وزارة التعليـم العالــي والبحـث العلمي
المركز الجامعي عبد الحفيظ بوالصوف –ميلة
معهد الحقوق

القسم: الحقوق
الشعبة: قانون عام
التخصص: قانون جنائي

الرقم التسلسلي: .....
الرمـــــــــز: .....

مرحلة التحقيق في الجرائم المعلوماتية في ظل التشريع الجنائي الجزائري

مذكرة ضمن متطلبات نيل شهادة الماستر

من إعداد الطالبتين:
- باغي صبرينة
- قريقة غادة

إشراف الأستاذ:
د. حمدوني علي

السنة الجامعية: 2025/2024

وزارة التعليـم العالــي والبحـث العلمي
المركز الجامعي عبد الحفيظ بوالصوف –ميلة
معهد الحقوق

القسم: الحقوق
الشعبة: قانون عام
التخصص: قانون جنائي

الرقم التسلسلي: .....
الرمـــــــــز: .....

مرحلة التحقيق في الجرائم المعلوماتية في ظل التشريع الجنائي الجزائري

مذكرة ضمن متطلبات نيل شهادة الماستر

من إعداد الطالبتين:
- باغي صبرينة
- قريقة غادة

إشراف الأستاذ:
د. حمدوني علي

أعضاء لجنة المناقشة:

د. بوصبع فؤاد	**المركز الجامعي عبد الحفيظ بوالصوف ميلة**	**أستاذ محاضر أ**	**رئيسا**
د. حمدوني علي	**المركز الجامعي عبد الحفيظ بوالصوف ميلة**	**أستاذ محاضر ب**	**مشرفا ومقررا**
د. بولعراس أحمد	**المركز الجامعي عبد الحفيظ بوالصوف ميلة**	**أستاذ محاضر ب**	**عضوا مناقشا**

السنة الجامعية: 2025/2024

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

قال الله تعالى:

﴿...يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ...﴾

سورة المجادلة، الآية 11.

الشكر والتقدير

الحمد لله الذي وفّقنا ويسّر لنا سُبل العلم والمعرفة، وأعاننا على إتمام هذا العمل المتواضع، فله الحمد أولاً وآخراً.

نتقدّم بخالص الشكر والتقدير للأستاذ الفاضل حمدوني علي على ما بذله من جهد في توجيهينا ومرافقتنا طيلة مراحل إعداد هذه المذكرة، وعلى صبره وحرصه الدائم على تقديم النصح والتصويب، فجزاه الله عنا كل خير.

كما لا يفوتني أن أتوجّه بالشكر إلى كل من قدّم لي يد العون، من أساتذة أجلّاء وزملاء أعزاء، ولكل من شجعني وساندني خلال هذه الرحلة العلمية.

الإهداء

أهدي عملي هذا

إلى والداي العزيزان أطال الله في عمرهما

إلى إخوتي و أخواتي على دعمهم وتشجيعهم في كل خطوة

إلى أولاد أختي تسنيم وأنس و"غيث رحمه الله"

إلى كل من ساعدوني في هذه المرحلة

إلى العائلة والأصدقاء

أهدي هذا العمل تقديرا وإمتنانا .

"باغي صبرينة"

الإهداء

إلى أمي أطال الله في عمرها

إلى أبي الغالي رحمه الله

إلى إخوتي و أخواتي وأولادهم

إلى العائلة والأصدقاء

أهدي هذا العمل إلى كل من ساندني

"قريقة غادة "

قائمة المختصرات:

ق إ ج ج: قانون الإجراءات الجزائية الجزائري

ق ع ج: قانون العقوبات الجزائري

ق ع ف: قانون العقوبات الفرنسي

ق ع: قانون العقوبات

ق: قانون

ص: الصفحة

ط أ: الطبعة الأولى

ج ر: الجريدة الرسمية

إلخ: إلى أخره

ص ص: من الصفحة إلى الصفحة

مقدمة

المقدمة

أضحى العالم المعاصر يشهد ثورة معلوماتية وتكنولوجية غير مسبوقة، كان لها بالغ الأثر على جميع جوانب الحياة الإنسانية، سواء على المستوى الاقتصادي، الاجتماعي، السياسي أو القانوني. فقد أصبحت الوسائل التقنية جزءًا لا يتجزأ من الحياة اليومية، من خلال الاعتماد المتزايد على شبكات الإنترنت، وأجهزة الحاسوب، والهواتف الذكية، وقواعد البيانات، والتطبيقات المختلفة، التي غيّرت شكل التفاعل البشري وفرضت نمطًا جديدًا من السلوك والمعاملات. هذا التوسع الرقمي، على الرغم من فوائده الجمة، إلا أنه رافقه في المقابل ظهور شكل جديد من الجريمة، يُعرف بالجريمة المعلوماتية، والتي أفرزت بدورها واقعًا قانونيًا وأمنيًا معقدًا يتطلب تكييفًا خاصًا في مجال التجريم والعقاب، وكذا على مستوى الإجراءات المتبعة في ملاحقة مرتكبيها.

إن الجريمة المعلوماتية، أو ما يصطلح عليها أحيانًا بالجريمة الإلكترونية أو السيبرانية، تتميز بكونها جريمة غير تقليدية، تتطلب وسائل غير تقليدية كذلك في مواجهتها. فهي ترتكب في الفضاء الرقمي باستخدام وسائل تكنولوجية معقدة، وغالبًا ما يكون مرتكبوها على دراية كبيرة بالتقنيات الحديثة، ويقومون بإخفاء آثارهم باحترافية تجعل من اكتشافهم أمرًا صعبًا، مما يطرح تحديات كبيرة على أجهزة إنفاذ القانون، خصوصًا في مرحلة التحقيق التي تُعد من أهم المراحل في مسار الدعوى العمومية، لما لها من دور محوري في جمع الأدلة، وتحقيق التوازن بين مصلحة المجتمع في ملاحقة الجناة، وضمان حقوق الأفراد وحرياتهم.

وقد بات من الضروري أن يواكب التشريع الجنائي هذه التحولات، من خلال استحداث قواعد إجرائية تتلائم مع خصوصية هذا النوع من الجرائم، وتمكين سلطات التحقيق من الوسائل القانونية والتقنية الضرورية لممارسة مهامها بكفاءة وفعالية.

حيث يهدف هذا البحث إلى دراسة مرحلة التحقيق في الجرائم المعلوماتية، باعتبارها المرحلة التي تُجمع فيها الأدلة ويتم من خلالها توجيه الاتهام، وهي مرحلة أساسية في مسار العدالة الجزائية. وقد اخترنا التركيز على هذه المرحلة لكونها تختلف في الجرائم المعلوماتية عن نظيرتها في الجرائم التقليدية، من حيث طبيعة الأدلة، سرعة ضياعها، الحاجة إلى خبرات تقنية متخصصة، وكذا من حيث الإجراءات الواجب اتباعها لضمان قانونية جمع المعلومات، واحترام خصوصية الأفراد.

وتكمن أهمية هذا الموضوع في كونه يعالج إشكالية حديثة ومعقدة لم تحظ بعد بدراسة وافية في الأدبيات القانونية الجزائرية، رغم تزايد معدلات الجريمة الإلكترونية، والتحديات التي باتت تفرضها على أجهزة العدالة. كما تبرز أهميته من خلال ارتباطه بالتحول الرقمي الذي يشهده العالم، وضرورة بناء عدالة جنائية رقمية قادرة على التصدي للجرائم المستحدثة دون المساس بالضمانات الدستورية للمواطنين.

وبناء على ما سبق، تبرز إشكالية موضوع البحث من خلال طرح التساؤل الأتي:

ما مدى فعالية نصوص التشريع الجنائية، لتنظيم مرحلة التحقيق في الجرائم المعلوماتية؟

ويتفرع عن هذه الإشكالية جملة من التساؤلات الفرعية، من أبرزها:

- ما هي الخصائص التي تميز الجريمة المعلوماتية عن باقي الجرائم؟
- ما هو الإطار القانوني المعتمد في تنظيم مرحلة التحقيق في هذا النوع من الجرائم؟
- ما هي أهم أنواع الجرائم المعلوماتية؟ وما الأركان اللازمة لتكييفها جنائيًا؟
- ما هي الوسائل والأدوات المعتمدة للتحقيق في الجرائم المعلوماتية؟
- كيف تختلف أساليب التحقيق التقليدية عن الأساليب المستحدثة لمواجهة هذا النوع من الجرائم؟

أما بالنسبة إلى **أسباب اختيار الموضوع** يعود اختيارنا لهذا الموضوع إلى عدة اعتبارات علمية وعملية، نلخصها فيما يلي:

- خصوصية الجريمة المعلوماتية وإختلافها عن الجرائم التقليدية: من حيث الطبيعة والأركان والدوافع وهو ما إستدعى التطرق لها بشكل مفصل في الفصل الأول من خلال تناول الإطار المفاهيمي.
- أهمية مرحلة التحقيق في مواجهة هذا النوع من الجرائم: لكونها مرحلة حاسمة في جمع الأدلة وتحديد المسؤوليات، خاصة في ظل تحديات إثبات الجريمة المعلوماتية.
- تعدد صور الجريمة المعلوماتية وتنوع مرتكبيها: بين الأفراد العاديين والعصابات المنظمة، مما يجعل مسألة التحقيق فيها أكثر تعقيدا وتتطلب أدوات متطورة ومقاربة قانونية دقيقة..

وبالنسبة إلى **أهداف الدراسة** فتسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف، نذكر منها:

- تحليل الإطار المفاهيمي والقانوني في الجرائم المعلوماتية من خلال توضيح مفهوم التحقيق الجنائي الإلكتروني، خصائصه، وتمييزه عن التحقيق التقليدي، وكدا إبراز الشروط والوسائل القانونية اللازمة.

- تحليل أساليب التحقيق المعتمدة في الجرائم المعلوماتية، سواء التقليدية أو المستحدثة.
- تقييم فعالية النصوص القانونية الجزائية في تنظيم مرحلة التحقيق في الجرائم المعلوماتية.

وأما عن **المنهج المتبع** فقد اعتمدنا في إعداد هذه الدراسة على المنهج الوصفي، من خلال عرض وتحليل المفاهيم العامة المرتبطة بالجريمة المعلوماتية، كخصائصها، وأركانها، ودوافع إرتكابها. كما تم توظيف المنهج تحليل المضمون وذلك من خلال التطرق إلى مضمون النصوص القانونية ذات الصلة بها، خاصة المواد من 394 مكرر إلى 394 مكرر7 من قانون العقوبات الجزائري. إضافة إلى ذلك، تم توظيف المنهج المقارن كمنهج ثانوي، من خلال مقارنة بعض جوانب التحقيق في الجرائم المعلوماتية بالتحقيق في الجرائم التقليدية. لهدف إبراز أوجه الإختلاف والخصوصية التي تميز هذا النوع من الجرائم المستحدثة.

أما **بالنسبة للدراسات السابقة** بالرغم من تعدد الدراسات التي تناولت موضوع الجريمة المعلوماتية، سواء من الناحية القانونية أو التقنية ، إلا أن أغلبها ركز على الجوانب العامة أو العقابية ، في حين أن الجانب الإجرائي ، وبالخصوص مرحلة التحقيق، لا يزال يحتاج إلى مزيد من البحث والتحليل في ظل ما يطرحه من إشكاليات قانونية وعملية. ومن هذا المنطلق، حاولت هذه المذكرة سد جزء من هذا الفراغ، من خلال دراسة تحليلية لمدى استجابة التشريع الجزائري لمتطلبات التحقيق في هذه الجرائم.

وبالنسبة **لصعوبات الدراسة** التي واجهتنا في إعداد هذه المذكرة فتتمثل في نقص الدراسات والمراجع، التي تتناول موضوع الجريمة المعلوماتية، بالإضافة إلى الطبيعة الفنية والقانونية للموضوع التي شكلت صعوبة خلال إنجاز بحثنا، نظراً لدقة وكثرة المصطلحات العلمية ذات الصلة بالموضوع.

أما في **خطة البحث** ولمعالجة الإشكالية المطروحة والإجابة عليها قسمنا بحثنا إلى فصلين رئيسيين وهما كالتالي:

الفصل الأول: تناولنا فيه ماهية الجريمة المعلوماتية، حيث تعرضنا لمفهومها القانوني واللغوي والفقهي، ثم انتقلنا إلى خصائصها، وسمات مرتكبيها ودوافعهم، لنختم بأنواع هذه الجرائم وأركانها القانونية

الفصل الأول:

الإطار المفاهيمي للجريمة المعلوماتية

الفصل الأول: الإطار المفاهيمي للجريمة المعلوماتية

لقد ساهم التطور التكنولوجي في إنتشار شبكات الحاسوب في كل أنحاء العالم حيث دخلت تطبيقات عديدة أدت إلي عصرنة المجتمعات مما أدى إلي توسيع التواصل بين شعوب العالم ووسعت من ترابط العلاقات إلي أنها من جانب آخر ساعدت علي تفشي الجريمة بمختلف أشكالها لتقود إلي ما يسمي بعولمة الجريمة.

والتطور السريع والمتواصل للإنترنت وما تتميز به من سرعة في إعداد ونقل وتخزين المعلومات ببالغ السرية، وبعيدا عن مرأى الجهات الأمنية وهو ما غير من صورة الإجرام التقليدي وتوسع نشاط الإجرام وذلك بإستخدام التكنولوجيا الحديثة لذلك سميت بالجريمة المعلوماتية.

فقد دخلت البشرية في بداية الألفية الثالثة مرحلة جديدة من التطور الهائل وذلك بفضل ثورة العولمة التكنولوجية في مجال المعلومات والإتصالات والتي غزت هذا العصر، وقد ساعدت علي الطفرة التكنولوجية العلمية في كل ميادين الحياة منها الإقتصادية، والإجتماعية، والثقافية، والعلمية، والتي إخترقت الحدود بين شعوب العالم، وأصبح العالم قرية صغيرة بما تتميز من تقلص المسافات والسرعة في تبادل المعلومات ودقتها وتخزينها ومعالجتها وتبادلها بين شعوب العالم داخل المجتمع الواحد أوبين الدول كافة حتي أصبح المجتمع عبارة مجتمع إلكتروني، وهو ما دفع المعظم يصفها بالثورة التكنولوجية الصناعية الثالثة، فكان الهدف من الثورة الأولي هو إختراع الآلة التي نابت علي الإنسان في مختلف قيامه بالأعمال اليدوية فإن غاية الثورة الثانية هو إختراع الأجهزة التكنولوجية التي تحل محل الفكر الإنساني.

وبالرغم من فوائد التكنولوجيا في جل مجالات الحياة إلي أنه لكل فعل ردة فعل تكون إيجابية أو سلبية، فقد برز جانب سلبي من هذه التقنية التي أثرت علي أمن المجتمعات، وذلك من الإستعمال السيئ لهذه التكنولوجيا وإستغلالها في الأفعال الغير مشروعة وبشكل يؤدي إلي إنعدام الأمن والإستقرار في كل نواحي الكرة الأرضية الذي أسفر عن دخول نوع من الجرائم لم يكن معهودا من قبل وسمي بجرائم تقنية المعلومات او الجرائم المعلوماتية.

ولهذا سنتطرق من خلال هذا الإطار المفاهيمي للجريمة الإلكترونية وسنتناول في **(المبحث الأول)** ماهية الجريمة المعلوماتية وخصائصها ودوافعها ثم في **(المبحث الثاني)** نتطرق إلى أنواع الجريمة المعلوماتية وأركانها.

المبحث الأول: ماهية الجريمة المعلوماتية

شهد العالم في السنوات الاخيرة تطوراً تكنولوجياً متسارعاً، أفرز معه أنماطا جديدة من الجرائم، من أبرزها الجريمة المعلوماتية التي تعد محور هذه الدراسة، خاصة من حيث أثارها المالية والإقتصادية.

وتصنف هذه الجريمة ضمن الجرائم حديثة العهد التي ظهرت نتيجة الإرتباط الوثيق بين النشاط الإجرامي والتقنيات الحديثة كأجهزة الحاسوب، شبكات الإنترنت، والمواقع الإلكترونية.

كما تُعد شبكة الإنترنت من أبرز الوسائل المساهمة في إنتشار هذا النوع من الجرائم، حيث أصبح بإمكان المجرم المعلوماتي إرتكاب أفعال خطيرة دون الحاجة إلى التنقل أو إستعمال وسائل عنف تقليدية، بل يتم تنفيذها في هدوء تام من خلف شاشات الحاسوب. ولهذا لسبب يطلق عليها البعض إسم "الجريمة الناعمة" نظرا لقدرتها على إحداث أضرار جسيمة، لاسيما على مستوى الإقتصاد العالمي كل هذا يمكن حدوثها بمجرد تنفيذ أوامر بسيطة من خلال لوحة المفاتيح.

ومما يزيد من خطورة هذه الجريمة هو طبيعتها العابرة للحدود، فهي ليست مرتبطة بمكان معين، بل تتم داخل الفضاء الإلكتروني الذي جعل من العالم قرية رقمية صغيرة، الأمر الذي سهل عمليات الإختراق والإعتداء على البيانات والمعلومات الرقمية.[1]

وبناء على ما سبق سنتطرق في هذا المبحث إلى مفهوم الجريمة المعلوماتية وخصائصها ضمن **(المطلب الأول)**، ثم نستعرض في **(المطلب الثاني)** دوافع الجريمة المعلوماتية.

المطلب الأول: مفهوم الجريمة المعلوماتية

إختلف الفقهاء في تحديد مفهوم دقيق وموحد للجريمة المعلوماتية، ويعود هذا الإختلاف إلى تنوع الزوايا التي عالج بها كل فقيه هذا المفهوم، فهناك من عرف الجريمة المعلوماتية بأنها كل سلوك غير مشروع يهدف إلى نسخ أو تعديل أو حذف أو الوصول إلى معلومات مخزنة داخل الحاسوب، أو تمر عبره وما نلاحظه على هذا التعريف أنه ركز على موضوع الجريمة وطبيعة السلوك المادي فقط، ما يجعله يضيق نطاق الجريمة المعلوماتية ويستبعد صوراً أخرى كعمليات الإحتيال المعلوماتي، أو الهجمات

[1] غربي جميلة، أليات مكافحة الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون، كلية الحقوق والعلوم السياسية، ، قسم القانون العام ، جامعة أكلي محند أولحاج–البويرة– ، 2020–2021 ، ص 4–5.

التي تستهدف الشبكات وتعطل المواقع الإلكترونية، وغيرها من الأفعال التي قد لا ينطبق عليها التعريف لكنها تشكل جرائم معلوماتية بالفعل.[1]

ومن جهة أخرى، إعتمد إتجاه فقهي أخر على معيار الوسيلة فعرف الجريمة المعلوماتية بأنها كل فعل إجرامي يتم إرتكابه بإستخدام الحاسوب كأداة رئيسية، أي أن الجريمة ترتبط هنا بوسيلة التنفيذ أكثر من إرتباطها بالموضوع أو النتيجة.[2]ومن خلال هذا المطلب سنتطرق إلى تعريف الجريمة المعلوماتية في **(الفرع الأول)** ثم خصائص الجريمة المعلوماتية في **(الفرع الثاني)** أما **(الفرع الثالث)** فقد خصص لصفات المجرم المعلوماتي وأصنافه

الفرع الأول: تعريف الجريمة المعلوماتية

في البداية تجدر الإشارة إلى عدم وجود تعريف قانوني موحّد ومتفق عليه للجريمة المعلوماتية، نظرا لحداثة هذا النوع من الجرائم وتعدد مظاهره. فقد إختلفت المصطلحات المستخدمة للدلالة عليه، فهناك من يطلق عليها "**جريمة الغش المعلوماتي**" وأخرون يطلقون عليها إسم "**جريمة الإختلاس المعلوماتي**" في حين أن البعض يفضل إستخدام مصطلح "الجريمة المعلوماتية".

وقد إنقسم الفقهاء بشأن تحديد مفهوم موحد لها، ويرجع هذا الإختلاف إلى تباين وجهات النظر حول نطاق هذه الجريمة[3]. ومن أجل فض هذا النزاع سنتطرق إلي تعريف الجريمة لغوياً **(أولا)** ثم فقهياً **(ثانيا)** وقانونياً **(ثالثا)**.

أولا: التعريف اللغوي

"الجريمة لغة هي كلمة مشتقة من الجرم، وهو التعدي أو الذنب، وجمع الكلمة إجرام وجروم هو الجريمة وقد جرم يجرم واجترم وأجرم فهو مجرم جريم، وهي طبقا للمفهوم الإجتماعي كل سلوك إرادي

[1] بن مالك اسمهان، خصائص الجريمة المعلوماتية وأسباب ارتكابها، مجلة البيان للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية حمد امين دباغين سطيف، السنة 2019، ص104.

[2] نفس المرجع، ص 104.

[3] غربي جميلة، مرجع سابق، ص 5-6.

غير مشروع يصدر عن شخص مسؤول جنائيا في غير حالات الإباحة عدوانا على مال أو مصلحة أو حق محمي بجزاء جنائي"[1]

وعرفت الجريمة أيضا على أنها "كل فعل غير مشروع يكون بإرادة أثمة يقر له القانون عقوبة أو تدبيرا إحترازيا، وتعتمد الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت على المعلومة بشكل رئيسي وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم"[2]

ثانيا: التعريف الفقهي

قدم الفقهاء والباحثون عدة تعاريف مختلفة للجريمة المعلوماتية، وتفاوتت هذه التعريفات بحسب المجال الذي ينتمي إليه كل باحث، وبحسب الطريقة التي إختارها في التعريف بها، ولهذا حاولنا جمع بعض من هذه التعاريف لأجل تكوين صورة واضحة وشاملة.[3]

ومن بين هذه التعريفات المطروحة، نرى بأن هناك من يعرف الجريمة بالإستناد إلى موضوع الجريمة، في حين أن البعض الأخر يستند في تعريفها إلى وسيلة إرتكاب الجريمة، وكدا من خلال طبيعة السلوك الإجرامي وهي كالتالي:

1-1 تعريف الجريمة المعلوماتية بالإستناد إلى موضوع الجريمة:

عرف الأستاذ والباحث "**روزنبلات**" الجريمة المعلوماتية بأنها "نشاط غير مشروع موجه موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة"

---

[1] بوديسة بجاد عبد الرؤوف، أليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق ، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج ، 2021-2022 ، ص 8.

[2] صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ، 2013، ص7.

[3] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية العلوم الإقتصادية وعلوم التسيير، قسم علوم التسيير، جامعة قاصدي مرباح ، ورقلة، 2018-2019 ، ص3.

وعرفها الفقيه "**سولارز**" بأنها "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات"[1]

أما الفقيه الألماني "**زيبر**" فقد عرف الجريمة المعلوماتية بأنها "كل تصرف غير مشروع يتعلق بالمعالجة الألية للمعطيات أو نقلها"[2]

2-1 تعريف الجريمة المعلوماتية بالإستناد إلى وسيلة إرتكاب الجريمة المعلوماتية:

يركز أنصار هذا الإتجاه في تعريف الجريمة المعلوماتية على إستخدام الحاسوب أو الشبكات كأداة أو هدف للجريمة، دون التركيز على طبيعة الفعل أو المعلومات المستهدفة وأهم هذه التعاريف ما يلي:

تعريف الأستاذ "**جون فورستر**" الذي يرى بأن الجريمة المعلوماتية هي "أي نشاط غير قانوني يستخدم فيه الحاسوب كأداة أو هدف لإرتكاب الفعل الإجرامي"[3]

ونجد أن الفقيه الألماني "**تايديمان**" قد عرفها بأنها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بإستخدام الحاسب الألي"[4]

كما عرفتها "**منظمة التعاون الإقتصادي والتنمية**" بأنها "كل سلوك غير مشروع، أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الألية للبيانات او بنقلها"[5]

---

[1] بوحفص راوية، الجريمة المعلوماتية في التشريع الجزائري ، مذكرة لنيل شهادة الماستر في الحقوق ، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة ، 2017-2018، ص7.

[2] معتوق عبد اللطيف، الإطار لقانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجستير في العلوم القانونية ، كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر، باتنة ، 2011-2012، ص7.

[3] عمار حشمان، مرجع سابق، ص4.

[4] عباسة محمد ياسين، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق ، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس ، مستغانم ، 2020-2021، ص9.

[5] معتوق عبد اللطيف، مرجع سابق، ص8.

وحسب الخبير الأمريكي "**باركر**" فإن الجريمة المعلوماتية هي "كل فعل إجرامي متعمد، أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل"[1]

أما الأستاذ "**دافيد وال**" فقد قام بتعريف الجريمة المعلوماتية بأنها "كل فعل غير مشروع يتعلق بشكل أو بأخر بالحاسب الألي"[2]

كما يعرف الأستاذ "**ماس**" الجريمة المعلوماتية بقوله أنها "الإعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[3]

1-3 تعريف الجريمة المعلوماتية بالإستناد إلى معيار التقنية:

على خلاف الإتجاهين السابقين اللذين ركزا وإستندا في تعريف الجريمة المعلوماتية على الموضوع أو الوسيلة المستخدمة فيها لتصنيفها كجريمة معلوماتية، ذهب إتجاه أخر إلى توسيع نطاق هذا المفهوم.[4] معتمدا على الصفات الشخصية، والسمات التي تكمن في مرتكب الجريمة كأساس لتعريفها، ومن بين تلك التعريفات ما يلي:

عرفت "**وزارة العدل الأمريكية**" الجريمة المعلوماتية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها عام 1979 بأنها "أي جريمة قام بها الجاني له دراية بالمعرفة الفنية للحاسبات".[5]

كما عرفها الأستاذ "**دافيد تومسن**" بأنها "أي جريمة يكون متطلبا لإقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الألي"[6]

---

[1] بن داني رانيا، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، قسم قانون عام، جامعة عبد الحميد بن باديس، مستغانم ، 2022-2023، ص11.

[2] معتوق عبد للطيف، مرجع سابق، ص7.

[3] مسعود شهيرة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد بن باديس ، مستغانم ، 2020-2021، ص6.

[4] معتوق عبد اللطيف، مرجع سابق، ص8.

[5] عمار حشمان، مرجع سابق، ص4.

[6] مسعود شهيرة، مرجع سابق، ص6.

ثالثا: التعريف القانوني للجريمة المعلوماتية:

إعتمد المشرع الجزائري مصطلح "**الجرائم المتصلة بتكنولوجيا الإعلام والإتصال**" للدلالة على الجرائم الإلكترونية، وقد عرفها بموجب أحكام المادة 02 من القانون رقم 09-04 بأنها "الجرائم المتعلقة بأنظمة المعالجة الألية للمعطيات المحددة في قانون العقوبات، وأي جريمة ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية، أو نظام للإتصالات الإلكترونية" [1]

إذ يتضح لنا من خلال هذا التعريف أن المشرع الجزائري قد تبنى معيار دور النظام المعلوماتي كعنصر جوهري لتحديد طبيعة الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم "المساس بأنظمة المعالجة الألية للمعطيات" ونظمها ضمن قانون العقوبات في المواد من 394 مكرر إلى 394 مكرر 7. وترك المجال أمام الجرائم المرتكبة بواسطة النظام المعلوماتي، والتي تشمل أي جريمة تستخدم فيها الوسائل التكنولوجية كوسيط أو وسيلة إرتكاب.[2]

وحسب المشرع الجزائري فإن الجريمة المعلوماتية قد تتحقق بمجرد إرتكاب الفعل أو تسهيل إرتكابه عن طريق منظومة معلوماتية أو نظام للإتصالات، وهو ما يعكس الطابع الواسع لهذا التعريف، حيث يشمل طائفة كبيرة من الجرائم، سواء كانت موجهة ضد الأنظمة المعلوماتية أو أرتكبت بواسطتها. إلا أن هذا التعريف لم يسلم من بعض الإنتقاذات أبرزها تكرار المفاهيم، حيث يُدرج "نظام الإتصالات الإلكترونية" ضمن مفهوم "المنظومة المعلوماتية" ما يجعل التوسع في العبارة نوعاً من الحشو غير الضروري، ومن أمثلة الجرائم المعلوماتية التي عرفت إنتشارا في الجزائر، تسريب أسئلة البكالوريا لسنة 2016 عن طريق مواقع التواصل الإجتماعي.

الفرع الثاني: خصائص الجريمة المعلوماتية

تتميز الجرائم المعلوماتية بعدة خصائص تجعلها مختلفة عن باقي الجرائم التقليدية من حيث طبيعتها ووسائل وأساليب إرتكابها، فهي مرتبطة بشكل مباشر بتطور التكنولوجيا وبإستخدام أجهزة

[1] القانون رقم 09-04 ، المؤرخ في 5 أوت 2009 ، المعدل والمتمم للأمر رقم 66-156 ، المؤرخ في 8 جوان 1966 ،المتضمن قانون العقوبات، الجريدة الرسمية، العدد 47 .

[2] القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم الأمر 66-156، المتضمن قانون العقوبات، ج/ر العدد 71.

الحاسوب وشبكات الإتصال الحديثة، إذ ساهم هذا هذا الإرتباط في منحها طابعا خاصا يميزها عن غيرها، سواء من حيث طرق التنفيذ أو من حيث شخصية مرتكبها لأن المجرم الإلكتروني لا يشبه المجرم العادي، كونه يمتلك مستوى عال من المعرفة التقنية والقدرة على إستغلال الأنظمة الإلكترونية بطريقة ذكية ودقيقة، كما أن ظهور شبكة الإنترنت وإنتشارها على نطاق واسع ساهم في بروز هذا النوع من الجرائم وأعطاها أبعادا جديدة لم تكن موجودة من قبل، ما جعلها أكثر تعقيداً وصعوبة في الكشف والمتابعة.[1] وتتمثل أهم هذه الخصائص في ما يلي:

أولا: الحاجة إلى جهاز إلكتروني والتحكم بتقنية إستخدامه:

تعد الجريمة المعلوماتية من الجرائم التي لا يمكن تصور إرتكابها إلا بوجود جهاز إلكتروني، سواء كان حاسوباً، هاتفاً ذكياً أو أي أداة رقمية أخرى قادرة على معالجة البيانات وتخزينها. ويشكل هذا الجهاز الوسيلة الرئيسية التي يتم من خلالها تنفيذ الجريمة، لأنها بمثابة الأداة التب تحل محل الوسائل التقليدية المستعملة في الجرائم العادية. ولهذا السبب سميت هذه الجريمة بـ"الإلكترونية" نظرا لإرتباطها الوثيق بالتقنية والمعلوماتية. إذ لا يقتصر الأمر على وجود الجهاز، بل لا بد أيضا من توافر شبكة الإنترنت التي تعد بيئة خصبة لإرتكاب هذا النوع من الجرائم، إلى جانب إمتلاك الجاني لمستوى معين من الدراية التقنية التي تتيح له التحكم في التكنولوجيا و إستغلالها في تنفيذ الفعل الإجرامي، إذ تكمن خطورة هذه الجريمة في أن الإعتداء يكون غالبا موجها نحو العناصر المعنوية للنظام المعلوماتي، مثل البيانات والبرامج والمعطيات، عكس الجرائم التقليدية التي تستهدف الممتلكات المادية، لآنه في الجريمة المعلوماتية لا يظهر أثر مادي مباشر كالسرقة أو الكسر، بل يكون التعدي على المعلومات المخزنة عبر نسخها أو تعديلها أو محوها أو حتى التلاعب بها وإستغلالها بطرق غير قانونية. إذ أنه كلما زادت قدرات الجاني التقنية، كلما زادت فاعليته في التسلل إلى النظم المعلوماتية وتنفيذ الجريمة دون ترك أثر مادي ظاهر.[2]

[1] عقباش بريزة، مبارك حنان، أليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، ، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي- برج بوعريريج- ، 2021-2022، ص13.

[2] عقباش بريزة ، مبارك حنان ، مرجع سابق، ص14.

ثانيا: الجريمة المعلوماتية جريمة عابرة للحدود

من أبرز ما يميز الجريمة المعلوماتية عن باقي أنواع الجرائم التقليدية هو أنها لا ترتبط بمكان معين، بل يمكن إرتكابها من أي نقطة في العالم دون حاجة لوجود الجاني في نفس المكان الذي توجد فيه الضحية أو محل الجريمة، فالمجرم من هذا النوع من الجرائم قد يكون في دولة، في حين أن نتائج فعله تظهر في دولة أخرى بعيدة كل البعد وهذا ما يجعلها تصنف ضمن الجرائم العابرة للحدود.[1]

فمن خلال إستخدام جهاز كمبيوتر متصل بالإنترنت، يستطيع المجرم تنفيذ إعتداءات مختلفة مثل إختراق قواعد البيانات الإحتيال عبر الإنترنت أو سرقة المعلومات وكل ذلك دون أن يغادر مكانه، مما يجعل تتبع الجريمة ومرتكبها أمرا بالغ الصعوبة.[2]

إن أن ما يميز هذه الخاصية هو أن الجريمة المعلوماتية لها القدرة على التأثير في أكثر من دولة في نفس الوقت، إذ قد تطال ضحايا في بلدان مختلفة بشكل متزامن، خاصة في ظل تطور وإزدهار التجارة الإلكترونية التي أزالت العديد من الحواجز الجمركية وسهلت حركة رؤوس الأموال عبر الدول.[3]

هذا الإمتداد الدولي للجريمة المعلوماتية خلق عدة إشكالات قانونية، خاصة فيما يتعلق بتحديد أس دولة تمتلك الحق في محاكمة الفاعل، هل هي الدولة التي نفذ فيها الفعل الإجرامي، أم التي لحقتها الأضرار؟ كما أن هذه الخاصية تطرح تساؤلات حول مدى كفاءة القوانين الحالية في مواجهة هذا النوع من الجرائم الحديثة، في ظل تعقيداتها وتشعباتها العابرة للحدود.[4]

ثالثا: جذب الجريمة المعلوماتية للمجرمين

إذ تعد الجرائم المعلوماتية مغرية للمجرمين نظرا لما يوفره عالم الحواسيب والإنترنت من فرص لتحقيق أهدافهم بسهولة وبأقل التكاليف، حيث لا تتطلب تجهيزات معقدة أو تخطيطاً طويل الأمد. كما أن

---

[1] بن داني رانيا، مرجع سابق، ص18.

[2] عماد بلغيث، جغلولي يوسف، صعوبات التحقيق في الجرائم الإلكترونية، ، مجلة الرسالة للدراسات والبحوث الإنسانية، مخبر سوسيولوجية جودة الخدمة العمومية ، الجزائر ، المجلد 06، العدد 03، سبتمبر 2021، ص18.

[3] عقباش بريزة، مبارك حنان، مرجع سابق، ص17.

[4] عماد بلغيث، جغلولي يوسف، مرجع سابق، ص18-19.

هذا النوع من الإجرام يوفر العديد من الوسائل المتطورة والمتنوعة التي تمكن الفاعل من التلاعب بالأنظمة المالية أو إختراق الحسابات البنكية، أو تنفيذ عمليات إحتيالية بإستخدام البطاقات المصرفية، دون أن يعرض نفسه لخطر المواجهة المباشرة.[1]

رابعا: الجريمة المعلوماتية جريمة مستحدثة

تعد الجريمة المعلوماتية من الجرائم حديثة النشأة، حيث ظهرت نتيجة للتطور الهائل في مجالي تكنولوجيا المعلومات والإتصالات، إذ تعتمد في إستخدامها بشكل كبير على المعرفة التقنية والبيئة الرقمية. وما يلاحظ عن هذه الجرائم أنها لم تحظى بعد بنصوص قانونية كافية وشاملة في الكثير من التشريعات، مما يخلق الكثير من الصعوبات في تصنيفها وتكييفها قانونياً، رغم توافر كل عناصر الجريمة من فاعل، ضحية، وسلوك إجرامي. وفي هذا السياق يقال بأن "الجريمة تسبق القانون" أي أن تطور الإجرام أسرع من تطور النصوص القانونية، وهو ما يمثل أحد التحديات الكبرى في مواجهة هذا النوع من الجرائم.[2]

خامسا: الجريمة المعلوماتية صعبة الإكتشاف والإثبات

إن الجريمة المعلوماتية تعد من أصعب الجرائم من ناحية الإكتشاف والإثبات، إذ أنه من بين الخصائص التي تميزها عن باقي الجرائم العادية، هي صعوبة إكتشافها وإثباتها وهذا راجع لعدة أسباب من بينها أنها لا تخلف أثار مادية واضحة مثل البصمات أو أي من علامات التخريب الظاهر أو الشهود، ففي الجرائم المعلوماتية غالبا ما تغيب الأدلة الملموسة لآن الأدلة فيها تكون إلكترونية أي أن الأثار فيها تكون رقمية يسهل محوها أو إخفاؤها بشكل سريع، وبالإضافة إلى ذلك فإن محدودية خبرة أجهزة الأمن والقضاء في التعامل مع هذا النوع من الجرائم، إلى جانب قصور القوانين الحالية عن مواكبة التطورات التكنولوجية، يجعل مهمة إثبات الجريمة ومعاقبة مرتكبها أكثر تعقيدا. فالجريمة المعلوماتية لا

[1] سعدات محمود فتوح محمد، خصائص الجريمة المعلوماتية وصفات مرتكبها في ظل مجتمع المعلوماتية، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ، دار المنظومة، السعودية ، 2015، ص38.

[2] عقباش بريزة، مبارك حنان، مرجع سابق، ص 14-15.

تحتاج إلى عنف أو أي تواجد مادي، لا تعتمد فقط على التلاعب بالمعلومات و البيانات الإلكترونية، مثل تعديلها أو حذفها أو تغييرها في ذاكرة الحاسوب، مما يجعل إكتشافها أمرا بالغ الصعوبة.[1]

سادسا: سرعة تنفيذ الجريمة المعلوماتية

تتسم الجريمة المعلوماتية بسرعة تنفيذها، حيث أنها لا تحتاج إلى وقت طويل لتنفيذها بل يمكن إتمامها في لحظات معدودة، ومن أي مكان في العالم الشيء الذي يجعلها أكثر خطورة من الجرائم العادية، لأنه من الممكن أن ينفذ الهجوم من طرف الجاني على نظام الضحية خلال ثوان معدودة، دون الحاجة إلى تهيئة مسبقة أو وجود فعلي في مكان الجريمة، وكل هذا يمكن حدوثه بإستخدام برامج وأدوات تقنية متخصصة فقط.[2]

سابعا: ضعف الإبلاغ عن الجريمة المعلوماتية

من العوامل التي تعرقل الكشف عن الجرائم المعلوماتية، هو التردد الكبير في الإبلاغ عنها إذ أنه في غالب الأحيان لا يتم إكتشاف الجريمة إلا بعد مرور فترة زمنية طويلة، وقد يكون ذلك بمحض الصدفة. ويعود هذا الإحجام عن التبليغ خاصة من قبل المؤسسات العامة والخاصة، وحتى الشركات متعددة الجنسيات، إلى خشيتهم من تأثير ذلك على سمعتهم ومكانتهم أمام الزبائن، لا سيما في القطاعات الحساسة كالبنوك والمؤسسات المالية. أما على مستوى الأفراد، فقد يمنعهم الخوف من الأثار النفسية والإجتماعية، أو التعرض للإبتزاز أو الفضيحة، من تقديم شكاوى، خاصة إذا تعلق الأمر بصور أو معلومات شخصية تهدد خصوصيتهم.[3]

الفرع الثالث: السمات والاصناف الخاصة بالمجرم المعلوماتي

لم يؤثر إرتباط الجريمة المعلوماتية بالحاسب الألي في تمييز هذا النوع من الجرائم عن الجرائم العادية فقط، بل إمتد ليشمل كذلك طبيعة مرتكبها أي المجرم المعلوماتي، حيث أظهرت بعض الدراسات وجود إختلاف واضح بينه وبين المجرم التقليدي، وقد إختلف الباحثون في تحديد الخصائص المميزة لهذا

---

[1] بن داني رانيا، مرجع سابق، ص19.

[2] سعدات محمود فتوح محمد، مرجع سابق، ص 38.

[3] عقباش زهرة، مبارك حنان، مرجع سابق، ص 17.

الصنف من المجرمين، غير أن الأستاذ "**باركر**" يعد من أبرز من إهتموا بهذا المجال، حيث قام بتقديم تحليلات دقيقة حول طبيعة المجرم المعلوماتي، بإعتباره شخصاً يرتكب فعلاً إجراميا يستوجب العقاب، مثله مثل باقي المجرمين، إلا أن ما يميزه هو إنتماؤه إلى فئة خاصة تقارب في سماتها فئة المجرمين "ذوي الياقات البيضاء" وذلك من حيث المستوى المعرفي والإجتماعي، وأسلوب تنفيذ الجريمة الذي في الغالب ما يكون معقد وغير عنيف.[1] وسنتطرق إلى السمات الخاصة بالجرم المعلوماتي **(أولا)** ثم أصناف المجرم المعلوماتي **(ثانيا)**

أولا: السمات الخاصة بالمجرم المعلوماتي

يتميز المجرم المعلوماتي بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ويرمز لها الأستاذ باركر بكلمة S.k.R.A.M والتي تعني:

_المهارة Skills

_المعرفة Knowledge

_الوسيلة Resources

_السلطة Anthority

_الباعث Motives[2]

1-1 المهارة:

تُعد المهارة التقنية من أبرز الصفات التي تميّز المجرم المعلوماتي، إذ تمثل المتطلب الأساسي لارتكاب الجريمة. وقد يُكتسب هذا النوع من المهارات بطرق مختلفة، إما من خلال الدراسة الأكاديمية المتخصصة في مجال تكنولوجيا المعلومات، أو عبر الخبرة العملية والتجريب، أو حتى بمجرد التفاعل الاجتماعي مع أفراد يملكون خلفية تقنية. ورغم ذلك، لا يُشترط أن يكون المجرم المعلوماتي خبيرًا أو

[1] بن شهرة شول، مراد مشوش، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية والسياسية، جامعة غرداية، المجلد 04، العدد01، جوان 2020، ص12.

[2] نفس المرجع ، ص 13-14.

متعلّمًا بشكل رسمي، حيث تُبيّن الوقائع أن بعض أنجح مرتكبي الجرائم المعلوماتية لم يحصلوا على تعليم تقني رسمي، بل اعتمدوا على مهارات مكتسبة بطريقة غير تقليدية.

2-1 المعرفة:

تتعلق المعرفة بالقدرة على فهم الظروف المحيطة بالجريمة وتقييم مدى نجاحها أو فشلها المحتمل. فالمجرم المعلوماتي غالبًا ما يكوّن تصورًا شاملًا عن النظام المستهدف، ويسعى إلى محاكاة بيئة مماثلة لاختبار خطته قبل تنفيذها فعليًا. هذه المعرفة التقنية تمنحه القدرة على التنبؤ بتفاصيل دقيقة حول مسرح الجريمة، ألا وهو النظام المعلوماتي، ما يعزز من فرص نجاح العملية.

3-1 الوسيلة:

المقصود بالوسيلة هي الأدوات أو الإمكانيات التي يعتمد عليها الفاعل أثناء تنفيذ الجريمة. وفي الجرائم المعلوماتية، غالبًا ما تكون الوسائل بسيطة ومتوفرة، ومع ذلك، فإن طبيعة النظام المستهدف قد تتطلب أدوات أكثر تعقيدًا، خصوصًا إذا كان هذا النظام غير مألوف أو يتميز بدرجة عالية من الخصوصية. وبفضل مهارته، قد يكون الفاعل قادرًا على ابتكار الوسائل التي يحتاجها، ما يجعل من الوسيلة عاملًا مرنًا ومتكيفًا حسب الجريمة.

4-1 السلطة:

تُشير السلطة إلى الحقوق أو الامتيازات التي يمتلكها الفاعل، والتي تمكّنه من الوصول إلى النظام المعلوماتي. قد تتمثل هذه السلطة في معرفة الشفرات السرية أو كلمات المرور التي تسمح له بفتح الملفات، تعديل البيانات، أو حتى مجرد الاطلاع عليها. كما قد تكون ناتجة عن موقعه المهني الذي يمنحه الحق في استخدام أجهزة الحاسوب أو إجراء بعض العمليات الحساسة.

5-1 الباعث:

يُعد الباعث أو الدافع عاملاً مهمًا في تفسير سلوك المجرم المعلوماتي، حيث لا يختلف كثيرًا عن دوافع مرتكبي الجرائم التقليدية. فالرغبة في تحقيق ربح مادي سريع وغير مشروع تظل من أهم الدوافع، تليها دوافع أخرى مثل التحدي والرغبة في اختراق الأنظمة المحمية، أو حتى الانتقام من جهة عمل أو

أحد الزملاء. ويجدر بالذكر أن بعض الجناة يبررون فعلهم برغبة في الإضرار بمؤسسة قادرة على تحمّل الخسائر، دون أن يعتبروا ذلك تصرفًا غير أخلاقي، على عكس الإضرار المباشر بالأفراد[1].

ثانيا: أصناف المجرم المعلوماتي

إن تعدد البواعث التي تحرك المجرم المعلوماتي، بين ما هو بسيط كحب الفضول والتجريب، وما هو خطير كالإرهاب، أدى إلى بروز عدة أصناف من مرتكبي الجرائم المعلوماتية، تراوحت هذه التصنيفات بين الهواة والمحترفين. ومع تنوع وتطور وسائل الإجرام الإلكتروني، وتزايد عدد وأنواع الهجمات السيبيرانية يوما بعد يوم، بات من الطبيعي ظهور أنماط جديدة من المجرمين.[2]

ويمكن تصنيف مرتكبي الجرائم المعلوماتية، إلى مجموعة من الفئات وهي كالتالي:

1 فئة العابثون:

يطلق عليهم أحيانا إسم "صغار نوابغ المعلوماتية" وهم في الغالب مراهقون تتراوح أعمارهم بين 15 و 20 سنة، يدخلون عالم الإجرام المعلوماتي بدافع التسلية أو الفضول أو إثبات الذات، دون إدراكهم لحجم الأضرار التي قد يسببونها، يستعملون أدوات جاهزة ومتوفرة في منتديات الإنترنت دون فهم عميق لتقنياتها، ومن أمثلتهم العابث البلجيكي الذي قام بتعطيل شبكة أحد مزودي الإنترنت وهو في سن الرابعة عشرة سنة فقط.[3]

1-1 فئة القراصنة الهواة – الهاكرز:

وهم عبارة عن أشخاص يملكون خبرة تقنية متقدمة، وغالبا ما يهدفون إلى إختراق الأنظمة المعلوماتية فقط لإثبات مهاراتهم التقنية. فهم لا يسعون بالضرورة إلى تحقيق مكاسب مادية، بل يرغبون في إستعراض قدراتهم، ويتركون أحيانا توقيعا يدل على إختراقهم.[1]

---

[1] بن شهرة شول، مراد مشوش، مرجع سابق ص 13 14.

[2] نفس المرجع، ص 13- 14.

[3] لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أكلي محمد أولحاج -البويرة- ، 2015-2014، ص22.

1-2 فئة القراصنة المحترفون – الكراكز:

وهم عبارة عن قراصنة محترفون يتعمدون تخريب الأنظمة أو سرقة البيانات بهدف الضرر أو الربح المادي، تضم هذه الفئة شباب تتراوح أعمارهم بين 25 و 40 سنة يعملون كمبرمجين أو محللين معلوماتيين، غالبا ما تكون لهم دوافع إجرامية واضحة، ويقومون بإعداد ونشر البرامج الخبيثة.2

1-3 فئة المجرمون المعلوماتيون المتطرفون:

يتمثلون في أفراد يحملون أفكار متطرفة دينية أو عنصرية، ويستخدمون الجرائم المعلوماتية كوسيلة للدفاع عن معتقداتهم، دون السعي وراء مكاسب مادية.[2]

1-4 فئة المبرمجون:

هذه الفئة تضم أفراد يمتلكون خبرة كبيرة لا تقل عن 5 سنوات في المجال المعلوماتي، وخاصة في مجال القرصنة المعلوماتية يأخدون مهام البرمجة، بحيث أنهم يعملون على إنشاء أو تعديل البرامج المعلوماتية الحديثة التي تعد كسلاح للجريمة المعلوماتية، إذ يشرعون في بيعها عبر شبكات الإنترنت والمواقع الخاصة إذ يستفسدون منها مجرمي المعلوماتية.[3]

1-5 فئة الحاقدون:

أصحاب هذه الفئة لا يمتلكون المعرفة التقنية الإحترافية، لكنهم يستطيعون الوصول إلى كافة العناصر المتعلقة بالفعل المراد إرتكابه، كما أنهم يعرفون بكونهم لا يملكون أهداف ودوافع الجريمة المتوفرة لدى غيرهم، لأنهم لا يهدفون إلى إثبات قدراتهم التقنية ومهاراتهم الفنية، وأيضا لا يهدفون إلى تحقيق مكاسب مادية. بل إن ما يحرك أنشطنهم هو حقدهم ورغبتهم في الإنتقام من صاحب العمل أو إحدى العاملين معهم في نفس القطاع.[4]

---

[1] ربيعي حسان، المجرم المعلوماتي شخصيته وأصنافه، مجلة العلوم الإنسانية ،جامعة محمد خيضر بسكرة، العدد 40 ، جوان 2015 ص296.

[2] بن شهرة شول، مراد مشوش، مرجع سابق ، ص 18.

[3] ربيعي حسان، مرجع سابق، ص299.

[4] عقباش بريزة، مبارك حنان، مرجع سابق، ص 21.

المطلب الثاني: دوافع إرتكاب الجريمة المعلوماتية

الدافع أو الهدف أو الغاية، كلها تشير إلى معنى واحد وهو النية الإجرامية التي تدفع الشخص لإرتكاب فعل مجرم قانونا. وغالبا ما يقصد بها القصد الجنائي، أي ما يدور في ذهن الفاعل لحظة إرتكابه للجريمة. هذا الدافع الإجرامي يعتبر المحرك الرئيسي الذي يوجه السلوك الإجرامي، سواء كان ذلك بدافع الحقد، الغضب، أو حتى الطمع. وقد تكون هناك رغبة داخلية قوية تدفع الجاني لإرتكاب الجريمة، لتحقيق هدف معين في ذهنه، وتجدر الإشارة الى أن طبيعة الدافع تختلف من شخص إلى أخر حسب العمر، الجنس، أو المستوى التعليمي، والبيئة التي يعيش فيها، كما ان نفس الجريمة يمكن أن ترتكب لأسباب مختلفة تماما من شخص إلى أخر.[1] والهدف المباشر من الجريمة هو النتيجة التي يسعى المجرم لتحقيقها بفعلته مثل الإعتداء، أو السرقة، أما الغاية فهي تكون أوسع كالرغبة في الإنتقام أو التشفي لكن

سواء كان الدافع مباشرا أو غاية بعيدة، فالقانون لا يفرق بينهما عند تقييم القصد الجنائي ما دام الفاعل كان مدركا لما يقوم به، وكان يقصده فالجريمة تتحقق قانونيا بتوفر عناصرها بغض النظر عن إذا كان الهدف نبيلا، أو دنيئا، المهم أن النية كانت متوفرة والفعل قد تم. وهنا يتدخل القانون لمعاقبة الجاني، وبما أن الجرائم المعلوماتية، تتعدد أسبابها فهناك دوافع داخلية ترتبط بالشخص ذاته، وأخرى مرتبطة بظروف المجتمع، أو المحيط الخارجي للشخص.[2]

وسوف نستعرض من خلال هذا المطلب نوعين من الدوافع التي يمكن أن تؤذي إلى إرتكاب الجرائم المعلوماتية وهذا في فرعين أساسيين يتمثل **(الفرع الأول)** في الدوافع الشخصية لإرتكاب الجريمة المعلوماتية أما **(الفرع الثاني)** فيحتوي على الدوافع الخارجية لإرتكاب الجريمة المعلوماتية

الفرع الأول: الدوافع الشخصية لإرتكاب الجريمة المعلوماتية

إن مرتكب الجريمة المعلوماتية، غالبا ما تحركه دوافع مالية أو قد يكون تحت تأثير رغبات نفسية وذهنة معينة، و تعتبر تلك الدوافع من أكثر الأسباب شيوعا في هذا النوع من الجرائم. ولتوضيح هذه الدوافع قمنا بتقسيمها إلى الدوافع المادية **(أولا)** والدوافع الذهنية **(ثانيا)**

[1] لفويلي ليلى، الجريمة الإلكترونية، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، كلية الحقوق، جامعة قسنطينة 1 ، 2012-2013، ص 30- 31.

[2] نفس المرجع، ص30.

أولا: الدوافع المادية

تعتبر الرغبة في الربح السريع، من أكثر الدوافع التي تدفع الجاني إلى إرتكاب الجرائم المعلوماتية، وهذا راجع إلى الإغراء الكبير الذي توفره هذه النوعية من الجرائم، بحيث يمكن للفاعل تحقيق مكاسب مالية ضخمة بوسائل بسيطة وبتكاليف أقل، مما يجعلها محل إستقطاب للكثيرين. ونظرا للتطور المتسارع في مجال تكنولوجيا المعلومات والإنتشار الواسع لإستخدام الأنظمة الإلكترونية، أصبح من السهل على المجرم إستغلال الثغرات الموجودة في الأنظمة المعلوماتية للوصول إلى أهدافه دون الحاجة إلى مجهود كبير أو فعلي في مكان إرتكاب الجريمة.[1] وغالبا ما يسعى مرتكب الجريمة الإلكترونية إلى التسلل لأنظمة المعالجة الألية للمعلومات الخاصة بالبنوك أو المؤسسات المالية، أو حتى إلى أجهزة الحاسوب الشخصية التابعة للأفراد، وذلك بهدف الإستيلاء على بيانات أو معلومات حساسة يمكن إستخدامها في تحقيق مكاسب مالية، إما من خلال بيعها أو عن طريق المساومة عليها أو إستعمالها في عمليات الإبتزاز. وفي هذا الإطار تشير الإحصائيات التي نشرت في إحدى المجلات المتخصصة في مجال الأمن المعلوماتي والتي بينت من خلال دراساتها أن: 34% من جرائم الغش المعلوماتي ترتكب بدافع إختلاس الأموال و 23%من أجل سرقة المعلومات، وأيضا 19% من أجل أفعال الإتلاف 15%من أجل الإستعمال غير المشروع للألة[2]

وما يمكن إستنتاجه من هذه الإحصائيات، هو أن الجانب المادي من أبرز المحركات الفعلية التي تدفع المجرم الإلكتروني إلى المغامرة والدخول للفضاء الرقمي، لأنه وفي كثير من الحالات تكون الضغوط المادية التي يمر بها الشخص سواء بسبب أزمات عائلية أو تراكم الديون أو حتى بسبب الخسائر الناتجة عن إدمان القمار أو المخدرات هذا المشاكل تعتبر سببا لإرتكاب هذه الجرائم ومثل هذه الحالات قد يرون بأن جميع الوسائل مباحة طالما أنها تحقق لهم الخروج من أزماتهم وفق مبدأ "الغاية تبرر الوسيلة" ومن الأمثلة الواقعية لهذه الحالات "حادثة وقعت في إحدى الشركات الألمانية، أين قام مبرمج يعمل بها بسرقة إثنين وعشرين شريطا يحتوي على بيانات حساسة تتعلق بعملاء الشركة وإنتاجها، ثم قام بإبتزاز المؤسسة التي يعمل بها وطالبهم بدفع مبلغ مالي حوالي 200.000 ألف دولار مقابل عدم

[1] نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الإداري، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أحمد دراية ، أدرار ، 2016-2017 ، ص 11-12.

[2] نفس المرجع ، ص12.

تسريب تلك المعلومات إلى جهات منافسة للشركة. ورغم خطورة الموقف فضلت الشركة الإستجابة لطلبه تفاديا للعواقب والخسائر التي قد تترتب عن تسريب تلك البيانات".[1]

ثانيا: الدوافع الذهنية

من بين العوامل التي تدفع بعض الأفراد إلى إرتكاب الجرائم المعلوماتية، نجد تلك المتعلقة بالرغبة في إثبات الذات أو الرغبة في التغلب على النظام المعلوماتي، إذ تتجسد الدوافع الذهنية لمرتكب الجريمة المعلوماتية في حب الإستطلاع، والتحدي، والسعي لفهم الأنظمة التقنية المعقدة، وغالبا ما يكون الدافع مجرد شغف بالتكنولوجيا والأنظمة الإلكترونية، ما يدفع البعض إلى محاولة تجاوز العراقيل الأمنية وكسر القيود التي تحيط بالأنظمة الرقمية، في شكل من أشكال التسلية أو المتعة الشخصية. فقد يجد بعض الأفراد متعة خاصة في إقتحام هذه الأنظمة، إذ يمثل ذلك بالنسبة لهم تحديا ذهنيا يثير فيهم الرغبة في السيطرة على التكنولوجيا وإبراز تفوقهم وتميزهم عليها، دون أن تكون لديهم نية حقيقية في الإضرار المباشر بالأنظمة أو المؤسسات أو الرغبة في التخريب، بل تنطلق من دافع شخصي يتمثل في حب التحدي وتحقيق الذات.[2]

ومن الأمثلة الواقعية نسبيا والدالة على هذا النوع من الدوافع، ما ورد في إحدى مذكرات الماجستير، حول عامل الطلاء الذي شاهد خلال زيارته لأحد البنوك كيف يقوم موظف الصيانة بإخراج النقود من ألة الصراف الألي بإستخدام بطاقة خاصة. وقد أثر فيه هذا المشهد بشدة، لدرجة أنه قد قرر تعلم البرمجة والمعلوماتية لمدة عامين، لينجح لاحقا في السطو على جهاز موزع آلي وسحب الأموال. غير أن السلطات ألقت القبض عليه قبل أن يتمكن من الإستفادة من أموا العملية ووجهت إليه تهمة السرقة. [3]

الفرع الثاني: الدوافع الموضوعية لإرتكاب الجريمة المعلوماتية

الإنسان بطبيعته كائن هش من الناحية النفسية، إذ قد يتأثر في لحظات معينة بالظروف والمواقف الخارجية، التي يخضع لها أو قد تدفعه بعض الدوافع المختبئة خلف سلوكه المخادع إلى إرتكاب أفعال

[1] لفويلي ليلى، المرجع السابق، ص32.

[2] نايري عائشة، مرجع سابق، ص 12-13.

[3] لفويلي ليلى، مرجع سابق، ص 32-33.

إجرامية ومن بين أبرز هذه الدوافع سنذكر، دافع الإنتقام وإلحاق الضرر برب العمل **(أولا)** ثم دافع المتعة والتحدي والرغبة في قهر النظام المعلوماتي وإثبات الذات **(ثانيا)** و**(ثالثا)** دافع التعاون والتواطؤ وأخيرا ارتباط الجريمة الإلكترونية بالبطالة **(رابعا)**

أولا: دافع الإنتقام وإلحاق الضرر برب العمل

في عالم العمل، تتولد أحيانا مناوشات سلبية سواء على مستوى سوق الشغل أو على بنية الوظيفة بحد ذاتها، وقد لاحظنا من خلال ما إطلعنا عليه، أن العاملين في قطاع التقنية أو حتى أولئك الذين يستخدمون التكنولوجيا في قطاعات أخرى، يتعرضون لمشاكل وضغوطات نفسية نتيجة لعلاقات العمل المتوترة أو البيئة المهنية المنفرة، هذا المناخ السلبي قد يزرع في نفوس بعضهم رغبة في تحقيق الربح بطرق غير مشروعة، لكن الأخطر من ذلك أن يكون الإنتقام هو المحرك الرئيسي لمثل هذه الرغبات، ففي حالات كثيرة كانت جرائم الحاسوب التي تتمثل في إتلاف البيانات أو زرع الفيروسات، نتيجة مباشرة لرغبة عارمة في الإنتقام من جهة مؤسسة العمل أو من المسؤولين فيها، وأبرز ما يحرك هذا السلوك هو الشعور العميق بالحقد إتجاه رب العمل الذي يؤذي بالشخص إلى الرغبة في الإنتقام منه.[1]

ثانيا: دافع المتعة والتحدي والرغبة في قهر النظام المعلوماتي وإثبات الذات

في أحيان أخرى يكون الدافع الأساسي لإرتكاب الجريمة المعلوماتية، هو الرغبة في إثبات الذات أو لفت الإنتباه إلى القدرات الفنية والتقنية، ومحاولة تحقيق الإنتصار على تقنية الأنظمة المعلوماتية، لكن بدون أن تكون لهم أي نوايا سيئة، وهذا يعود إلى وجود عجز في التقنية التي تتيح الفرصة لمبتكري برامج النظام المعلوماتي لإرتكاب تلك الجرائم.

ثالثا: دافع التعاون والتواطؤ

في العديد من الجرائم الإلكترونية، لا يكون المجرم شخصاً واحداً فقط، بل غالباً ما يكون هناك تعاون بين أكثر من طرف، حيث يتولى أحدهم، وهو عادة شخص متخصص في الأنظمة المعلوماتية، الجانب التقني من العملية، في حين يتكفل شريك آخر من داخل أو خارج المؤسسة المتضررة بتغطية آثار الجريمة وتحويل العوائد المالية الناتجة عنها. وغالباً ما تكون بين هؤلاء علاقة تبادل منتظم

[1] لعاقل فريال، مرجع سابق، ص 25-26.

للمعلومات ومراقبة للأنظمة بصفة مستمرة، هذا التواطؤ لا يكون فقط بهدف مادي، بل أحياناً بدافع نفسي، حيث يسعى مرتكبو هذا النوع من الجرائم إلى إشباع رغبات داخلية معينة أو تحقيق أهداف شخصية. ولذلك نجد الكثير منهم يشكلون مجموعات متخصصة في ارتكاب الجرائم الإلكترونية، يعملون بتنظيم ودقة عالية، ويتعاونون لتحقيق أهداف مشتركة، قد تكون مادية، نفسية، أو حتى لمجرد التحدي أو إثبات الذات.[1]

رابعا: ارتباط الجريمة الإلكترونية بالبطالة

مثلما ترتبط الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة، فإن الجريمة الإلكترونية هي الأخرى تتأثر بهذه العوامل. وتزداد خطورة الأمر حين تنتشر البطالة بين فئة الشباب، خاصة من يملكون قدرات ومعارف تقنية في مجال المعلوماتية. فهؤلاء قد يجدون أنفسهم مدفوعين نحو ارتكاب أفعال إجرامية في العالم الرقمي، إما كرد فعل وانتقام من المجتمع الذي لم يوفر لهم فرص عمل، أو كوسيلة للحصول على دخل يسد احتياجاتهم اليومية، الشباب العاطل عن العمل قد يرى في الجريمة الإلكترونية وسيلة لإثبات وجوده أو لاسترجاع حق يراه ضائعا، ويبرر هذا السلوك لنفسه بأنه رد فعل طبيعي على واقع مر يعيشه. وهنا، تلعب البطالة دورا في تهيئة المجرم نفسياً لقبول ما يفعله دون شعور بالذنب، بل وقد يتحول الفعل الإجرامي عند البعض إلى مصدر فخر، خاصة إذا كان معقدا تقنياً ونجح في تنفيذه دون أن يُكشف وهكذا تصبح البطالة بيئة خصبة لتفريخ هذا النوع من الجرائم، خاصة عندما تتقاطع الحاجة الاقتصادية مع المهارات التقنية.[2]

المبحث الثاني: أنواع الجريمة المعلوماتية وأركانها

إن الجرائم المعلوماتية كثيرة ومنتشرة، بحيث لم يوضع لها معايير محددة من أجل تصنيفها، وهذا راجع إلى التطور الكبير والمستمر الذي تشهده شبكة الإنترنت والخدمات التي تقدمها، إذ يُعتبر تصنيف الجريمة الإلكترونية أمرًا معقدًا مقارنةً بالجريمة التقليدية، لأنها لا تستهدف فئة واحدة فقط، بل تمتد لتشمل الأشخاص الطبيعيين والمعنويين وحتى الدول من حيث الأمن والاقتصاد. ولهذا السبب لم يتفق الفقهاء

[1] صابر بحري ، منى خرموش ، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية، مجلة دراسات في سيكولوجية الإنحراف، جامعة محمد لمين دباغين سطيف2 ، المجلد 07، العدد01، السنة 2021 ، ص 55-56.

[2] نفس المرجع ، ص55.

ورجال القانون على تصنيف موحد لها، والسبب يرجع أيضًا إلى طبيعتها المتشعبة وسرعة تطورها. فهناك من يعتمد في التصنيف على الجرائم التي تُرتكب على الحاسوب أو بواسطته، وآخرون ينظرون إلى الدافع الإجرامي وراء ارتكابها، بينما نجد من يُركّز على الوسيلة المستعملة والأسلوب المتبع، ومنهم من يعتمد على طبيعة الضحية أو محل الجريمة.[1]

وقد سبق لنا أن تطرقنا في بداية هذا البحث إلى مفهوم الجريمة المعلوماتية في التشريع الجزائري، كما تحدثنا أيضًا عن طبيعتها القانونية وخصائصها.[2]

وفي هذا المبحث بالتحديد سنتناول أنواع الجريمة المعلوماتية في **(المطلب الأول)** ثم سنتحدث عن الأركان الأساسية للجريمة المعلوماتية في **(المطلب الثاني)**

المطلب الأول: أنواع الجرائم المعلوماتية

تعد الجرائم المعلوماتية متعددة ومتنوعة، ويصعب وضع تصنيف دقيق وشامل لها، وذلك بسبب التطور المستمر لشبكة الإنترنت والخدمات المرتبطة بها وقد اختلفت آراء الباحثين حول كيفية تصنيف هذه الجرائم، فهناك من صنفها حسب موضوع الجريمة، وآخرون فضّلوا تصنيفها وفقًا لطريقة ارتكابها. ومن بين التصنيفات المعروفة، نجد التصنيف الذي وضعه "معهد العدالة القومي" في الولايات المتحدة الأمريكية سنة 1985، والذي اعتمد على مدى علاقتها بالجرائم التقليدية، وتصنف الجرائم المعلوماتية على النحو التالي إذ أن **الصنف الأول** يشمل الجرائم المنصوص عليها في قانون العقوبات، والتي تُرتكب باستخدام شبكة الإنترنت كوسيلة لتنفيذها أما **الصنف الثاني** فيتعلق باستخدام الشبكة لدعم أنشطة إجرامية، مثل غسيل الأموال، والاتجار بالمخدرات والأسلحة، حيث تُستخدم الإنترنت كوسيلة للترويج والتمويه في هذه الجرائم **والصنف الثالث** يخص الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات، من خلال الدخول غير المشروع إلى هذه الأنظمة أو تغيير البيانات أو حذفها، مما يؤثر على سير عمل الحاسوب **والصنف الرابع** يندرج ضمن جرائم الاتصالات، ويشمل كل الانتهاكات التي تمس شبكات الهاتف من خلال استغلال ثغرات الإنترنت.

---

[1] عقباش بريزة، مبارك حنان، مرجع سابق، ص ص25-26.

[2] بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2015-2016، ص 43.

وعلى هذا الأساس، فإن تصنيف الجرائم الإلكترونية يظل مرتبطًا بالأداة المستعملة، وهي شبكة الإنترنت، ما يجعلها تتطور باستمرار مع تطور هذه التقنية.[1]

وفي هذا المطلب سنتحدث عن الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي في **(الفرع الأول)** ثم الجرائم الواقعة على أمن الدولة في **(الفرع الثاني)** وفي **(الفرع الثالث)** نتطرق إلى الجرائم الواقعة على النظام المعلوماتي

الفرع الأول: الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي

في هذا النوع من الجرائم، لا يكون النظام المعلوماتي هو محل الجريمة، وإنما يُستخدم كوسيلة لتسهيل ارتكاب الفعل الإجرامي وتحقيق النتيجة الإجرامية. ويهدف الجاني من خلال هذا النوع إلى تحقيق منافع غير مشروعة، كالربح السريع، أو الاعتداء على أموال الغير، أو المساس بالأشخاص وسمعتهم، أو حتى المساس بأمن الدولة وأسرارها[2]، وفي هذا الفرع سنتطرق إلى الجرائم الواقعة على الأشخاص **(أولا)** ثم الجرائم الواقعة على الأموال **(ثانيا)**

أولا: الجرائم الواقعة على الأشخاص

رغم الفوائد الكبيرة التي وفّرتها شبكة الإنترنت والتسهيلات التي منحتها للأفراد، إلا أنها جعلت هؤلاء عرضة للعديد من الانتهاكات[3] ، ومن أبرز الجرائم الواقعة على الأشخاص ما يلي:

1 جريمة التهديد

وهي كل وعيد يُقصد به زرع الخوف في نفس الضحية، من خلال الضغط على إرادته وتخويفه بإلحاق ضرر به أو بمن له صلة به، ويشترط أن يكون التهديد على قدر من الجسامة المتمثلة في التوعد بإلحاق الأذى، سواء ضد النفس أو المال، دون أن يُشترط تنفيذ هذا الوعيد فعلًا. وقد يكون الهدف من

[1] سورية ديش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية ، المركز الديمقراطي العربي ، العدد الأول، يناير 2018، ص 240.

[2] غربي جميلة، مرجع سابق، ص 18.

[3] فكرون عادل سعيد، الجرائم المعلوماتية الواقعة على الحق في الخصوصية، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور –الجلفة– ، 2018–2019، ص 38.

التهديد هو إجبار المجني عليه على القيام بفعل معين أو الامتناع عنه، أو حتى بدافع الانتقام. وتُعد شبكة الإنترنت وسيلة فعّالة لارتكاب هذا النوع من الجرائم، نظرًا لتعدد الوسائط المتاحة كالرسائل الإلكترونية وصفحات الويب.[1]

2 جريمة إنتحال شخصية

وتتمثل في استخدام هوية شخص آخر بهدف الاستفادة من ماله أو مكانته أو سمعته، وقد انتشرت هذه الجريمة بسرعة خاصة في الأوساط التجارية.

وتتم عن طريق جمع أكبر عدد من المعلومات الشخصية، إذ أنه غالبًا ما يبدأ الجاني بجمع معلومات شخصية عن الضحية، من خلال وسائل احتيالية، كاستدراج الشخص للإفصاح عن بياناته الخاصة مثل الاسم والعنوان ورقم بطاقة الائتمان، ليتم استخدامها لاحقًا في تنفيذ الجريمة والوصول إلى مال الضحية أو سمعته عن طريق الغش والإحتيال. [2]

3 جريمة إنتحال شخصية أحد المواقع

وفي هذا النوع، يقوم الجاني باختراق موقع إلكتروني معروف والسيطرة عليه، ثم يُدخل برنامجًا خاصًا به يعمل باسم الموقع الحقيقي. وتهدف هذه العملية إلى استغلال ثقة المستخدمين بالموقع الأصلي لجمع بياناتهم أو خداعهم بطرق احتيالية[3].

4 جرائم السب والقذف

وهي تلك الأفعال التي تمس شرف الغير وسمعتهم، سواء كانوا أشخاصًا طبيعيين أو معنويين، وتتم عادة عبر وسائل إلكترونية، كالبريد الإلكتروني أو صفحات الويب، من خلال نشر عبارات أو معلومات كاذبة أو مشينة تمس كرامة الضحية. وتتميز هذه الجرائم بسرعة انتشارها، حيث تصل الرسائل المسيئة إلى عدد كبير من مستخدمي الإنترنت في وقت قصير[4].

---

[1] فكرون عادل سعيد ، مرجع سابق ، ص 38-39.

[2] سورية ديش، مرجع سابق، ص 240-242.

[3] غربي جميلة، مرجع سابق، ص 18.

[4] فكرون عادل سعيد، مرجع سابق، ص 39.

5 جريمة التشهير وتشويه السمعة

تُعد جريمة التشهير من الجرائم الخطيرة التي تهدد سمعة الأفراد ومكانتهم الاجتماعية، وتتمثل في نشر معلومات قد تكون خاصة أو مغلوطة عن الضحية، سواء كان شخصًا عاديًا أو شخصية عامة، أو حتى مؤسسة تجارية أو سياسية يعتمد مرتكبو هذا النوع من الجرائم على عدة وسائل، من بينها إنشاء مواقع إلكترونية مخصصة لنشر هذه المعلومات، أو إرسالها عبر البريد الإلكتروني إلى عدد كبير من المستخدمين، أو نشرها على وسائل التواصل الاجتماعي. وتُستعمل هذه الأساليب أحيانًا لأغراض الابتزاز، أو لتصفية حسابات سياسية أو فكرية من خلال بث الشائعات والتقليل من شأن الرموز الوطنية أو الدينية.[1]

ومن المهم التأكيد على أن كل هذه الاعتداءات تمس الحياة الخاصة للأفراد، والتي كفلها القانون الجزائري صراحة، حيث تنص المادة 40 من الدستور على أن: "تضمن الدولة عدم انتهاك حرمة الإنسان وتمنع أي عنف بدني أو معنوي أو أي مساس بالكرامة". وبالتالي فإن أي اعتداء عبر الوسائط الإلكترونية على الحياة الشخصية أو الكرامة الإنسانية يُعد مخالفة صريحة للقانون ويُعاقب عليه.

ثانيا: الجرائم الواقعة على الأموال

أدى تطور تكنولوجيا المعلومات والانتشار الواسع لاستخدام الإنترنت في المعاملات اليومية إلى ظهور أنواع جديدة من الجرائم التي تستهدف الأموال، فقد أصبح من الشائع اليوم إتمام عمليات البيع والشراء والإيجار والدفع إلكترونيًا، ما فتح المجال لابتكار طرق جديدة للاحتيال المالي، مثل التحويلات غير القانونية، سرقة الحسابات البنكية، والقرصنة. [2]ومن أبرز هذه الجرائم ما يلي:

1 السرقة الواقعة على البنوك

حيث يُقدم الجاني على اختراق الأنظمة المعلوماتية للمؤسسات المالية وسرقة بيانات الحسابات، أو استغلال ثغرات أمنية لتحويل أموال من حسابات الضحايا إلى حسابات وهمية. كما تُستعمل تقنيات متقدمة لنسخ بطاقات الصراف الآلي، وإنشاء مواقع مزيفة تحاكي مواقع البنوك الرسمية لخداع

[1] فكرون عادل سعيد ، مرجع سابق ، ص 40.

[2] نفس المرجع ، ص 40.

المستخدمين وسرقة معلوماتهم السرية، أين تدفع هذه المواقع المزيفة بالعملاء إلى إدخال بياناتهم وتحديث معلوماتهم الشخصية ما يؤذي ذلك إلى السطو على أموالهم وسرقتها، [1] كما تتم سرقة الأموال عن طريق إرسال الرسائل وهمية مجهولة المصدر عبر البريد الإلكتروني أين توهم صاحب البريد الإلكتروني بأنه قد فاز بجائزة قيمة أو مبلغ مالي، ثم يطلب منه الجاني إرسال رقم حسابة المصرفي أو بطاقته الإئتمانية قصد إيداع الجائزة في حسابه أين تتم سرقته فور وقوعه في الفخ.

2 جريمة غسيل الأموال

أدى التطور التكنولوجي إلى توسيع نطاق الجرائم المالية، حيث أصبح الجناة يعتمدون على الشبكة المعلوماتية لممارسة أنشطة غسيل الأموال. فباستخدام الإنترنت، يتم تسهيل عمليات تحويل الأموال غير المشروعة، مع تجاوز الحواجز الجغرافية وتفادي القيود القانونية، فضلاً عن استخدام وسائل التشفير لإخفاء هوية المتورطين، مما يضفي على الأموال المغسولة طابعاً شرعياً ويصعب تعقبها.[2]

3 جريمة الاستعمال غير المشروع للبطاقات الائتمانية

رافقت عملية استخدام البطاقات الائتمانية الإلكترونية ظهور أساليب احتيالية للاستيلاء عليها، باعتبارها تمثل بديلاً رقمياً للنقود. ويتم ذلك عبر سرقة بيانات البطاقة وبيعها للغير، أو عن طريق اختراق أنظمة الحاسوب للحصول على كلمات المرور باستخدام وسائل خداعية، مثل إيهام الضحية بربح جائزة ليقدم معلوماته طوعاً. كما تُستعمل البطاقات المسروقة أو المزورة في سحب الأموال أو اقتناء السلع والخدمات.

4 تجارة المخدرات عبر الإنترنت

تُعد تجارة المخدرات عبر الإنترنت من أخطر أشكال الجرائم الإلكترونية، إذ أن هنا مواقع إلكترونية يتم فيها الترويج لهذه المواد الخطيرة، وكدا بيعها ومحاولة تحريض الأفراد على تعاطيها أو حتى تصنيعها بمختلف أنواعها، مما يؤذي ذلك إلى إنتشارها بسرعة بين الناس، وذلك من خلال استغلال ثغرات

[1] فكرون عادل سعيد، مرجع سابق، ص 40.

[2] نفس المرجع، ص 41.

الخصوصية التي توفرها الشبكة العنكبوتية والوسائل التقنية المتقدمة التي تعيق اكتشاف مرتكبي هذه الأفعال.[1]

5 جريمة القمار عبر الإنترنت

وتتم هذه الجرائم عن طريق النوادي الإفتراضية التي ظهرت في المواقع الإلكترونية، خاصة بألعاب القمار يتم فيها المراهنة بمبالغ مالية كبيرة، لكنها غير مشروعة ولا يسمح بممارسة مثل هذه النشاطات.

6. جريمة التحويل الإلكتروني للأموال

نظام التحويل الإلكتروني يحوز على أهمية خاصة للبنوك التي تعمل بالأنترنت، حيث أن هذا النظام يقوم بتحويل المال من حساب بنكي إلي آخر بطريقة جد فعالة وآمنة. ونظام التحويل الإلكتروني للأموال المفهوم منه هو منح إمتيازات لأحد البنوك بتداول الأموال أي القيام بتحويلات مالية دائنة ومدينة إلكترونيا من حساب بنكي إلي آخر، إذ أن نقل الأموال للزبائن من حساب لأخر يعتبر من أهم أنشطة البنوك الإلكترونية، إذ تعدّ عمليات تحويل الأموال من أبرز الخدمات التي تقدمها البنوك الإلكترونية، حيث تُحوّل الأموال من حساب بنكي لآخر عبر أنظمة المقاصة الإلكترونية، خلافًا للتحويلات التقليدية التي تتطلب تدخلًا بشريًا من طرف بنك مرخص له بذلك. ويتم هذا التحويل عبر أجهزة الحاسوب باستخدام برمجيات مخصصة، وتقع الجريمة عندما يتم تنفيذ هذا التحويل بشكل غير مشروع، بحيث تُحوّل الأموال من حساب الضحية إلى حساب الجاني أو إلى حساب مستفيد أجنبي دون علم أو موافقة صاحب الحساب ويُنفّذ هذا النوع من الجرائم عادة من خلال عدة طرق، أبرزها التلاعب بالبرامج الخاصة بعمليات التحويل المالي، استخدام بطاقة بنكية تعود للضحية من أجل سحب أمواله بطريقة غير مشروعة، استغلال البيانات والمعلومات الشخصية للضحية بغرض إصدار بطاقة ممغنطة ثانية باسمه، تُستعمل في تنفيذ عمليات السحب أو التحويل الاحتيالية.[2]

7 جريمة التزوير الإلكتروني: وتعتبر هذه الجريمة من أخطر الجرائم الواقعة على الأموال والتي يرتكبها المجرم المعلوماتي، نظرا لما يتمتع به الحاسب الألي من خطورة كبيرة، فالتزوير يتم بواسطة أكثر الوسائل

[1] عقباش بريزة ، مبارك حنان، مرجع سابق، ص28.

[2] نفس المرجع، ص 27-28.

المتطورة، ومن أمثلته تزوير العملات عن طريق الماسح الضوئي وكدا تزوير بطاقات الإئتمان، وأيضا تزوير وتقليد الوثائق والبيانات والمستندات المهمة، وكدا التواقيع وبالتالي فإن التزوير يسبب أضرار كبيرة تمس بالإقتصاد الوطني بالدرجة الأولى.[1]

الفرع الثاني: الجرائم الواقعة على أمن الدولة

تعتبر الجرائم الموجهة ضد أمن الدولة من أخطر أنواع الجرائم المعلوماتية، لأنها تمس بشكل مباشر السيادة الوطنية والمصالح العليا للدولة، خصوصًا عندما يتم استخدام الأنظمة المعلوماتية كوسيلة لتنفيذ هذه الأفعال الإجرامية. وتشمل هذه الجرائم حالات إفشاء أسرار تمس الدفاع الوطني أو الأمن العام، أو حتى التورط في أعمال التجسس والإرهاب وقد أكد المشرّع الجزائري على خطورة هذا النوع من الجرائم، حيث نص في المادة 394 مكرر 2 من قانون العقوبات على أنه: "تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد." مما يدل على أن الدولة تأخذ هذه التهديدات على محمل الجد وتسعى لتشديد العقوبات عليها.[2] وفي هذا الفرع سنتناول الإرهاب الإلكتروني **(أولا)** ثم التجسس الإلكتروني **(ثانيا)**

أولا: الإرهاب الإلكتروني

مع تطور وسائل الاتصال والتكنولوجيا، أصبحت الجماعات الإرهابية تعتمد بشكل كبير على الفضاء السيبراني في تنفيذ وتحقيق أهدافها. فالإنترنت أصبح وسيلة فعالة للتواصل بين أفراد هذه الجماعات، وتنسيق العمليات، ونشر الأخبار الكاذبة، بل وحتى غسل الأدمغة وتجنيد الشباب والمراهقين الذين يسهل التأثير عليهم. كما تلجأ هذه الجماعات إلى جمع الأموال عبر الإنترنت وتمويل أنشطتها الإرهابية بطرق خفية يصعب تتبعها. بل الأكثر من ذلك، أنهم يستهدفون أحيانًا مواقع إلكترونية حساسة تابعة لمؤسسات أمنية أو عسكرية من أجل سرقة المعلومات أو تعطيل الأنظمة، مستغلين في ذلك سهولة الحصول على برامج اختراق قوية ومتاحة على نطاق واسع.[3]

---

[1] عقباش بريزة، مبارك منال ، مرجع سابق، ص 28-29.

[2] فكرون عادل سعيد، مرجع سابق، ص 43.

[3] نفس المرجع ، ص 43.

ثانيا: التجسس الإلكتروني

يُعد التجسس من بين الجرائم التقليدية، لكنه تطور بشكل ملحوظ مع دخول العالم الرقمي، فأصبح يُمارس عبر الوسائط الإلكترونية والتقنيات الحديثة. ويستهدف هذا النوع من الجرائم عادةً المؤسسات الحكومية، الشركات الكبرى، والمنظمات الدولية، وقد يكون الغرض منه عسكريًا، سياسيًا أو اقتصاديًا. حيث يسعى الجناة إلى الوصول إلى معلومات حساسة وسرية غير مسموح بالاطلاع عليها، وغالبًا ما تكون محفوظة ضمن قواعد بيانات مؤمنة داخل أنظمة معلوماتية محمية.

أما من الناحية الإقتصادية، فالتجسس يستهدف إقتصاد المؤسسات الكبرى التابعة للدولة، إذ قد يُمارس هذا التجسس من طرف دولة ضد دولة أخرى، أو من طرف شركات كبرى تنافس بعضها البعض، مما يهدد بشكل كبير أمن الدولة واستقرارها.[1]

الفرع الثالث: الجرائم المعلوماتية الواقعة على النظام المعلوماتي

بالإضافة إلى الجرائم التي تُرتكب باستخدام النظام المعلوماتي كوسيلة، هناك صنف آخر لا يقل خطورة، يتمثل في الجرائم التي تستهدف النظام المعلوماتي نفسه. هذا التصنيف يُبنى على محل الجريمة، ويشمل بالخصوص الاعتداءات التي تُرتكب على مكونات النظام المعلوماتي، سواء المادية منها أو المنطقية

وبما أن المكونات المادية كالحواسيب والأجهزة المحيطة بها تحظى بالحماية الجزائية ضمن إطار الجرائم التقليدية (كالسرقة والتخريب)، فإن التركيز هنا سينصب على الجرائم الموجهة ضد المكونات المنطقية للنظام المعلوماتي، أي البرمجيات والمعلومات المدرجة ضمنه، والتي تتطلب غالبًا معرفة تقنية متقدمة في مجال البرمجة وهندسة الأنظمة. [2] ومن خلال هذا الفرع سنتطرق إلى جرائم الإعتداء على المكونات المادية للنظام المعلوماتي **(أولا)** ثم الجرائم الواقعة على نظام التشغيل **(ثانيا)** وبعدها جرائم الإعتداء على المعلومات المدرجة بالنظام المعلوماتي **(ثالثا)**.

---

[1] عقباش بريزة، مبارك حنان، مرجع سابق، ص 29-30.

[2] بوعرعارة إبراهيم زياد، خصوصية الجريمة المعلوماتية، مذكرة ماستر في الحقوق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة غرداية-الجزائر- 2021-2022، ص 35.

أولا: جرائم الإعتداء على المكونات المادية للنظام المعلوماتي: ويقصد بهذه الجرائم إلحاق الضرر بالأجهزة والمعدات، إذ تستلزم للقيام بها المعرفة في مجال البرمجة ومنها:

1-الجرائم الواقعة على البرامج التطبيقية

في هذه الحالة، يُقدم الجاني على استهداف برنامج معين داخل النظام (مثل برامج التسيير أو المحاسبة) والتلاعب به لتحقيق منفعة مادية شخصية، وتتمثل أبرز صور هذه الجرائم في: [1]

1-1تعديل البرامج

يُعد التعديل غير المشروع للبرامج من أخطر الأفعال التي تستهدف البرامج التطبيقية، وغالبًا ما يكون الهدف منه اختلاس مبالغ مالية، خاصة في الأنظمة البنكية. ومن أشهر الأمثلة على ذلك قضية مبرمج في أحد البنوك الأمريكية قام بإدخال تعديل بسيط على برنامج الحسابات، بحيث يُضيف دولارًا واحدًا لكل حساب يحتوي على أكثر من عشرة دولارات، ووجه تلك الأموال إلى حساب خاص به وقد استمر في هذا الفعل لفترة طويلة إلى أن كُشف أمره صدفة عند تحضير البنك لحملة دعائية.[2]

1-2 التلاعب بالبرامج باستعمال وسائل خفية

يلجأ بعض المبرمجين إلى زرع برامج فرعية غير مرئية داخل النظام الأصلي، تُعرف بـ "القنابل المنطقية" تُمكنهم من الدخول لاحقًا إلى النظام والوصول إلى عناصره الحساسة دون أن يتم اكتشافهم، بفضل دقة هذه الأكواد وصغر حجمها.[3]

ثانيا: الجرائم الواقعة على نظام التشغيل

هذه الجرائم تُرتكب عندما يقوم الفاعل بإضافة تعليمات سرية داخل نظام التشغيل، تُسهل له لاحقًا الحصول على المعلومات السرية للنظام. وتُقسم هذه الجرائم إلى نوعين:

1 المصيدة

---

[1] بوعرعارة إبراهيم زياد ، مرجع سابق ص 35.

[2] نفس المرجع ، ص 35.

[3] فكرون عادل سعيد، مرجع سابق، ص 44.

يُبرمج الجاني النظام عمداً بأخطاء غير ظاهرة، ويُدخل فيه تفرعات سرية تُمكنه لاحقًا من الولوج للنظام وتعديله، دون أن يتم كشف ذلك بسهولة أثناء التشغيل العادي للبرنامج.

2-1 تصميم برامج وهمية

يتمثل هذا النوع في إعداد برنامج خادع مخصص لارتكاب الجريمة، كما حدث مع إحدى شركات التأمين الأمريكية التي صممت برنامجًا يُنتج وثائق تأمين لأشخاص غير موجودين فعليًا (وهميين)، وتمكنت من خلاله من خلق أكثر من 46 ألف اسم مزيف، وتحصلت على عمولات كبيرة من باقي شركات التأمين.[1]

ثالثا: جرائم الإعتداء على المعلومات المدرجة بالنظام المعلوماتي

تُعد المعلومات المُخزنة داخل النظام المعلوماتي من بين الأهداف الرئيسية للجريمة المعلوماتية، باعتبارها قلب النظام ومصدره الأساسي، وتتنوع أشكال الاعتداءات على هذه البيانات بين التلاعب المتعمد والإتلاف الكلي أو الجزئي وتتمثل في:

1 التلاعب بالمعلومات

قد يكون التلاعب مباشرًا أو غير مباشر فالتلاعب المباشر يتم غالبًا من قبل الموظفين المصرّح لهم بالوصول إلى النظام، كإدخال بيانات مزيفة مثل أسماء مستخدمين وهميين، أو الاحتفاظ بأسماء مستخدمين غادروا المؤسسة، مما يؤذي إلى إستغلال هذه الأسماء في أغراض غير مشروعة أما التلاعب غير المباشر يتم عبر وسائط تخزين خارجية مثل الأشرطة الممغنطة. مثال على ذلك، قيام أحد الموظفين في إحدى الشركات بإرسال شريط يحتوي على 139 إذن دفع إلى البنك، لكن الشريط رفض عند معالجته بسبب عيب تقني، ولو نجحت العملية لتمكن الجاني من الاحتيال على البنك بمبلغ يقارب 21 مليون فرنك.[2]

[1] بوعرعارة إبراهيم زياد، مرجع سابق، ص 36.

[2] نفس المرجع ، ص 37.

2-1 جريمة إتلاف المعلومات الإلكترونية

تُعتبر جريمة إتلاف المعلومات من أخطر صور الاعتداء على النظام المعلوماتي، وتتمثل في استخدام برمجيات خبيثة يُطلق عليها "**الفيروسات**"، والتي تهدف إلى تخريب أو تدمير المكونات المنطقية لأنظمة المعالجة الآلية للمعطيات. هذه البرمجيات تتسبب في تعطيل الأجهزة، محو البيانات، أو تشويهها، مما يؤدي إلى أضرار جسيمة سواء للأفراد أو المؤسسات. وتتنوع الفيروسات بحسب طريقة عملها وتأثيرها، ومن بين أشهر الأنواع ما يلي:

- **حصان طروادة**

هو نوع من البرمجيات الخبيثة التي تُستخدم للاختراق، حيث يتخفى داخل برامج عادية تبدو غير ضارة، وعند تشغيل البرنامج، ينشط الفيروس تلقائيًا لتنفيذ الأوامر المبرمجة فيه، مثل تعديل الملفات أو حذفها أو حتى تدمير النظام بأكمله. من أشهر الأمثلة على استخدام هذا النوع من الفيروسات، ما قام به الدكتور "**بوب**" من ولاية أوهايو الأمريكية سنة 1989، حين أرسل أقراصًا مرنة **(ديسكات)** تحمل فيروس "حصان طروادة" إلى آلاف الأشخاص حول العالم بهدف الابتزاز، وقد تسبب هذا الفعل في إلحاق الضرر بحوالي عشرين ألف شخص في مدينة لندن وحدها.

- **فيروس الدودة**

يُعتبر من أكثر الفيروسات انتشارًا، ويتميز بقدرته على الانتقال من جهاز إلى آخر دون الحاجة لتدخل المستخدم، على عكس حصان طروادة، هذا النوع من الفيروسات لا يلتصق بنظام التشغيل، لكنه يقوم باستهلاك موارد الحاسوب مثل الذاكرة والمعالج مما يؤدي إلى بطء في الأداء، وقد يصل إلى حد تعطيل الجهاز كليًا. ومن أشهر حوادث هذا الفيروس هي "**دودة موريس**" التي ظهرت على يد طالب دكتوراه يُدعى "**موريس**" بجامعة كورنيل، حيث تسربت إلى نظام البريد الإلكتروني، وانتشرت بشكل واسع من خلال استغلال ثغرة أمنية، وتمكنت من اختراق كلمات السر وتسببت في شلل الآلاف من الحواسيب.

- **القنبلة الموقوتة**

هي نوع من الفيروسات التي تبقى خاملة داخل النظام إلى غاية حدوث واقعة محددة، مثل تاريخ معين، أو إدخال كلمة مرور معينة، أو تشغيل برنامج معين. عند تحقق هذا الشرط، ينشط الفيروس ويبدأ

في تنفيذ برمجته التخريبية، كحذف الملفات، تعطيل البرامج، أو إتلاف قواعد بيانات خاصة بالعملاء أو المعاملات.[1]

المطلب الثاني: أركان الجريمة المعلوماتية

تتكوّن الجريمة المعلوماتية مثل باقي الجرائم، من ثلاثة أركان أساسية، والتي تتمثل في الركن الشرعي والركن المادي، والركن المعنوي، ولكن أركان الجريمة المعلوماتية تختلف عنها في بعض الخصوصيات التي تميز هذا النوع من الجرائم نظراً لكونها من الجرائم المستحدثة التي ترتبط إرتباطا وثيقا بالتطور التكنولوجي، وسنتناول في هذا المطلب هذه الأركان بشكل مفصل من أجل الفهم الدقيق لها، حيث سنبدأ أولا بالركن الشرعي للجريمة المعلوماتية في **(الفرع الأول)**، ثم ننتقل إلى الركن المادي في **(الفرع الثاني)**، ثم الركن المعنوي في **(الفرع الثالث)**.[2]

الفرع الأول: الركـن الشرعـي للجريمة المعلوماتية

يعتمد الركن الشرعي في الجريمة المعلوماتية على مبدأ الشرعية الجزائية، وهو مبدأ أساسي نصت عليه المادة الأولى من قانون العقوبات الجزائري بقولها أنه: "**لا جريمة ولا عقوبة أو تدابير أمن بغير قانون**" ومن هذا المنطلق قام المشرع بتجريم بعض الأفعال المرتبطة بالمساس بأنظمة المعالجة الألية للمعطيات، وهذا من خلال القانون رقم 04-15، والذي تضمن نصوصاً خاصة بعقاب مرتكبي هذه الأفعال ضمن القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وذلك ضمن الفصل الثالث من الباب الثاني المتعلق بالجنايات والجنح ضد الأفراد، حيث وردت هذه الأحكام في المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات بعد تعديله وتتميمه.

كما تشمل هذه المواد عدة جرائم مثل الدخول والبقاء عن طريق الغش في نظام معلوماتي، وعرقلة تشغيل النظام، وتغيير أو حذف أو إدخال بيانات بدون ترخيص وغيرها.

[1] فريجة حسين، الجرائم الإلكترونية والإنترنت، مجلة المعلوماتية ، السعودية، دار المنظومة، العدد36، أكتوبر 2011، ص6.

[2] حمز خضري، عشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، ، المجلد 06 العدد 02 جوان 2020، ص 173.

وبالإضافة إلى ذلك جاء القانون رقم 09-04 مكملًا لهذا الإطار التشريعي، حيث تضمن قواعد وقائية تهدف إلى الحد من ارتكاب الجرائم المعلوماتية، من خلال وضع إجراءات تقنية تمكّن من مراقبة الاتصالات الإلكترونية وتسجيلها في وقتها، إلى جانب السماح بالتفتيش داخل الأنظمة المعلوماتية. ويُعد لجوء المشرع إلى تجريم هذه الأفعال بشكل صريح تكريسًا لمبدأ الشرعية، بحيث لا يمكن للقاضي الجنائي أن يعتمد على القياس لتجريم أفعال لم يرد نص صريح بتجريمها، أي لا يجوز له أن يُطبّق العقوبة على فعل لم يُذكر في القانون لمجرد أنه يشبه فعلاً آخر ورد فيه نص تجريمي.[1]

الفرع الثاني: الركن المادي للجريمة المعلوماتية

يعتبر الركن المادي في الجريمة هو الجانب الظاهر لها، أي الفعل الخارجي الملموس الذي نص عليه المشرّع، فالقاعدة القانونية تقول: "لا جريمة بدون ركن مادي" أو "لا جريمة بدون فعل" لكن ما يميز الركن المادي في الجريمة المعلوماتية هو اختلافه النسبي عن نظيره في الجرائم التقليدية[2]، حيث يتجسد في ثلاثة أشكال متعددة لفعل الاعتداء وهي كالتالي:

أولا: الدخول أو البقاء غير المشروع في نظام المعالجة الألية للمعطيات

إن جريمة الدخول أو البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات تعد من أبرز صور الاعتداءات على هذا النظام، حيث نصت عليها المادة الثانية من الاتفاقية الدولية لمكافحة الإجرام المعلوماتي، كما وردت أيضاً في المادة 394 مكرر من قانون العقوبات الجزائري، حيث جاء فيها أنه:

"يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"

[1] حمز خضري، عشاش حمزة، مرجع سابق، ص 173

[2] نفس المرجع ، ص 174

كما أنه "**تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج**"[1]

وبالتالي نستنتج من النص السابق وجود صورتين لفعل الدخول أو البقاء غير المشروع في نظام المعالجة الألية للمعطيات الأولى بسيطة والأخرى مشددة وتتمثل في:

1- الصورة البسيطة: ويشمل النشاط الإجرامي في هذه الصورة فعلين وهما:

1-1 فعل الدخول غير المشروع: ويقصد به التسلل أو الولوج غير المصرح به إلى نظام المعالجة الألية للمعطيات، دون إذن أو تفويض مسبق سواء كان ذلك باستخدام وسائل تقنية أو إلكترونية، ويعد هذا الفعل مجرما بمجرد وقوعه، أي أنه بغض النظر عن نية الفاعل أو ما إذا كان الهدف منه إلحاق الضرر بالنظام أو لا[2]، نظراً لأن المشرع لم يحدد وسيلة الدخول أو الطريقة التي تم بها الدخول إلى النظام. ويصنف كجريمة كاملة الأركان وهذا وفقا لنص المادة 394 مكرر من قانون العقوبات الجزائري والتي تنص على أنه "يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الألية للمعطيات أو يحاول ذلك"

وتنص نفس المادة على أنه تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة بقولها "وإذا ترتب عن الأفعال الذكورة أعلاه تخريب نظام إشتغال المنظومة، تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات وغرامة من 100.000 دج إلى 300.000 دج." [3]

فقد نصت هذه المادة بوضوح على أن المشرع الجزائري جرم فعل الدخول بطريقة غير مشروعة إلى المنظومة المعلوماتية، وإعتبره بمثابة جريمة شكلية حيث أنه بمجرد حدوث إختراق جهاز الحاسوب لأي

---

[1] القانون رقم 24-06 ، المؤرخ في 28 أفريل 2024، المتضمن الوقاية من الجرائم السيبرانية ومكافحتها، المعدل والمتمم للأمر 66-156 المؤرخ في 8 جويلية 1966 المتضمن قانون العقوبات ج/ر ، العدد 30

[2] راضية عيمور، الجريمة الإلكترونية وأليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية ، مخبر الحقوق والعلوم السياسية، المجلد 06، العدد الأول، 2022، ص 99.

[3] القانون رقم 04-15 ، المادة 394 مكرر المذكور سابقاً،

سبب كان فهذا يعد إنتهاكا للنظام المعلوماتي. فالقانون لم يشترط طريقة معينة لهذا الدخول فمن الممكن أن يتم بأي وسيلة سواء كانت مباشرة أو غير مباشرة. ويقصد بفعل الدخول في نظام الحاسب الألي الدخول المعنوي أي مجرد الإتصال الذهني أو التقني بنظام المعالجة الألية للمعطيات، ويمكن أن يتم ذلك بإستخدام تقنيات متنوعة مثل التطرق لإستعمال برامج خاصة تستخدم لتجاوز أنظمة الحماية والأمان، أو عن طريق ما يسمى بالأبواب وهو عبارة عن مصطلح فني يقصد به ترك فواصل في البرامج أثناء إعدادها، وتستعمل لاحقا في تنفيذ عمليات التلاعب داخل النظام.[1]

1-2 البقاء غير المشروع: ويقصد بالبقاء غير المشروع في نظام المعالجة الألية للمعطيات، هو إستمرار الشخص في التواجد داخل هذا النظام بدون إذن من صاحب النظام أو من له سلطة السيطرة عليه وبمعنى أخر، يتعلق الأمر ببقاء شخص داخل نظام معالجة مملوك للغير، بعد ولوجه إليه عن طريق الخطأ أو بالصدفة، رغم علمه بأن بقاءه غير مرخص به، وقد تباينت آراء الفقه في القانون المقارن حول تكييف جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، فهناك من إعتبرها من الجرائم المستمرة، ومنهم من صنّفها ضمن الجرائم الوقتية أو جرائم الاعتياد، كما ثار خلاف فقهي حول لحظة بداية وانتهاء هذه الجريمة. فالبعض يرى أن الجريمة تكتمل بمجرد الدخول أو البقاء غير المشروع داخل النظام، بينما يرى آخرون أن استمرار الجاني داخل النظام حتى بعد انتهاء المدة المصرح بها يُعد امتداداً للجريمة وركن من أركانها.[2]

2 الصورة المشددة:

لقد نصت المادة 394 من قانون العقوبات الجزائري في فقرتها الثانية أن المشرّع الجزائري قد شدد العقوبة إذا نتج عن فعل الدخول أو البقاء غير المشروع، محو أو تعديل للمعطيات المخزنة في النظام، أو تعطيل لوظائفه، كما نصت الفقرتان الثانية والثالثة من المادة 394 مكرر على أنه " **تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا عن الأفعال المذكورة أعلاه تخريب نظام**

[1] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011-2012 ، ص55.

[2] نفس المرجع ، ص56.

إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج"

وتتجلى الظروف المشددة في حالتين أساسيتين:

الحالة الأولى: عندما يُسفر الدخول أو البقاء عن محو أو تعديل لمعطيات النظام

الحالة الثانية: عندما يؤذي ذلك إلى تعطيل النظام أو شل حركته وعدم صلاحيته لأداء مهامه

ومن المهم الإشارة إلى أن العلاقة بين الفعل **(الدخول أو البقاء)** والنتيجة الضارة التي تلحق بالنظام أو البيانات، يجب أن تكون علاقة سببية واضحة، فإذا ثبت أن الفعل هو السبب المباشر للضرر، فإن الجريمة تكون قائمة وتستوجب العقاب.[1]

ثانيا: الاعتداءات العمدية على المعطيات

تُعد الاعتداءات العمدية على المعطيات من أخطر صور الجريمة المعلوماتية، وقد تناولتها كل من المواد 3، 4، و8 من الاتفاقية الدولية للإجرام المعلوماتي، كما ورد النص عليها في التشريع الجزائري من خلال المادتين 394 مكرر 1 و394 مكرر 2 من قانون العقوبات إذ نصت المادة 394 مكرر 1 على تجريم الاعتداءات العمدية التي تستهدف المعطيات الموجودة داخل النظام المعلوماتي، في حين عالجت المادة 394 مكرر 2 حالة المساس العمدي بالمعطيات خارج النظام، وذلك على النحو الآتي: [2]

1 جرائم الاعتداءات العمدية على المعطيات داخل النظام المعلوماتي:

نص المشرع الجزائري في المادة 394 مكرر 1 من قانون العقوبات المعدلة بموجب القانون 04-15 والقانون 24-06، على أنه "**يعاقب بالحبس من (1) سنة إلى (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الألية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها**" إذ أنه من خلال هذا النص، يتضح لنا أن

[1] طرشي نورة ، مرجع سابق ، ص 56.

[2] بعرة سعيدة، مرجع سابق، ص 55-56.

المشرع يجرم ثلاث صور من الإعتداءات العمدية على المعطيات داخل النظام المعلوماتي، والتي ترتكب عن طريق الغش وتتمثل هذه الصور في ما يلي:

1-1 الإدخال: و يقصد به إضافة معطيات جديدة إلى دعامة تخزين المعطيات، سواء كانت هذه الدعامة فارغة أو تحتوي على بيانات سابقة. ويتحقق هذا الفعل في حالات متعددة، مثل استخدام بطاقة السحب أو بطاقة الائتمان بطريقة تتجاوز الرصيد الحقيقي، أو إدخال برامج خبيثة مثل الفيروسات، وأحصنة طروادة، والقنابل المعلوماتية التي تؤدي إلى إدخال معطيات غير مصرح بها داخل النظام.

2-1 المحو: يتمثل في إزالة أو حذف جزء من المعطيات المسجلة، أو تدمير وسائط التخزين كليًا أو جزئيًا، أو نقل تلك المعطيات إلى مواقع أخرى داخل الذاكرة الرقمية، بما يؤدي إلى فقدانها أو تعطيل الوصول إليها.

3-1 التعديل: يعني تغيير المعطيات الأصلية داخل النظام واستبدالها بمعطيات أخرى، وغالبًا ما يتم ذلك باستخدام برمجيات ضارة تُحدث تغييرًا في بنية المعلومات، كبرامج الفيروسات، أو "الممحاة"، أو القنابل المعلوماتية الخاصة بالتعديل.

ويُلاحظ أن المشرع قد حصر هذه الأفعال الثلاثة (الإدخال، المحو، التعديل) حصراً دقيقاً، مما يعني أن الأفعال الأخرى – مثل النسخ أو النقل أو التنسيق – لا تدخل ضمن دائرة التجريم ما لم تكن مندرجة ضمن الصور المحددة قانونًا. كما أن الجريمة تتحقق بمجرد ارتكاب إحدى هذه الأفعال دون الحاجة لاجتماعها معًا، طالما قد تحقق عنصر التلاعب غير المشروع في المعطيات التي يحتويها النظام

2 صورة المساس العمدي بالمعطيات خارج النظام

لا يقتصر التجريم في مجال الجرائم المعلوماتية على الدخول غير المشروع فحسب، بل يشمل كذلك كل الأفعال التي تمس بأمن وسلامة المعطيات المخزنة أو المتداولة داخل نظام المعالجة الألية، حتى وإن تم الدخول إليه بطريقة مشروع ويقصد بهذه الأفعال كل تصرف من شأنه أن يساهم في تغيير البيانات، أو حذفها، او نسخها، وكدا تعطيل البرامج، أو التأثير على السير العادي للنظام، سواء أرتُكب هذا الفعل عمداً أو عن طريق إستخدام وسائل إلكترونية أو برمجيات متطورة بشكل غير قانوني.[1]

[1] طرشي نورة، المرجع السابق، ص57.

وقد نصت المادة 394 مكرر2 من ق.ع المعدلة بموجب ق 24-06 على أنه "يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة مالية من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يلي:

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

- حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"[1]

ومن خلال هذه المادة يتضح لنا أن المشرع حاول تغطية أكبر عدد من الأفعال التي قد تشكل تهديدا حقيقيا للمعطيات الرقمية، سواء كانت هذه المعطيات ذات طابع شخصي أو تمس جهات حساسة كالمؤسسات الحكومية أو الدفاع الوطني. فتجريم مثل هذه الأفعال يهدف إلى حماية الخصوصية ومنع تداول المعلومات الخطيرة التي قد تستخدم للإضرار بالأفراد أو بالمصلحة العامة.[2]

أما فيما يخص الإعتداء العمدي على سير نظام المعالجة الألية للمعطيات، فالمشرع الجزائري لم يتضمن نصاً صريحاً يجرم الإعتداء العمدي على سير النظام بحد ذاته، بل اقتصر على تجريم الأفعال التي تمسّ المعطيات المخزنة داخل النظام، ويُفسر هذا التوجه باعتبار أن الاعتداء على المعطيات من شأنه أن يؤثر على فعالية النظام وأدائه الوظيفي، لكن نصت على هذا النوع من الجرائم المادة 323-2 من قانون العقوبات الفرنسي، التي جاء فيها أنه " أنه يعاقب بالحبس.. كل من يعيق أو يفسد تشغيل نظام معلوماتي"[3] وقد اختلف الفقه حول ما إذا كان الاعتداء العمدي على المعطيات يُعد وسيلة لبلوغ غاية، أم هو غاية في ذاته ؟ ففي حال كان الاعتداء مجرد وسيلة، فإن الجريمة تُصنّف ضمن جرائم الاعتداء العمدي على المعطيات. أما في ظل غياب نص خاص يُجرّم الاعتداءات التي تستهدف سير النظام ذاته

[1] القانون رقم 24-06 ، المادة 394 مكرر 2 ، المذكور سابقا .

[2] طرشي نورة، المرجع السابق، ص 57

[3] القانون رقم 2015-912، المؤرخ في 24 جويلية 2015، المتضمن قانون العقوبات الفرنسي ،المادة 323-2 ، الجريدة الرسمية للجمهورية الفرنسية، العدد 0171، بتاريخ 26 جويلية 2015

عند الدخول المشروع إليه، فإن هذه السلوكات قد تخرج من دائرة التجريم، بالرغم من ما تسببه من أضرار وتأخذ الأفعال الإجرامية في هذا السياق شكلين رئيسيين، يتمثلان في التعطيل أو العرقلة والإفساد[1]

الفرع الثالث: الركن المعنوي للجريمة المعلوماتية

يتمثل الركن المعنوي في الجرائم الماسة بأنظمة المعالجة الألية للمعطيات في توافر القصد الجنائي، باعتبارها من الجرائم العمدية التي يشترط فيها أن يتوفر لدى الجاني كل من العلم والإرادة.

أولا: الركن المعنوي في جريمة الدخول أو البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات

يتخذ القصد الجنائي في هذه الجريمة صورة القصد العام، حيث عبّرت المادة 394 مكرر من قانون العقوبات الجزائري عن هذا القصد بعبارة "**عن طريق الغش**"، وهي ذات العبارة التي استخدمها المشرع الفرنسي في المادة 323-1 من قانون العقوبات "frauduleusement" وتفيد هذه العبارة علم الجاني بأن فعله غير مشروع، وأنه يتعمد الدخول أو البقاء في نظام معلوماتي دون وجه حق.

ويستلزم القصد الجنائي أن يحيط الجاني علماً بكافة العناصر الجوهرية المكونة للجريمة، وعلى رأسها الركن المادي. ويجب أن يعلم بأن فعله موجه نحو نظام معلوماتي يحتوي على بيانات وبرامج محمية قانوناً. فإذا كان الجاني يعتقد – لسبب معقول – أنه يقوم بعملية حسابية عادية على الحاسوب دون إدراكه بأنه يخترق نظاماً معلوماتياً، فإن القصد لا يتوفر لديه.[2]

كذلك يجب أن يكون الجاني على وعي بخطورة فعله، وأن يتوقع النتيجة الإجرامية التي ستترتب عنه، أي الدخول أو البقاء غير المشروع داخل النظام. ولا يشترط أن يتوقع الضرر الناتج عن هذا الفعل، بل يكفي أن يكون على دراية بأن ما يقوم به يشكل اختراقاً غير مشروع. كما يبقى القصد متوافراً حتى إن أدى فعله إلى الدخول إلى نظام آخر غير الذي كان ينوي اختراقه وفي بعض الحالات، يعاقب الجاني على نتائج لم يقصدها شخصياً، إذا كانت هذه النتائج أشد جسامة وتحققت بفعل منه.

وهذا ما نصت عليه الفقرتان الثانية والثالثة من المادة 394 مكرر من القانون 04-15+ق24-06 بقولها في الفقرة 2 " **تضاعف العقوبة إذا ترتب على ذلك حذف أو تغير لمعطيات المنظومة**" والفقرة 3

[1] بعرة سعيدة، مرجع سابق، ص 55.

[2] لعاقل فريال، مرجع سابق، ص 38.

تنص على أنه "**إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة، تكون العقوبة الحبس من سنة إلى ثلاث سنوات والغرامة من 100.000 دج إلى 300.000 دج**"، حيث نلاحظ بأن المشرع قد شدد العقاب على النتائج الخطيرة التي تترتب عن فعل الدخول أو البقاء غير المشروع، ولو لم يتوقعها الفاعل.

أما من ناحية الإرادة، فيجب أن تتجه إرادة الجاني إلى تحقيق الدخول أو البقاء غير المشروعين، بغض النظر عن دافعه، سواء كان بدافع الفضول، أو التحدي، أو حتى بغرض نبيل كالكشف عن ثغرات النظام. فالعبرة هنا بتحقق الفعل لا بالغاية من ورائه ولا يتوفر القصد الجنائي إذا كان الجاني يجهل وجود حظر أو يعتقد أنه يملك الإذن بالدخول أو البقاء، ما دام ذلك الجهل أو الاعتقاد قائماً على أساس معقول.[1]

ثانياً: الركن المعنوي في الاعتداءات على سير النظام والمعطيات داخل وخارج النظام

تُعد الاعتداءات الموجهة نحو سير النظام (من خلال التعطيل أو العرقلة أو الإفساد)، أو الاعتداءات الماسة بالمعطيات، من الجرائم العمدية التي يشترط فيها توافر القصد الجنائي العام، المتمثل في العلم والإرادة يجب أن يعلم الجاني بأن فعله يمس المعطيات أو النظام بشكل غير مشروع، وأن ما يقوم به هو إدخال أو حذف أو تعديل للبيانات، وأن يدرك خطورة هذا الفعل وما قد يترتب عنه من آثار قانونية.[2]

كما يشترط أن تتجه إرادته بشكل صريح نحو هذا السلوك، فلا يُسأل من قام به عن طريق الخطأ أو الإهمال.

وقد أكدت المادة 394 مكرر 1 على ضرورة أن ترتكب هذه الأفعال "بطريق الغش"، أي أن يكون الجاني على علم بعدم مشروعية تصرفه، دون أن تشترط القصد الجنائي الخاص، مثل نية الإضرار أو تحقيق الربح، خلافاً لبعض التشريعات التي كانت تشترط ذلك.

---

[1] لعاقل فريال، مرجع سابق، ص 38-39.

[2] بعرة سعيدة، مرجع سابق، ص 62.

وقد تم انتقاد هذا التوجه في التشريعات السابقة لأنه كان يؤدي إلى إفلات بعض الجناة من العقاب في حال عدم توافر نية الإضرار، رغم جسامة الفعل المرتكب، كإتلاف بيانات علمية أو بحثية من هنا، استبعد المشرع الفرنسي القصد الخاص من هذا النوع من الجرائم في تعديله للمادة 323-3، وهو ما سار عليه المشرع الجزائري باعتماده لعبارة "بطريق الغش" دون الإشارة إلى نية الإضرار أو تحقيق مكسب.[1]

أما فيما يخص الاعتداءات العمدية الماسة بالمعطيات الموجودة خارج النظام، فقد نصت المادة 394 مكرر 2 من القانون 24-06 على أنه "يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمداً وعن طريق الغش..."، ما يدل بوضوح على ضرورة توافر القصد الجنائي العام.

كما أنه يجب أن يعلم الجاني في هذه الحالة بأن المعطيات التي يتعامل معها (سواء بتصميمها، أو تجميعها، أو نشرها، أو الاتجار بها) هي معطيات مخزنة أو معالجة أو مرسلة عبر منظومة معلوماتية، وأن فعله قد يسهم في ارتكاب اعتداءات ضد نظام المعالجة الآلية. ويشترط كذلك أن تتجه إرادته إلى هذا السلوك، مع وعيه بخطورته والنتائج التي قد تترتب عنه.[2]

[1] لعاقل فريال، مرجع سابق، ص 41.

[2] نفس المرجع ، ص42.

ملخص الفصل:

تُعتبر الجرائم المعلوماتية من أبرز جرائم هذا العصر وأحدثها، فهي تُرتكب في بيئة وهمية تستعمل فيها وسائل إلكترونية متطورة، وتستهدف الأفراد، المؤسسات، وحتى الدول. وقد أفرزت هذه الجرائم تحديات حقيقية أمام الأنظمة القانونية، نظرًا لطبيعتها الخاصة التي تختلف عن الجرائم التقليدية من حيث الأسلوب، والأدوات، وحتى شخصية المجرم المعلوماتي. ومن خلال دراسة هذا الفصل، تبيّن أن هذه الجرائم لا تنشأ من فراغ، بل تُغذّيها دوافع متعددة، منها ما هو شخصي كالرغبة في الكسب أو الانتقام أو التسلية، ومنها ما هو موضوعي، مرتبط بضعف الوعي المعلوماتي، أو بوجود ثغرات أمنية وقانونية. كما أظهر التحليل أن تنوع الجرائم المعلوماتية واختلاف أركانها يفرض ضرورة مراجعة مستمرة للمنظومة القانونية، وتحديث آليات المواجهة بما يتماشى مع تطور البيئة الرقمية. وعليه، فإن الجريمة المعلوماتية تُعد من أخطر الظواهر الإجرامية المستحدثة، مما يستوجب مقاربات جديدة على مستوى التشريع، التحقيق، والمتابعة، لضمان أمن المجتمع الرقمي، وحماية الحقوق والحريات في هذا الفضاء الافتراضي المتسارع

الفصل الثاني:

مرحلة التحقيق في الجرائم المعلوماتية

الفصل الثاني: مرحلة التحقيق في الجرائم المعلوماتية

بعد أن تطرقنا في الفصل الأول إلى الإطار المفاهيمي للجريمة المعلوماتية، من حيث تعريفها وخصائصها وأنواعها وأركانها، ننتقل في هذا الفصل إلى مرحلة غاية في الأهمية ضمن مراحل العدالة الجزائية، وهي مرحلة التحقيق في الجرائم المعلوماتية، وتكمن أهمية هذه المرحلة في كونها الأساس الذي تُبنى عليه باقي الإجراءات، لما لها من دور محوري في كشف الحقيقة وجمع الأدلة المتعلقة بهذا النوع المستحدث من الجرائم. التطور السريع في وسائل التكنولوجيا، والتوسع المستمر في استعمال الإنترنت والشبكات المعلوماتية، أدّى إلى ظهور أساليب إجرامية معقدة يصعب كشفها أو التعامل معها بالطرق التقليدية، مما فرض على الأجهزة القضائية والأمنية مواكبة هذا التغير من خلال تطوير أساليب التحقيق والاستعانة بوسائل تقنية حديثة تُمكن من جمع الأدلة الرقمية وتحليلها بطريقة دقيقة وفعالة. كما أن التحقيق في الجرائم المعلوماتية لا يقتصر على مجرد جمع المعلومات، بل يتطلب إلمامًا بالجوانب التقنية والقانونية معًا، بالإضافة إلى التنسيق بين مختلف الجهات المعنية وتوفير بيئة قانونية تسمح للمحقق بأداء مهامه في إطار من الشرعية واحترام حقوق الأفراد. وقد أصبح من الضروري اليوم أن يتسلّح المحقق في هذا المجال بالخبرة والمعرفة التقنية، إلى جانب الكفاءة القانونية، نظرًا لخصوصية هذا النوع من الجرائم وصعوبة إثباتها. انطلاقًا من ذلك، جاء هذا الفصل ليسلط الضوء على ماهية التحقيق الجنائي في الجرائم المعلوماتية، من خلال بيان مفهومه، وخصائصه، وشروطه، بالإضافة إلى الوسائل والأدوات والأساليب المعتمدة في إدارته، سواء التقليدية أو المستحدثة، وذلك في ضوء ما جاء به التشريع الجزائري من أحكام لمواكبة هذا التطور.

المبحث الأول: ماهية التحقيق الجنائي في الجرائم المعلوماتية

يُعدّ التحقيق من أهم الإجراءات التي تُتخذ بعد وقوع الجريمة، نظراً لما له من دور محوري في التأكد من وقوع الفعل الإجرامي، وإقامة الإسناد المادي على مرتكبه من خلال أدلة الإثبات بمختلف أنواعها. وهو كما يدل اسمه عليه، عملية استجلاء للحقيقة، تهدف إلى الوصول إلى إدانة المتهم أو عدمها بعد جمع الأدلة المتعلقة بالجريمة.

كما أن التحقيق ، بمفهومه العام، هو البحث والتحري عن حقيقة أمر معين ، ينطلق منذ لحظة تلقي المحقق بلاغاً عن وقوع جريمة ، ويمر عبر سلسلة من الإجراءات التي يسلكها بقصد كشف غموض الجريمة وكيفية ارتكابها، من أجل إيصال الدعوى العمومية الناتجة عنها إلى القضاء للفصل فيها، وتحديد المسؤولية الجنائية للفاعل وإنزال العقوبة به. ويتميّز التحقيق في الجرائم الإلكترونية بخصوصية فنية وتقنية تجعله مختلفاً عن التحقيق في الجرائم العادية، وذلك نظراً لحداثة هذا النوع من الجرائم ، وارتفاع درجة المهارة التقنية لدى مرتكبيها ، فضلاً عن الطابع غير المادي للأدلة المستخلصة منها، مما يجعل التحقيق أكثر تعقيداً ويتطلب أدوات وخبرات خاصة

وإذا كان التحقيق يعني، في صورته العامة، مجموعة الإجراءات التي تباشرها سلطة التحقيق عند وقوع جريمة أو حادثة بغرض التنقيب عن الأدلة وجمعها، فإن الأمر يقتضي في مجال الجرائم الإلكترونية التوقف عند خصوصية هذا النوع من التحقيق[1]، ومن أجل بيان مفهوم التحقيق الجنائي بدقة سنقوم بتعريفه وذكر خصائصه من خلال **(المطلب الأول)** ثم نمر إلى شروطه ووسائله في **(المطلب الثاني)** وأخيرا نقوم بالتطرق إلى المحقق الجنائي من خلال **(المطلب الثالث)**

المطلب الاول: مفهوم التحقيق الجنائي في الجرائم المعلوماتية

يعد التحقيق من أبرز مراحل الإجراءات الجنائية ، إذ يهدف إلى الكشف عن الحقيقة سواء بالنسبة للجريمة المرتكبة أو للمتهم ، ويمر التحقيق بمجموعة من الخصائص التي تحدد طبيعته وفعاليته، وتختلف هذه الخصائص بناء على نوع الجريمة المرتكبة ، سواء كانت تقليدية أو إلكترونية ، كما يعتبر التحقيق عملية منهجية وموضوعية تهدف إلى جمع الأدلة والشهادات وتحقيق العدالة وحماية حقوق الأطراف المتورطة، وفيما يخص التحقيق في الجرائم المعلوماتية ، فإن خصائصه تتسم بتحديات خاصة

[1] خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة ، ص3

تتطلب تقنيات ومهارات متطورة على عكس التحقيقات التقليدية ، كما أن خصائص التحقيق تستند إلى المبادئ القانونية التي تكفل حقوق ، المتهم مثل مبدأ "المتهم بريء حتى تثبت إذانته"[1] وفي نفس السياق سنعرف التحقيق الجنائي في **(الفرع الأول)** ثم نتطرق لخصائص التحقيق في **(الفرع الثاني)** ثم خصائصه في **(الفرع الثالث)**.

الفرع الأول: تعريف التحقيق الجنائي في الجريمة الإلكترونية

لا يختلف التحقيق في الجريمة الإلكترونية ، من حيث الهدف العام ، عن التحقيق في الجرائم التقليدية ، إذ يسعى كلاهما إلى كشف الحقيقة من خلال جمع وتحليل الأدلة ، غير أنّ خصوصية الفضاء الرقمي تتطلب معالجة خاصة وسنتناول في هذا الفرع تعريف التحقيق الجنائي من حيث اللغة والاصطلاح.

أولاً: المقصود بالتحقيق الجنائي في الجريمة الإلكترونية

يقصد بالتحقيق الجنائي عموماً ، البحث والتنقيب عن الأدلة من أجل كشف حقيقة وقوع الجريمة وتحديد مرتكبها ، وذلك انطلاقاً من إجراءات قانونية محددة.

1 تعريف التحقيق لغة:

التحقيق في اللغة مأخوذ من كلمة "حقق، يحقق، تحقيقاً" ، ويُقال "حقق الظن" أي صدقه ، و"حقق الأمر" أي أحكمه ، كما يُقال "حقق مع فلان في قضيته" أي استجوب رأيه وبحث عن الحقيقة فيها.

2 تعريف التحقيق إصطلاحاً:

في معناه العام عرف التحقيق بأنه: "إتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها"[2]

كما يُعرف أيضاً بأنه "مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتُكبت، وتجميعها، ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة"

---

[1] خالد علي نزال الشعار ، مرجع سابق ، ص 3

[2] محمد بوعمرة ، سيد علي بنينال ،جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري ، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية ، كلية الحقوق والعلوم السياسية ، قسم القانون الخاص، جامعة أكلي محند أولحاج–البويرة ، 2019–2020، ص 17

ووفقاً لتعريف آخر، يُقصد به: "مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهدف التنقيب عن الأدلة وتقديرها والكشف عن الحقيقة"[1]

كما يمكن تعريف التحقيق الجنائي الإلكتروني في الجرائم الإلكترونية بأنه "عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجريمة الإلكترونية من فاعل لها ودليل إلكتروني لتقديمهم إلى سلطات التحقيق القضائي المتخصصة في هذا النوع من الجرائم لإقامة العدل."[2]

الفرع الثاني: التمييز بين التحقيق الجنائي الإلكتروني والتحقيق الجنائي التقليدي

بعدما تطرقنا في الفرع السابق إلى تعريف التحقيق الجنائي بوجه عام، وإلى التحقيق في الجرائم الإلكترونية ، فإننا الآن نقف عند مسألة بالغة الأهمية ، وهي إلى أي مدى يختلف التحقيق في الجرائم الإلكترونية عن نظيره في الجرائم التقليدية؟ هذا التساؤل لم يأت من فراغ ، بل فرض نفسه بقوة نتيجة ما شهدته البيئة الرقمية من تطورات متسارعة ، رافقها نمو مضطرد في أساليب ارتكاب الجرائم الإلكترونية، سواء من حيث طبيعة الفعل الإجرامي ، أو من حيث تعقيد وسائل ارتكابه وصعوبة كشفه ، ما جعل من التحقيق في هذا النوع من الجرائم ميدانًا جديدًا ، يحتاج أدوات وإجراءات مغايرة لما هو معتمد تقليديًا. ويمكن تبيان أبرز أوجه الاختلاف بين النوعين على النحو التالي[3]:

1 اختلاف المفاهيم والمصطلحات الإجرائية

التحقيق في الجرائم الإلكترونية يفرض استعمال مصطلحات تقنية حديثة ، تتلائم مع طبيعة الوسط الذي تُرتكب فيه هذه الجرائم، على سبيل المثال يتم استخدام مصطلح "الولوج" كبديل عن "التفتيش"، و"النسخ الإلكتروني" بدلًا من "الضبط المادي"، وهي مفاهيم تستجيب لواقع الفضاء الافتراضي الذي تُرتكب فيه الجرائم. هذا التحول المفاهيمي لا يعكس فقط تطور اللغة القانونية، وإنما يُمثل ضرورة عملية لحسن سير إجراءات التحقيق، بحيث يتم تجاوز الإطار التقليدي للضبطيات الجنائية.

[1] حسن الجوخدار ، التحقيق الإبتدائي في قانون الأصول المحاكمات الجزائية، دار الثقافة ،عمان ، ط/الأولى ،2008 ، ص 11

[2] خالد علي نزال الشعار ، مرجع سابق ، ص 5

[3] نفس المرجع ، ص 5-6

2 خصوصية الجريمة الإلكترونية وذاتية التحقيق فيها

يستمد التحقيق في الجرائم الإلكترونية طابعه الخاص من خصوصية هذه الجريمة، كونها لا تقوم على اعتداء مادي تقليدي، بل ترتكز في الغالب على التلاعب بالمعطيات الرقمية، وانتهاك الخصوصيات الإلكترونية، والاعتداء على أنظمة المعلومات وهذا ما يجعل من مسرح الجريمة فضاءً افتراضيًا لا تدركه الحواس، بل يحتاج إلى أدوات تحليل رقمية متطورة وتقنيات تتبع إلكترونية معقدة. فالتحقيق هنا لا ينحصر في جمع الأدلة المادية، بل يتعداه إلى تتبع الأنشطة الرقمية الخفية، مما يتطلب محققًا له دراية بالأنظمة المعلوماتية.

3 طبيعة الأدلة الإلكترونية وصعوبات التعامل معها

الأدلة في الجرائم الإلكترونية لا تكون تقليدية كالبصمات أو الشهادات، بل تكون غالبًا عبارة عن ملفات رقمية، سجلات دخول، تراسل بريد إلكتروني، أو حركة مالية عبر الإنترنت. هذه الأدلة تتميز بكونها غير مرئية، سريعة التلاشي، وقابلة للتعديل أو الإخفاء بسهولة، مما يتطلب التعامل معها وفق قواعد دقيقة تضمن سلامة سلسلتها وشرعية الحصول عليها ، وهو أمر لا يمكن مقارنته بالأدلة التقليدية.

4 صعوبات الإقناع القضائي بطبيعة الجريمة

من الصعوبات البارزة التي تواجه جهات التحقيق في هذا المجال هي كيفية عرض الأدلة الرقمية وتفسيرها أمام القضاء. فغالبًا ما تكون هذه الأدلة معقدة وتتطلب فهماً تقنياً معيناً قد لا يتوفر للقضاة أو المحامين، وهو ما يسهل زرع الشك في وجدان المحكمة. كما أن غياب فرق متخصصة في التحقيق والمحاكمة في هذا المجال يؤدي إلى ضعف الإقناع وتهديد مبدأ العدالة الجنائية.

5 خصوصية شخصية المشتبه فيه

غالبًا ما يكون مرتكب الجريمة الإلكترونية شخصًا يتمتع بمستوى عالٍ من الذكاء والمهارات التقنية، وقد يكون على دراية بأساليب التمويه الرقمي، واستخدام الشبكات الافتراضية الخاصة، وتقنيات إخفاء الهوية. وهو ما يتطلب من المحقق أن يكون مؤهلاً ليس فقط قانونيًا، بل تقنيًا أيضًا، حتى يستطيع ملاحقة الجاني وكشف نشاطه الإلكتروني.

6 ضعف الإطار التشريعي والتعاون الدولي

الطابع العابر للحدود في الجريمة الإلكترونية يجعل من الصعب إخضاع مرتكبيها للسلطة القضائية الوطنية، خاصة مع غياب إطار قانوني موحد بين الدول، وضعف التعاون الأمني والتقني الدولي. فالجرائم المرتكبة انطلاقًا من دولة ما قد تُحدث آثارًا في دول أخرى دون إمكانية تتبع مصدرها أو ملاحقة مرتكبيها، مما يجعل من الفضاء الإلكتروني ملاذًا آمناً للمجرمين.

7 الحاجة لتشريعات خاصة واستحداث آليات جديدة

إن طبيعة التحقيق في الجرائم الإلكترونية، بما تحمله من تعقيد في إجراءات البحث، والتعامل مع أدلة غير مادية، والمشتبه فيهم ذوي قدرات عالية، تفرض على المشرّع ضرورة إعادة النظر في القواعد التقليدية المنظمة للتحقيق الجنائي. فلا بد من سنّ تشريعات خاصة تأخذ بعين الاعتبار خصوصية هذا المجال، من حيث آليات البحث، قواعد الإثبات، وتنظيم عمل الخبراء التقنيين، كما فعل المشرّع المصري في القانون رقم 175 لسنة 2018 المتعلق بمكافحة جرائم تقنية المعلومات، الذي وضع إطارًا قانونيًا دقيقًا يشمل إجراءات الضبط والتحقيق والمحاكمة في الجرائم الإلكترونية[1].

الفرع الثالث: خصائص التحقيق الجنائي في الجريمة المعلوماتية

يتميز التحقيق الجنائي في الجرائم المعلوماتية، بسمات ذاتية وخصائص تميزه عن التحقيق الجنائي في الجرائم التقليدية وتعود هذه الذاتية للأسباب التالية:

- مرتكبي الجرائم المعلوماتية يمتلكون قدرات عالية تمكنهم من إتلاف وإضاعة الأدلة الإلكترونية في وقت قصير.
- نوعية هذه الجرائم الرقمية لا تترك أثار مادية في مسرح الجريمة.
- التحقيق في الجرائم المعلوماتية يحتاج إمكانيات مادية وقواعد وإجراءات تختلف عن التحقيق في الجرائم التقليدية من حيث طبيعة السلوك الإجرامي المعلوماتي[2].

---

[1] خالد علي نزال الشعار، مرجع سابق ، ص 6-7-8

[2] بوحزمة نصيرة، التحقيق الجنائي في الجرائم الإلكترونية ، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية ، قسم الحقوق، جامعة الجيلالي اليابس، سيدي بلعباس، 2021-2022 ، ص 121

كما يتميز التحقيق بخصائص فنية أخر تتمثل في الكتابة والتدوين **(أولا)** ثم سرية التحقيق **(ثانيا)**

أولا: الكتابة والتدوين

إن إجراءات التحقيق يجب أن تكون كلها ثابتة وموثقة بالكتابة، لأن التدوين هو الذي يعطي للمعلومات طابع رسمي ويجعله حجة يعتمد عليها ، وهذا حتى يستطيع القاضي الرجوع إليها وقت الحاجة لأنه إذا لم يتم التدوين لا يعتبر التحقيق قد حدث ، كما أن القانون يفرض على المحقق تدوين كل الإجراءات التي يقوم بها مثل سماع الشهود وإستجواب المتهمين، والتفتيش وضبط الأشياء المتحصل عليها من إجراء التفتيش فالمشرع لم يعتمد على الأقوال الشفوية ولا على ذاكرة القاضي ، لأن مثل هذه الأمور يمكن أن تتغير أو تنسى مع مرور الوقت ، خاصة في القضايا المعقدة والطويلة مثل الجرائم الإلكترونية ولهذا فرض المشرع أن كل إجراء يتم تسجيله كتابيا بطريقة واضحة ، وتكون المحاضر حسب القانون تحتوي على المكان والزمان الذي دار فيه الإجراء، وكدا أسماء الأطراف وكل التفاصيل الدقيقة المرتبطة به فالمحاضر لا تقتصر على غير أقوال الشهود أو المتهم ، بل حتى تقارير الخبراء والمعاينات وكل تصرف يتم أثناء التحقيق ، كما أن كل هذه الوثائق تجمع وترسل إلى النيابة العامة ، مرفقة بكل الأدلة والأشياء المضبوطة ، وهذا من أجل أن تكون لهم صورة كاملة على القضية.[1] ولكي تكون هذه المحاضر قانونية يجب أن يقوم بكتابتها كاتب ضبط تابع للمحكمة ، وأن يكون حاضر في كل إجراء وذلك حتى يتم الرجوع إليها عند الضرورة وهذا ما نصت عليه المادة 68-2 من ق.إ.ج التي تؤكد على أنه: "**تحرر نسخة من هذه الإجراءات ، وكدا جميع الأوراق ويؤثر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة مطابقتها للأصل** "

لكن في بعض الحالات يمكن للكاتب أن يتغيب لسبب معين ، وفي هذه الحالة يمكن للقاضي أن يكمل الإجراء لوحده لأنه لا يجب أن تتعطل إجراءات التحقيق ، وبالتالي يمكنه الإستعانة بخدمات أحد أفراد الضبطية القضائية ، وهذا من أجل ضمان مواصلة التحقيق بشكل جيد ، ولكن بشرط أن يقوم القاضي بتدوين سبب غياب الكاتب في المحضر ويؤكد أن هذا الغياب لم يؤثر على سير التحقيق. وإذا تكلمنا عن الجرائم المعلوماتية فنرى بأن الأمور هنا تزداد دقة وحدة ، لأن الأدلة الموجودة فيها حساسة جدا ويمكن أن تتغير أو تمحى بسهولة ، لهذا فالتوثيق الكتابي يعتبر ضروري جدا وكل تفصيل مهما كان

[1] بوحزمة نصيرة ، مرجع سابق ، ص122

صغير يجب أن يسجل ويدون في محضر رسمي وموثق ، كما أن المحضر يجب أن يكون مستوفيا لجميع الشروط الشكلية ، وتكون موقعة من طرف قاضي التحقيق وكاتبه والشاهد إن وجد. فالغاية هنا من تدوين إجراءات التحقيق ، هي تمكين قاضي التحقيق من التركيز الذهني والفكري أثناء سير التحقيق ، لأن عملية التدوين تترك لكاتب التحقيق بإعتباره مساعدا فنيا ، يقوم هذا الأخير بتسجيل كل ما يصدر عن أطراف الدعوى من أقوال وإجابات، بما يساهم في تشكيل قناعة القاضي لاحقا ، وتعتبر محاضر التحقيق وثائق رسمية تحتوي على كل ما دار خلال جلسات التحقيق ، وهي التي تمكن الخصوم من الإطلاع على كل ما جاء فيها ومناقشتها.

كما أن القانون يشترط وجود كاتب من أجل تدوين كل خطوات التحقيق ، ويشترط أن يوقع المحضر من طرف قاضي التحقيق والكاتب والشاهد إن وجد ، وهذا حتى يكون له حجية قانونية كما يجب أن يكون المحضر خاليا من أي فراغات بين السطور ، ويصادق على كل شطب أو تصحيح من قبل القاضي والكاتب والشاهد ، وكدا المترجم عند الحاجة وهذا من باب ضمان المصداقية القانونية للمحضر[1].

ثانيا: سرية التحقيق

السرية تعتبر من الضمانات الأساسية للتحقيق ، والتي يقصد بها عدم السماح للجمهور بحضور إجراءات التحقيق ، بل القيام به في سرية تامة بعيدا عن أنظار الجمهور ، وهذا ما نصت عليه الفقرة الأولى من المادة 11 من ق.إ.ج بقولها "**تكون إجراءات التحري والتحقيق سرية ما لم ينص القانون خلاف ذلك ودون الإضرار بحقوق الدفاع**" بمعنى أن إجراءات البحث والتحري يجب أن تكون سرية ، إلا إذا نص القانون صراحةً على أنها علنية ، ومع ذلك يجب أن لا تمس هذه السرية حقوق الدفاع ، أي أنه لا يجوز إستخدامها كذريعة لحرمان المتهم أو محاميه من الإطلاع على الملف ، أو ضمانات المحاكمة العادلة. كما أن القانون يلزم كل المشاركين في إجراءات التحقيق، مثل ضباط الشرطة القضائية أو القضاة أو حتى الكتاب والمترجمين ، بكتمان السر المهني وعدم نشر أي شيء يتعلق بالتحقيق بحيث لا تعرض محاضر التحقيق لكي يطلع عليها العامة ولا يجوز إذاعتها أو نشرها في الصحف وهذا ما نصت عليه الفقرة الثانية من نفس المادة على أنه "**كل شخص يساهم في هذه الإجراءات ملزم بالحفاظ على**

[1] بوحزمة نصيرة ، المرجع السابق ، ص122-123

السر المهني تحت طائلة العقوبات المنصوص عليها في التشريع الجزائ" فالمادة تنص بصريح العبارة ، على أنه كل من يخالف هذا فإنه يعرض نفسه للعقوبات المنصوص عليها في القانون الجزائي فالغرض هنا من السرية ، هو ضمان المحافظة على خصوصية المتهم بحيث يؤذي هذا إلى تعزيز شعوره بالأمان والراحة ، وعدم التفكير المفرط في أنه قد تم تعريضه إلى التشهير ، وبالتالي يمكن أن يؤثر عليه هذا الأمر بالسلب ، بحيث لا يمكنه العودة إلى ممارسة حياته بشكل طبيعي ، خاصة وأن هذا الأمر إلى يمكن أن يصل إلى عائلته ما يزيد في تعقيد الأمور أكثر و أكثر، وتؤذي إلى ترك أثار سلبية إستنادا إلى مبدأ "**المتهم بريء ما لم تتم إدانته**" وبالتالي يمكن أن تظهر براءته بعد إنتهاء القضية المنسوبة إليه ، ما يرجح إلى أنه قد يجد نفسه محاط بالإنتقاذات اللاذعة نظرا لكونه قد تعرض للتشهير والإساءة ، ما أذى إلى إنتشار الشائعات عليه بين أفراد المجتمع . وعلى غرار مبدأ السرية الذي يعد الأصل في إجراءات التحقيق ، فإن القانون يقر علانية التحقيق بالنسبة لأطراف الدعوى ، سواء كانوا متهمين أو مدعين مدنيين أو وكلاء نيابة ، حيث يعتبر من حقهم حضور إجراءات التحقيق بإعتبار أن لهم مصلحة مباشرة فيه. لذلك أوجب القانون إعلامهم بمواعيد التحقيق بدقة ، بداية من يوم التحقيق إلى غاية الساعة والمكان. كما يمنح القانون للمتهم الحق في إصطحاب محاميه عند حضوره جلسات التحقيق. وهذا ما أكدته المادة 100 من ق.إ.ج التي ألزمت قاضي التحقيق عند أول إستجواب للمتهم ، بأن يبلغه بالوقائع المنسوبة ، إليه ويحيطه علما بحقه في إلتزام الصمت إلى غاية حضور المحامي. وفي حال عدم تعيين محامي يحق للمتهم طلب تأجيل الإستجواب ، بل يعين له محام تلقائيا ، إذا لم يختر واحداً كما شددت المادة على ضرورة بطلان كل إجراء يتم دون إحترام هذه الضمانات.

أما بالنسبة إلى الخصوم في الدعوى ، فإن القاعدة بالنسبة لهم تتلخص في مباشرة حضورهم ومتابعتهم لجميع الإجراءات ، لأن هذا يغرس في نفوسهم الثقة والإطمئنان ، وكدا يجعلهم على معرفة تامة بسير التحقيق مما يعطيهم الفرصة في إبداء أي إعتراض ، على أي إنحراف أو خطأ قد يقع فيه المحقق، وعليه يذكر بأن التحقيق الأولي يكون سري بالنسبة لعامة الناس ، وعلني بالنسبة للخصوم ووكلائهم وعلى هذا الأساس فإن إجراء التحقيق بصورة سرية ، يؤذي إلى تفادي محاولات المتهم أو المشتركين معه في إفساد الأدلة ، أو محاولة التأثير على الرأي العام ، كما يهدف أيضا إلى حماية الإجراءات اللاحقة التي ستقوم بها سلطات التحقيق، ومن هذا يُستنتج بأنه قد تكون سرية التحقيق لازمة

في بعض الأحيان للوصول إلى الحقيقة ، كما أنها ضمانة لحيادية المحقق حتى لا يكون متأثرا بالرأي العام وبالتالي تتحقق إستقلاليته فيما يقوم به من تحقيقات.[1]

المطلب الثاني: شروط التحقيق ووسائله وأدواته

يشترط القانون من أجل فتح التحقيق ، جملة من الشروط القانونية والموضوعية ، ومنها أن تكون الجريمة قائمة أو مرجح وقوعها، وأن تتوفر أدلة كافية للبحث عن مرتكبها ، كما أنه يشترط أن يكون الفعل مجرما قانونا ، إذ تُستعمل في هذا النوع من التحقيقات وسائل تقنية ، وإجراءات تتلائم مع طبيعة الجريمة المعلوماتية، والتي تتطلب أحيانا وسائل إستثنائية مقارنة بالجرائم التقليدية[2] ، وفي هذا الصدد سنتناول في **(الفرع الأول)** شروط التحقيق ثم نعرج إلى **(الفرع الثاني)** لنتكلم عن وسائل التحقيق ثم في **(الفرع الثالث)** سنتطرق لأدوات التحقيق

الفرع الأول: شروط التحقيق في الجرائم المعلوماتية

من خلال دراسة أحكام قانون الإجراءات الجزائية ، يتبين لنا أن المشرع الجزائري قد وضع وحدد جملة من الشروط والضوابط ، التي تحكم سير التحقيق الجنائي وذلك بهدف تحقيق التوازن بين مصلحة المجتمع في متابعة الجريمة، وضمان حقوق الأفراد وحرياتهم، فالتحقيق في الجرائم المعلوماتية بل والتقليدية أيضا، يتطلب عدة شروط أساسية والتي سنتطرق لها من خلال أن يكون التحقيق بصدد جريمة **(أولا)** ثم أن تكون الجريمة قد وقعت فعليا أو يرجح وقوعها **(ثانيا)** و**(ثالثا)** أن يجرى التحقيق في مواجهة المتهم أو بقصد الوصول إليه

أولا: أن يكون التحقيق بصدد جريمة (جناية أو جنحة)

يعد هذا الشرط من الشروط الأساسية، التي يقوم عليها التحقيق الإبتدائي في أي جريمة، بما فيها الجرائم المعلوماتية ، إذ لا يجوز مباشرة التحقيق إلا إذا تعلق الأمر بجريمة يعاقب عليها القانون ، أي أن الفعل محل التحقيق يجب أن يكون منصوصا عليه في التشريع الجزائي ، سواء في قانون العقوبات أو في القوانين الخاصة ، مثل قانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال. ويُكرس هذا الشرط مبدأ دستوري معروف في المجال الجنائي ، والذي يتمثل في قاعدة "**لا جريمة ولا عقوبة إلا بنص**"

---

[1] بوحزمة نصيرة ، مرجع سابق ، ص ص 124-127

[2] خالد علي نزال الشعار ، المرجع السابق ، ص 37

والتي تقضي بعدم إمكانية تحريك الدعوى العمومية ، أو فتح التحقيق ما لم يوجد نص قانوني يجرم الفعل ويوجب العقاب عليه ، وبناء عليه إذا لم تتوافر أركان الجريمة المنصوص عليها في القانون فإن أي إجراء يتم إتخاذه في هذا السياق ، يعد باطلا وقد يؤذي إلى إصدار قرار بحفظ الملف أو إصدار أمر عدم وجود وجه للمتابعة. كما تنص على ذلك المادة 66 من قانون الإجراءات الجزائية ، على أن التحقيق يكون وجوبيا في الجنايات أي أنه لا يمكن بأي حال من الأحوال إحالة المتهم إلى المحكمة مباشرة دون المرور بمرحلة التحقيق القضائي، وذلك نظرا لخطورة العقوبة المقررة للجنايات والتي قد تصل إلى السجن المؤبد أو الإعدام، ولأن التحقيق في هذه الحالات يعد وسيلة لضمان حقوق الدفاع والتثبت من الوقائع. أما في قضايا الجنح فإن التحقيق يكون جوازيا أي إختياريا، إلا إذا نص القانون صراحة على وجوبه في حالات معينة وفقا للفقرة الثانية من نفس المادة والتي تجيز لوكيل الجمهورية أن يطلب من قاضي التحقيق مباشرة التحقيق، متى إقتضت خطورة الجريمة أو كلما كانت القضية معقدة، وبالتالي يكون التحقيق في مواد الجنح وسيلة لضمان الوصول إلى الحقيقة في الجرائم المعقدة لاسيما الجرائم المعلوماتية التي تتسم غالبا بالغموض والتقنيات العالية.

ويصبح التحقيق ضروريا أيضا عندما يكون الجاني مجهول الهوية، أو في حالة فراره أو تواجده في خارج الوطن.[1]

أما بالنسبة للمخالفات، وهي الجرائم الأقل خطورة في التدرج القانوني فإن التحقيق فيها يكون جوازي ويشترط طلبه من وكيل الجمهورية مع الإشارة إلى أن الضحية لا يمكنه مباشرة تأسيس نفسه كطرف مدني إلا إذا تم فتح التحقيق، كما لا يمنع ذلك من تأسيسه إذا تم فتحه أصلا من طرف النيابة. ويكفي لفتح التحقيق أن يتوفر الركن المادي للجريمة، والذي يتطلب تحديد الفعل الإجرامي والسلوك المجرم بنص قانوني الأمر الذي يساعد القاضي على التكييف القانوني.[2]

وفي الجرائم الإلكترونية، غالبا ما يتمثل السلوك الإجرامي في إستخدام الحاسوب وأحيانا في ضرورة الإتصال بشبكة الإنترنت، ويختلف هذا السلوك بإختلاف نوع الجريمة الواقعة فقد يكون أنياً

[1] بن عنطر سيهام ، التحقيق الجنائي في الجرائم الإلكترونية ، مذكرة لنيل شهادة الماستر في القانون ، كلية الحقوق والعلوم السياسية، قسم الحقوق ، جامعة مولود معمري ، تيزي وزو ، 2023 ، ص 29

[2] عمارة فوزي ، قاضي التحقيق ، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم ، كلية الحقوق، جامعة الإخوة منتوري ، قسنطينة ، 2009-2010 ، ص 39

كجريمة سرقة البيانات، أو مستمرا مثل ما يكون في حالات التحريض أو الترويج للإرهاب عبر مواقع إلكترونية أما الركن المعنوي فإن أغلب هذه الجرائم تعتبر عمدية ، وتتطلب توافر القصد الجنائي المتمثل في العلم والإرادة وإن كان يختلف من جريمة لأخرى حسب طبيعتها.[1]

ثانيا: أن تكون الجريمة قد وقعت فعليا أو يرجح وقوعها

لا يجوز فتح تحقيق بشأن جريمة محتملة الوقوع ، إذ يشترط أن تكون الجريمة قد ارتكبت فعلاً أو يحتمل وقوعها ، وبالتالي لا يجري التحقيق بشأن جريمة محتملة، وإلا فإن الإجراء يعتبر باطلا ، وفي هذا السياق يطرح إشكال بشأن مدى مشروعية ، الإجراءات السابقة على التحقيق الإبتدائي وكذلك مدى جواز التدخل الإداري لمنع وقوع الجريمة.

كما يجوز لضباط الشرطة القضائية ، مباشرة أعمال الإستدلال وجمع المعلومات في حال توفرت ، دلائل على وقوع الجريمة ، كما يمكنهم التحقق من حالة التلبس في الجرائم المعلوماتية عند مشاهدة الجاني بصدد إختراق نظام معلوماتي مثلا ، وقد تظهر الجريمة الإلكترونية في حالة تلبس عن بعد ، مثل كما لو لاحظ صاحب مقهى إنترنت شخصا يبث محتوى إباحي ، وقام بإخطار الجهات المختصة فورا غير أن حالة التلبس تعترضها عدة إشكالات قانونية أبرزها مشروعية الإجراء المتخذ لكشف الجريمة، إذ أن بعض وسائل الكشف تتداخل مع حقوق الأفراد وحرياتهم ، كالتخفي عبر الإنترنت أو إنتحال صفة للدخول إلى غرف المحادثة بقصد الإستدلال على نشاط إجرامي.[2]

كما يثار إشكال أخر مرتبط بزمن التلبس، والذي يصعب ضبطه في الجرائم الإلكترونية مقارنة بالجرائم التقليدية إذ أن المطاردة عبر الشبكة قد تتطلب وقتا أطول. وفي سبيل تعقب الجناة ، تم تطوير برمجيات متقدمة تعتمد على تتبع "البصمة الإلكترونية" كتقنية **(ATICD)** التي تمكن من تتبع أول أثر للجريمة وربطها بعنوان الإنترنت الخاص بالجهاز، مما يساعد على تحديد هوية المستخدم ، ومكان إقامته إنطلاقا من معطيات البريد الإلكتروني التي تكشف هوية الجهاز المستخدم ، لأنه يوجد في البريد الإلكتروني رقم IP الخاص بكل جهاز متصل بالإنترنت في خانة header ، ثم بعدها يقوم رجال الضبط القضائي بالذهاب إلى mail option ثم general preference ، ثم إضافة Header، ثم يقوم

[1] بوحزمة نصيرة ، مرجع سابق ، ص 101

[2] بن عنطر سيهام ، مرجع سابق ، ص 30-31

باختيار Show all Header on Inconing Message ثم يذهب إلى الرسالة المرسلة فيجب الـ **(IP)** المرسل المكون من أربعة أرقام يفصل بينهما نقطه في X-Originating- IP ، وبعد التوصل إلى **(IP)** الخاص بالجهاز المستخدم الذي يمكننا من تحديد الموقع الجغرافي، ومزود الخدمة و خط التليفون الأراضي أو شبكة **(ADSL)** لمستخدم الجهاز الذي تم التوصل إلى **(IP)** الخاص بجهازك، ويمكننا بالتالي من تحديد محل إقامة مالكه[1].

ثالثا: أن يجرى التحقيق في مواجهة المتهم أو بقصد الوصول إليه

يعد هذا الشرط من الشروط الأساسية التي تضمن الشروع الفعلي في التحقيق في الجريمة المعلوماتية، حيث لا يمكن أن يفتح التحقيق دون أن يكون الهدف هو الوصول إلى المتهم أو التعرف عليه ، وكما هو معروف فإن التحقيق يجب أن يكون مصوب على الشخص المتهم بإرتكاب الجريمة، سواء كان ذلك عن طريق التعرف عليه وتوجيه التهمة إليه مباشرة ، أو عن طريق البحث المتواصل عنه في حال كان غير معروف أو متوار عن الأنظار ، ففي الجريمة التقليدية يكون عادة هناك عنصر يسهل الوصول إلى المتهم ، مثل مكان السكن أو وسيلة الإتصال المباشرة ، أما في الجرائم الإلكترونية فتزداد الصعوبة في تحديد هوية الجاني، خاصة في حال كان قد إستخدم وسائل التخفي عبر الإنترنت ، لذلك يتطلب في هذه الجرائم إستخدام تقنيات متطورة مثل تحليل بيانات الإتصال أو تتبع البصمات الإلكترونية، إن التحقيق في مواجهة المتهم يساعد في ضمان سلامة الإجراءات القانونية، ويعد خطوة أساسية لضمان تحقيق العدالة. ففي حال تعذر الوصول إلى المتهم مباشرة، يمكن إستخدام أساليب البحث الميداني أو تقنيات البحث الإلكتروني، والتي تتيح للسلطات الكشف عن هويته ومكانه. ووفقا لذلك يتحتم على السلطات المختصة إتخاذ التدابير اللزمة لضمان التوصل إلى الجاني، سواء عبر التعاون مع شركات الإنترنت أو من خلال تقنيات أمنية متقدمة تسمح بتحديد مواقع الإتصال أو الأجهزة المستخدمة في إرتكاب الجريمة.

الفرع الثاني: وسائل التحقيق في الجرائم المعلوماتية

[1] خط الإشتراك الرقمي غير المماثل (ADSL) يعرف بأنه تقنية الشبكة التي تقوم بنقل البيانات بسرعة عبر خطوط الهواتف الحاسبة التناظرية (ANALOGE) وبشكل غير مماثل ، حيث تتحرك البيانات في إتجاه واحد وبسرعة أكبر من الإتجاهات الأخرى.

عند الشروع في بدء التحقيق في الجرائم المعلوماتية، لابدا ومن الضروري أن يلتزم المحقق بالتشريعات والقوانين ذات الصلة ، مع ضرورة إحترام القواعد الإجرائية التي تضمن المشروعية ، وتُعتبر سهولة الوصول إلى الأدلة هي إحدى أبرز سمات هذ النوع من الجرائم ، مما يتطلب من المحقق إمتلاك معرفة دقيقة بأليات وقوع الجريمة ،وكيفية تعقب وتحديد شخصية مرتكبها ،ومن أجل تحقيق ذلك تستخدم وسائل فنية وتقنية تساعد في الوصول إلى الحقيقة وهناك نوعان من الوسائل تساعد في ذلك وهي الوسائل المادية **(أولا)** والوسائل الإجرائية **(ثانيا)**

أولا: الوسائل المادية

وهي مجموعة من الوسائل والأدوات والأنظمة التي تستعمل أثناء التحقيق ، مهمتها الأساسية تتمثل في تقديم الدعم التقني للكشف عن الجريمة ،وتشمل أجهزة وبرمجيات تتيح جمع البيانات وتحليلها مع مراعاة طبيعة الجريمة الإلكترونية الحديثة وتعقيداتها ،وفي هذا العنصر سنتناول أهم هذه الوسائل والأدوات والتي تتمثل في:

1-عناوينIP، MCA والبريد الإلكتروني، وبرامج المحادثة

يعد عنوان الإنترنت ، من أبرز الوسائل التي يعتمد عليها في التحقيقات الإلكترونية ، فهو الذي يمثل البصمة الرقمية للجهاز المتصل بالإنترنت، ويستخدم لتعقب مصدر الرسائل المرسلة عبر الشبكة سواء لأغراض إجرامية أو غير ذلك. فمثلا البريد الإلكتروني يتيح نقل المعلومات بسرعة ويمكن تحديد موقع المرسل من خلال تحليل العنوان الشبكي المرافق، فكل رسالة تمر من خلال عدة محطات منها ما يسمى بخوادم البريد الكبرى ،وتقسم الرسالة إلى عدة أجزاء صغيرة ترسل عبر شبكة من العقد وغالبا ما تمر كل رسالة بأربع أو خمس محطات على الأقل، قبل أن تصل إلى وجهتها. وعادة ما يتم تسجيل المسار الكامل من الجهاز المرسل إلى الجهاز المستقبل ،مما يسمح بكشف مصدر الرسالة وتتبع الأجهزة المتورطة في العملية.

فعند تسجيل أي نشاط تخريبي أو إختراق إلكتروني ،فإن أول إجراء يتم إتخاذه هو تحديد عنوان الجهاز الذي صدرت منه العملية ، فهذا يساعد على تحديد موقع الجاني بشكل تقريبي. كما أن بعض الجهات كخدمات الإنترنت العالمية ، يمكنها مراقبة مثل هذه الأنشطة بشرط توفر الإمكانيات التقنية المناسبة.

كما أن هناك طرق تقنية مباشرة للحصول على عنوان(IP)منها ما يستخدم في أنظمة التشغيل مثل

Widows حيث يمكن إدخال الأمر "**winpcfg**" في نافدة التشغيل فيظهر عنوان الجهاز المتصل، لكن من الضروري الإنتباه إلى عنوان الشبكة، فقد لا يكون ثابتا إذ أنه قد يتغير في كل مرة يتصل فيها الجهاز بالإنترنت ، خاصة في حالة إستخدام مزود يقدم عناوين إنترنت ديناميكية[1].

2-البروكسي (Proxy) :

يعد البروكسي وسيطً بين المستخدمين وشبكة الإنترنت، حيث تعتمد عليه الشركات الكبرى المزودة خدمات الإتصال وهذا من أجل إدارة شبكاتها وتعزيز مستوى الأمان، وكدا توفير خدمة التخزين المؤقت وفكرة البروكسي بصفة عامة تقوم على تلقيه طلبا من المستخدم للوصول إلى صفحة معينة، فيبدأ أولا بالبحث عنها ضمن الذاكرة المؤقتة المحلية، فإذا كانت الصفحة قد تم تنزيلها سابقا يعيد إرسالها مباشرة إلى المستخدم دون الحاجة إلى الإتصال بالشبكة العالمية، مما يساهم في توفير الوقت والتقليل من إستهلاك البيانات. أما إذا لم تكن الصفحة متوفرة مسبقا، فهنا سيقوم البروكسي بإرسال طلب إلى الشبكة العالمية مستخدما أحد عناوين **IP** الخاصة به.

ومن بين أبرز مزايا البروكسي أنه يحتفظ في ذاكرته المؤقتة بسجلات العمليات التي جرت عليه، وهو ما يساعد على إستخدام هذه البيانات كوسيلة للإثبات، من خلال فحص العمليات المحفوظة التي قد تكون متعلقة بالمتهم مما يسهل عملية تعقب النشاطات الإجرامية عند مزود الخدمة.[2]

3- برامج التتبع:

تستخدم هذه البرامج للكشف عن محاولات الإختراق وتحديد مصدرها، حيث تقدم تقريرا تفصيليا للمستخدم الذي تعرض جهازه للإختراق، ويشمل هذا التقرير إسم الحدث ، وتاريخه ، وعنوان الإنترنت الذي تم من خلاله تنفيذ عملية الإختراق ، بالإضافة إلى إسم الشركة المزودة بخدمة الإنترنت التي ينتمي إليها المخترق ، وكدا أرقام المنافذ المستخدمة أثناء العملية ، وغيرها من المعلومات التقنية المهمة، وتعد هذه البرامج فعالة في تحليل الهجمات السيبرانية ومساعدة الجهات المختصة في تعقب الفاعلين.

---

[1] عز الدين عثماني ، إجراءات التحقيق والتفتيش في الجرائم المحاسبة بأنظمة الإتصال والمعلوماتية ، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية بجامعة تبسة ، العدد الرابع، ، 2018، ص 55.

[2] حسين بن سعيد الغافري، السياسة الجنائية لجرائم الإنترنت (دراسة مقارنة) ، دار النهضة العربية ، القاهرة ، 2006 ، ص 513.

4- نظام كشف الإختراق:

يعتبر هذا النظام من أهم الوسائل التقنية المستخدمة لحماية الشبكات وأنظمة الحاسوب، حيث يعمل هذا النظام على مراقبة وتحليل الأنشطة الجارية داخل النظام أو الشبكة بشكل مستمر، بحثاً عن مؤشرات قد تدل على وجود أي تهديدات أمنية ، يقوم نظام كشف الإختراق بتحليل حزم البيانات أثناء إنتقالها عبر الشبكة، ويراقب ملفات نظام التشغيل الخاصة بتسجيل الأحداث لحظة وقوعها ، ويعتمد في عمله على مقارنة هذه البيانات بسجل يعرف بـ"التواقيع" وهو عبارة عن مجموعة من الخصائص أو الأنماط المرتبطة بالإعتداءات السيبرانية المعروفة ، وفي حال قام النظام بالكشف عن وجود أي تطابق بين إحدى التواقيع المسجلة وسلوك مريب في الشبكة، سيقوم فورا بإرسال إنذار إلى مدير النظام فورا حيث يسجل هذا النظام كافة البيانات المرتبطة بمحاولة الإعتداء داخل سجلات رقمية مخصصة، ما يتيح لفريق التحقيق الإستفادة منها لاحقا لفهم كيفية إرتكاب الجريمة والأسلوب المتبع فيها، بل وقد تساهم أحيانا في تحديد مصدر الهجوم.[1]

5- نظام جرة العسل:

يعد هذا النظام بمثابة فخ إلكتروني صُمم خصيصا لإستدراج المهاجمين، حيث تم إنشاؤه ليبدو كهدف سهل لكن دون إحتواءه على أي بيانات حقيقة. فبمجرد أن تتم محاولة إختراقه سيتمكن القائمون على حماية النظام من مراقبة خطوات المهاجم وجمع معلومات دقيقة حول أسلوبه، فالهدف الأساسي هو تشتيت المهاجم وإبعاده عن الأنظمة الفعلية في الشبكة، وفي نفس الوقت يتم تحليل بيانات الهجوم بشكل معمق، ما يساعد لاحقاً في كشف الجريمة وفهم أبعادها والغاية منها وكدا تقديم بيانات تقنية مهمة لفريق التحقيق.

6- أدوات الضبط:

تعد عملية ضبط ماديات الجريمة من المهام الأساسية التي تقع على عاتق جهات التحقيق، إذ لا يكفي فقط الكشف عن وقوع الجريمة بل يجب توثيق الادلة بشكل يحافظ على سلامتها وإمكانية نسبها للجاني تمهيداً لتقديمها أمام النيابة العامة كوسيلة إثبات، ولهذا الغرض يتم الإعتماد على مجموعة من

[1] خالد علي نزال الشعار ، المرجع السابق ، ص 38-39

الأدوات التقنية المتنوعة التي تساعد على تحقيق هذا الهدف، مثل برامج الحماية وأدوات المراجعة وأنظمة مراقبة المستخدمين داخل الشبكة، كما تعتبر التقارير الصادرة عن نظم أمن البيانات مصدرا هاما لتوثيق الوقائع. والجدير بالذكر أنه في كثير من الأحيان يمكن إستخدام نفس الأدوات التي إستُعملت في إرتكاب الجريمة كوسيلة ضبط، مثل أدوات جمع وتحليل بيانات الزائرين حيث يمكن أن تحتوي على معلومات تفيد في تتبع أثر الجاني وكشف هويته.[1]

7- أدوات فحص ومراقبة الشبكات:

تستخدم هذه الأدوات في تحليل الشبكة والكشف عن الثغرات أو العمليات المشبوهة، ويمكن أن يستخدم المحقق عدة أدوات منها وهي:

- **أداةARP** : تستخدم هذه الأداة لتحديد الموقع الفعلي للحاسب الألي عبر الشبكة من خلال عناوين كروت الشبكة.
- **برنامج Visual Route**: وهو عبارة عن برنامج يكشف عن المسارات التي سلكها المهاجم أثناء محاولته إختراق بيانات الشبكة ، وبعد معرفة عنوان الإنترنت الخاص به يتم عرضها بشكل مرئي يساعد في تتبع الهجوم.
- **أداة التتبعTracer** : تتعقب المسار الكامل الذي تمر به البيانات عبر الشبكة، موفرة معلومات دقيقة حول العناوين التي زارها الجاني وتحدد المدة الزمنية التي قضاها في كل منها، إعتمادا على خاصية "**TTL**"
- **أداة تفحص حالة الإنترنت:** هي أداة تقوم بفحص وتحليل حالة الإتصال الحالي للبروتوكول ولها عدة مهام تتمثل في عرض جميع الإتصالات الحالية، ومنافذ التنصت، وعرض المنافذ والعناوين بصورة رقمية وكدا عرض كامل لجدول التوجيه.[2]

---

[1] علي عدنان الفيل ، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث ، الإسكندرية- مصر- 2012 ، ص 102

[2] نبيلة هبة هروال، الجوانب الإجرائية في جرائم الإنترنت في مرحلة جمع الإستدلالات ، ط/الأولى ، دار الفكر الجامعي ، الإسكندرية، 2007 ، ص 50

ثانيا: الوسائل الإجرائية

ويقصد بها تلك الإجراءات التي يعتمد عليها، أثناء التحقيق والتي تتم وفق أساليب تقنية دقيقة ومختلفة، تهدف إلى إثبات وقوع الجريمة وتحديد هوية مرتكبها وطبيعة الأسلوب المستخدم فيها وتتمثل هذه الوسائل فيما يلي:

1-إقتفاء الأثر:

يعد من أخطر الوسائل في ميدان الجرائم المعلوماتية وأكثر شيء يخشاه المجرم، لأنه يسمح بتتبع أثره خلال إرتكابه للجريمة أو بعد تنفيذها، كما أن هناك العديد من المواقع المتخصصة التي يستخدمها القراصنة والتي تقدم نصائح لتفادي تتبع أثارهم، مثل نصيحة "قم بمسح أثارك" لكن في حال عدم إتقان المجرم لعملية إخفاء أثره فمن المحتمل أن يتم إلقاء القبض عليه خاصة إذا تمت العملية بشكل سريع وبدون تغطية كافية، ويمكن تتبع هذا الأثر من خلال البريد الإلكتروني ،أو من خلال الجهاز الذي تم إستعماله في الإختراق.[1]

1-1 الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته

من اللازم على المحقق أن يطلع على مكونات النظام المعلوماتي، سواء كانت شبكات أو تطبيقات أو خدمات، إلى جانب معرفة كيفية إدارة قاعدة البيانات وحمايتها وخطة التعامل مع الثغرات الأمنية. كما ينبغي عليه معرفة أنواع الأجهزة المستعملة وكيفية تصنيفها ومدى تخصيصها لأدوار معينة، بالإضافة إلى أليات توزيع الصلاحيات للمستخدمين، وكلمات المرور وطرق النسخ الإحتياطي كذلك من المهم معرفة ما إذا كانت هناك برامج حماية وكيف يتم الدخول إلى البيانات وتقارير دورية توثق أسلوب الحماية المعتمد.

2-1 الإستعانة بالذكاء الإصطناعي

أصبحت أدوات الذكاء الإصطناعي تلعب دورا كبيرا في تحليل الأدلة الرقمية، حيث أنها تساهم في جمعها وتصنيفها وفهمها بشكل أسرع وأكثر دقة، وذلك من خلال تقنيات متطورة تمكن من حصر

[1] حسين بن سعيد الغافري ، المرجع السابق ، ص 519.

الحوادث وتحديد مصيرها ،هذه التكنولوجيا تساعد المحقق بشكل كبير في الوصول إلى نتائج دقيقة يمكن الإعتماد عليها في إعداد تقارير الخبرة الجنائية وتحليل البيانات وفقاً للمعايير التقنية المعتمدة.[1]

الفرع الثالث: أدوات التحقيق في الجرائم الإلكترونية

تعتبر أدوات التحقيق من الوسائل الأساسية التي ينبغي على المحقق في الجرائم الإلكترونية التسلح بها، نظراً لطبيعة هذا النوع من الجرائم وما تتطلبه من دقة تقنية وسرعة في جمع الأدلة الرقمية، وتتمثل أهم هذه الأدوات فيما يلي:

أولاً: برنامج التفتيش (Computer Search Warrant Program)

هذا البرنامج يعد بمثابة قاعدة بيانات متكاملة تسمح بإدخال كافة المعلومات الهامة المتعلقة بالأدلة الرقمية، من حيث ترقيمها وتسجيل البيانات الخاصة بها، كما يمكّن لهذا الجهاز إصدار إيصالات إستلام الأدلة، والبحث داخل قوائم الأدلة المضبوطة لتحديد موقع دليل معين، أو الشخص الذي قام بضبطه، ويُفضل أن يكون هذا البرنامج محمولاً على قرص مرن أو قرص صلب خارجي بحوزة المحقق.

ثالثا: برنامج (X Tree Pro Gold)

وهو من البرامج الفعالة في معالجة الملفات، إذ يمكنه استعراض جميع الملفات الموجودة سواء على القرص الصلب أو الشبكة، ويُستخدم لتقييم محتوى وسائط التخزين المضبوطة، والبحث عن ملفات أو كلمات معينة قد تكون ذات صلة بالجريمة.

رابعاً: برنامج(Laplink)

يمكن تشغيل هذا البرنامج من خلال قرص مرن، ويُستخدم لنقل البيانات من جهاز الحاسب الخاص بالمتهم إلى وسائط تخزين أخرى عبر المنافذ المختلفة، وتبرز أهمية هذا البرنامج في سرعة نسخ المعلومات قبل أن يحاول المتهم إتلافها أو حذفها.

[1] عز الدين عثماني ، المرجع السابق ، ص 55

خامساً: برنامج كشف الفيروسات وتدميرها

تُستخدم برامج مكافحة الفيروسات، لحماية جهاز المحقق من الإصابة بالبرمجيات الخبيثة التي قد تكون مرفقة بملفات الجريمة ، فالفيروسات قد تُفعّل بمجرد فتح الملف أو تلقي بريد إلكتروني يحتوي على شفرة ضارة، مما قد يؤدي إلى تلف الأدلة أو فقدانها.

سادساً: برامج الدمج وفك الدمج(PKZIP)

تُستعمل هذه البرامج لفك ضغط الملفات المدمجة، إذ قد يلجأ المتهم إلى ضغط برامجه أو بياناته الحساسة لإخفائها، ولا يمكن الوصول إلى محتواها إلا بعد فك هذا الضغط.

سابعاً: برنامج الاتصالات مثل (Lantastic)

يسمح هذا البرنامج بربط جهاز الحاسب الخاص بالمحقق بجهاز المتهم، ما يُمكن من نسخ البيانات وحفظها بطريقة أمنة قبل تحليلها[1].

المطلب الثالث: مفهوم المحقق الجنائي في الجرائم المعلوماتية

مهنة المحقق الجنائي من أسمى وأشرف المهن، لما تحمله من رسالة نبيلة تتمثل في إحقاق الحق وتحقيق العدالة، فالشعور بالسعادة والرضا والثقة بالنفس ، الذي يناله المحقق وهو يسعى بصدق لكشف الحقيقة، يُعد خير تعويض عن الجهد والتعب الذي يبذله في أداء مهمته، ويجعله دائم الفخر بعمله، قوي الإيمان برسالته، ويستمد المحقق الجنائي هذه الرسالة من مبادئ دينية سامية، حيث يقول الله عز وجل:

"**وَإِذْ قَالَ رَبُّكَ لِلْمَلَائِكَةِ إِنِّي جَاعِلٌ فِي الْأَرْضِ خَلِيفَةً**[2]"

ويقول سبحانه أيضاً: "**إِنَّا عَرَضْنَا الْأَمَانَةَ عَلَى السَّمَاوَاتِ وَالْأَرْضِ وَالْجِبَالِ فَأَبَيْنَ أَن يَحْمِلْنَهَا وَأَشْفَقْنَ مِنْهَا وَحَمَلَهَا الْإِنسَانُ ۖ إِنَّهُ كَانَ ظَلُومًا جَهُولًا**[3]."

فالمحقق الجنائي يُكلف بأخطر وأهم مهمة على الإطلاق، وهي تحقيق العدالة، لذلك ينبغي أن يتحلى بمجموعة من الصفات الأساسية، كالعزيمة القوية، والصبر، واليقظة، والانتباه، والحزم، إلى جانب

---

[1] بوحزمة نصيرة ، المرجع السابق ، ص ص131-133

[2] سورة البقرة، الأية 30.

[3] سورة الأحزاب ، الأية 72.

القدرة على تحليل المعطيات واستخلاص النتائج الدقيقة. كما ينبغي أن يكون مستعدًا لمواجهة التحديات، والتضحية بكل ما هو غالي في سبيل أداء مهمته إضافة إلى ذلك، يُفضل أن يكون المحقق مُلمًّا بلغات متعددة، خاصة في مجال الجريمة الإلكترونية الذي يتطلب فهمًا للبيانات والمصطلحات التقنية المتداولة عالميًا.

ولكي يؤدي المحقق مهامه بالشكل المطلوب، عليه أن يلتزم بالعناية التامة في دراسة القضايا المعروضة عليه، وأن يتحلى بالحياد والنزاهة في اتخاذ الإجراءات، مع الحرص على التطبيق السليم للقانون ، بما يعكس احترامه لخصوصية مهمته وتعزيزه لسيادة القانون[1]، وفي هذا الإطار سيتم تناول تعريف المحقق الجنائي وأنواعه في الجريمة الإلكترونية في **(الفرع الأول)** ثم صفات المحقق وصعوبات التحقيق في **(الفرع الثاني)**

الفرع الأول: تعريف المحقق الجنائي وأنواعه

يعتبر التحقيق إجراءً أساسياً في القضايا الناشئة عن وقائع إجرامية تم تحريك ومباشرة الدعوى العمومية بشأنها، ولا يقتصر دوره على الجوانب الشكلية أو الإجرائية فقط، بل يحمل في طياته جانباً إنسانياً يتجسد في التفاعل القائم بين المحقق، والمشتبه فيه، وكذا الوقائع موضوع التحقيق ، فالمحقق يضطلع بمهمة التحقيق عبر مجموعة من الإجراءات والأساليب القانونية التي توضح كيفية سير العملية من بدايتها إلى نهايتها، وذلك بهدف الوصول إلى الحقيقة وكشف ملابسات الجريمة[2]. وللتعرف على المحقق الجنائي سنقوم بتعريفه **(أولا)** ثم معرفة أنواعه **(ثانيا)** وإختصاصه القضائي **(ثالثا)**

أولا: تعريف المحقق الجنائي في الجريمة المعلوماتية

تعددت التعريفات للمحقق الجنائي عند فقهاء القانون الجنائي، فمنهم من عرفه على أنه: "الشخص أو الموظف أو المكلف بخدمة عامة مختص ومؤهل، يتبع مجموعة من الإجراءات والوسائل المشروعة بهدف الوصول إلى الحقيقة، بعد جمع الأدلة التي تثبت حقيقة وقوع الجريمة، وكيفية ارتكابها، وأسبابها، ومعرفة مرتكبيها[3]"

[1] بوحزمة نصيرة ، المرجع السابق ، ص 150

[2] نفس المرجع ، ص 151

[3] محمد ظاهر ، تنظيم التحقيق الإبتدائي في الجرائم ، دار وائل للنشر ، عمان ، ط/الأولى ، 2013 ، ص 53

كما عرّفه أيضًا بأنه: "المكلف بالتحقيق في الجرائم عبر الكمبيوتر وشبكاته".

أما تعريف المحقق الجنائي في الجرائم الإلكترونية، فقد ورد بأنه: "الشخص المكلف بالبحث عن الحقيقة في الجريمة الإلكترونية، لكشف مرتكبيها، وجمع أدلة البراءة أو الإدانة ضدهم، تمهيداً لإحالتهم إلى المحكمة، ويتحدد دورهم بتنفيذ إجراءات القانون المقررة، كلٌّ حسب اختصاصه، سواء في دائرة اختصاصه المكاني، أو على مستوى الدولة[1]".

كما عرفه البعض بأنه: "من عهد إليه القانون التحقيق في الجرائم بموجب الصلاحيات المخولة له من أحكام القوانين الشكلية[2]".

وبالتالي، فإن المحقق الجنائي هو الشخص القائم بأعمال إجراءات التحقيق الجنائي، ولا يختلف تعريفه في الجرائم التقليدية عن الجرائم الإلكترونية، حيث يكمن الفرق في نوعية الجريمة وليس في طبيعة مهمة المحقق، ولهذا فالمحقق يبقى دائما ذلك الشخص القانوني الذي حدده القانون على وجه التحديد ، وحدد واجباته ومهامهم ، أي أنه يعمل في إطار من القانون.[3]

ويتضح من التعريفات السابقة أن الاختلاف راجع إلى الاختلاف في نطاق النظر إلى عمل المحقق، أو تحديده من حيث ما يقوم به من إجراءات ووسائل، في حين اتجهت تعريفات أخرى إلى النظر إليه من حيث مهامه والأعمال المنوطة به.

ثانيا: أنواع المحققين في الجرائم المعلوماتية

إن مهمة التحقيق في الجرائم الإلكترونية تنسب إلى نوعين من المختصين ، يجمعان بين المعرفة التقنية والخبرة القانونية[4]، وذلك لضمان تحقيق فعّال ومتكامل في هذا النوع المعقد من الجرائم ويتمثلان في:

---

[1] مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الإلكترونية ، ط/الأولى ، مطابع الشرطة ، القاهرة ، 2008 ، ص 253

[2] مجيد خضر السبعاوي ، مولان قادر أحمد، الضرورة الإجرائية في مرحلة التحقيق الإبتدائي (دراسة تحليلية مقارنة) المركز القومي للإصدارات القانونية، القاهرة ، 2017 ، ص 148

[3] بوحزمة نصيرة ، مرجع سابق ، ص 152

[4] خالد علي نزال الشعار ، مرجع سابق ، ص 27

أولاً: الخبرة الفنية

وهم المختصون في مجال الأجهزة الإلكترونية وشبكات الاتصالات، كالحواسيب والهواتف الذكية والأجهزة المحمولة المختلفة، وتتم الاستعانة بهم لاكتشاف الجرائم الإلكترونية، وضبط الأدلة الرقمية، والتحقيق الفني مع المتهمين، تمهيداً لتقديمهم للمحاكمة، وتكمن أهمية هؤلاء الخبراء في قدرتهم على تحليل الأنظمة الرقمية واسترجاع البيانات المخفية أو المحذوفة.

ثانياً: الكفاءة المهنية

وهم المحققون المتخصصون في المجال الجنائي، ممن يمتلكون المهارة في استجواب المتهمين وسماع أقوال الشهود، بناءً على قواعد مهنية دقيقة. فطريقة طرح الأسئلة، وترتيبها، واستنتاج الحقائق من خلال لغة الجسد ونبرة الصوت، تعتبر مهارات لا يتقنها إلا من تلقى تكويناً قانونياً ومهنياً في مجال التحقيق.

ونظراً لطبيعة الجرائم الإلكترونية التي تجمع بين الجانب التقني والجانب الجنائي، فإنه من الضروري الجمع بين هذين النوعين من الخبرات، لضمان تحقيق ناجع ومتكامل.

كما ينبغي على المحقق في الجرائم الإلكترونية أن يعمل باستمرار على تطوير معارفه التقنية، من خلال القراءة والدورات التدريبية، وذلك لتحقيق التوازن الفكري والتقني اللازم، ولا يقلّ عن ذلك أهمية تحقيق التوازن الاجتماعي، والجسدي، وحتى الاقتصادي، من خلال توفير الموارد التي تُمكنه من استخدام الأدوات الإلكترونية الحديثة في التحقيق[1].

ثالثا: الإختصاص القضائي للمحقق:

يُعد الاختصاص القضائي للمحقق الجنائي من الركائز الأساسية التي تُمكنه من أداء مهامه بفعالية، وقد نظم المشرع الجزائري هذا الاختصاص وفقًا لطبيعة الجريمة وظروف ارتكابها، حيث يُقسم إلى اختصاصات عادية، واختصاصات في حالة التلبس، وأخرى استثنائية.

[1] بوحزمة نصيرة ، المرجع السابق ، ص 153

1 الاختصاصات العادية

تتمثل المهام العادية للمحقق الجنائي في تلقي الشكاوى والبلاغات من الأشخاص المتضررين، وجمع الاستدلالات عبر اتخاذ الإجراءات الكفيلة بالكشف عن الجريمة، تحديد هوية مرتكبيها، والظروف المحيطة بها، وتعقبهم لتقديمهم أمام العدالة. كما يملك صلاحية توقيف المشتبه فيه، واستعمال القوة العمومية في حال تخلفه عن الحضور رغم توجيه استدعائين، شرط الحصول على إذن مسبق من وكيل الجمهورية، وفقًا للمادة 65 فقرة 1 من قانون الإجراءات الجزائية، وتُختتم هذه الإجراءات بتحرير محاضر مفصلة تتضمن كل ما تم القيام به، مع ذكر تاريخ ومكان اتخاذها، وهوية المحقق، ثم تُحال إلى وكيل الجمهورية المختص.

1-2 الاختصاصات في حالة التلبس

في حالات التلبس، يمنح القانون للمحقق الجنائي صلاحيات موسعة، بشرط أن تكون واقعة التلبس سابقة على إجراءات التحقيق، وأن يتم اكتشافها بطرق مشروعة. وتشمل هذه الصلاحيات: منع الأشخاص من مغادرة مسرح الجريمة إلى حين انتهاء التحريات، الاستعانة بالخبراء للمعاينات المستعجلة، توقيف المشتبه فيه مع تدوين ساعة بدء سماعه، القيام بعمليات التفتيش، وضبط الأدلة المادية التي تُسهم في كشف الحقيقة[1].

1-3 الاختصاصات الاستثنائية

تماشيًا مع تطور الجريمة وتعقيد وسائلها، خول المشرع الجزائري للمحقق الجنائي صلاحيات استثنائية في بعض الجرائم الحساسة، كجرائم المخدرات، تبييض الأموال، المساس بأنظمة المعالجة الآلية للمعطيات، الجرائم ذات الطابع الإرهابي، والجرائم المنظمة عبر الحدود. وقد جاء هذا التوسيع بموجب التعديل الصادر بتاريخ 2006/12/20 بمقتضى القانون رقم 22/06 المعدل والمتمم لقانون الإجراءات الجزائية. وتشمل هذه الصلاحيات: مراقبة الأشخاص والأموال، اعتراض المراسلات، تسجيل الأصوات والصور، إجراء التسرب، وتوسيع آجال التوقيف للنظر بحسب نوع الجريمة، حيث قد تمتد من مرتين في الجرائم المتعلقة بأمن الدولة، إلى خمس مرات في الجرائم الإرهابية كما يحق للمحقق تفتيش الأماكن في

[1] بوعوينة أمين شعيب ، مهلب حمزة ، إختصاصات الضبطية القضائية في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية ، قسم القانون الخاص ، جامعة عبد الرحمان ميرة ، بجاية ، 2012-2013 ، ص 13- 14

أي وقت، ليلاً أو نهارًا، مع إخطار وكيل الجمهورية، وتحت رقابة النائب العام لدى المجلس القضائي المختص إقليميًا[1].

الفرع الثاني: صفات وخصائص المحقق الجنائي وصعوبات التحقيق.

إن التحقيق في الجرائم المعلوماتية ، يتطلب أشخاصا ذو كفاءة عالية ، نظرا للصعوبات والمعوقات التي تؤثر على عملية التحقيق، لهذا فالمحقق الجنائي يجب أن تتوفر فيه بعض الصفات والخصائص، وهذا حتى يتمكن من التصدي لتلك الصعوبات والمعوقات التي تواجهه ، ولهذا سنتناول في هذا الفرع صفات المحقق الجنائي وخصائصه الفنية **(أولا)** ثم صعوبات ومعيقات التحقيق **(ثانيا)**

أولا: صفات المحقق الجنائي وخصائصه الفنية

إن المحقق الجنائي يجب أن يتميز بمجموعة من الصفات والخصائص، التي تميزه عن غيره من المحققين ويمكن حصر هذه الصفات الذاتية والخصائص الفنية في ما يلي :

1 صفات المحقق الجنائي

لم يحدد المشرع بصورة صريحة الصفات الواجب توافرها في المحقق الجنائي، غير أن طبيعة الدور الحساس الذي يقوم به هذا الأخير تقتضي أن يتسم بمجموعة من الصفات الجوهرية، والتي يجب على كل محقق جنائي أن تتوفر فيه، وخاصة من ناحية الجانب الأخلاقي حتى يتمكن من أداء مهامه بكفاءة وعلى أكمل وجه ، فبقدر ما توفرت في المحقق هذه الصفات سيتمكن من تحقيق أهدافه، وبالتالي يستطيع التغلب على المجرمين والخروج من الصراع منتصراً ، ومن أبرز هذه الصفات:

1-1 النشاط

يُعد النشاط من الصفات الأساسية للمحقق، إذ يجب أن يتحلى بالهمة والحيوية الذهنية والبدنية، وأن يكون سريع الاستجابة والتنقل لمكان الحادث، مع القدرة على التصرف الفوري لحماية الأدلة وآثار الجريمة، إذ أن النشاط والحيوية يسهمان في كشف غموض الحوادث وسرعة تعقب الجناة.

[1] بوعوينة أمين شعيب ، مهلب حمزة ، مرجع سابق ، ص 17-18

1-2 قوة الملاحظة

وهي القدرة على الانتباه للتفاصيل الدقيقة التي قد تمر على الأشخاص العاديين دون انتباه، سواء في مسرح الجريمة أو أثناء استجواب المتهمين وسماع الشهود، إذ تساعد قوة الملاحظة في اكتشاف آثار مهمة قد تكون حاسمة في مسار التحقيق.

1-3 العدالة

يجب على المحقق أن يتحلى بروح العدالة والحياد، وألا يتسرع في إصدار الأحكام، وأن يُبقي على قرينة البراءة إلى أن تثبت الإدانة بأدلة قانونية، كما يجب أن يفسر الوقائع بموضوعية دون تحريف أو تأويل يخالف مصلحة العدالة،

1-4 قوة الذاكرة وسرعة البديهة

تُمكِّن قوة الذاكرة المحقق من استرجاع المعلومات وتحليلها وربطها ببعضها البعض، في حين أن سرعة البديهة تُمكنه من اتخاذ قرارات فورية بناءً على المواقف المفاجئة، مثل التعرف على مشتبه به أو الاستجابة السريعة لمعلومة جديدة.

1-5 الشجاعة والإقدام:

تتمثل في قدرة المحقق على التصدي للأخطار، سواء في مواجهة المجرمين أو في التعامل مع أصحاب النفوذ، دون تردد أو خوف، مع تحليه بالشجاعة الأدبية عند اتخاذ قرارات قد تكون حساسة أو صعبة.

1-6 الاعتماد على النفس

يتعين على المحقق إنجاز مهامه بنفسه وعدم الاتكال كلياً على الآخرين، إلا في حدود المساعدة الفنية أو الاستشارية، الاعتماد على النفس يعزز دقة النتائج ويمنع تسرب المعلومات أو تضليل مجريات التحقيق[1].

[1] أحمد عرابي ، التحقيق الجنائي، الطبعة الأولى، مدار لخدمات التصميم الفني والمطبوعات ، دبي ، 2021 ، ص 18-19

1-7 كتمان الأسرار

على المحقق الحفاظ على سرية المعلومات التي يطلع عليها أثناء التحقيق، خاصة تلك التي لا ترتبط مباشرة بالوقائع الجنائية أو قد تؤثر على سمعة أطراف القضية، فكتمان الأسرار يُعد من متطلبات نجاح التحقيق وسلامته.

1-8 الصبر والمثابرة

قد يواجه المحقق صعوبات وتعقيدات في الوصول إلى الحقيقة، لذلك عليه التحلي بالصبر وعدم اليأس، مع مواصلة العمل حتى في غياب نتائج فورية، فالمثابرة تؤدي في النهاية إلى كشف الوقائع وتحقيق العدالة.

1-9 الدقة في العمل

يجب على المحقق أن يكون دقيقاً في كل خطواته، من معاينة مسرح الجريمة إلى تحرير المحاضر واستجواب الأطراف، فالدقة تمنع إغفال أو ضياع تفاصيل مهمة قد تكون حاسمة في القضية.

1-10 إحترام حقوق المتهم

يتعين على المحقق احترام حقوق المتهم وعدم اللجوء إلى أساليب غير قانونية كالضغط أو الإكراه أو سوء المعاملة، ويجب عليه الإنصات لأقوال المتهم ودفاعه، كما يجب التعامل بإنسانية وفقاً لمبادئ العدالة وحقوق الإنسان[1].

2 الخصائص الفنية للمحقق الجنائي: وإضافة إلى الصفات الواجب توفرها في المحقق الجنائي كالاستقامة في حياته الشخصية، العمل بروح الفريق، البعد عن الصغائر والشبهات، أن يكون قدوة لمرؤوسيه، ويتصف بجمال الخلق واحترام الذات، وقوة الشخصية وحسن المظهر وسمو الشعور والإدراك، وأن يكون صبورًا هادئًا، يتحلى بالشجاعة والاعتماد على النفس وحسن المعاملة حتى يكتسب ثقة الخصوم ويرسخ اعتقاد الناس في سلامة إجراءات التحقيق؛ فإن هذه الصفات تبقى ضرورية لكل محقق جنائي ، غير أن هناك بعض المهارات الإضافية التي يجب أن تتوفر في المحقق الجنائي في مجال الجرائم الإلكترونية، كون هذه الأخيرة ناتجة عن التطور التكنولوجي الهائل الذي أفرز أنماطًا جديدة من الجرائم،

[1] أحمد عرابي ، المرجع السابق ، ص 20

تتطلب قدرات فنية وتقنية عالية لم يعهدها رجال الضبطية القضائية سابقًا، مما يجعل من الضروري أن يتحلّى المحقق الإلكتروني بقدرات خاصة تؤهله للتعامل مع هذا النوع من الجرائم،[1] ومن بين هذه المهارات ما يلي:

2-1 التعرف على المكونات المادية للحاسوب وآلية عمل الشبكات

يتعين على المحقق أن يكون على دراية بالمكونات المادية للحاسوب، وآلية تخزين البيانات، وكيفية استرجاعها والتعامل معها دون الإضرار بالأدلة الرقمية. كما يجب عليه فهم كيفية عمل الشبكات والربط بين الأجهزة، لاسيما أن أغلب الجرائم الإلكترونية ترتكب من خلال الإنترنت، ما يستوجب معرفة جيدة بمبادئ الاتصال، وآليات انتقال البيانات، وتقنيات التشفير، وغيرها.

2-2 تمييز أنظمة تشغيل الحاسوب المختلفة ومعرفة صيغ معطيات الحاسوب

من الضروري أن يكون المحقق قادرا على التمييز بين مختلف أنظمة التشغيل، ومعرفة خصائص كل منها، وكيفية التعامل معها خلال التحقيق، سواء من حيث استخراج الأدلة أو المحافظة عليها. كما يجب أن يلم بصيغ الملفات المختلفة وكيفية قراءتها وتحليلها، كونها الوعاء الأساسي للمعلومات التي تُعد أدلة رقمية في القضايا.

2-3 معرفة الأساليب المستخدمة في ارتكاب جرائم الحاسوب وتقنيات الأمن المعلوماتي

على المحقق أن يحيط علماً بالأساليب التي يستخدمها المجرمون الإلكترونيون في ارتكاب جرائمهم، مثل البرمجيات الخبيثة، الهندسة الاجتماعية، والاختراقات، كما أن الإلمام بتقنيات الأمن المعلوماتي يُعد من الأمور الجوهرية، إذ تساعده على فهم الإجراءات الوقائية التي كانت متبعة، وتحليل مدى فعاليتها، والتفاعل بفعالية مع التقارير الفنية المعدّة من طرف خبراء الحوسبة[2].

[1] بوحزمة نصيرة ، مرجع سابق ، ص 158-159

[2] محمد بوعمرة ، سيد علي بنينال ، مرجع سابق، ص 23

2- 4 القدرة على المتابعة المستمرة والتكوين المتخصص

بما أن الجرائم الإلكترونية تتطور بوتيرة سريعة، فإن المحقق في هذا المجال مطالب بالمتابعة المستمرة لكل ما هو جديد في عالم التقنية والمعلومات، عبر الدورات التكوينية المتخصصة، ومطالعة النشرات الأمنية الصادرة عن الجهات الرسمية والدولية المهتمة بأمن المعلومات.

إن هذه الصفات والمهارات الإضافية لا تقل أهمية عن الصفات الأخلاقية والشخصية، بل إنها باتت ضرورية في عصر أصبحت فيه الجريمة تأخذ أشكالاً رقمية معقدة تتطلب مزيجًا من الفطنة القانونية والكفاءة التقنية.[1]

ثانيا: صعوبات ومعوقات التحقيق في الجريمة المعلوماتية

تواجه سلطات البحث والتحقيق في مجال الجريمة المعلوماتية جملة من التحديات التي تؤثر بشكل مباشر على مدى فعاليتها ، فالعبء الواقع على عاتق هذه الجهات كبير، نظرًا لصعوبة التعرف على هوية مرتكب الجريمة المعلوماتية، وتعقيد الوسائل المستخدمة في تتبعه وجمع الأدلة ضده، وقد سعت أغلب الدول إلى اعتماد تقنيات الحاسوب الحديثة كوسيلة أساسية لتعقب المجرمين الإلكترونيين، وأصبحت هذه التقنيات تشكل أداة محورية في منظومة الأمن المعلوماتي. ورغم هذا التطور التكنولوجي، إلا أن التحقيق في هذا النوع من الجرائم لا يزال يواجه العديد من العراقيل، التي قد تحد من فعاليته وتؤثر سلبًا على نتائجه. فهذه المعوقات قد تنعكس على المحقق نفسه، من خلال شعوره بالعجز وفقدان الثقة في قدراته، كما قد تؤدي إلى اهتزاز ثقة المجتمع في مؤسسات تنفيذ القانون، خاصة عندما تظهر عاجزة عن تقديم الحماية في هذا النوع من الجرائم. ومن جهة أخرى فإن المجرم المعلوماتي قد يستمد من هذا الوضع ثقة إضافية، تدفعه إلى الاستمرار في نشاطه الإجرامي وربما ارتكاب جرائم أكثر تعقيدًا وخطورة[2]. ويمكننا حصر أهم هذه الصعوبات والعراقيل في ما يلي:

[1] بوحزمة نصيرة ، مرجع سابق ، ص 163

[2] ربيعي حسين، أليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2015 – 2016 ، ص 279

1 معوقات مصدرها مدى ملائمة إجراءات التحقيق الابتدائي لمبدأ الشرعية في ظل غياب نص تشريعي

يُعدّ غياب النصوص القانونية الصريحة التي تُجرِّم أفعال الجريمة المعلوماتية أحد أبرز التحديات التي تواجه التحقيق الابتدائي في هذا المجال، إذ أن تطور هذه الجرائم وسرعة انتشارها يقابلها فراغ تشريعي يجعل من عملية مكافحتها والحد منها أكثر صعوبة ، وقد يؤدي هذا الفراغ إلى تفاقم الظاهرة، خاصة في ظل التحول نحو الرقمنة واعتماد المعاملات الإلكترونية في مختلف القطاعات.

وقد تطرق المشرع الجزائري لهذا الإشكال من خلال ما نصّت عليه الفقرة الثانية من المادة 5 من القانون 04/09 حيث جاء فيها: "إذا تبين مسبقا أن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يتم بمساعدة السلطات االمختصة في الدولة المعنية وفقاً لمبدأ المعاملة بالمثل". ما يعكس محدودية صلاحيات سلطات التحقيق في ظل غياب نصوص واضحة تُجيز هذا النوع من التعاون التقني، ويؤكد على حاجة المشرع إلى تحديث الإطار القانوني بما يتماشى مع طبيعة هذه الجرائم العابرة للحدود.

كما أن المحقق الجنائي يجد نفسه في مواجهة جرائم غير تقليدية دون وجود سند قانوني يوضح طبيعتها أو يحدد سُبل متابعتها، الأمر الذي يُثير التساؤل حول مدى مطابقة الإجراءات المتخذة لمبدأ الشرعية، والذي يقضي بعدم تجريم فعل أو توقيع جزاء إلا بموجب نص قانوني صريح. وبالتالي، فإن مباشرة التحقيق في مثل هذه الحالات قد تؤول إلى البطلان لعدم استنادها إلى نص قانوني يحكمها وفي ظل هذا الوضع، يمكن رصد أهم المعوقات التي تؤثر سلباً على فعالية التحقيق الابتدائي في الجرائم المعلوماتية[1] كما يلي:

1-1 عدم مواكبة النصوص الجزائية الكلاسيكية للجريمة الإلكترونية

تتميّز الجريمة المعلوماتية بخصوصية بالغة من حيث الوسائل المستعملة وطبيعة محل الاعتداء، إذ أنها ترتكَب عبر وسائل تكنولوجية متطورة وتستهدف معطيات غير مادية، ما يجعلها تختلف عن الجرائم التقليدية، فالنصوص القانونية التقليدية وضعت منذ زمن بعيد لمواجهة جرائم مادية بطابع ملموس، وفق مفاهيم تقليدية كـ "المال المنقول" أو "الملكية المادية" وعلى سبيل المثال، فإنّ اختراق نظام حاسوبي

[1] حيمي سيدي محمد، معوقات التحقيق الجنائي في الجرائم الإلكترونية، جامعة أبو بكر بلقايد تلمسان، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، العدد الأول، 2020، ص 1743

وسرقة بيانات لا يُعتبر سرقة بالمعنى التقليدي، لأن المعلومات لا تُعدّ مالاً منقولاً، كما أن أخذ نسخة من ملف دون سحب الأصل لا يحقق ركن "نقل الحيازة"، وبالتالي لا ينطبق عليه مفهوم "السرقة" في القانون الجنائي الكلاسيكي، هذا الفراغ جعل العديد من الأفعال المستحدثة غير مجرّمة قانوناً رغم خطورتها على الأمن العام[1].

2-1 عدم مواكبة جهات التحقيق للتطور السريع للجرم المعلوماتي

يُضاف إلى الإشكال التشريعي قصور عملي يتمثل في ضعف تأهيل الجهات المكلفة بالتحقيق، فالتطور المتسارع للتكنولوجيا يفرض على القائمين بالتحقيق أن يكونوا على درجة عالية من الخبرة التقنية والدراية بالمجال الرقمي، غير أن الواقع يكشف عن وجود فجوة معرفية لدى بعض المحققين، ما ينعكس سلباً على فعالية التحقيقات.

كما أن صعوبة معاينة مسرح الجريمة الإلكترونية والذي غالباً ما يكون افتراضياً، تُضعف من فرص الكشف عن الجناة وتحديد الأدلة، ويُعزَّز هذا الضعف بإمكانية تلاعب الجاني بالبيانات عن بُعد أو محوها كلياً بعد ارتكاب الجريمة، فضلاً عن أن طول الفترة الزمنية بين ارتكاب الفعل الإجرامي واكتشافه قد يتيح للعديد من الأشخاص الوصول إلى الأدلة الرقمية والتأثير فيها[2].

2 الصعوبات المتعلقة بالشق الميداني للتحري وجمع الاستدلالات في الجرائم المعلوماتية

تفرض الطبيعة التقنية المعقّدة للجريمة المعلوماتية جملة من التحديات الميدانية على أجهزة الضبط القضائي، لاسيما عند مرحلة التحري وجمع الاستدلالات، حيث يواجه المحققون صعوبات في التكيّف مع خصوصية هذا النوع من الجرائم، وتتمثل هذه المعيقات في:

2-1 المعوقات المتعلقة بإجراءات الحصول على الدليل

يختلف الدليل في الجريمة المعلوماتية عن نظيره في الجرائم التقليدية، إذ غالبًا ما يكون في شكل بيانات رقمية غير مرئية، ممثلة في نبضات مغناطيسية أو إشارات كهربائية يصعب إدراكها بالحواس، وهو ما يجعل آليات التحري الكلاسيكية مثل المعاينة أو سماع الشهود غير فعالة.

---

[1] حيمي سيدي محمد، المرجع السابق ، ص 1744

[2] نفس المرجع ، ص 1745

كما أن الطابع غير المادي لهذا الدليل يجعله عرضة للمحو أو التلاعب بسهولة، حيث يمكن للجاني، وبضغطة زر، إتلاف الدليل أو تعديله أو إخفائه، مما يُصعّب من مهمة الضبطية القضائية في الحفاظ عليه أو توثيقه.

2-2 معوقات ناتجة عن كثرة المعلومات المطلوب التحري عنها

تشكل الكمية الهائلة من البيانات الإلكترونية أحد العوائق الكبرى أمام رجال التحري، إذ يُطلب منهم فحص آلاف الملفات والبرمجيات على أجهزة الحاسوب من أجل الوصول إلى دليل واحد. وهذا الكم الكبير يتطلب جهدًا ووقتًا مضاعفين، كما يجعل مهمة فرز البيانات المشبوهة عن غيرها مهمة شاقة ومعقدة، وقد يتعذر في كثير من الأحيان الوصول إلى الدليل وسط هذا التدفق الهائل من المعلومات، ما يؤدي إلى ضياع فرص ثمينة لإثبات الجريمة، أو على الأقل يطيل من أمد التحقيق ويُثقله بتعقيدات تقنية ومعلوماتية.

2-3 معوقات متعلقة بالامتناع عن التبليغ بوقوع الجريمة المعلوماتية

من العقبات البارزة في ميدان التحقيق في الجرائم الإلكترونية، إحجام العديد من الضحايا " خاصة من المؤسسات " عن التبليغ عند اكتشافهم لتعرضهم للاعتداءات المعلوماتية. ويرجع هذا السلوك غالبًا إلى مخاوف مرتبطة بسمعة المؤسسة، أو خشية زعزعة ثقة الزبائن والجمهور، مما يدفعهم إلى الاكتفاء بإجراءات داخلية دون إشعار السلطات المختصة، وهكذا تبقى العديد من الجرائم المعلوماتية مجهولة وغير مسجلة، مما يضعف من قدرة أجهزة إنفاذ القانون على رصد الظاهرة وتحليل أنماطها، ويحول دون تطوير أساليب فعالة لمكافحتها.

2-4 صعوبة تحديد هوية المجرم الإلكتروني:

غالبًا ما يلجأ مرتكبو الجرائم الإلكترونية إلى وسائل تقنية متقدمة تُخفي هويتهم، مثل استخدام شبكات VPN ، أو اختراق أجهزة حواسيب الغير، أو الولوج من مقاهي الإنترنت التي لا تحتفظ بسجلات دخول المرتادين، مما يصعب من مهمة التتبع والتعقب. هذا التخفي الرقمي يُعدّ حاجزًا حقيقيًا أمام أجهزة

التحري، إذ أن تحديد عنوان الجاني أو تحديد موقعه الجغرافي بدقة غالبًا ما يحتاج إلى تعاون دولي وتخصص تقني دقيق، وهو ما قد لا يتوفر دائمًا لدى أجهزة تنفيد القانون التقليدية.[1]

المبحث الثاني: أساليب التحقيق الجنائي في الجرائم المعلوماتية

إنّ الطبيعة الخاصة التي تتميّز بها الجريمة الإلكترونية مقارنةً بالجرائم التقليدية أفرزت صعوبات جمّة أمام أجهزة التحري والتحقيق، وهو ما فرض على المشرّع ضرورة استحداث أساليب وإجراءات خاصة تتماشى مع خصوصية هذه الجرائم، إلى جانب الأساليب التقليدية المعمول بها، وقد استلهم المشرّع الجزائري هذه الأساليب من جملة الاتفاقيات والمواثيق الدولية، لا سيما "**اتفاقية باليرمو**" لمكافحة الجريمة المنظمة عبر الوطنية، والتي دعت الدول إلى اتخاذ التدابير اللازمة لاعتماد أساليب خاصة، على غرار المراقبة الإلكترونية والعمليات المستترة، قصد كشف هذا النوع من الجرائم.

ولا شك أن عملية جمع الأدلة الإلكترونية تقتضي وجود منظومة قانونية وقضائية فعّالة، تضمن مشروعية إجراءات الحصول على الدليل واعتماده أمام الجهات القضائية. كما يتوقف نجاح التحقيق في الجرائم الإلكترونية أيضاً على كفاءة المحقق، من خلال ما يتحلى به من ذكاء وفطنة وقوة ملاحظة وسرعة بديهة، نظراً لطبيعة هذه الجرائم التي تتطلب دقة كبيرة في التحري[2].

وبناءً عليه، سنُقسّم هذا المبحث إلى مطلبين، نتناول في أولهما الأساليب التقليدية لإجراءات التحقيق في الجريمة المعلوماتية في **(المطلب الأول)** ثم نتطرق إلى الأساليب المستحدثة في **(المطلب الثاني)**

المطلب الأول: الأساليب التقليدية للتحقيق في الجرائم المعلوماتية

في بداية ظهور الجرائم المعلوماتية، اضطرت الدول إلى الاعتماد على النصوص الجزائية التقليدية، بشقيها الموضوعي والإجرائي، لغياب نصوص متخصصة تتلاءم مع هذا النوع المستحدث من الإجرام ، غير أن التطور السريع في مجال المعلوماتية، وما رافقه من تغيرات في أساليب ارتكاب الجريمة وطبيعة مرتكبيها، كشف عن قصور هذه النصوص وعدم فعاليتها

[1] حيمي سيدي محمد ، المرجع السابق ، ص ص 1746- 1748

[2] بوسنة شيماء نور الهدى، بن سلامة كوثر، البحث والتحري في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق، قسم القانون الخاص، جامعة الإخوة منتوري ، قسنطينة1 ، 2022-2023 ، ص 84

وقد سعى المشرع إلى توسيع نطاق بعض الإجراءات التقليدية لتشمل الجرائم الإلكترونية، خصوصًا تلك التي تطرح صعوبات عملية مثل: التفتيش، الضبط، المعاينة والخبرة، بالنظر إلى خصوصية الدليل الإلكتروني، أما الإجراءات العادية مثل سماع الأطراف، الاستجواب والمواجهة، فتبقى قابلة للتطبيق دون إشكال[1].

وعليه سنركز في هذا المطلب على دراسة الفئة الأولى من هذه الإجراءات التقليدية التي تتطلب تكييفًا خاصًا مع طبيعة الجريمة المعلوماتية وهذا من خلال التطرق إلى المعاينة في **(الفرع الأول)** والتفتيش في **(الفرع الثاني)** ثم الضبط في**(الفرع الثالث)** والخبرة في **(الفرع الرابع)** وأخيرا الإستجواب في **(الفرع الخامس)**

الفرع الأول: المعاينة في الجريمة المعلوماتية

تعتبر المعاينة من أهم إجراءات التحقيق، حيث ينتقل بموجبها المحقق أو القاضي إلى مكان وقوع الجريمة لمعاينته ميدانياً، بهدف مشاهدة الآثار المادية المرتبطة بها وجمع كل ما من شأنه المساهمة في كشف الحقيقة، ويُنظر إلى مسرح الجريمة باعتباره "شاهداً صامتاً" يمكن أن يُفصح عن معطيات دقيقة إذا تم التعامل معه بمهنية وذكاء، وتستند أهمية المعاينة إلى ما يُعرف بـ"نظرية تبادل الآثار" للعالم الفرنسي "**إدموند لوكارد**" سنة 1918، والتي تفيد بأنه: "عند احتكاك جسمين، ينتقل دائماً شيء من كل منهما إلى الآخر، ويترك كل منهما أثراً على الآخر". وهي نظرية ما تزال تُعدّ من ركائز التحقيق الجنائي، بما في ذلك الجرائم المعلوماتية، إذ يمكن تعقب آثار رقمية تُثبت وقوع الجريمة أو تحدد هوية مرتكبها[2].

[1] بن نعوم خالد أمين، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق ، كلية الحقوق والعلوم السياسية، قسم قانون خاص، 2018-2019 ، ص49

[2] شنتير خضرة، الأليات القانونية لمكافحة الجريمة المعلوماتية ، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية ، أدرار ، 2020-2021 ، ص 64

أولا: تعريف المعاينة وأهميتها

لم تتناول أغلب التشريعات تعريف المعاينة بشكل صريح، مما دفع بالفقه القانوني إلى محاولة ضبط هذا المفهوم وتحديد معالمه، وقد عرفها بعض الفقهاء بأنها: "رؤية بالعين لمكان أو شخص أو شيء بغرض إثبات حالته ومعرفة كل ما من شأنه أن يسهم في كشف الحقيقة"[1]

بينما ذهب جانب آخر من الفقه إلى تعريفها بتعبير أكثر دقة، معتبراً إياها: "مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خشية تلفها أو ضياعها أو التلاعب بها."

ومهما اختلفت التعاريف، فإن المعاينة تقتضي بالضرورة انتقال المحقق إلى المكان المعني بها، للوقوف شخصياً على حالته وتوثيق كل ما من شأنه أن يفيد في كشف ملابسات الجريمة، سواء تعلق الأمر بالأشخاص أو الأشياء أو المكان محل الجريمة[2].

وتكمن أهميتها في أنها تحتل مكانة محورية ضمن إجراءات البحث والتحري في الجرائم التقليدية، نظراً لدورها الحيوي في تصوّر ظروف وملابسات ارتكاب الجريمة، وتوفير الأدلة المادية التي يتم جمعها عن طريقها، فضلاً عن دورها في تمحيص وتقييم الأدلة الأخرى والتنسيق بينها وفقاً للمعلومات المتوفرة، ويُعد هذا كله أساساً للتخطيط السليم لسير التحقيقات وتوجيهها نحو الكشف عن الحقيقة

أما في مجال الجرائم الإلكترونية، فإن للمعاينة نفس القدر من الأهمية، رغم اختلاف طبيعتها، فبينما يرتبط مسرح الجريمة التقليدية بمكان مادي محدد يحتوي على آثار مادية محسوسة، فإن الجرائم الإلكترونية غالباً ما تفتقر إلى مثل هذا المسرح الملموس. وأقرب ما يمكن اعتباره مسرحاً لها، هو الموقع أو المكتب الذي تتواجد فيه الأنظمة الإلكترونية والمعدات المستعملة في ارتكاب الجريمة أو التي كانت محلاً لها ، غير أن هذا "المسرح الإلكتروني" غالباً ما يكون محدود الفعالية في كشف ملابسات الجريمة، وذلك لسببين رئيسيين: أولاً، ندرة وجود آثار مادية تقليدية ناتجة عن ارتكاب الجريمة الإلكترونية؛ وثانياً، احتمالية مرور فترة زمنية طويلة بين ارتكاب الفعل الجرمي واكتشافه، مما يزيد من فرص التغيير أو التلف أو العبث بالأدلة الرقمية، وقد يؤدي حتى إلى زوالها، وهو ما يُضعف القيمة الإثباتية للمعاينة، رغم

[1] كحيو صونيا، بن الشيخ الفقون محمد سليم برهان الدين، إجراءات المتابعة الجزائية للجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر، كلية الحقوق، قسم القانون الخاص، جامعة الإخوة منتوري ، قسنطينة1 ، 2018-2019 ، ص15

[2] بركاني أحمد ياسين، عبادلي فاطمة الزهراء، وسائل وأدلة الإثبات في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة1 ، 2016-2017 ، ص 89

ذلك، تبقى المعاينة إجراءً ضرورياً، إذ تبادر الجهات المختصة، بمجرد تلقي بلاغ عن جريمة إلكترونية والتأكد من صحة البيانات الأساسية، إلى الانتقال لمسرح الجريمة، لكن هذا الانتقال لا يتم في العالم المادي، بل في الفضاء الافتراضي، وهو ما يُعرف بالقضاء الإلكتروني[1].

ثانيا: احكام المعاينة

تعتبر المعاينة من أولى وأهم خطوات التحقيق التي يلجأ إليها المحقق في الجرائم التقليدية والمعلوماتية على حد سواء، لما لها من دور فعال في تثبيت الأدلة المادية وتوثيق الحالة الأولية لمسرح الجريمة. وتنقسم أحكام المعاينة إلى جملة من النقاط الأساسية، من بينها كيفية معاينة مسرح الجريمة والإجراءات القانونية التي يتبعها المحقق أثناء ذلك، بالإضافة إلى دراسة مدى قابلية الجريمة المعلوماتية لمثل هذا النوع من المعاينات، بالنظر لطبيعتها غير المادية، وتكشف هذه العناصر مجتمعة عن مدى قدرة المعاينة على المساهمة في إثبات الجرائم المعلوماتية، رغم ما تطرحه من إشكاليات تقنية وقانونية وفي هذا الإطار سنتعرض إلى النقاط التالية:

1 معاينة مسرح الجريمة الإلكترونية:

يقع مسرح الجريمة الإلكترونية داخل بيئة الحاسوب، بما تحتويه من بيانات رقمية، سواء تلك التي تُخزن في ذاكرته أو في الأقراص الصلبة داخله، أو التي تنتقل عبر شبكاته. وتتمثل معاينة هذا المسرح في تتبع الآثار والبصمات الإلكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت، والتي قد تشمل الرسائل الإلكترونية المرسلة أو المستلمة، وسجلات الاتصالات عبر الحاسوب أو الشبكة العالمية، كما

تُجرى المعاينة ، داخل الأجهزة الإلكترونية نفسها، وقد تمتد إلى شبكة الإنترنت، من خلال تحليل بيانات المتهم، كمعاينة بريده الإلكتروني أو حساباته على مواقع التواصل الاجتماعي، ويمكن عبر هذه المعاينة تحديد المواقع الإلكترونية التي قام بزيارتها، والملفات التي حمّلها، وكذا الحسابات التي اخترقها أو حاول الوصول إليها وتجدر الإشارة إلى أن المعاينة في الجرائم الإلكترونية لا تقتضي دائماً الانتقال الفعلي إلى مكان مادي، بل تتم غالباً عبر العالم الافتراضي، وهناك عدة طرق تتيح لسلطة التحقيق أو لمأمور الضبط القضائي الولوج إلى هذا الفضاء، نذكر منها:

[1] بوحزمة نصيرة، مرجع سابق ، ص 351-352

- ✓ مباشرة المعاينة من مكتب القاضي أو المحقق باستعمال الحاسوب الخاص به.
- ✓ اللجوء إلى مقهى الإنترنت إذا ثبت استعماله في ارتكاب الجريمة.
- ✓ الانتقال إلى مقر مزود خدمة الإنترنت، الذي يُعد من أنسب الأماكن للقيام بالمعاينة نظراً لما يوفره من بيانات تقنية دقيقة.
- ✓ الانتقال إلى مكتب الخبير التقني المختص، إذا سمح القانون بذلك، وهو ما نجده في بعض النماذج المقارنة ، من خلال إدارة مكافحة الجرائم الإلكترونية التابعة لوزارة الداخلية[1].

2 الإجراءات المتبعة في المعاينة:

لضمان فعالية المعاينة في الجرائم المعلوماتية، ينبغي على الجهات المختصة مراعاة مجموعة من الإجراءات الفنية والآلية الدقيقة التي تسهم في المحافظة على سلامة الأدلة الرقمية وتوثيقها بطريقة موثوقة ومن بين أهم هذه الإجراءات مايلي:

- ✓ القيام بتصوير الحاسوب والأجهزة الطرفية المتصلة به، وكذا تصوير الوضعية العامة لمكان وجوده، مع التركيز على توثيق الجوانب الخلفية للجهاز. ويجب تسجيل تاريخ، وقت، ومكان التقاط كل صورة بدقة.
- ✓ إيلاء أهمية خاصة لملاحظة كيفية إعداد النظام المعلوماتي، مع توثيق حالة التوصيلات والكابلات المرتبطة بمكوناته، بما يتيح إمكانية المقارنة والتحليل لاحقاً.
- ✓ تجنب التسرع في نقل أو التعامل مع المواد المعلوماتية قبل التأكد من خلو البيئة المحيطة من أي مؤثرات مغناطيسية قد تؤدي إلى إتلاف البيانات.
- ✓ ربط الأقراص الحاملة للأدلة بجهاز يمنع إجراء أي عملية كتابة عليها، مما يسمح بقراءتها دون تغيير محتواها الأصلي.
- ✓ التحفظ على مستندات الإدخال والمخرجات الورقية المرتبطة بالجريمة، لما قد تحتويه من بيانات ذات قيمة إثباتية.

[1] شنتير خضرة ، مرجع سابق ، ص 65-66

- ✓ ضبط الدعائم الأصلية للبيانات، وتجنب الاكتفاء بالنسخ، مع مراعاة ظروف التخزين المناسبة، كعدم وضعها بالقرب من محطات إرسال لاسلكية أو في أماكن مليئة بالغبار، تفادياً لتلفها.
- ✓ جمع محتويات سلة المهملات الرقمية، وفحص جميع الوسائط المادية مثل الأوراق، الأشرطة، الأقراص المضغوطة وغيرها.
- ✓ منع إدخال أي بيانات جديدة إلى الجهاز أو ذاكرته أثناء المعاينة، مع ضبط البرامج المستخدمة في تحميل النظام، حفاظاً على الحالة الأصلية للأدلة الرقمية[1].

3 مدى صلاحية مسرح الجريمة المعلوماتية للمعاينة:

لا تحظى المعاينة في مجال الجرائم المعلوماتية بنفس الدرجة من الأهمية والإفادة التي تتمتع بها في الجرائم التقليدية، ويُعزى ذلك إلى طبيعة هذه الجرائم، التي غالباً ما تُرتكب دون أن تخلف آثاراً مادية محسوسة، كما أن البيئة الإلكترونية التي تُرتكب فيها تُعد بيئة هشّة، إذ يسهل إتلاف أو العبث بالأدلة الرقمية من قبل المترددين على مسرح الجريمة، ما يجعل الحفاظ على آثارها تحدياً كبيرا ولتقدير مدى صلاحية مسرح الجريمة المعلوماتية للمعاينة، يُستحسن التمييز بين حالتين رئيسيتين:

3-1 الجرائم الواقعة على المكونات المادية للحاسوب:

في هذه الحالة، يتعلق الأمر باعتداءات تمس العناصر المادية للحاسوب وملحقاته، كالوحدات المركزية، الأقراص الصلبة، أو الأجهزة الطرفية. وهنا لا تبرز صعوبة كبيرة في تقرير صلاحية مسرح الجريمة للمعاينة، إذ يمكن للمحقق الانتقال ميدانياً إلى الموقع، ومباشرة المعاينة التقليدية، مع تثبيت الأختام على الأماكن المعنية، وضبط الأدوات المستعملة في ارتكاب الجريمة، والتحفظ عليها، مع إعلام النيابة المختصة بذلك. وتعد هذه المعاينة فعالة في إثبات وقوع الجريمة ونسبتها إلى شخص معين، بالنظر إلى الطابع المادي للمكونات المعنية.

[1] كريمي شيماء، محسن شروق، دور القضاء الجنائي في الحد من الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق، القسم الخاص، جامعة الإخوة منتوري، قسنطينة 1 ، 2022-2023 ، ص 86-87

3-2الجرائم الواقعة على المكونات غير المادية للحاسوب أو بواسطتها:

تتعلق هذه الفئة من الجرائم بالبرمجيات والبيانات الإلكترونية، سواء باعتبارها محلاً للجريمة أو وسيلة لارتكابها، وهنا تظهر عدة صعوبات تحدّ من فعالية المعاينة ويمكن حصرها في نقطتين أساسيتين:

- ✓ ندرة أو انعدام الآثار المادية التي قد تخلفها مثل هذه الجرائم، نظراً لكون الأفعال الجرمية تتم داخل بيئة رقمية غير مرئية.
- ✓ احتمالية تردد عدد كبير من الأشخاص على مسرح الجريمة، مما يُسهّل حدوث تغييرات في المعطيات الإلكترونية، أو العبث بها، أو حتى محوها، وهو ما يُضعف من قيمة الدليل المستمد من المعاينة ويثير الشكوك حول مصداقيته.

لهذا يظل من الضروري أن يتخذ المحقق كافة التدابير التقنية الكفيلة بتأمين مسرح الجريمة المعلوماتية، فور اكتشافها، تفادياً لفقدان الأدلة الرقمية أو التلاعب بها، ويتطلب ذلك تقييد الوصول إلى الأجهزة والمعلومات، والاستعانة بالخبرة الفنية عند الحاجة، وذلك حفاظاً على سلامة إجراءات الإثبات وسير التحقيقات وفقاً لمبدأ الشرعية والضمانات القانونية المكفولة[1].

الفرع الثاني: التفتيش في الجريمة المعلوماتية

يعتبر التفتيش من أهم إجراءات التحقيق الابتدائي، ويُقصد به البحث عن الأدلة المادية المتعلقة بجناية أو جنحة يُشتبه في وقوعها، بغرض التحقق من ارتكابها أو نفي ذلك، كما يأخذ التفتيش طابعاً قانونياً دقيقاً حينما يُباشره مأمور الضبط القضائي، سواء تعلق بشخص أو مكان أو شيء، حسب ما تقتضيه طبيعة الجريمة، وذلك بهدف ضبط ما يُمكن أن يُستعمل كدليل إثبات. وتكمن أهمية هذا الإجراء في كونه يُلامس أحد أبرز الحقوق المكفولة دستورياً، وهو حق الفرد في احترام حياته الخاصة، وفي إطار الجرائم الإلكترونية، يتخذ التفتيش طابعاً خاصاً، إذ ينصبّ أساساً على الحاسوب وأنظمة المعالجة الآلية للمعطيات، باعتبارها الوسيلة التي تُرتكب من خلالها هذه الجرائم، كما أنها تُشكل في الوقت نفسه محلّاً للأدلة الرقمية، ويمكن التمييز هنا بين مكونات الحاسب الآلي المادية، مثل وحدة الإدخال والمعالجة، والمكونات المعنوية التي تتجسد في البيانات والمعلومات والبرمجيات والتطبيقات، والتي تُعتبر ذات خصوصية عالية في عملية التفتيش. فالغاية من هذا الإجراء في مثل هذه الجرائم ليست فقط ضبط الأدلة

[1] بركاني أحمد ياسين، عبادلي فاطمة الزهراء، مرجع سابق، ص 89-90

المادية، بل أيضاً الوصول إلى المعطيات الرقمية التي تُسهم في كشف الحقيقة وتمكين العدالة من الوصول إلى الجاني[1].

أولا: تعريف التفتيش

يعرف التفتيش على أنه البحث في مستودع السر عن أشياء تفيد في الكشف عن الجريمة وقعت ونسبتها إلى مرتكبيها، وهو "إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقًا لإجراءات قانونية محددة"، وعرفه البعض الآخر بأنه: "البحث عن الأشياء المتعلقة بالجريمة لضبطها وضبط كل ما يفيد في كشف حقيقتها ويجب أن يكون التفتيش سند من القانون"

من خلال هذه التعريفات، يتضح أن التفتيش يُعتبر إجراء مناسبًا للجرائم التي تترك آثارًا مادية، حيث لا يطرح صعوبات كبيرة أثناء تنفيذه، بما أنه يُستخدم من أجل الوصول إلى أدلة ملموسة تساعد في كشف الجريمة وتحديد هوية مرتكبها[2].

ثانيا: نطاق التفتيش

يشمل النظام المعلوماتي مكونات مادية، كأجهزة الحاسوب والملحقات المرتبطة بها، ومكونات غير مادية أو معنوية، كالمعطيات والبرمجيات، إضافة إلى الشبكات المعلوماتية بمختلف مستوياتها: المحلية، الإقليمية والدولية. وتُعدّ هذه العناصر محلاً للتفتيش في إطار التحقيق في جرائم الإنترنت، وذلك بغرض الوصول إلى الدليل الجنائي الإلكتروني، المتمثل في البيانات والمعلومات المخزنة أو المتداولة عبر هذه الوسائل التقنية، ويتم ذلك من خلال استخدام برمجيات وتطبيقات متخصصة وتقنيات رقمية متطورة، بهدف توثيق وقوع الجريمة وتحديد هوية مرتكبيها[3].

[1] أيت حمودة كاهنة، البحث والتحري الجنائي في مسرح الجريمة الإلكترونية، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية جامعة عمار ثلجي الأغواط ، المجلد السابع ، العدد الأول ، 2023 ، ص 187

[2] بوديسة بجاد عبد الرؤوف، مرجع سابق ، ص 49- 50

[3] نفس المرجع ، ص 50

1 تفتيش المكونات المادية للحاسوب

يُعد تفتيش المكونات المادية للحاسوب إجراءً مشروعًا يخضع للقواعد العامة المتعلقة بتفتيش الأشياء المادية، ويُطبق عليه ذات الأحكام المعمول بها في إجراءات التفتيش التقليدي، وذلك بحسب طبيعة المكان الذي توجد فيه هذه المكونات، سواء كان مكانًا خاصًا أو عامًا. فإذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإن تفتيشها لا يجوز إلا وفقًا للشروط والإجراءات القانونية المنصوص عليها، كما هو الحال في القانون الجزائري، الذي يشترط في مواده من 44 إلى 47 من قانون الإجراءات الجزائية، الحصول المسبق على إذن كتابي من وكيل الجمهورية أو قاضي التحقيق في حالة التلبس، مع وجوب تقديم هذا الإذن قبل مباشرة التفتيش، وتنفيذه في الفترة الممتدة بين الخامسة صباحًا والثامنة مساءً، وبحضور صاحب المسكن أو ممثله، أو شاهدين من غير الموظفين في حال تعذر حضوره، كما ينبغي التفرقة بين ما إذا كانت المكونات المادية للحاسوب منعزلة، أو متصلة بأجهزة أخرى في أماكن مغايرة كمساكن الغير، ففي الحالة الثانية، يجب احترام الشروط الخاصة بتفتيش تلك الأماكن، بما في ذلك الضمانات الإجرائية المرتبطة بها.

أما إذا وُجدت هذه المكونات في أماكن عامة، سواء بطبيعتها كالمتنزهات والطرقات، أو بالتخصيص كمقاهي الإنترنت ومحلات صيانة الحواسيب، فإن تفتيشها يتم وفقًا للإجراءات الخاصة بتلك الأماكن. وينطبق الأمر ذاته على المكونات الموجودة بحوزة أشخاص، بصرف النظر عن صفاتهم، كالمبرمجين أو عمال الصيانة أو الموظفين في شركات البرمجيات، حيث يخضع تفتيشهم للأحكام الخاصة بتفتيش الأشخاص، مع مراعاة الشروط القانونية المقررة لذلك[1].

1-1 تفتيش مكونات النظام المعلوماتي المعنوية:

قد يتضمن التفتيش مكونات النظام المعلوماتي المعنوية، التي تتمثل في المعطيات المعالجة آليًا. ومن الأمثلة العملية الشائعة في هذا المجال هو فحص البرمجيات، التي تُعد من الوسائل الأساسية للكشف عن جرائم الاعتداء على نظم المعالجة الآلية. فوجود برمجيات غير مصنفة تعمل في بيئة الاختراق أو تدعمها، مثل البرمجيات المخصصة للكشف عن الأبواب المفتوحة، قد يشير بشكل كافٍ إلى

[1] براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018 ، ص 15-16

احتمال ارتكاب الشخص جريمة الدخول غير المشروع إلى النظام المعلوماتي، خصوصًا إذا تزامن ذلك مع اعتراف شفوي من الجاني.

وقد نص المشرع الجزائري في المادة 05 من القانون رقم 09-04 على تفتيش المعطيات المعلوماتية، حيث أجازت هذه المادة للسلطات القضائية المختصة وضباط الشرطة القضائية، وفقًا لأحكام قانون الإجراءات الجزائية، إجراء التفتيش في الحالات المنصوص عليها في المادة 04 من نفس القانون، وتشمل هذه الحالات توافر معلومات تشير إلى احتمال حدوث اعتداء على المنظومات المعلوماتية، ما قد يهدد النظام العام أو الاقتصاد الوطني، وبالتالي، يتيح القانون الدخول إلى المنظومات المعلوماتية بغرض التفتيش، بما في ذلك الوصول عن بُعد إلى هذه المنظومات أو أجزاء منها، وكذلك المعطيات المخزنة فيها، ومنظومات تخزين المعطيات[1].

ثالثا: شروط تفتيش الجرائم الإلكترونية:

تخضع عملية التفتيش في مجال الجرائم الإلكترونية إلى مجموعة من الشروط التي يمكن تقسيمها إلى قواعد موضوعية وأخرى شكلية، تضمنًا لاحترام الضوابط القانونية وتحقيق فعالية الإجراءات:

1 القواعد الموضوعية للتفتيش: تشترط القواعد الموضوعية لتفتيش الأنظمة المعلوماتية في الجرائم الإلكترونية توافر مجموعة من الشروط الأساسية، تتمثل في:

- ✓ وقوع جريمة معلوماتية، أي فعل غير مشروع يتم باستخدام الحاسوب أو الأنظمة المعلوماتية، بقصد تحقيق أهداف غير مشروعة.
- ✓ وجود شبهة تورط شخص أو عدة أشخاص في ارتكاب الجريمة أو المشاركة فيها.
- ✓ توفر مؤشرات قوية أو قرائن موضوعية تُرجح وجود أدوات أو أجهزة أو معطيات رقمية يمكن أن تساهم في كشف الحقيقة.
- ✓ أن يكون محل التفتيش محددًا، ويتمثل في الحاسوب بمكوناته المادية (كالأجهزة والملحقات) والمعنوية (كالبيانات والبرمجيات)، إلى جانب شبكات الاتصال المرتبطة به[2].

[1] بوديسة بجاد عبد الرؤوف ، مرجع سابق ، ص 51-52

[2] براهيمي جمال ، مرجع سابق ، ص ص 32-34

1-1 القواعد الشكلية للتفتيش:

أما من الناحية الشكلية، فهناك عدد من الشروط الإجرائية التي يجب احترامها أثناء التفتيش، منها:

- ✓ أن يُنجز التفتيش باستخدام الوسائل التقنية الحديثة، وبطريقة إلكترونية سريعة تتماشى مع طبيعة الأدلة الرقمية القابلة للتلف أو التغيير.
- ✓ ضرورة أن يكون أمر التفتيش مسببًا، أي مرفقًا بتبريرات قانونية تستند إلى معطيات واقعية تبرر القيام بالإجراء.
- ✓ يجب أن يتكون فريق التفتيش من عناصر ذات كفاءة عالية، ويشمل فنيين مختصين في مجال الحاسوب والأنظمة الإلكترونية (خبراء مسرح الجريمة الرقمية)، إلى جانب أفراد الشرطة، مع ضرورة وجود إشراف مباشر من الجهة المسؤولة عن التحقيق، وتنظيم الفريق بشكل يضمن التعاون بين الجوانب التقنية والأمنية[1].

الفرع الثالث: ضبط الأدلة في الجرائم المعلوماتية

الضبط عبارة عن إجراء من إجراءات التحقيق التي تُتخذ بعد التفتيش، ويهدف إلى جمع الأدلة التي تُسهم في كشف الحقيقة وتحديد هوية الجناة. وينشأ الحق في الضبط كنتيجة مباشرة لعملية التفتيش، بشرط أن تتم هذه الأخيرة وفقًا للشروط الموضوعية والشكلية التي ينص عليها القانون. فالضبط يُشكل الأثر الطبيعي للتفتيش، ويستند إلى العلاقة الوثيقة بين الأشياء المضبوطة والجريمة موضوع التحقيق، سواء كانت هذه الأشياء تُدين المشتبه فيه أو كانت في صالحه، وفي الجرائم التقليدية درجت الجهات القضائية على ضبط الأدلة المادية المحسوسة كالأسلحة أو المستندات الورقية، لكن الأمر يختلف في مجال الجرائم الإلكترونية، إذ إن الطبيعة التقنية والعلمية المعقدة لهذا النوع من الجرائم تفرض التعامل مع أدلة ذات طابع رقمي وغير مادي، فالبيئة الافتراضية لا تُنتج أدلة تقليدية مثل الأسلحة البيضاء أو النارية، وإنما تُنتج بيانات رقمية ونبضات إلكترونية تُشكّل جوهر الدليل الإلكتروني، وعليه فإن الضبط في الجرائم الإلكترونية يكتسي طابعًا خاصًا، ويستوجب تعريفًا دقيقًا له، وتحديد نطاقه[2].

---

[1] بوديسة بجاد عبد الرؤوف ، مرجع سابق ، ص 54

[2] بوحزمة نصيرة ، مرجع سابق ، ص 328-329

أولا: تعريف الضبط في الجرائم المعلوماتية ونطاقه

يعرف البعض الضبط في البيئة الإلكترونية بأنه "وضع اليد على الدعائم المادية المخزن فيها البيانات الإلكترونية أو المعلومات التى تتصل بجريمة من الجرائم الإلكترونية وقعت، وتفيد فى كشف الحقيقة عنها وعن مرتكبها[1]"

أما بالنسبة لنطاق الضبط في الجرائم المعلوماتية، فيعتبر الضبط إجراءً يُمارس على أشياء مادية في الأصل، مما يجعل من السهل تطبيقه في الجرائم التي تمس المكونات المادية للنظام المعلوماتي، كرفع البصمات أو حجز الأجهزة، غير أن الإشكال يتوقف عند محاولة ضبط الوسائل التقنية المستخدمة في ارتكاب الجريمة، نظرًا لعدم وجود دليل مادي مرئي في هذه الحالة، وسهولة إتلافه في ثوانٍ معدودة. ومن هنا يُطرح التساؤل: هل تصلح البيانات الإلكترونية لأن تكون محلًا للضبط؟

وقد انقسم الفقه بشأن الإجابة إلى اتجاهين: الأول يرى أن بيانات الحاسب الآلي لا تصلح لأن تكون محلًا للضبط لغياب الكيان المادي الملموس عنها، ولا يمكن ضبطها إلا بعد نقلها إلى وسيط مادي كالتصوير الفوتوغرافي أو النسخ على دعامات مادية أخرى. ويستند هذا الاتجاه إلى أن النصوص القانونية المنظمة لإجراء الضبط تنطبق فقط على الأشياء المادية المحسوسة، في المقابل يرى الاتجاه الثاني أن البيانات الإلكترونية، وإن كانت عبارة عن ذبذبات أو إشارات كهرومغناطيسية، إلا أنها قابلة للتسجيل والتخزين والنقل، مما يجعل وجودها المادي أمرًا لا يمكن إنكاره. وهذا ما دفع ببعض التشريعات المقارنة إلى تعديل نصوصها، أو سن قوانين خاصة بجرائم الحاسوب، تُمكّن من ضبط هذا النوع من البيانات وفق قواعد إجرائية تتناسب مع طبيعتها[2].

أما المشرع الجزائري، فقد تدخل هو الآخر لحسم هذا الإشكال، حيث نص في المادة 6 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، على أنه "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل

---

[1] هند نجيب، ضبط الأدلة في الجرائم الإلكترونية بين الإجراءات التقليدية والإجراءات الحديثة ، المجلة الجنائية القومية، المركز القومي للبحوث الإجتماعية والجنائية، المجلد 61، العدد 03 ، نوفمبر 2018 ص 89

[2] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه في علوم القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2017-2018 ، ص 292-293

البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز، والوضع في أحراز وفقًا للقواعد المقررة في قانون الإجراءات الجزائية "

ثانيا: الأدلة القابلة للضبط:

تتعدد الأدلة التي يمكن ضبطها في إطار التحقيق في الجرائم المعلوماتية، إذ لا تقتصر على الأدلة التقليدية فقط، بل تشمل كذلك وسائل رقمية وتقنية ترتبط بطبيعة هذا النوع من الجرائم. ومن أبرز هذه الأدلة نذكر ما يلي:

- ✓ الوثائق والمستندات المطبوعة التي تُستخرج من الحاسوب، والتي قد تحتوي على معلومات لها علاقة بالجريمة أو تساعد في كشف ملابساتها.
- ✓ الأجهزة المعلوماتية بمختلف أنواعها، لاسيما الحواسيب ومكوناتها كالوحدة المركزية، ولوحة المفاتيح، وغيرها من الملحقات التي قد تُستعمل في تنفيذ الجريمة.
- ✓ وسائط التخزين المختلفة، مثل الأقراص المرنة، والأقراص الصلبة، والشرائط الممغنطة، باعتبارها تحمل معطيات رقمية قد تُفيد سير التحقيق.
- ✓ أجهزة الاتصال الشبكي، وخاصة أجهزة المودم، التي تتيح الربط بين الحواسيب، وقد تُستخدم في نقل البيانات محل الجريمة.
- ✓ البرمجيات بأنواعها، باعتبارها الوسائل الفنية التي يعتمد عليها الجناة في ارتكاب أفعالهم الإجرامية ، البطاقات الممغنطة، وبطاقات الائتمان والمواد المستعملة في تزويرها أو إعدادها، والتي تُعد من أهم قرائن الإثبات في هذا المجال[1].

ثالثا: قواعد إحراز وتأمين المضبوطات الإلكترونية:

لا يثير إحراز المضبوطات المادية، مثل أجهزة الحاسوب وملحقاتها كالطابعات والماسحات الضوئية، إشكالات كبيرة، إذ تسري عليها القواعد التقليدية المنصوص عليها في قانون الإجراءات الجزائية، لكن الإشكال الحقيقي يبرز حين يتعلق الأمر بالمضبوطات الإلكترونية، إذ لا يمكن التعامل

[1] بركاني أحمد ياسين ، عبادلي فاطمة الزهراء ، مرجع سابق ، ص 96

معها بنفس الطرق الكلاسيكية، بل تقتضي طبيعتها التقنية والجغرافية الخاصة اللجوء إلى أساليب تقنية تتماشى مع خصوصيتها[1]. ومن بين أبرز هذه القواعد نذكر:

1 تحديد المادة الإلكترونية المراد ضبطها:

نظرًا لسهولة التلاعب بالبيانات الرقمية دون ترك أثر، يتعيّن على المحقق تحديد المعلومات المطلوب ضبطها بدقة، مع اتخاذ تدابير مادية لحمايتها، كنسخها على أقراص أو أشرطة ممغنطة، وتوثيق عملية النسخ بمحضر رسمي يتضمن توقيع المحقق ومشغل النظام، مع ختم الأحراز ووضعها في حاويات مخصصة لضمان سلامتها[2].

1-2 تأمين البرامج المضبوطة قبل التشغيل:

في حال تم ضبط برمجيات إلكترونية، يتوجب على المحقق إنشاء نسخة مطابقة وآمنة منها قبل عرضها على الخبراء، وذلك لتفادي تلفها أو تحويلها إلى برمجيات مدمّرة عند تشغيلها بطرق غير سليمة، مما قد يؤدي إلى فقدان الدليل.

1-3 الالتزام بالقواعد الفنية لنقل المضبوطات:

تتطلب عملية نقل البيانات الإلكترونية المضبوطة عناية خاصة، ويجب تجنّب تعريض وسائط التخزين كالقرص الصلب أو الشرائط الممغنطة للغبار أو الأشعة الكهرومغناطيسية التي قد تؤدي إلى إتلاف محتواها.

1-4 مراعاة شروط التخزين المناسبة:

ينبغي احترام ظروف التخزين المتعلقة بدرجة الحرارة والرطوبة عند حفظ الأدلة الإلكترونية، تفاديًا لتدهور محتوى الأقراص أو الأشرطة الممغنطة بمرور الوقت.

---

[1] رابحي عزيزة، مرجع سابق ، ص 294

[2] بوحزمة نصيرة ، مرجع سابق ، ص 333

1-5 ضبط النسخ الأصلية من الوسائط:

من الضروري أن يشمل الضبط الوسائط الأصلية وليس مجرد نسخ عنها، مع السماح للجهة التي كانت تحتفظ بها بالحصول على نسخة منها للاستمرار في أنشطتها، خاصة في حال تأخر الفصل في القضية.

1-6 الاستعانة بالأشخاص المتمكنين من النظام:

تنص المادة 19 الفقرة 4 من اتفاقية بودابست على إمكانية تمكين الجهات المختصة من إصدار أوامر لأشخاص مطلعين على تشغيل النظام المعلوماتي أو تدابير حمايته، قصد توفير المعلومات اللازمة لتسهيل إجراءات التفتيش والضبط[1].

1-7 التفتيش عبر الحدود

وفقًا للمادة 32 من الاتفاقية، يمكن تفتيش وضبط بيانات رقمية مخزنة خارج الإقليم الوطني في حالتين الأولى إذا كانت البيانات متاحة للعموم، والثانية إذا أعطى الحائز أو مالك البيانات موافقته على ذلك[2].

الفرع الرابع: الخبرة الفنية في الجرائم المعلوماتية

تعتبر الخبرة من الوسائل المهمة التي يعتمد عليها المحقق في الجانب الفني من التحقيق، خاصةً عندما يتعلق الأمر بوقائع تقنية أو أدلة معقدة يصعب فهمها أو تفسيرها بالوسائل التقليدية. وتُعرّف الخبرة القضائية على أنها استعانة الجهة القضائية بشخص مختص يُطلق عليه اسم "**الخبير**"، ويكون هذا الأخير ذا دراية ومعرفة فنية أو علمية في مجال معين، مما يُمكّنه من مساعدة القاضي أو المحقق في تفسير وقائع أو أدلة تقنية خارجة عن نطاق المعرفة العامة[3].

[1] إتفاقية بودابست المتعلقة بالجريمة المعلوماتية ، المادة 19 الفقرة 4 ،الموقعة في بودابست بتاريخ 23 نوفمبر 2001

[2] بوحزمة نصيرة ، مرجع سابق ، ص 333-331

[3] محمد بوعمارة، سيد علي بنينال ، مرجع سابق ، ص 46

أولا: تعريف الخبرة

عرّفها بعض الفقهاء بأنها عبارة عن تفسير فني للأدلة، يتم من خلال الاعتماد على معلومات ومهارات الخبير، فيما يرى آخرون أن الخبير هو كل شخص يملك معرفة خاصة في مسألة معينة ويستعين به المحقق متى شعر بأن تلك المسألة تتجاوز حدود تكوينه العام، كأن يتعلق الأمر بتقرير الطب الشرعي في قضايا القتل، أو تحليل مادة مشكوك فيها في جريمة تسمم، أو فحص خط اليد، أو تحليل البصمة الوراثية(DNA) ، وغيرها من المسائل التي تتطلب خبرة متخصصة[1].

ثانيا: الخبرة في الجريمة المعلوماتية

مع تطور التكنولوجيا، أصبحت الجريمة الإلكترونية من الجرائم المعقدة التي تستوجب تدخّل خبراء مختصين في مجالات متعددة مثل برمجة الحواسيب، الشبكات، تحليل البيانات، الأمن السيبراني وغيرها. فدور هؤلاء الخبراء لا يقتصر فقط على تقديم الدعم الفني، بل يشمل أيضًا تحليل الأدلة الرقمية، تتبّع مصادرها، وإعداد تقارير تقنية تساعد في فهم كيفية ارتكاب الجريمة.

ويُعدّ نجاح التحقيق في مثل هذه القضايا مرهونًا بدرجة كبيرة بكفاءة هؤلاء الخبراء، مما يُحتّم على المحقق أن يُحدّد للخبير مهمته بدقة، خاصةً وأن خصوصية الجرائم الإلكترونية قد تفتح المجال أحيانًا للاستعانة بأشخاص سبق لهم ارتكاب مثل هذه الجرائم، بعد تأهيلهم، للاستفادة من معارفهم التقنية في كشف الجرائم وملاحقة مرتكبيها.

ثالثا: أساليب عمل الخبير في الجرائم الإلكترونية

يعتمد الخبير في هذا النوع من القضايا على أسلوبين أساسيين ويتمثلان في ما يلي:

الأسلوب الأول: يتمثل في تجميع وتحليل محتوى المواقع الإلكترونية التي تُشكّل جرائم في حد ذاتها، مثل مواقع التهديد، الاحتيال، أو نسخ البرامج المحمية. ويقوم الخبير بفحص البنية البرمجية لهذه المواقع، وتحليل حركتها الرقمية، وتحديد مصدرها باستخدام عناوينIP ، مما يُساعد في تتبع الجهاز الذي انطلقت منه الجريمة.

[1] عبد العزيز أحمد، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي، سعيدة، 2021-2022 ، ص 85

الأسلوب الثاني: يتعلق بالمواقع التي لا تُعدّ مخالفة بحد ذاتها، ولكن يتم استغلال محتواها في ارتكاب الجرائم، مثل تلك التي تُقدّم إرشادات حول كيفية تحضير مواد مخدرة أو صنع متفجرات. في هذه الحالة، يقوم الخبير بتحليل المحتوى لتحديد مدى خطورته، ومتابعة الأنشطة المشبوهة المرتبطة به.

كما يتولّى الخبير الرقمي مهمة أساسية أخرى، وهي استخراج الأدلة الرقمية من الأجهزة أو المنصات الإلكترونية دون التسبب في تلفها أو فقدانها، من خلال استخدام مهارات تقنية متقدمة مثل فك التشفير، استرجاع البيانات، تتبع تحركات الجاني داخل البيئة الافتراضية، وفهم نظام التشغيل والبرمجيات المستعملة[1].

الفرع الخامس: الإستجواب في الجرائم المعلوماتية

يعتبر الاستجواب من أهم إجراءات التحقيق التي يلجأ إليها قاضي التحقيق بهدف مواجهة المتهم بالتهم الموجهة إليه، وهو ما ينطبق كذلك على الجرائم المعلوماتية، غير أن خصوصية هذه الأخيرة تجعل من الاستجواب إجراءً أكثر حساسية ودقة مقارنة بباقي الجرائم التقليدية، نظراً للطابع التقني الذي يميزها.

ففي الجرائم المعلوماتية، غالباً ما يكون المتهم شخصاً ذا دراية بالتقنيات الحديثة، مثل استخدام الشبكات، البرمجيات أو حتى أساليب التشفير، وهو ما يجعل من عملية استجوابه أمراً يتطلب من المحقق أو القاضي الإلمام ولو جزئياً بالجوانب التقنية المرتبطة بالجريمة، وما يزيد من أهمية هذا الإجراء في الجرائم المعلوماتية هو أنه قد يُسهم في كشف أساليب ارتكاب الجريمة، أو أدواتها، وحتى الأشخاص الآخرين المتورطين فيها، خاصةً وأن بعض هذه الجرائم تُرتكب ضمن شبكات منظمة أو باستعمال تقنيات يصعب تتبعها إلا من خلال المعلومات التي قد يدلي بها المتهم نفسه أثناء استجوابه[2]. وفي هذا الصدد سنتناول تعريف الاستجواب **(أولاً)** ثم خصوصية الاستجواب في الجرائم المعلوماتية **(ثانيا)** ثم شروط وضمانات الاستجواب **(ثالثا)** وفي الأخير سنتحدث عن دور الاستجواب في كشف الحقيقة **(رابعا)**.

[1] عبد العزيز أحمد ، مرجع سابق، ص ص 85-86

[2] بلغفور مريم، عتروز صليحة ، أليات البحث والتحقيق في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر في القانون، كلية الحقوق، قسم القانون الخاص ، جامعة الإخوة منتوري ، قسنطينة، 2015-2016 ، 97

أولاً: تعريف الاستجواب

يُعدّ الاستجواب من أهم مراحل التحقيق، ويقصد به مواجهة المتهم بالتهم المنسوبة إليه ومطالبته بالرد عليها بكل وضوح، حيث يُمنح الفرصة للدفاع عن نفسه وتقديم دفوعاته. ويُعتبر وسيلة فعّالة تساعد المحقق أو قاضي التحقيق على جمع المعلومات والكشف عن ملابسات الجريمة.

ثانياً: خصوصية الاستجواب في الجرائم المعلوماتية

تتميز الجرائم المعلوماتية بطابعها الفني والتقني، وهو ما يفرض تحديات خاصة عند استجواب المتهمين في هذا النوع من الجرائم. فالمتهم قد يكون على دراية كبيرة بالتكنولوجيا والأنظمة المعلوماتية، وقد يستغل هذه المعرفة لإخفاء الأدلة أو تضليل التحقيق. لذلك يجب أن يكون المحقق ملمًّا ولو جزئياً بالمفاهيم التقنية حتى يتمكن من طرح الأسئلة بدقة وفهم الأجوبة بشكل صحيح.

إضافة إلى ذلك، الاستجواب في هذا النوع من القضايا قد يكشف تفاصيل مهمة مثل البرامج المستعملة، طريقة اختراق النظام، أو كيفية إخفاء الهوية عبر الإنترنت، ما يجعله إجراءً محوريًا في الوصول إلى الحقيقة[1].

ثالثاً: شروط وضمانات الاستجواب

من الضروري أن يتم الاستجواب وفقاً للضمانات القانونية التي تحمي حقوق المتهم. فيجب إعلامه بالتهم الموجهة إليه بلغة واضحة، وله الحق في حضور محامٍ أثناء الاستجواب، كما يُمنح الحق في عدم الإجابة على الأسئلة إذا أراد ذلك، دون أن يُعتبر صمته إدانة له.

أما في الجرائم المعلوماتية، فالضمانات تأخذ بعداً إضافيًا نظرًا لاحتمال تعقيد القضية وتشعبها تقنياً، وقد يحتاج المتهم إلى خبير تقني يوضح له بعض المصطلحات أو الإجراءات المذكورة في التهم.

رابعاً: دور الاستجواب في كشف الحقيقة

الاستجواب لا يهدف فقط إلى إثبات التهم بل يمكن من خلاله أيضًا الوصول إلى أدلة جديدة أو أسماء شركاء آخرين في الجريمة. فقد يعترف المتهم ببعض التفاصيل التقنية التي لم تكن معروفة لدى

[1] بلغفور مريم ، عتروز صليحة ، مرجع سابق ، ص 98

المحقق، مثل روابط إلكترونية، كلمات مرور، برامج خبيثة أو حتى هويات افتراضية، مما يساعد على توسيع التحقيق والوصول إلى نتائج أدق[1].

المطلب الثاني: الأساليب المستحدثة للتحقيق في الجرائم المعلوماتية

تُثير الجريمة المعلوماتية تحديات كبيرة من الناحية الإجرائية، إذ يصعب استخدام أساليب التحقيق التقليدية كالتفتيش والمعاينة والضبط في مواجهة طبيعة هذا النوع من الجرائم، التي ترتكب غالبًا في بيئة افتراضية وباستخدام وسائل تقنية متطورة، فالمجرم الإلكتروني يعتمد على وسائل علمية دقيقة ويحرص على اتخاذ احتياطات تقنية معقدة لتضليل أجهزة العدالة، مما يُعيق عملية جمع الأدلة وإثبات الجريمة، ولأن هذه الجرائم لا يمكن أن تبقى دون عقاب، فقد سعت الجزائر إلى تحديث ترسانتها القانونية من أجل مواكبة التحديات التي تفرضها الجريمة الإلكترونية، وذلك من خلال تعديل قانون العقوبات بموجب القانون رقم 06-22، حيث تم إدراج إجراءات جديدة خاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما صدر القانون رقم 09-04 المتعلق بالقواعد الخاصة بالإعلام والاتصال، والذي تضمّن كذلك آليات جديدة للبحث والتحري في الجرائم المعلوماتية[2].

وعليه، سنتناول في هذا المطلب عرضًا تفصيليًا لأهم الأساليب الحديثة المعتمدة في التحقيق في الجرائم الإلكترونية، من خلال التطرق إلى المراقبة الإلكترونية في **(الفرع الأول)** ثم إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور في **(الفرع الثاني)** في **(الفرع الثالث)** ثم التسرب في **(الفرع الرابع)** وفي **(الفرع الخامس)** سنتطرق إلى الحفظ والإفشاء العاجلان

الفرع الأول: المراقبة الإلكترونية

من خلال استقراء أحكام القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يتضح أن المشرع الجزائري لم يضع تعريفًا صريحًا للمراقبة الإلكترونية، بل ترك هذه المهمة للفقه، وقد عرّفها بعض الفقهاء على أنها عملية أمنية أساسية تعتمد على نظام معلوماتي إلكتروني، يتم من خلالها تتبع نشاط معين باستخدام الوسائل التكنولوجية، عبر شبكة الإنترنت، بغرض

[1] بلغفور مريم ، عتروز صليحة ، مرجع سابق ، ص 99

[2] بوسنة شيماء نور الهدى، بن سلامة كوثر، مرجع سابق، ص93

تحقيق هدف محدد، وتُفرغ نتائجها في ملف إلكتروني خاص[1]، ويُمكن تلخيص الأساسيات القانونية للمراقبة الإلكترونية في ضرورة الإشراف القضائي **(أولا)** ثم ضرورة الإذن المسبق من السلطة القضائية المختصة **(ثانيا)** و**(ثالثا)** تحديد الهدف من المراقبة بدقة أما **(رابعا)** تسجيل نتائج المراقبة في ملف إلكتروني مؤمَّن

أولًا: ضرورة الإشراف القضائي

حيث اشترط المشرع أن تتم المراقبة الإلكترونية تحت سلطة القضاء، وهو ما نصّت عليه المادة 04 من القانون رقم 09-04 ويُعد هذا الإشراف ضمانة قانونية أساسية لحماية الحقوق والحريات، وخاصة الحق في الخصوصية وسرية المعطيات الشخصية، ومنع أي تعسف في استعمال هذه التقنية.

ثانيًا: ضرورة الإذن المسبق من السلطة القضائية المختصة

لا يجوز البدء في إجراءات المراقبة الإلكترونية إلا بعد الحصول على إذن صريح من الجهة القضائية المختصة، ما يُعزز من شرعية هذه الإجراءات ويضفي عليها الطابع القانوني. ويُعتبر هذا الإذن شرطًا جوهريًا لصحة عملية المراقبة وضمان قبول نتائجها كأدلة أمام القضاء.

وبالتالي، فإن المراقبة الإلكترونية، وإن كانت وسيلة فعالة في مكافحة الجرائم المعلوماتية، فإن استخدامها يبقى محاطًا بقيود قانونية صارمة تهدف إلى تحقيق التوازن بين مقتضيات الأمن واحترام الحقوق الأساسية للمواطن[2].

ثالثًا: تحديد الهدف من المراقبة بدقة

من بين الشروط الأساسية لاستخدام تقنية المراقبة الإلكترونية، أن يكون هناك غرض محدد وواضح من العملية، كالكشف عن جريمة معينة أو تتبع نشاط غير مشروع. فلا يجوز أن تكون المراقبة عامة أو عشوائية، بل يجب أن تُوجَّه نحو وقائع أو أشخاص معينين، لتجنب انتهاك الخصوصية بشكل غير مبرر.

---

[1] بطيحي نسمة، محاضرات في مقياس الوقاية من الجرائم الإلكترونية، كلية الحقوق والعلوم السياسية، قسم الحقوق ، جامعة محمد لمين دباغين ، سطيف 2 ، 2012-2022 ، ص 13

[2] بطيحي نسمة ، مرجع سابق ، ص 14

رابعًا: تسجيل نتائج المراقبة في ملف إلكتروني مؤمَّن

ينبغي أن تُوثق نتائج المراقبة بطريقة تقنية دقيقة، داخل ملف إلكتروني يُحترم فيه مبدأ حماية المعطيات الشخصية وسرية المعلومات. كما يجب أن تكون هذه النتائج قابلة للاستخدام كأدلة قانونية، ما يستوجب احترام المعايير الفنية والإجرائية أثناء جمعها وتخزينها.[1]

الفرع الثاني: إعتراض المراسلات في الجرائم المعلوماتية

يُعد اعتراض المراسلات من بين الأساليب الخاصة التي أتاحها القانون في إطار التحقيق في الجرائم الإلكترونية، ويقصد به المراقبة السرية للمراسلات السلكية واللاسلكية، بهدف كشف الجريمة وجمع الأدلة ضد المشتبه فيهم أو المشاركين في ارتكابها، كما لم يُخصّص المشرع الجزائري تعريفًا دقيقًا لهذا الإجراء، بل تركه مفتوحًا ليتماشى مع التطورات التكنولوجية في مجال وسائل الاتصال، واكتفى بتحديد الضوابط القانونية التي يتم في ظلها تنفيذ هذا الإجراء، خاصة من حيث الجهات المختصة والإذن القضائي.وتنصب عملية الاعتراض على نوعين من المراسلات، النوع الأول يتمثل في المراسلات الإلكترونية، وتشمل الرسائل النصية والبريد الإلكتروني والمحادثات عبر التطبيقات، أما النوع الثاني فيتمثل في المراسلات البريدية التقليدية، والتي تشمل الرسائل التي تُرسل عبر البريد أو بواسطة ناقل شخصي، ويمكن اعتراضها في إطار قانوني معين إذا توافرت الشروط اللازمة لذلك.[2]

أولا: مفهوم عملية اعتراض المراسلات

يناط باعتراض المراسلات تلك العملية التي تسمح بالمراقبة السرية للمراسلات السلكية واللاسلكية، في إطار البحث والتحري عن الجريمة، وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في ارتكابها، وقد عرفت المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائية عملية اعتراض المراسلات بأنها: "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية"، ولم تُحدد المادة طبيعة هذه المراسلات، مما يفتح المجال لتشمل كل أنواعها، سواء كانت مكتوبة أو مرئية أو صوتية، ورقية أو رقمية، مثل الرسائل النصية، البريد الإلكتروني، الفاكس،

[1] بطيحي نسمة ، مرجع سابق ، ص 15

[2] بلفيحج صهيب، حمادي عبد الكريم عماد، أليات مكافحة الجرائم السيبرانية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق، قسم القانون الخاص، جامعة الإخوة منتوري، قسنطينة، 2022-2023، ص 51

التلغرام، أو المحادثات عبر الهاتف، وبالتالي تتم عملية الاعتراض عن طريق ترتيبات تقنية سرية، توضع دون علم أو موافقة الأشخاص المعنيين[1].

ثانيا: الشروط المطلوبة في المراسلات محل الاعتراض

يشترط في المراسلات التي يمكن أن تكون محلًا لإجراء الاعتراض أو المراقبة أن تتسم بطابع السرية والخصوصية، وهو ما لا يتحقق إلا بتوافر عنصرين أساسيين:

– أن يتضمن فحوى الرسالة معلومات أو أفكارًا شخصية وسرية لا يرغب المرسل في اطلاع الغير عليها.

– أن يكون المرسل إليه محددًا، مع وجود نية واضحة في عدم السماح لأي طرف ثالث بالاطلاع على محتوى المراسلة.

– ويُلاحظ أن المشرع الجزائري لم يُدرج مراقبة الاتصالات الإلكترونية كإجراء من إجراءات التحقيق القضائي أو التحري بموجب القانون رقم 09-04، بل منح الجهات القضائية فقط صلاحية استخدام الاعتراض بهدف الوقاية من بعض الجرائم التي تمس بأمن الدولة.

– وفي هذا الإطار، تم استحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بموجب المادة 13 من القانون رقم 09-04 التي تنص على أنه: "يُنشأ جهاز وطني للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، تحدد تشكيلته وتنظيمه وسيره عن طريق التنظيم"، حيث أوكل لها القانون مهمة التنسيق مع السلطات القضائية في مجال الوقاية والمكافحة، وتُعد هذه الهيئة سلطة إدارية مستقلة، تتمتع بالشخصية المعنوية والاستقلال المالي، ومقرها الجزائر العاصمة، وقد تم تحديد تنظيمها وتشكيلتها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015[2].

[1] مجدوب نوال، الأليات الإجرائية للكشف عن الجريمة المعلوماتية ، مجلة البحوث القانونية والإقتصادية، المركز الجامعي مغنية، المجلد 06، العدد 03، 2023، ص 202

[2] نفس المرجع ، ص 203

ثالثا: الشروط القانونية لإعتراض المراسلات

تبقى عملية اعتراض أو مراقبة المراسلات مرهونة بتوفر مجموعة من الشروط القانونية، أبرزها:

– الحصول على إذن كتابي صادر عن الجهة القضائية المختصة، أي وكيل الجمهورية في مرحلة التحقيق الابتدائي، أو قاضي التحقيق في مرحلة التحقيق القضائي، وذلك تحت طائلة بطلان الإجراء،

ويُعد الإذن شرطًا جوهريًا نظرًا لأن اعتراض المراسلات يتم دون علم الأشخاص المعنيين، ما يجعله من الإجراءات الخطيرة رغم فعاليته في كشف الجرائم المعلوماتية، حيث أنه يُعتبر مساسًا بسرية الاتصالات وحرمة الحياة الخاصة التي يحميها الدستور، ويشترط في هذا الإذن أن يتضمن:

– تحديد طبيعة الجريمة التي تبرر اللجوء إلى هذا الإجراء وذلك وفقا للإجراءات التي حددها المشرع في المادة 65 مكرر 5 من قانون إ.ج.ج "التي تجيز لوكيل الجمهورية أو قاضي التحقيق، في بعض الحالات الخطيرة، إعتراض المراسلات السلكية واللاسلكية ، وتسجيلها أو الإطلاع عليها"

– أن تكون من الجرائم التي يسمح القانون باعتراض المراسلات بشأنها.

– تحديد نوع المراسلات المراد اعتراضها بصفة دقيقة[1].

1 شروط صحة هذه الإجراءات

أجاز المشرع الجزائري لضباط الشرطة القضائية إذا إقتضت الضرورة في التحري عن الجريمة المتلبس بها او التحقيق الإبتدائي ، القيام بإعتراض المراسلات لكنه قيد هذا الإجراء بجملة من الشروط لتكون إجراءاتهم صحيحة ومنتجة وتتمثل في:

– أن يقوم الضباط بهذه الأعمال بغرض الكشف عن الجرائم التي حددها المشرع في المادة 65 مكرر5 السابقة الذكر والتي تتمثل في جرائم المخدرات، الجرائم العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، وجرائم الفساد، ونلاحظ أن المشرع الجزائري قد عدد هذه الجرائم على سبيل الحصر وهذا يرجع إلى درجة الخطورة الإجرامية التي تتسم بها هذه الجرائم ومدى تأثيرها على السياسة العامة في الدولة وإقتصادها، أما إذا كانت هذه الأعمال في غير هذه الجرائم فإن إجراؤها باطل.

[1] مجدوب نوال، مرجع سابق، ص 203

– أن يصدر الإذن إلى ضباط الشرطة القضائية للقيام بالأعمال المحددة في المادة 65 مكرر5 ويكون مكتوباً من وكيل الجمهورية أو قاضي التحقيق المختصين بأن يأذنوا بما يلي:

– أن يكون الاعتراض مبررًا ومرتبطًا بجريمة محددة، مثل الجرائم المذكورة في المادة 65 مكرر 5.

– أن يتم الاعتراض على وسائل الاتصال السلكية أو اللاسلكية.

– أن يتم الاعتراض دون علم المعنيين بالأمر.

– أن يكون الاعتراض محددًا في الزمان والمكان وموجهًا إلى أشخاص معينين.

– أن يتم في إطار الضمانات القانونية المنصوص عليها في المادة 47 من الدستور.[1]

الفرع الثالث: تسجيل الأصوات وإلتقاط الصور

أصبح تطور الجريمة الإلكترونية يتطلب وسائل حديثة للتحري، ومن بين أبرز هذه الوسائل نجد تسجيل الأصوات والتقاط الصور، وهي إجراءات نص عليها المشرع الجزائري في المواد من 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية، وخص بها الجرائم الخطيرة ومنها الجرائم المعلوماتية، لما لها من خصوصية في الإثبات وصعوبة كشف مرتكبيها بالطرق التقليدية وفي هذا الصدد سنقوم بتعريف تسجيل الأصوات **(أولا)** ثم تعريف إلتقاط الصور **(ثانيا)** والشروط القانونية لتسجيل الأصوات وإلتقاط الصور **(ثالثا)** وفي الأخير الضمانات القانونية أثناء تنفيذ الإجراء **(رابعا)**

أولا: تعريف تسجيل الأصوات

يقصد بتسجيل الأصوات، عملية مراقبة الأحاديث التي تجري عبر الهاتف أو بشكل مباشر بين الأشخاص، وذلك باستعمال أجهزة إلكترونية مخصصة، بغرض جمع أدلة تتعلق بجريمة معينة، ويشترط أن يكون هذا الإجراء بإذن كتابي من وكيل الجمهورية أو قاضي التحقيق، عندما يتعلق الأمر بجناية أو جنحة معقدة يصعب إثباتها بوسائل أخرى، وقد أشار إلى ذلك القانون في المادة 65 مكرر 5 من قانون الإجراءات الجزائية[2].

[1] مجدوب نوال، مرجع سابق ، ص 203–204

[2] كحيو صونيا، بن الشيخ الفقون محمد سليم برهان الدين ، مرجع سابق ، ص 34

ثانيا: تعريف التقاط الصور

أما التقاط الصور، فهو إجراء يسمح فيه المشرع بتصوير أشخاص أو أماكن معينة، قد تكون خاصة أو عامة دون علم أصحابها، وهذا بهدف دعم التحقيق الجنائي، ويتم ذلك أيضًا بناء على إذن قضائي ويُراعى فيه مبدأ التناسب بين المساس بالحياة الخاصة ومصلحة التحقيق وقد ورد في نفس المادة 65 مكرر 5 السابقة الذكر أن ضباط الشرطة القضائية يمكنهم تنفيذ هذا الإجراء في إطار الجرائم الخطيرة، تحت رقابة القضاء[1].

ثالثا: الشروط القانونية لتسجيل الأصوات والتقاط الصور

حدد المشرع مجموعة من الشروط التي يجب توفرها حتى يكون هذا الإجراء قانونيا، وتتمثل في ما يلي:

1 إذن مسبق من الجهة القضائية المختصة: يجب أن يُستصدر الإذن من وكيل الجمهورية أو قاضي التحقيق، حسب الحالة، ويكون مبررا ومعللا، ويُبين فيه بدقة طبيعة الجريمة، وهوية الأشخاص المعنيين، والمكان والوسيلة المستعملة.

1-2 ضرورة الجريمة: لا يتم اللجوء إلى هذا الإجراء إلا في إطار التحقيق في جنايات أو جنح خطيرة مذكورة على سبيل الحصر في القانون، مثل جرائم الإرهاب، الجريمة المنظمة، أو الاعتداء على أنظمة المعالجة الآلية للمعطيات.

1-3 تحديد مدة الإجراء: يجب أن تُحدد مدة تنفيذ الإجراء في الإذن، بحيث لا تتجاوز الشهرين، قابلة للتجديد مرة واحدة فقط، وفقا للمادة 65 مكرر 9.

1-4 الخصوصية في التنفيذ: يجب أن يُنفذ الإجراء في ظروف تحترم الحياة الخاصة، وتحت إشراف مباشر من الجهة المصدرة للإذن.

رابعا: الضمانات القانونية أثناء تنفيذ الإجراء

لتفادي التعسف أو المساس غير المشروع بالحياة الخاصة للأفراد، أقر المشرع مجموعة من الضمانات القانونية، من أبرزها:

[1] كحيو صونيا، بن الشيخ الفقون محمد سليم برهان الدين ، مرجع سابق ، ص 35

1 الرقابة القضائية المباشرة: يتعين على ضباط الشرطة القضائية تنفيذ هذه الإجراءات تحت إشراف ومراقبة مستمرة من وكيل الجمهورية أو قاضي التحقيق.

1-2 إعداد محضر مفصل: ينص القانون على ضرورة تحرير محضر دقيق يتضمن كل العمليات المنجزة، ويتم إيداعه لدى الجهة القضائية المختصة، حيث يلتزم ضابط الشرطة القضائية بإعداد محضر مفصل عن كل ما تم تسجيله أو تصويره، وتسليمه للجهة التي أصدرت الإذن.

1-3 سرية الإجراء: يجب الحفاظ على سرية التسجيلات والصور وعدم استعمالها إلا في إطار التحقيق وبما يخدم مصلحة العدالة فقط.

1-4 إتلاف التسجيلات غير المفيدة: إذا تبين أن التسجيلات أو الصور لا علاقة لها بالجريمة، وجب إتلافها وعدم الاحتفاظ بها، ضمانا لعدم انتهاك الحياة الخاصة دون مبرر.

الفرع الرابع: التسرب الإلكتروني

استحدث المشرع الجزائري إجراء التسرب في إطار مكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، عدة إجراءات للكشف عن الجريمة ومرتكبها، وذلك كحل بديل بعد ما أثبتت طرق البحث والتحري التقليدية عدم فعاليتها أمام الجرائم المستحدثة، خاصة الجريمة الإلكترونية، فجاء هذا الإجراء كآلية جديدة تسمح بالكشف عن الجرائم ومرتكبيها وخاصة الجرائم الإلكترونية وتقديمهم للعدالة[1].

كما قد تم إدراج التسرب بموجب القانون 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-155 المتعلق بقانون الإجراءات الجزائية، بحيث خصص له الفصل الخامس تحت عنوان "في التسرب"، والذي يشمل المواد من 65 مكرر 11 إلى 65 مكرر 18، وينظم من خلال هذه المواد تعريف التسرب، شروطه، العمليات المبررة به، وكذلك الحماية القانونية المقررة أثناء تنفيذه[2].

[1] كحيو صونيا، بن الشيخ الفقون محمد سليم برهان الدين ، مرجع سابق ، ص 23

[2] القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 ، والمتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية ، العدد 84 ، المعدل والمتمم للأمر رقم 155/66 المؤرخ في 8 جوان 1966

أولاً: مفهوم عملية التسرب

من الناحية الأمنية، يُقصد بالتسرب تلك العملية التي تكون محضّرة ومنظمة مسبقًا، بهدف التوغل داخل وسط معين لمعرفة ما يدور فيه من نشاطات، خاصة إذا كان هذا الوسط مشبوها، وهذا قصد الحصول على معلومات دقيقة ومخفية يستفيد منها المحققون.

أما من الناحية القانونية، فقد عرّف المشرع الجزائري التسرب في المادة 65 مكرر12 من ق.إ.ج.ج بأنه: "تنفيذ ضابط أو عون من الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة، بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف"[1]

ثانيا: شروط وإجراءات التسرب

نظرا لما قد يرافق عملية التسرب من خطر المساس بالحياة الخاصة للمتهم، فقد وضع المشرع مجموعة من الشروط والإجراءات سواء من حيث الشكل أو المضمون لضمان قانونية هذا الإجراء، وسنتناولها فيما يلي:

1 شروط إجراء عملية التسرب

حسب ما جاء في المادة 65 مكرر 11من قانون الإجراءات الجزائية، لا يمكن اللجوء إلى عملية التسرب إلا إذا كانت هناك ضرورة ملحة في إطار التحري أو التحقيق، أي عندما تكون الأدلة قليلة أو من الصعب الحصول عليها بالطرق التقليدية، أما إذا توفرت أدلة كافية ، فلا حاجة للمجازفة بهذا الإجراء، كما أن المشرع حصر استعمال التسرب في الجرائم الخطيرة والمعقدة فقط، والمذكورة بشكل حصري في المادة 65 مكرر 5، ومن بين هذه الجرائم نجد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وبالتالي لا يمكن استخدام هذا الأسلوب إلا في الجرائم المنصوص عليها حصرا في هذه المادة.

2 شروط صحة عملية التسرب

لتكون عملية التسرب قانونية وصحيحة، يجب احترام عدة إجراءات أهمها:

[1] كحيو صونيا، بن الشيخ الفقون محمد سليم برهان الدين، مرجع سابق ، ص 24

2-1 صدور إذن قضائي

يجب أن يحصل العون المتسرب على إذن مسبق من وكيل الجمهورية أو قاضي التحقيق حسب الحالة، ويكون هذا الإذن مكتوبا وصادرا عن الجهة المختصة. وإذا كان الإذن من طرف قاضي التحقيق، فعليه إعلام وكيل الجمهورية بذلك مسبقًا، وتُذكر في الإذن هوية ضابط الشرطة القضائية المسؤول عن العملية.

2-2 الإذن يجب أن يكون مكتوبًا ومسببًا

فحسب المادة 65 مكرر 15، يجب أن يكون الإذن مكتوبًا مع ذكر سبب اللجوء إليه، وتحديد نوع الجريمة ومدة العملية، التي لا يمكن أن تتجاوز 4 أشهر. ويمكن تمديدها لنفس المدة إذا اقتضى التحقيق ذلك، لكن في نفس الشروط. ويمكن للقاضي أن يقرر إيقاف العملية في أي وقت إذا رأى ضرورة لذلك

وبعد نهاية العملية، يُوضع الإذن في ملف الإجراءات، ويُحفظ سريًا طيلة مدة العملية ولا يطلع عليه إلا القاضي الآمر بها، وضابط الشرطة القضائية، والعون المتسرب.

يحرر ضابط الشرطة القضائية المشرف على العملية تقريرًا يتضمن التفاصيل الضرورية، دون المساس بسرية وهوية المتسرب، وهذا ما نصت عليه المادة 65 مكرر 13. وفي حال انتهاء مدة التسرب وعدم التمديد، يمكن للعون المتسرب أن يواصل عمله لفترة قصيرة لتأمين انسحابه بطريقة آمنة، دون أن يتحمل أية مسؤولية جزائية، بشرط ألا تتجاوز هذه الفترة المعقولة[1].

ثالثا: الجهات المختصة بالتسرب

المخول لهم تنفيذ عمليات التسرب هم ضباط الشرطة القضائية المنصوص عليهم في المادة 15 من نفس القانون، ويُستثنى من ذلك الولاة ورؤساء البلديات لأسباب ميدانية، كما يجوز تسخير أعوان الشرطة القضائية (المادة 19) بشرط أن يعملوا تحت إشراف ضابط الشرطة القضائية، كما يمكن تجنيد أي شخص، سواء من الذكور أو الإناث، يرى فيه الضابط منفعة لإنجاح المهمة، وذلك دائمًا تحت رقابة القضاء.

[1] رابحي عزيزة ، مرجع سابق ، ص 297 - 298

ويجوز سماع ضابط الشرطة القضائية فقط كشاهد على العملية، وليس غيره. ويُعاقب كل من يكشف هوية الضابط أو العون المتسرب خلال مختلف مراحل الإجراءات، وهذا لحمايتهم.

رابعا: آثار التسرب

بمجرد صدور الإذن بالتسرب، يباشر العون المتسرب مهامه حسب ما هو مطلوب منه، وتُسخّر له الوسائل اللازمة، سواء كانت مادية أو قانونية. وطبقًا للمادة 65 مكرر 14، يمكنه اقتناء أو نقل أو إعطاء أموال أو معلومات أو وسائل تم الحصول عليها من الجرائم أو استُعملت في ارتكابها، كما يمكنه استعمال وسائل قانونية كوثائق رسمية مزورة لضمان استمرار العملية بسرية.

وبعد الانتهاء من التسرب، تتمكن الجهات المختصة، مثل وكيل الجمهورية وقاضي التحقيق، من الاطلاع على تفاصيل دقيقة حول الجرائم المرتكبة، ويتم تحرير محاضر تساعد في إثبات الجرائم ، وتُعرض أمام المحكمة وفقًا لما يسمح به القانون، وتُعتبَر هذه المحاضر أدلة قانونية إذا تم احترام الشروط الشكلية والموضوعية.

من جهة أخرى، يمكن أن يتعرض العون المتسرب لخطر كبير حتى بعد انتهاء مهمته، وقد يمس ذلك حياته أو حياة أفراد أسرته، ولهذا وفر له القانون حماية خاصة، حيث يعاقب بالسجن والغرامة كل من يكشف هويته، وتزداد العقوبة إذا نتج عن الكشف ضرر جسدي أو وفاة، كما هو مبين في المادة 65 مكرر 16 من قانون الإجراءات الجزائية التي تنص على أنه: " يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة مالية تتراوح بين 50.000 دج و200.000 دج كل من يكشف هوية ضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات إذا أدى هذا الكشف إلى أعمال عنف أو ضرب وجرح ضد أحد هؤلاء الأشخاص أو أزواجهم أو أصولهم المباشرين، تكون العقوبة الحبس من خمس (5) إلى عشر (10) سنوات وغرامة من مائتي ألف (200.000 دج) إلى خمسمائة ألف (500.000 دج) دينار جزائري وفي حال تسبب الكشف في وفاة أحد هؤلاء الأشخاص، تكون العقوبة الحبس من عشر (10) إلى عشرين (20) سنة وغرامة من خمسمائة ألف (500.000 دج) إلى مليون (1.000.000 دج) دينار جزائري" ويتم أيضًا حماية هوية العون بعدم

مطالبته بالإدلاء بشهادته، بل يكتفي ضابط الشرطة القضائية المسؤول عن العملية بالإدلاء بشهادته نيابة عنه[1].

الفرع الخامس: الحفظ والإفشاء العاجلان للمعطيات الإلكترونية

يُعد إجراء الحفظ والإفشاء العاجل للمعطيات الإلكترونية من بين الآليات الحديثة التي أقرها المشرع الجزائري للكشف عن الجرائم السيبرانية، حيث نصّ عليه في المادة 10 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ويُناط تنفيذ هذا الإجراء بمقدمي خدمات الإنترنت، من خلال قيامهم بحيازة المعطيات الإلكترونية وحفظها على شكل أرشيف، وذلك بغرض حماية محتواها من التلف أو التغيير أو فقدان صفتها الأصلية. وتُقدَّم هذه المعطيات إلى الجهات المختصة بالتحقيق فور طلبها، بما يضمن الحفاظ على الأدلة الرقمية وتمكين السلطات من استخدامها في إطار الإجراءات القضائية ذات الصلة[2]، ولهذا سنتطرق إلى مفهوم الحفظ العاجل لمعطيات السير **(أولا)** ثم ضمانات المشتبه فيه أثناء عملية حفظ معطيات المرور(**ثانيا)** ثم نتطرق إلى مفهوم الإفشاء العاجل لمعطيات المرور.

أولاً: مفهوم الحفظ العاجل لمعطيات السير

يُقصد بالحفظ العاجل للمعطيات الإلكترونية، استنادًا إلى ما سبق، قيام مزودي خدمات الاتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة، والعمل على حفظها وحيازتها ضمن أرشيف منظم، بهدف استخدامها لاحقًا من قبل الجهات المختصة بالاستدلال والتحقيق، ويتم هذا الحفظ وفق ترتيب معيّن يضمن الحفاظ على المعطيات من التلف أو التحريف أو ضياع صفتها الأصلية.

وتجدر الإشارة إلى أن طريقة تنفيذ عملية الحفظ أو الوسيلة التقنية المعتمدة لا تخضع لنموذج موحد، بل يُترك لكل دولة حرية اختيار النموذج القانوني والتقني الأنسب، على أن تُنفذ العملية وفق إطار قانوني يضمن فعاليتها واحترامها للحقوق الأساسية. كما ينبغي التنويه إلى أن الحفظ العاجل لا يشمل

[1] رابحي عزيزة، مرجع سابق ، ص 299

[2] بومحراث ليندة، إجراءات التحقيق الخاصة بالجرائم السيبيرانية، يوم دراسي حول الجريمة السيبيرانية، مجلس قضاء قسنطينة بالتعاون مع جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة ، 2022 ، ص 21

كافة أنواع المعطيات الإلكترونية، بل يقتصر على ما يُعرف بـ"**معطيات المرور**" أو "**حركة السير**"، وهي تلك التي عرّفها المشرع الجزائري في الفقرة الأخيرة من المادة 02 من القانون 09-04 بأنها:

"أية معطيات متعلقة بالاتصالات عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءًا في حلقة الاتصالات، توضح مصدر الاتصال، والوجهة المرسلة إليها، والطريق الذي يسلكه، وتاريخ ووقت الاتصال، وحجمه، ومدة الاتصال، ونوع الخدمة المستعملة".

وقد حدّد المشرع الجزائري في المادة 11 من القانون 09-04 معطيات المرور التي يتوجب حفظها، وهي:

- ✓ المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- ✓ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال (مثل الرقم التسلسلي ونوع الجهاز)
- ✓ الخصائص التقنية للاتصال، بالإضافة إلى تاريخه ووقته ومدته.
- ✓ المعطيات التي تسمح بالتعرف على المرسل والمرسل إليه (كأرقام الهواتف، عناوينIP ، الموقع الجغرافي)[1].

ويزداد تعقيد عملية الحفظ عندما ترتبط معطيات المرور بعدة مقدمي خدمات، حيث يحتفظ كلّ منهم بجزء من البيانات، مما يقتضي التنسيق بينهم لتجميع كافة المعطيات المطلوبة، ويتم ذلك إما بأوامر منفصلة موجهة لكل مقدم خدمة، أو بأمر موحّد يُبلّغ إليهم بالتتابع أو وفق نظام إخطار متسلسل بينهم.

ثانياً: ضمانات المشتبه فيه أثناء عملية حفظ معطيات المرور

نظرًا لما تنطوي عليه عملية الحفظ من مساس محتمَل بالحق في الخصوصية، فرض المشرع مجموعة من الضمانات القانونية التي يجب احترامها، سواء من قبل مقدمي الخدمات أو الجهات المخوّلة بالحفظ، ومن أبرزها:

[1] بن نعوم خالد أمين، مرجع سابق، ص ص 105- 107

1 احترام مدة الحفظ:

يُعد الحفظ العاجل تدبيرًا مؤقتًا تأمر به الجهة القضائية المختصة، ويُلزم مزود الخدمة بالاحتفاظ بالمعطيات الإلكترونية لمدة محددة. وقد حدد القانون 09-04 هذه المدة بسنة واحدة، تبدأ من تاريخ تسجيل المعطيات. وبانقضاء هذه المدة، يجب على مزود الخدمة حذف المعطيات أو اتخاذ ترتيبات تقنية تضمن عدم الاطلاع عليها حفاظًا على سريتها، وإلا تعرّض لعقوبات قد تكون إدارية أو جزائية، كما نصت المادة 11 في فقرتها الأخيرة من القانون المذكور سابقا على معاقبة المخالفين بالحبس من 6 أشهر إلى 5 سنوات وبغرامة مالية تتراوح بين 50.000 دج و500.000 دج.

1-2 الالتزام بسرية المعطيات وعمليات الحفظ:

يُلزم مقدمو الخدمات بكتمان كافة الإجراءات المتعلقة بعملية الحفظ وعدم إفشاء محتواها، إلا للسلطات القضائية المختصة. ويهدف هذا الالتزام إلى حماية الحياة الخاصة، ومنع التلاعب بالبيانات أو حذفها من قبل أطراف أخرى. ويُعد خرق هذا الالتزام إفشاءً لأسرار التحقيق، ويُعرض مرتكبه للمساءلة القانونية[1].

ثالثا: مفهوم الإفشاء العاجل لمعطيات المرور

يُعد الإفشاء العاجل لمعطيات المرور من الالتزامات القانونية التي تقع على عاتق مقدمي خدمات الإنترنت، وهو إجراء مكمل لعملية الحفظ العاجل للبيانات، الغاية منه مساعدة السلطات القضائية المختصة في التحقيق في الجرائم الإلكترونية. وقد نص المشرع الجزائري على هذا الالتزام صراحة في المادة 10 من القانون 09-04، التي جاء فيها:

"في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية، وذلك بوضع المعطيات التي يتعين عليهم حفظها وفقًا للمادة 11، تحت تصرف السلطات المذكورة".

وبذلك، فإن السلطة القضائية بعد إصدارها أمرًا بالحفظ العاجل لمعطيات المرور، يمكنها أن تلزم مقدمي الخدمات بالكشف الفوري عن تلك المعطيات، أو عن جزء منها، ووضعها تحت تصرف الجهات

[1] بن نعوم خالد أمين، مرجع سابق ، ص 107

المكلفة بالتحقيق. ويتم هذا الإجراء بشكل مستعجل قبل أن تُتلف البيانات أو يتم التلاعب بها، خاصة إذا كان الهدف هو تحديد مصدر الاتصال، مساره، والجهات التي ساهمت في تمريره.

ويمكّن هذا الإجراء سلطات التحري من كشف هوية الأطراف المتورطة في الاتصالات الإلكترونية المشبوهة، مما يساعد في تتبع مصدر الجريمة والوصول إلى مرتكبيها في الوقت المناسب[1].

[1] بن نعوم خالد أمين ، المرجع السابق ، ص 108

ملخص الفصل:

تعتبر مرحلة التحقيق في الجرائم المعلوماتية من أدقّ وأصعب المراحل في مسار العدالة الجنائية، نظرًا لما تتطلبه من معرفة تقنية دقيقة وإلمام بالوسائل الحديثة. ومن خلال هذا الفصل، تبيّن أن التحقيق الجنائي في هذا النوع من الجرائم يختلف عن التحقيق في الجرائم التقليدية، سواء من حيث المفهوم أو الخصائص، إذ أنه يتم في بيئة افتراضية ويعتمد على وسائل إلكترونية متطورة، مما يفرض توفر شروط وأدوات خاصة لإنجاحه. كما أظهر الفصل أهمية تحديد هوية المحقق الجنائي، وصفاته، والصعوبات التي يواجهها أثناء أداء مهامه، خاصة في ظل التطور السريع للتقنيات المستخدمة في ارتكاب هذه الجرائم. وفي الجانب العملي، تم التطرق إلى الأساليب المعتمدة في التحقيق، سواء التقليدية منها، كالضبط والتفتيش والاستجواب، أو المستحدثة، كالمراقبة الإلكترونية، واعتراض المراسلات، والتسرب وهو ما يكشف عن ضرورة تحديث المنظومة القانونية باستمرار، وتوفير الوسائل اللازمة للمحققين، من أجل التكيّف مع واقع الجريمة المعلوماتية وضمان تحقيق العدالة في ظل التحديات الرقمية المتزايدة.

الخاتمة

خاتمة

يُظهر تحليل مرحلة التحقيق في الجرائم المعلوماتية في ظل التشريع الجنائي الجزائري أنّ هذه المرحلة تتميز بطابع خاص، يفرضه اختلاف الجريمة المعلوماتية عن الجرائم التقليدية، سواء من حيث الوسائل المستعملة، أو طبيعة الجناة، أو طبيعة الأدلة التي تكون غالبًا رقمية، دقيقة، وسريعة التلف. هذا الواقع أوجب على السلطات القضائية والأمنية تطوير أساليبها، من خلال تعزيز الكفاءات البشرية وتوفير الوسائل التقنية اللازمة، قصد تمكين المحقق من أداء مهامه بكفاءة تتناسب مع طبيعة الجريمة.

وفي هذا الإطار، تدخل المشرّع الجزائري من خلال تعديل قانون العقوبات، بإضافة نصوص تجرّم أفعالًا مستحدثة تتعلق بالجريمة المعلوماتية، كما أدخل تعديلات على قانون الإجراءات الجزائية، تُمكّن جهات التحقيق من استخدام وسائل مستحدثة، كالتسرب، الاعتراض الإلكتروني، والتقاط الصور وتسجيل الأصوات. إلا أن هذه الإجراءات، على الرغم من أهميتها، تبقى بحاجة إلى مزيد من التكييف والضبط، خاصة من حيث التفاصيل الإجرائية والضمانات القانونية، بما يحقق التوازن بين فعالية التحقيق وحماية الحقوق الفردية، في ظل التحديات المتزايدة التي تفرضها الجرائم المعلوماتية.

ورغم الخطوات التشريعية التي تم اتخاذها، على غرار استحداث بعض النصوص في قانون العقوبات الجزائري، والتي تهدف إلى التصدي لمختلف صور الجريمة المعلوماتية، إلا أن واقع التحقيق يكشف عن نقائص متعددة، أبرزها قلة التخصص، وصعوبة التكييف القانوني للأفعال، ومحدودية الإمكانيات التقنية المتاحة للمحققين. كما أن غياب التنسيق الكافي بين الجهات القضائية والتقنية، وعدم وجود نصوص إجرائية تفصيلية تنظم مراحل التحقيق الرقمي، من شأنه أن يُضعف فعالية هذا التحقيق، ويؤثر سلبًا على الوصول إلى الحقيقة في الوقت المناسب.

ومن خلال دراستنا لمرحلة التحقيق في الجرائم المعلوماتية، تبيّن أنها تختلف فعليًا عن نظيرتها في الجرائم التقليدية، سواء من حيث طبيعة الأدلة المطلوب جمعها، أو من حيث الإجراءات الواجب اتباعها لضمان قانونية التحقيق وسلامة النتائج. فالجرائم المعلوماتية تُرتكب في فضاء افتراضي، وتتطلب أدوات تقنية ومعرفة متخصصة لا تفرضها الجرائم العادية، مما يجعل مراحل التحقيق فيها أكثر تعقيدًا، ويستلزم مقاربة مغايرة تتماشى مع طبيعتها الخاصة.

ومن خلال ما سبق، يمكن الخروج **بجملة من النتائج:**

- تتمتع الجريمة المعلوماتية بخصائص فريدة تجعلها مغايرة تمامًا للجرائم التقليدية، من حيث طابعها غير المادي، وارتكابها في بيئة افتراضية يصعب تعقب آثارها، بالإضافة إلى الطبيعة التقنية المعقدة لوسائل ارتكابها، وهو ما يستدعي مقاربة خاصة أثناء التحقيق.
- الإطار القانوني المعتمد في تنظيم التحقيق في هذا النوع من الجرائم لا يزال في طور التطوير، حيث قام المشرّع الجزائري بإدراج بعض الأحكام المتعلقة بالجرائم المعلوماتية ضمن قانون العقوبات وقانون

الإجراءات الجزائية، إلا أن هذه النصوص تبقى عامة في كثير من الأحيان وتفتقر إلى الدقة التقنية والإجرائية الكافية، ما يُضعف من فعاليتها في التطبيق العملي.

- تتنوع الجرائم المعلوماتية بين جرائم تُرتكب بواسطة الأنظمة المعلوماتية (كالاحتيال والابتزاز الإلكتروني)، وجرائم تمس بأمن الدولة أو بالأشخاص أو بالمؤسسات، ويشترط لقيامها توافر الأركان التقليدية للجريمة: الشرعي، المادي، والمعنوي، مع مراعاة الخصوصية الرقمية التي تميز العناصر المكوّنة لها.
- تعتمد مرحلة التحقيق في هذا النوع من الجرائم على وسائل وأدوات خاصة، تشمل الوسائل المادية كالمعاينة والتفتيش والضبط، ووسائل إجرائية وتقنية حديثة مثل الاعتراض الإلكتروني، التسرب، تسجيل الأصوات والتقاط الصور، والتي تتطلب تأهيلًا عاليًا للمحققين وقدرات تقنية متطورة.
- تختلف أساليب التحقيق التقليدية عن الأساليب المستحدثة من حيث طبيعتها وإجراءاتها، إذ لم تعد الأساليب التقليدية كافية لكشف مرتكبي الجرائم المعلوماتية بسبب قدرتهم على إخفاء هويتهم، مما استدعى إدماج وسائل رقمية متقدمة تتيح تعقّبهم إلكترونيًا، وهو ما شكّل نقلة نوعية في آليات التحري والاستدلال.

أما بالنسبة إلى **التوصيات أو الإقتراحات** التي نراها ضرورية فتتمثل فيما يلي:

- ضرورة إصدار تشريع خاص بالتحقيق في الجرائم المعلوماتية، يتضمن قواعد إجرائية دقيقة تراعي خصوصية هذا النوع من الجريمة.
- إدماج وحدات متخصصة في التحقيق الرقمي ضمن هيئات الشرطة والقضاء، وتوفير تكوين مستمر ومكثف لها.
- تجهيز المخابر التقنية بالأدوات اللازمة لتحليل الأدلة الرقمية وفق معايير علمية دقيقة ومعترف بها دوليًا.
- تشجيع التعاون بين الخبراء القانونيين والتقنيين لإنشاء بيئة تحقيق متكاملة.
- تطوير آليات التعاون الدولي من خلال اتفاقيات ثنائية ومتعددة الأطراف، لتسهيل تبادل المعلومات وتوحيد إجراءات الملاحقة.
- تعزيز الوعي القانوني والتقني لدى مختلف الفاعلين في المنظومة القضائية حول خصوصيات الجريمة المعلوماتية.
- تشجيع البحوث العلمية والجامعية التي تتناول التحقيق الرقمي، وتوفير الدعم لها باعتبارها ركيزة أساسية للتطوير المستقبلي.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

اولا: القران الكريم

1. سورة البقرة
2. سورة الأحزاب

ثانيا: الاتفاقيات

1. إتفاقية بودابست المتعلقة بالجريمة المعلوماتية ، المادة 19 الفقرة 4 ،الموقعة في بودابست بتاريخ 23 نوفمبر 2001

ثالثا: النصوص القانونية

1. الأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية ، العدد 49، سنة 1966
2. القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المتعلق بقمع الجرائم المرتبطة بتكنولوجيات الإعلام والإتصال، الجريدة الرسمية ، العدد 71 ، سنة 2004
3. القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 ، المعدل والمتمم للأمر رقم 155/66 المؤرخ في 8 جوان 1966، والمتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية ، العدد 84
4. القانون رقم 09-04 الصادر بموجب دستور 1996 ، المؤرخ في 5 أوت 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد 47 ، الصادرة بتاريخ 2009/08/05
5. القانون رقم 24-06 ، المؤرخ في 28 أفريل 2024، المتضمن الوقاية من الجرائم السيبرانية ومكافحتها، الجريدة الرسمية العدد 30 السنة 1961

رابعا: الكتب

1. أحمد عرابي ، التحقيق الجنائي، الطبعة الأولى، مدار لخدمات التصميم الفني والمطبوعات ، دبي ، 2021
2. حسن الجوخدار ، التحقيق الإبتدائي في قانون الأصول المحاكمات الجزائية، دارالثقافة ،عمان ، الطبعة الأولى ،2008

3. حسين بن سعيد الغافري ، السياسة الجنائية لجرائم الإنترنت (دراسة مقارنة) ، دار النهضة العربية ، القاهرة ، 2006
4. علي عدنان الفيل ، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث ، الإسكندرية- مصر- 2012
5. مجيد خضر السبعاوي ، مولان قادر أحمد، الضرورة الإجرائية في مرحلة التحقيق الإبتدائي (دراسة تحليلية مقارنة) المركز القومي للإصدارات القانونية، القاهرة ، 2017
6. محمد ظاهر ، تنظيم التحقيق الإبتدائي في الجرائم ، دار وائل للنشر ، عمان ، الطبعة الأولى 2013
7. مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الأولى ، مطابع الشرطة ، القاهرة ، 2008
8. نبيلة هبة هروال، الجوانب الإجرائية في جرائم الإنترنت في مرحلة جمع الإستدلالات ،الطبعة الأولى دار الفكر الجامعي ، الإسكندرية، 2007

خامسا: الرسائل الجامعية

1 أطروحات الدكتوراه

1. جمال براهيمي ، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018
2. حسين ربيعي ، أليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2015 - 2016
3. خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة
4. خضرة شنتير ، الأليات القانونية لمكافحة الجريمة المعلوماتية ، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية ، أدرار ، 2020-2021
5. عزيزة رابحي ، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه في علوم القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2017-2018

6. فوزي عمارة ، قاضي التحقيق ، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم ، كلية الحقوق، جامعة الإخوة منتوري ، قسنطينة ، 2009-2010
7. نصيرة بوحزمة ، التحقيق الجنائي في الجرائم الإلكترونية ، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية ، قسم الحقوق، جامعة الجيلالي اليابس، سيدي بلعباس، 2021-2022

2 رسائل الماجيستير:

1. عبد اللطيف معتوق ، الإطار لقانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجستير في العلوم القانونية ، كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر ،باتنة ، 2011-2012
2. ليلى لفويلي ، الجريمة الإلكترونية، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، كلية الحقوق، جامعة قسنطينة 1 ، 2012-2013
3. نورة طرشي ، مكافحة الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011-2012

3 مذكرات الماستر:

1. إبراهيم زياد بوعرعارة ، خصوصية الجريمة المعلوماتية، مذكرة ماستر في الحقوق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة غرداية-الجزائر- 2021-2022
2. أحمد عبد العزيز ، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي، سعيدة، 2021-2022
3. أحمد ياسين بركاني ، عبادلي فاطمة الزهراء، وسائل وأدلة الإثبات في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة1 ، 2016-2017
4. أمين شعيب بوعوينة ، مهلب حمزة ، إختصاصات الضبطية القضائية في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية ، قسم القانون الخاص ، جامعة عبد الرحمان ميرة ، بجاية ،2012-2013

5. بجاد عبد الرؤوف بوديسة ، أليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق ، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج ، 2021-2022
6. بريزة عقباش ، حنان مبارك ، أليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، ، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج ، 2021-2022
7. جميلة غربي ، أليات مكافحة الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون، كلية الحقوق والعلوم السياسية، ، قسم القانون العام ، جامعة أكلي محند أولحاج ، البويرة ، 2020-2021
8. خالد أمين بن نعوم ، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون قضائي، كلية الحقوق والعلوم السياسية، قسم قانون خاص، 2018-2019
9. رانيا بن داني ، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، قسم قانون عام، جامعة عبد الحميد بن باديس، مستغانم ، 2022-2023
10. راوية بوحفص ، الجريمة المعلوماتية في التشريع الجزائري ، مذكرة لنيل شهادة الماستر في الحقوق ، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة ، 2017-2018
11. سعيدة بعرة ، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2015-2016
12. سيهام بن عنطر ، التحقيق الجنائي في الجرائم الإلكترونية ، مذكرة لنيل شهادة الماستر في القانون ، كلية الحقوق والعلوم السياسية، قسم الحقوق ، جامعة مولود معمري ، تيزي وزو ، 2023
13. شهيرة مسعود ، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد بن باديس ، مستغانم ، 2020-2021

14. شيماء كريمي ، محسن شروق، دور القضاء الجنائي في الحد من الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق، القسم الخاص، جامعة الإخوة منتوري، قسنطينة 1 ، 2023-2022

15. شيماء نور الهدى بوسنة ، بن سلامة كوثر، البحث والتحري في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق، قسم القانون الخاص، جامعة الإخوة منتوري ، قسنطينة1 ، 2023-2022

16. صهيب بلفيحج ، حمادي عبد الكريم عماد، أليات مكافحة الجرائم السيبرانية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق، قسم القانون الخاص، جامعة الإخوة منتوري، قسنطينة، 2022-2023

17. صونيا كحيو ، بن الشيخ الفقون محمد سليم برهان الدين، إجراءات المتابعة الجزائية للجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر، كلية الحقوق، قسم القانون الخاص، جامعة الإخوة منتوري ، قسنطينة1 ، 2018-2019

18. عادل سعيد فكرون ، الجرائم المعلوماتية الواقعة على الحق في الخصوصية، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور-الجلفة- ، 2018-2019

19. عائشة نايري ، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الإداري، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أحمد دراية -أدرار- ، 2017-2016

20. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية العلوم الإقتصادية وعلوم التسيير، قسم علوم التسيير، جامعة قاصدي مرباح ، ورقلة، 2018-2019

21. فريال لعاقل ، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أكلي محمد أولحاج -البويرة- ، 2015-2014

22. محمد بوعمرة ، سيد علي بنينال ،جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري ، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية ، كلية الحقوق والعلوم السياسية ، قسم القانون الخاص، جامعة أكلي محند أولحاج-البويرة ، 2019-2020

23. محمد ياسين عباسة ، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق ، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس–مستغانم– ، 2020–2021

24. مريم بلغفور ، عتروز صليحة ، أليات البحث والتحقيق في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر في القانون، كلية الحقوق، قسم القانون الخاص ، جامعة الإخوة منتوري ، قسنطينة، 2016–2015

25. يوسف صغير ، الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ، 2013

سادسا: المقالات

1. اسمهان بن مالك ، خصائص الجريمة المعلوماتية وأسباب إرتكابها، مجلة البيان للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية حمد امين دباغين سطيف، السنة 2019

2. أيت حمودة كاهنة، البحث والتحري الجنائي في مسرح الجريمة الإلكترونية، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية جامعة عمار ثلجي الأغواط ، المجلد السابع ، العدد الأول ، 2023

3. حسان ربيعي ، المجرم المعلوماتي شخصيته وأصنافه، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، العدد 40 ، جوان 2015

4. حسين فريجة ، الجرائم الإلكترونية والإنترنت، السعودية، مجلة المعلوماتية، دار المنظومة، العدد36، أكتوبر 2011

5. حمزة عشاش ، حمز خضري، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية ، جامعة محمد بوضياف المسيلة، المجلد 06 العدد 02 جوان 2020

6. حيمي سيدي محمد، معوقات التحقيق الجنائي في الجرائم الإلكترونية، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة أبو بكر بلقايد تلمسان ، المجلد السادس، العدد الأول، 2020

7. راضية عيمور، الجريمة الإلكترونية وأليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية ، مخبر الحقوق والعلوم السياسية، ، المجلد 06، العدد الأول، 2022

8. سورية ديش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي ، ،العدد الأول، يناير 2018

9. صابر بحري ، منى خرموش ، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية، مجلة دراسات في سيكولوجية الإنحراف ، جامعة محمد لمين دباغين سطيف 2 ، المجلد 07، العدد01، السنة 2021
10. عز الدين عثماني ، إجراءات التحقيق والتفتيش في الجرائم المحاسبة بأنظمة الإتصال والمعلوماتية ، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية بجامعة تبسة ، العدد الرابع، 2018
11. عماد بلغيث، يوسف جغلولي ، صعوبات التحقيق في الجرائم الإلكترونية، مجلة الرسالة للدراسات والبحوث الإنسانية، مخبر سوسيولوجية جودة الخدمة العمومية ، الجزائر ، المجلد 06، العدد 03، سبتمبر 2021
12. مراد مشوش ،بن شهرة شول ، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية والسياسية، جامعة غرداية، المجلد 04، العدد01، جوان 2020
13. نوال مجدوب، الأليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والإقتصادية، المركز الجامعي مغنية، ، المجلد 06، العدد 03، 2023
14. هند نجيب، ضبط الأدلة في الجرائم الإلكترونية بين الإجراءات التقليدية والإجراءات الحديثة، المجلة الجنائية القومية، المركز القومي للبحوث الإجتماعية والجنائية، المجلد 61، العدد 03 ، نوفمبر 2018

سابعا: الايام الدراسية

1. بومحراث ليندة، إجراءات التحقيق الخاصة بالجرائم السيبيرانية، يوم دراسي حول الجريمة السيبيرانية، مجلس قضاء قسنطينة بالتعاون مع جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة ، 2022

ثامنا: المحاضرات

2. بطيحي نسمة، محاضرات في مقياس الوقاية من الجرائم الإلكترونية، كلية الحقوق والعلوم السياسية، قسم الحقوق ، جامعة محمد لمين دباغين ، سطيف 2 ، 2012-2022

الفهرس

الملخص

تطرح الجريمة المعلوماتية العديد من التحديات القانونية والتقنية، باعتبارها من الجرائم المستحدثة التي ارتبط ظهورها بتطور وسائل الاتصال الحديثة والتوسع في استخدام الأنظمة المعلوماتية. فقد أصبحت هذه الجريمة تمس الأفراد، المؤسسات، وحتى أمن الدول، ما فرض على المشرّع ضرورة مواكبة هذا التطور بوضع نصوص قانونية وآليات تحقيق ملائمة.تهدف هذه الدراسة إلى تسليط الضوء على الإشكاليات التي تطرحها الجريمة المعلوماتية من حيث طبيعتها وخصائصها، وأنواعها المختلفة، إضافة إلى تحليل مرحلة التحقيق فيها، انطلاقاً من شروطه، وأساليبه، ووسائله التقليدية والمستحدثة، مع التركيز على دور المحقق وصفاته والصعوبات التي تواجهه أثناء ممارسة مهامه، وقد اعتمدت الدراسة على منهج وصفي تحليلي، في ضوء التشريع الجنائي الجزائري، من أجل محاولة الإحاطة بجوانب هذه الظاهرة المعقدة، والمساهمة في إبراز أهمية تعزيز الإطار القانوني والمؤسساتي للتعامل مع هذه الجرائم بشكل فعّال.

الكلمات المفتاحية: الجريمة المعلوماتية، التحقيق، التشريع الجنائي الجزائري، مرحلة التحقيق

Abstract:

Cybercrime raises numerous legal and technical challenges, being a modern crime that emerged alongside the development of communication technologies and the growing use of information systems. It now affects individuals, institutions, and even state security, prompting lawmakers to adopt appropriate legal texts and investigative mechanisms.This study aims to highlight the complexities surrounding cybercrime, including its nature, characteristics, and various types. It also analyzes the investigation phase, focusing on its conditions, methods, and both traditional and modern tools, while emphasizing the role and qualities of the investigator and the difficulties faced during the process.The research adopts adescriptive and analytical approach within the framework of Algerian criminal legislation, seeking to explore the different dimensions of this complex phenomenon and underline the importance of strengthening legal and institutional frameworks to effectively combat such crimes.

Keywords: Cybercrime, Investigation, The Algerian Criminal Legislation, The Investigation Phase.