوين كفاءات وطنية قادرة على مواكبة التطورات التقنية الحديثة.

- العمل على تحقيق التوازن بين متطلبات مكافحة الجرائم المعلوماتية وضمان احترام الحقوق والحريات الأساسية، خاصة الحق في الخصوصية وحماية المعطيات الشخصية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

I- المصادر

1- النصوص التشريعية:

- أمر رقم 156/66 مؤرخ في 8 جويلية 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم بالقانون رقم 04-15، المؤرخ في 01فيفري 2015، ج ر عدد71 الصادرة في 30 ديسمبر 2015.
- قانون الإجراءات الجزائية الجزائري رقم 25-14، المؤرخ في 03أوت 2025، ج ر عدد54 الصادرة في 13 أوت 2025.
- قانون رقم 04/09 المؤرخ في 08 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47 الصادرة في 16 أوت 2009.
- القانون العضوي رقم 23-14، المتعلق بالإعلام، المؤرخ في 27 أوت 2023، ج ر عدد 56 الصادرة في 29 أوت 2023.

2- النصوص التنظيمية:

المرسوم الرئاسي رقم 19-172، المتعلق بتحديد تشكيلة الهيئة الوطنية لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، المؤرخ في 6جوان 2019، ج ر عدد37 الصادرة في 9 جوان 2019.

II- المراجع:

أولا: الكتب

1- بوسقيعة أحسن، التحقيق في الجرائم المعلوماتية، دار هومة للطباعة والنشر والتوزيع، 2021.

2- جندل أحمد محمد، الجرائم الإلكترونية، دار المعتز للنشر والتوزيع، 2022.

3- خينش دليلة، الجريمة الإلكترونية والأمن الاجتماعي، ديوان المطبوعات الجزائرية، 2023.

4- عباسي صلاح الدين، سلسلة العلوم الإجرامية: دراسات في علم الإجرام، Alpha Doc، 2015.

5- ياكر الطاهر، الجرائم الإلكترونية: الأحكام الموضوعية والإجرائية – دراسة مقارنة، دار بلقيس، 2024.

6- أبو القاسم طاهر محمود، الجرائم المعلوماتية: صعوبات وسائل التحقيق فيها وكيفية مواجهتها، المنظمة العربية للتنمية الإدارية، 2019.

7- العتوم محمد الشبلي، جرائم تكنولوجيا المعلومات: النظرية العامة للجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، 2021.

ثانيا: أطروحات الدكتوراه (بالنسبة للأطروحات ترتب بعد الكتب أي ثانيا)

1- غازي زامل صهيب سهيل، "البحث والتحري عن الدليل الإلكتروني في المسائل الجزائية – دراسة حالة –"، أطروحة دكتوراه، جامعة وهران 2، 2020-2021.

ثالثا: المقالات العلمية

1- بن جديد فتحي، "حماية برامج الحاسوب بين قانون حقوق المؤلف الجزائري والاتفاقات الدولية"، مجلة صوت القانون، 9(2)، 2023، https://asjp.cerist.dz/en/article/221469.

2- بن دعاس سهام وبن عثمان فادية، "ضمانات حماية المعطيات الشخصية في البيئة الرقمية في التشريع الجزائري"، مجلة الحقوق والعلوم الإنسانية، 15، 2022، https://asjp.cerist.dz/en/downArticle/315/15/1/186266.

3- بن مالك أحمد، "خصوصية الجريمة المعلوماتية وسبل مكافحتها في التشريع الجزائري"، المجلة الجزائرية للحقوق والعلوم السياسية، 8(1)، 2023، https://asjp.cerist.dz/en/article/222122.

4- بن يحيى إسماعيل، "التعريف بمراقبة الاتصالات الإلكترونية كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية"، مجلة صوت القانون، عدد 8(2)، 2022، https://asjp.cerist.dz/en/downArticle/268/8/3/194283.

5- بوزبورة سهيلة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية"، المجلة النقدية للقانون والعلوم السياسية، 17(2)، 2022، https://asjp.cerist.dz/en/article/209229.

6- بوضياف أسمهان، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع.11، 2018، https://asjp.cerist.dz/en/article/81720.

7- بوكحيل حكيمة وسامية بن عديد، "الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية"، الدراسات القانونية المقارنة، 7، 2021، https://asjp.cerist.dz/en/article/156755.

8- حابت أمال، "الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 04-15 و09-04"، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، 7(25)، 2023، https://asjp.cerist.dz/en/article/218900.

9- حابت أمال، "دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، المجلة الدولية للبحوث القانونية والسياسية، 5(3)، 2021، https://asjp.cerist.dz/en/article/174814.

10- حبيباتني بثينة، "معوقات مكافحة الجريمة المعلوماتية"، مجلة العلوم الإنسانية، ع.50، 2018، https://revue.umc.edu.dz/h/article/view/2827/2973.

11- حمزة خضري وحمزة عشاش، "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، 6(2)، 2020، https://asjp.cerist.dz/en/article/116332.

12- حوحو رمزي، منيرة بلورغي، "مواجهة الجريمة المعلوماتية في الجزائر"، مجلة الحقوق والحريات، ع.2، 2014، https://asjp.cerist.dz/en/article/139253.

13- ضو خالد، "حجية الدليل الإلكتروني وشروط قبوله في الإثبات الجنائي"، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، 5(8)، 2022، https://asjp.cerist.dz/en/article/183140.

14- طمين سهيلة، "إشكالية التفتيش في الجريمة المعلوماتية"، المجلة النقدية للقانون والعلوم السياسية، 20، 2025، https://asjp.cerist.dz/en/article/271847.

15- عبد الحميد عائشة، "الجرائم المعلوماتية وكيفية مكافحتها"، مجلة الإناسة وعلوم المجتمع، 7، 2020.

16- عثماني عز الدين، "إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية"، مجلة دائرة البحوث والدراسات القانونية والسياسية، 2(4)، 2018، https://asjp.cerist.dz/en/article/132110.

17- قرانة عادل وبوحديد فارس، "مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري"، مجلة العلوم القانونية والاجتماعية، 7(2)، 2021، https://asjp.cerist.dz/en/article/152268.

18- كحلاوي عبد الهادي وبن زيطة عبد الهادي، "آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون رقم 18-07"، مجلة القانون والعلوم السياسية، 7(2)، 2021، https://asjp.cerist.dz/en/article/163125.

19- مقري صونيا وبن بلعامر وليد، "المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي رقم 20-05"، مجلة البحوث في العقود وقانون الأعمال، 2، 2025، https://asjp.cerist.dz/en/article/281092.

20- ناني لحسن وزقاي بغشام، "ضوابط وإجراءات مراقبة الاتصالات الإلكترونية في التشريع الجزائري"، الدراسات القانونية المقارنة، 9، 2023، https://asjp.cerist.dz/en/article/225601.

21- تابري مختار، "الخبرة في الجريمة المعلوماتية"، الحوار المتوسطي، 11(3)، 2020، https://asjp.cerist.dz/en/article/142535.

22- عراب مريم، "الاختصاص القضائي في الجرائم المعلوماتية"، حوليات كلية الحقوق والعلوم السياسية، 7(3)، 2015، https://asjp.cerist.dz/en/article/80969.

23- بن أحمد محمد، "الأحكام القانونية لأركان الجريمة المعلوماتية: دراسة في التشريع الجزائري والمقارن"، مجلة البحوث في الحقوق والعلوم السياسية، 10(2)، 2024، https://asjp.cerist.dz/en/article/258272.

24- شرف الدين وردة، "مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري"، مجلة المفكر، 10(2)، 2017، https://asjp.cerist.dz/en/article/62283.

25- رابح وهيبة، "الجريمة المعلوماتية في التشريع الإجرائي الجزائري"، مجلة الباحث للدراسات الأكاديمية، 4، 2014، https://asjp.cerist.dz/en/article/5724.

رابعا: الوثائق

القوانين المقارنة:

1- قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018، رقم 175، الجريدة الرسمية للجمهورية المصرية، عدد 32 مكرر.

2- نظام مكافحة الجرائم المعلوماتية، المرسوم الملكي السعودي رقم م/17، قرار مجلس الوزراء رقم 79، المؤرخ في 8 ربيع الأول 1428هـ الموافق لـ 26 مارس 2007.

3- قانون الجرائم الإلكترونية الأردني لسنة 2023، رقم 17، الجريدة الرسمية الأردنية عدد 5843.

قائمة المحتويات

الفهرس

مقدمة: 2

الفصل الأول: الإطار المفاهيمي والقانوني للبحث والتحري عن الجرائم المعلوماتية 8

المبحث الأول: مفاهيم عامة حول الجرائم المعلوماتية. 9

المطلب الأول: مفهوم الجريمة المعلوماتية..... 9

الفرع الأول: تعريف الجريمة المعلوماتية 9

أولا: تعريف الجريمة 9

ثانيا: تعريف المعلوماتية 10

ثالثا: تعريف الجرائم المعلوماتية "Information Crimes" 10

الفرع الثاني: خصائص الجريمة المعلوماتية 18

الفرع الثالث: أركان الجريمة المعلوماتية..... 21

أولا: الركن الشرعي 21

ثانيا: الركن المادي 22

ثالثا: الركن المعنوي 25

المطلب الثاني: صور الجرائم المعلوماتية 27

الفرع الأول: الجرائم الواقعة على البرامج 27

أولا: الجرائم الواقعة على البرامج التطبيقية 27

ثانيا: الجرائم الواقعة على برامج التشغيل..... 28

الفرع الثاني: الجرائم الواقعة على الأشخاص 29

الفرع الثالث: الجرائم الواقعة على الأموال 30

المبحث الثاني: الإطار القانوني لعميات البحث والتحري على الجرائم المعلوماتية..... 31

المطلب الأول: التكريس القانوني لسلطة البحث والتحري عن الجرائم المعلوماتية 31

الفرع الأول: تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل القوانين العامة 32

أولا: تكريس سلطة البحث والتحري في ظل قانون الإجراءات الجزائية 32

ثانيا: تكريس سلطة البحث والتحري في ظل قانون العقوبات الجزائري 33

الفرع الثاني: تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل القوانين الخاصة 34

أولا: تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل قانون الإعلام والقانون رقم 03_05 35
ثانيا: تكريس سلطة البحث والتحري عن الجرائم المعلوماتية في ظل قانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال رقم09-04: 36
المطلب الثاني: صعوبات البحث والتحري عن الجرائم المعلوماتية 37
الفرع الأول: الصعوبات المرتبطة بالمنظومة القانونية 37
أولا: عدم ملاءمة القواعد الإجرائية التقليدية لطبيعة الجرائم المعلوماتية 37
ثانيا: إشكالات الإثبات بالدليل الرقمي 38
ثالثا: تحديات تحقيق التوازن بين متطلبات البحث والتحري والحق في الخصوصية..... 39
الفرع الثاني: الصعوبات المادية 39
الفرع الثالث: الصعوبات المتعلقة بالمورد البشري 40
أولا: ضعف التكوين المتخصص 40
ثانيا: قلة الخبراء المتخصصين في مجال الأدلة الرقمية 41
الفصل الثاني: الآليات المؤسساتية في مجال البحث والتحري عن الجرائم المعلوماتية .... **Error! Bookmark not defined.**
المبحث الأول: الأجهزة المكلفة بالوقاية في الجرائم المعلوماتية والتحري عنها..... 45
المطلب الأول: الهيئات الرقابية في مجال الجرائم المعلوماتية 45
الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 45
أولا: الإطار القانوني والتنظيمي للهيئة..... 46
ثانيا: مهام وصلاحيات الهيئة 48
الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي 50
أولا: الإطار القانوني والتنظيمي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي..... 50
ثانيا: مهام وصلاحيات السلطة..... 53
المطلب الثاني: الأجهزة المكلفة بالبحث والتحري عن الجرائم المعلوماتية..... 55
الفرع الأول: الضبطية القضائية المتخصصة في مجال البحث والتحري عن الجرائم المعلوماتية..... 55
أولا: جهات الضبطية القضائية:..... 55

ثانيا: مهام الضبطية القضائية المتخصصة في الجرائم المعلوماتية 58
الفرع الثاني: دور النيابة العامة في التوجيه والمتابعة 59
أولًا: دور النيابة العامة في توجيه أعمال الضبطية القضائية 59
ثانيًا: دور النيابة العامة في متابعة أعمال الضبطية القضائية 59
المبحث الثاني: وسائل وإجراءات التحري عن الجرائم المعلوماتية 60
المطلب الأول: الوسائل المستخدمة في مجال البحث والتحري عن الجرائم المعلوماتية 60
الفرع الأول: دور الخبرة التقنية في عملية البحث والتحري عن الجرائم المعلوماتية 61
أولاً: مفهوم الخبرة التقنية في الجرائم المعلوماتية 61
ثانياً: الأساس القانوني للخبرة التقنية في التشريع الجزائري 61
ثالثاً: أهمية الخبرة التقنية في مجال البحث والتحري 62
رابعاً: دور الخبير التقني في المحافظة على الدليل الإلكتروني 62
الفرع الثاني: مراقبة الاتصالات الإلكترونية 63
أولاً: الاتصالات الإلكترونية 63
ثانيا: مراقبة الاتصالات الإلكترونية: 64
ثالثا: ضمانات إجراء المراقبة الإلكترونية 66
المطلب الثاني: الإجراءات المتبعة للتفتيش في الجرائم المعلوماتية 67
الفرع الأول: الشروط الشكلية للتفتيش في الجرائم المعلوماتية 68
الفرع الثاني: الشروط الموضوعية للتفتيش في الجرائم المعلوماتية 69
خاتمة 72
قائمة المصادر والمراجع 72