المركز الجامعي صالحي أحمد بالنعامة

معهد الحقوق

قسم الحقوق

مذكرة تخرج لنيل شهادة الماستر

تخصص قانون جنائي و العلوم الجنائية

إجراءات التحقيق والتفتيش في الجريمة الإلكترونية

إعدد الطلبة

- سايح عبد الباسط.
- طالبي محمد.

تحت إشراف

- أ . د براهيمي سهام.

لجنة المناقشة

- د-حشيفة مجدوب..... رئيسا.
- أ . د براهيمي سهام.....مشرفا.
- د-كبير أمين .....مناقشا.

السنة الجامعية: 2023 / 2024

"وقل ربي زدني علما"

الشـــكـــروعـــرفـــان

الحمدُ لله على نعمة العلم، كل عظيم شكري وامتناني للمولى عز وجل مصداقاً لقوله تعالى: "**وَلَئِنْ شَكَرْتُمْ لَأَزِيدَنَّكُمْ**".

أما بعد يشرفنا أن نتقدم بالشكر الجزيل والعرفان إلـــى الأستاذة دكتورة المشرفة " **براهيمي سهام**" على تفضلها بالإشراف على هذه المذكرة وكل المجهودات التي بذلتها والتي كانت ثمارها إنجاز هذا العمل حيث لم تبخل علينا بالتوجيه والنصيحة إلى آخر لحظة.

كما لا ننسى في هذا المقام تقديم الشكر للدكتورين "**حشيفة مجدوب**" و "**كبير أمين**".

إهـــداء

قال تعالى: "**قل اعملوا فسيرى الله عملكم ورسوله والمؤمنين**"

نشكر الله ونحمده حمدا كثيرا مباركا على هذه النعمة الطيبة والنافعة نعمة العلم والبصيرة

إلى روحك أبي الغالي.

إلى أمي، حفظها الله وأطال في عمرها.

إلى زوجتي سندي والشمعة التي تنير دربي وحياتي.

إلى أبنائي منصف الدين، مهتدى تاج الدين وميار.

عبد الباسط

الإهداء

الحمد لله الذي هدانا لهذا وما كنا لنهتدي لولا أن هدانا الله نحمده حق حمده الذي وفقنا لإتمام هذا العمل المتواضع الذي نرجوا أن يكون خالصا لوجهه، وأن ينفعنا به وأن غيرنا فيه منفعته.

نهدي ثمرة جهدنا إلى أبي العزيز رحمه لله الذي له كل الفضل وأمي التي سهرت على نجاحي وإلى كل إخوتي، وإلى زوجتي ورفيقة دربي وإلى أبنائي ألاء هبة الرحمان هاجر طه همام وعلي أنس.

واخص الشكر للأستاذة الفاضلة الأستاذة **الدكتورة براهيمي سهام التي لم تذخر جهدا في مساعدتنا.**

كما لا نسى زميلي ورفيقي في المذكرة سايح عبد الباسط الذي كان نعم الأخ والصديق والسند.

كما لا أنسى أصدقائي حاج عبد المجيد وحاج عبد القادر بومدين اللذان كان دائما إلى جانبي.

طالبي محمد.

مقدمة

مقدمة:

في الفترة الأخيرة، دخل العالم مرحلة جديدة من التطور الفكري والمعرفي الهائل والغير مسبوق، وذلك بفضل التطور العلمي في مجال تكنولوجيا الإعلام والاتصال. وقد أفرز هذا التطور مناخًا خصبًا لنهضة علمية تكنولوجية شاملة غير مسبوقة في جميع مجالات الحياة الاقتصادية، الاجتماعية، الثقافية، والعلمية. لا شك أن هذه الثورة المعلوماتية الهائلة قد إنعكست بصورة إيجابية على العديد من جوانب الحياة المعاصرة، نظرًا لتوفيرها الوقت والجهد والتكلفة، مما جعل الحياة اليومية أكثر سهولة، وقد أصبح جهاز الكمبيوتر وسيلة لا يمكن الاستغناء عنها في حياتنا اليومية.

على الرغم من التقدم العلمي الهائل والمستمر في جميع المجالات، إلا أن هذه الثورة التكنولوجية جلبت معها أيضًا تحديات وانعكاسات سلبية خطيرة. فقد أدى الاستخدام المفرط للتكنولوجيا إلى استخدامها في أغراض غير مشروعة، مما أسفر عن ظهور ظاهرة جديدة من الجريمة في العالم الافتراضي تعرف بـ "الجريمة الإلكترونية"، وهي واحدة من أخطر وأعقد أشكال الجريمة التي يتم مواجهتها في الوقت الحاضر.

الجريمة الإلكترونية هي جريمة سرية تقنية، يتم ارتكابها في الخفاء وفي بيئة إلكترونية افتراضية، حيث يستخدم المرتكبون الحواسيب وشبكة الإنترنت في تنفيذ أفعالهم. يتمتع مرتكبو هذه الجرائم بالذكاء والمهارات التقنية العالية، وعادةً ما يكونون غير عدوانيين ولا يتمتعون بالعنف. تتميز الجريمة الإلكترونية بعدة خصائص تميزها عن الجريمة التقليدية، حيث تكون عابرة للحدود وتتم عبر شبكة اتصال لامتناهية وغير مرئية. إثبات هذه الجرائم يشكل تحديًا نظرًا لعدم ترك آثار خارجية وصعوبة العثور على دليل مادي. وتتكون الجريمة الإلكترونية من أركان متشابهة مع الجريمة التقليدية، مثل الركن الشرعي والركن المادي. في الجريمة الإلكترونية، يتجلى الركن المادي في السلوك الجرمي، والنتيجة الجرمية، والعلاقة السببية بينما يتجسد الركن المعنوي في الإرادة الجنائية لدى الفاعل وتوجيه هذه الإرادة للقيام بأعمال غير مشروعة.

التمييز بين الجرائم الإلكترونية والجرائم التقليدية إجرائيًا يعتبر أمرًا هامًا للغاية، سواء من حيث الاختصاص أو إجراءات التحقيق أو وسائل الإثبات. في التحقيق في الجرائم الإلكترونية، تتخذ النيابة موقفًا متخصصًا وتتبع إجراءات وقواعد إثبات محددة، ويساعدها في ذلك ضباط قضائيون متخصصون في هذا المجال. بالمقابل، في الجرائم التقليدية، يتم التحقيق فيها بواسطة النيابة العامة بمساعدة ضباط قضائيين ذوي اختصاص عام، وفقًا لقواعد التحقيق والإثبات التقليدية.

ونظرا لخصوصية الجريمة كونها ترتكب في بيئة رقمية فإنه بات من الضروري وضع إطار قانوني مع تطوير أساليب التحقيق الجنائي وإجراءات فعالة تمكن جهات التحقيق من كشف الجريمة، معاينتها، جمع الأدلة وإجراء الخبرة اللازمة للتعرف على مرتكبيها وتقديمهم أمام العدالة.

الأمر الذي سعى المشرع الجزائري إلى تجسيده من خلال استحداث نصوص قانونية أوجد بموجبها قواعد إجرائية تتماشى والطبيعة التنفيذية للجريمة المعلوماتية أين يشكل التحقيق الإلكتروني إحدى أهم الإجراءات التي جاء بها القانون رقم: 09-04 المؤرخ في: 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

إشكالية البحث:

- ما مدى خصوصية التحقيق في الجريمة الإلكترونية؟

اهمية البحث:

أهمية الدراسة في مجال التحقيق والتفتيش في الجريمة الإلكترونية تتجلى في الضغوط المتزايدة التي تواجه الأجهزة القضائية نتيجة لتطور التكنولوجيا واستخدامها في ارتكاب الجرائم. فالتحقيق في الجرائم الإلكترونية يتطلب فهمًا عميقًا للتقنيات والأساليب المستخدمة في هذا المجال، واتباع الإجراءات القانونية الصحيحة لجمع الأدلة بطريقة قانونية وموثوقة. تعتمد فعالية التحقيق والتفتيش في هذا السياق على تحديث المعرفة والمهارات المتعلقة بالتحقيق الرقمي وبالتالي يلعب الدور المعرفي دورًا مهمًا في تزويد الأفراد بالمعارف اللازمة لمواجهة هذه التحديات وتحقيق العدالة بشكل أكثر فعالية.

اهداف البحث:

هدف هذه الدراسة إلى تسهيل إجراءات التحقيق وتطوير السياسات الملائمة لضمان فعالية التحقيق في مجال الجرائم الإلكترونية. بالإضافة إلى ذلك، تهدف الدراسة إلى استكشاف وتحليل العوامل المؤثرة في نجاح التحقيقات الجنائية، وتقديم الحلول لتخطي الصعوبات والتحديات التي تعترض تحقيق العدالة في هذا النطاق. من خلال فحص هذه العوامل، يمكن تحسين العمليات التحقيقية وتطوير استراتيجيات أكثر فاعلية لمكافحة الجريمة الإلكترونية وتحقيق نتائج إيجابية في هذا المجال.

اسباب اختيار الموضوع:

1. الأسباب الذاتية:

-الرغبة والميل في معرفة ودراسة هذا النوع من الجرائم واكتشاف الأسباب والدوافع من وراء اقترافها مقارنة بالجرائم التقليدية الأخرى.

-غموض الجرائم الإلكترونية يجعلها مجالا مثيرا للبحث بالنظر للخصوصية التي تتميز بها من خطورة وصعوبة الكشف عنها وإثباتها.

2. الأسباب الموضوعية:

-انتشار حالات الجرائم الإلكترونية مع ضرورة فهمها ومكافحتها.
-تطور التكنولوجيا وانعكاسه على اجراءات التحقيق والتفتيش.
-أهمية حماية البيانات الشخصية والأمن الرقمي.
-غاية التحقيق في الجرائم الإلكترونية وضرورة تحقيقها.

المنهج المتبع:

نظرًا لطبيعة الموضوع وخصوصيته القانونية، التي تتطلب اعتماد منهج شامل يسلط الضوء على جوانبه المختلفة، فقد اعتمدنا المنهج الوصفي التحليلي. ويتضمن هذا المنهج تحليل النصوص القانونية المتعلقة بالموضوع، والاستناد إلى الأبحاث والمراجع القانونية السابقة، بالإضافة إلى جمع الحقائق والبيانات ذات الصلة وتحليلها بشكل دقيق. من خلال هذا المنهج، نسعى إلى فهم عميق لتفاصيل الموضوع وتقديم تحليل شامل يعكس تعقيداته وتحدياته القانونية بدقة ووضوح.

الصعوبات:

تتضمن صعوبات متعددة تحيط بهذا الموضوع، والتي ترجع أساسًا إلى حداثة الجانب العلمي له وتفرده في مجال القانون. فعلى الرغم من أهمية الجريمة الإلكترونية، إلا أنها لم تحظَ بالاهتمام الكافي في البحث والدراسة في ميدان القانون، مما ينتج عنه ندرة المراجع والمؤلفات التي تتناول الجوانب الإجرائية للتحقيق والتفتيش في هذا النوع من الجرائم. وتركز معظم الدراسات القانونية المتعلقة بالجريمة الإلكترونية على الجوانب الموضوعية فقط، مما يجعل هذا المجال متحديًا ومثيرًا للاهتمام بالنسبة لنا كباحثين، ويشجعنا على الاهتمام بالجوانب الإجرائية والقانونية لهذا النوع من الجرائم.

تقسيمات الموضوع:

تم تقسيم الموضوع إلى فصول ومباحث فرعية لتسهيل فهمه وتنظيم المعلومات بشكل منطقي ومنظم. يتناول الفصل الأول الإطار المفاهيمي للتحقيق والتفتيش في الجريمة الإلكترونية، حيث يتم تقسيمه إلى مباحث فرعية تتناول مفهوم مرحلة التحقيق والتفتيش، وتعريفها وشروطها في الجرائم الإلكترونية، بينما يتناول الفصل الثاني آليات التحقيق في الجرائم الإلكترونية، حيث يتم تقسيمه إلى مباحث تتناول إجراءات الحصول على الدليل الإلكتروني وقيمته القانونية. هذا التقسيم يسهل فهم المفاهيم المختلفة ويوفر تنظيمًا هرميًا للموضوع يسهل المراجعة والاستفادة منه.

الفصل الأول: الإطار المفاهيمي التحقيق والتفتيش الجريمة الإلكترونية

تمهيد:

يُعد التحقيق والتفتيش في الجريمة الإلكترونية مجالًا متطورًا وحيويًا يتطلب فهمًا عميقًا للتحديات والتطورات التكنولوجية والقانونية. يأتي هذا الفصل ليقدم لنا الإطار المفاهيمي الضروري لفهم مفاهيم التحقيق والتفتيش في سياق الجرائم الإلكترونية. من خلال استكشاف مفهوم مرحلة التحقيق والتفتيش وتحليل شروطها وخصائصها، نتطلع إلى فهم أعمق لعملية التحقيق في هذا المجال المتطور. كما سنقوم بتسليط الضوء على مفهوم الجريمة الإلكترونية وأساسياتها، مما سيسهم في بناء قاعدة معرفية قوية تمكننا من الانتقال إلى دراسة آليات التحقيق الفعّالة في الفصل الثاني.

المبحث الأول: مفهوم مرحلة التحقيق والتفتيش

يُعتبر التحقيق والتفتيش من المراحل الأساسية في عمليات البحث الجنائي والقضائي، حيث تلعب هذه المرحلة دورًا حاسمًا في جمع الأدلة وتحديد الحقائق المتعلقة بالقضايا المطروحة. هذه المرحلة تتطلب دقة واحترافية عالية لضمان صحة وسلامة الإجراءات المتبعة، مما يضمن تحقيق العدالة وحماية الحقوق. ولأهمية هذه العملية، فقد تناولها العديد من العلماء والباحثين بالدراسة والتحليل لتطوير أفضل الممارسات والأساليب التي يمكن استخدامها في الميدان.

في هذا المبحث، سنتناول مفهوم مرحلة التحقيق والتفتيش من حيث التعريف اللغوي والاصطلاحي، وسنسلط الضوء على أهمية هذه المرحلة في النظام القضائي، وأهدافها، والأساليب المتبعة فيها، بالإضافة إلى التحديات التي قد تواجه المحققين والمفتشين خلال أداء مهامهم. فهم هذه المرحلة بشكل دقيق يساعد على تطبيق القانون بشكل أكثر فعالية ويعزز من نزاهة وشفافية العملية القضائية.

المطلب الأول: تعريف مرحلة التحقيق والتفتيش

تُعتبر مرحلة التحقيق والتفتيش من أهم المراحل التي تسبق اتخاذ القرارات النهائية في الإجراءات القانونية والقضائية. خلال هذه المرحلة، يتم جمع المعلومات والأدلة اللازمة لكشف الحقيقة حول الوقائع المدروسة. تتسم هذه المرحلة بالدقة والحرص الشديد، إذ يتطلب الأمر استخدام مختلف الأدوات والأساليب العلمية والعملية للوصول إلى الحقائق بشكل موضوعي ومحايد.

في هذا المطلب، سنقدم تعريفًا مفصلًا لمرحلة التحقيق والتفتيش، حيث سنشرح التعريفين اللغوي والاصطلاحي لكل من التحقيق والتفتيش، مع توضيح الفروقات بينهما. سنستعرض أيضًا أهمية هذه المرحلة في النظام القضائي والدور الذي تلعبه في ضمان تحقيق العدالة وكشف الحقائق. فهم هذه المرحلة بدقة يساعد على تطبيقها بشكل صحيح ويعزز من تطوير آلياتها بما يتماشى مع المتطلبات القانونية والمهنية.

الفرع الأول: التعريف اللغوي والاصطلاحي لتحقيق

- **التعريف اللغوي:**

كلمة "تحقيق" مشتقة من الجذر الثلاثي "حقَّ"، والذي يعني التأكد والتثبت من صحة شيء ما. وفي المعاجم اللغوية، يقال "حقَّق الشيء" أي دقَّق فيه وأثبته، و"تحقيق" تعني التثبت والتدقيق.[1]

- **التعريف الاصطلاحي:**

في الاصطلاح، يشير "التحقيق" إلى العملية المنهجية التي تهدف إلى إخراج النصوص القديمة والمخطوطات بصورة دقيقة وصحيحة. هذه العملية تتجاوز مجرد نقل النص، إذ تشمل سلسلة من الخطوات الدقيقة والمتأنية لضمان دقة وموثوقية النص المنشور. تبدأ عملية التحقيق بجمع النسخ المختلفة للمخطوط قيد الدراسة. يُعد جمع النسخ المختلفة من أهم الخطوات الأولى

[1] ابن منظور، محمد بن مكرم. لسان العرب. تحقيق: عبد الله علي الكبير، محمد أحمد حسب الله، هاشم محمد الشاذلي. دار صادر، بيروت، الطبعة الأولى، 1955، الجزء 10، صفحة 25.

في عملية التحقيق، حيث يسعى المحقق إلى الحصول على أكبر عدد ممكن من النسخ الأصلية أو المنسوخة التي قد تحتوي على اختلافات أو تصحيحات مهمة.[1]

بعد جمع النسخ، تأتي مرحلة المقارنة بينها، وهي عملية دقيقة يقوم فيها المحقق بمقارنة النصوص المختلفة لتحديد الفروق والاختلافات بينها. تساعد هذه المقارنة في الكشف عن الأخطاء والتحريفات التي قد تكون حدثت خلال النسخ اليدوي على مر العصور. من خلال هذه العملية، يمكن للمحقق تحديد النص الأقرب إلى الأصل وضبط النصوص بناءً على ذلك، مما يساهم في إنتاج نسخة أكثر دقة وموثوقية من النص الأصلي.[2]

ثم تأتي مرحلة التثبت من النصوص، وهي مرحلة حاسمة يتأكد فيها المحقق من صحة النصوص عبر الرجوع إلى مصادرها الأصلية والموثوقة. في هذه المرحلة، يستخدم المحقق مجموعة من الأدوات والموارد مثل المراجع التاريخية واللغوية والأدبية لضمان صحة النصوص. يمكن هذا التثبت المحقق من استبعاد النصوص المشكوك فيها أو التي قد تكون تعرضت للتحريف، مما يضمن أن النسخة النهائية تكون دقيقة وموثوقة.

بعد ذلك، يضيف المحقق الشروح والتعليقات الضرورية. في هذه المرحلة، يقوم المحقق بشرح وتوضيح النصوص الغامضة، وتعديل النصوص وتوضيح المعاني. هذه الشروح والتعليقات تساعد القارئ على فهم النص بشكل أفضل وتوفير سياق أوسع للنصوص المعروضة.[3]

وأخيراً، يتم إعداد النسخة النهائية للنشر. في هذه المرحلة، يقوم المحقق بإعداد النسخة النهائية وإضافة الهوامش والتعليقات الضرورية. قد تتضمن هذه الهوامش ملاحظات حول

[1] الزركلي، خير الدين. الأعلام: قاموس تراجم لأشهر الرجال والنساء من العرب والمستعربين والمستشرقين. دار العلم للملايين، بيروت، الطبعة الخامسة، 1980، المجلد 1، صفحة 300.

[2] الزبيدي، مرتضى الحسيني. تاج العروس من جواهر القاموس. دار الهداية، القاهرة، 1965، الجزء 1، صفحة 50.

[3] المرعشي، عبد الكريم. أصول التحقيق في التراث العربي. دار الغرب الإسلامي، بيروت، الطبعة الأولى، 1989، صفحة 45.

الاختلافات بين النسخ، وتفسيرات للشروح، وإشارات إلى المصادر والمراجع المستخدمة. تمثل النسخة النهائية خلاصة عمل المحقق وجهوده لضمان تقديم نص دقيق وموثوق يمكن الاعتماد عليه في الدراسات الأكاديمية والبحثية.

الفرع الثاني: تعريف التفتيش في الجرائم الإلكترونية

قبل الحديث عن مفهوم التفتيش، يجدر بنا الإشارة إلى أن المشرع الجزائري لم يضع تعريفًا تشريعيًا للتفتيش الإلكتروني في القانون رقم 04/09، بل اكتفى بتنظيم أحكامه وضوابطه وترك تعريفه للفقه. وبالرجوع إلى التعريفات الفقهية، يقصد بالتفتيش بشكل عام "البحث عن أشياء تفيد في الكشف عن جريمة وقعت ونسبتها إلى المتهم"، أو هو "إجراء من إجراءات التحقيق يهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في مكان يتمتع بحرمة المسكن أو الشخص، وذلك بهدف كشف الجريمة أو نسبتها إلى المتهم وفقًا للإجراءات القانونية المحددة.[1]

يعد التفتيش الإلكتروني إجراءً مستحدثًا في مجال الجرائم الإلكترونية نظرًا لحداثة هذه الجرائم، لكنه يبقى إجراءً معروفًا منذ القدم. ومن بين أهم التعريفات التي أجمع عليها الفقه الجنائي: "أن التفتيش، كإجراء من إجراءات التحقيق، يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في مكان يتمتع بالحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقًا للضمانات والضوابط المقررة قانونًا.[2]

[1] هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، سنة 1997، صفحة 47.

[2] عبد الفتاح بيومي حجاري، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي، مصر، 2006، صفحة 192.

كما عُرّف التفتيش أيضاً على أنه البحث في مستودع سر المتهم عن أشياء تفيد في كشف الحقيقة ونسبتها إليه، أو الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، سواء كان هذا المحل مسكناً أو ما في حكمه أو كان شخصاً.[1]

أما تعريف التفتيش الإلكتروني أو التفتيش في البيئة الافتراضية فقد اختلف الفقه حول مصطلحه، حيث اعتبره البعض ينصب على أنظمة وبرامج أو مواقع صفحات إلكترونية، وبالتالي المصطلح الأدق هو "الولوج" أو "النفاذ". في حين فضل اتجاه آخر الإبقاء على مصطلح "التفتيش" كونه عامًا يشمل التفتيش التقليدي والتفتيش الإلكتروني.[2]

نستنتج في النهاية أنه يمكن تعريف التفتيش الإلكتروني بأنه إجراء من إجراءات التحقيق يهدف إلى الوصول إلى الأدلة الناتجة عن جناية أو جنحة تحقق وقوعها فعلياً داخل نظام المعالجة الآلية للمعطيات، وذلك لإثبات ارتكابها ونسبتها إلى متهم معين. وينبغي التعامل مع الأدلة المعلوماتية بحيطة وحذر لتفادي تلفها أو ضياعها.[3]

المطلب الثاني: شروط التحقيق في الجرائم الإلكترونية وخصائصه

مع تطور التكنولوجيا وانتشار استخدام الإنترنت، أصبحت الجرائم الإلكترونية تشكل تحدياً أمنياً جديداً يواجه العديد من الدول حول العالم. ومن أجل مكافحة هذه الجرائم بفعالية، يتطلب الأمر وضع شروط تحقيقية خاصة تتناسب مع طبيعتها الرقمية وخصائصها المتفردة. يأتي المطلب الثاني لتسليط الضوء على هذه

[1] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 2012، صفحة 115.

[2] مانع سلمى، "التفتيش كإجراء التحقيق في الجرائم المعلوماتية"، مجلة العلوم الإنسانية، عدد 22، جامعة بسكرة، جوان 2011، صفحة 227.

[3] همیسي رضا، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، عدد 11، جامعة الوادي، جوان 2012، صفحة 164.

الشـروط والخصـائص، ودورهـا فـي تسـهيل عمليـات التحقيـق وتحقيـق العدالـة فيمـا يتعلق بالجرائم الإلكترونية.

الفرع الاول: شروط التحقيق في الجرائم الإلكترونية

اولا: أن يكون التحقيق بصدد الجريمة (جناية أو جنحة)

يقصـــد بذلك أن تكون الجريمة معاقبًا عليها في القانون، فبمجرد وقوع الجريمة يبدأ عمل الجهات المكلفة بالتحقيق للتأكد من وقوعها، ومعرفة من ارتكبها، وما نوع هذه الجريمة وما هو النص القانوني الذي ينطبق عليها. لا يجب إصـــدار أمر بعدم المتابعة أو حفظ الأوراق لعدم وجود جريمة، إلا بناءً على أمر صادر من السلطة المختصة. يعتبر هذا الشرط تطبيقًا لمبدأ "لا جريمة ولا عقوبة إلا بنص"، وبناءً عليه، لا يمكن توجيه اتهام ضـــد أي شخص ما لم يكن الفعل منصوصًا عليه قانونيًا.[1]

فالمبدأ العام في القضـــايا الجنائية هو أن التحقيق فيها إلزامي، وهذا ما نصـــت عليه المادة 66 من قانون الإجراءات الجزائية. لا يجوز إحالة المتهم بجناية إلى جهات الحكم دون المرور عبر التحقيق، وذلك نظرًا لخطورة هذا النوع من الجرائم والعقوبات المترتبة عليها.[2]

وكـون التحقيـق وسـيلة دفـاع للمـتهم، ووسـيلة مسـاعدة لقضـاة الحكـم فـي تقـدير العقوبة أو التدبير الملائم للمتهم من جانب آخر.

[1] نصيرة بوحزمة، التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، رسالة دكتوراه في العلوم القانونية، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الجيلالي اليابس، سيدي بلعباس، 2022، صفحة 18.

[2] أمر رقم 66-155، مؤرخ في 08 يونيو سنة 1966، يتضمن قانون الإجراءات الجزائية، معدل ومتمم لاسيما بالقانون رقم 17-07 المؤرخ في 27 مارس 2017.

أما التحقيق في مواد الجنح فيكون مطلوبًا وضـــروريًا كلما كانت القضـــية معقدة وخطيرة، وكلما تطلب الأمر اتخاذ إجراء من إجراءات التحقيق، ويكون اختياريًا ما لم يكن هناك نصوص خاصة طبقًا للمادة 66 فقرة 2 من قانون الإجراءات الجزائية.

كما أن فتح التحقيق يعد ضـــروريًا إذا ما بقي مرتكب الجريمة مجهولًا أو فارًا أو لجأ إلى خارج الوطن.

فيما يخص مواد المخالفات، والتي تعد أقل الجرائم خطورة، فإن التحقيق فيها يكون دائمًا جوازيًا بحيث يجوز إجراء التحقيق فيها بشرط طلبه من وكيل الجمهورية طبقًا للمادة 66 فقرة 2 من قانون الإجراءات الجزائية.

وبالتالي، يفهم من نص هذه المادة أنه من كان ضحية مخالفة لا يمكنه التأسيس كطرف مدني بغرض تحريك الدعوى العمومية، وبالتالي فتح التحقيق، غير أنه لا يوجد أي مانع يحول دون تأسيسه كطرف مدني إذا ما فتح التحقيق بناءً على طلب وكيل الجمهورية.

وعليـه يكفـي أن يتـوافر فـي الجريمـة محـل التحقيـق ركنهـا المـادي، ومـن القواعـد العامــة للــركن المــادي فــي الجريمــة أن يحــدد المشــرع الجزائــري الســلوك الإجرامــي فــي كـل جريمـة علـى نحـو يمكـن القاضـي مـن تكييـف هـذا السـلوك أو الفعـل الإجرامـي ورده إلى القاعدة القانونية أو النص التجريمي الذي يحكمه ويتضمنه.[1]

وفي الجرائم الإلكترونية يتطلب لقيام السلوك الإجرامي وجود حاسوب آلي، وأحيانًا يتطلب الجرم أيضًا أن يكون متصلاً بشبكة الإنترنت. ويختلف السلوك الإجرامي في الجرائم الإلكترونية حسب نوع الجريمة، فقد يكون وقتيًا أي يبدأ وينتهي بمجرد ارتكابها مثل جريمة السرقة المعلوماتية، وقد يكون استمرارها مثل إنشاء مواقع تحريض القصر على العنف والدعارة أو مواقع معادية بغرض الترويج للإرهاب.

[1] فوزي عمارة، قاضي التحقيق، أطروحة دكتوراه في العلوم، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2009-2010، صفحة 39.

أما الركن المعنوي في الجريمة الإلكترونية، فيمكن القول بأنها جرائم عمدية، يستوجب المشرع فيها توفر القصد الجنائي بركنيه العلم والإرادة. ويختلف الركن المعنوي في الجريمة الإلكترونية من جريمة لأخرى.

ثانيا: أن تكون الجريمة قد وقعت فعلا أو يرجح وقوعها

العبرة في اتخاذ الإجراءات في شـــأن الجرائم الإلكترونية أن تكون الجريمة محل التحقيق قد وقعت فعلاً أو ترجح وقوعها، فلا يجري التحقيق بشـأن جريمة محتملة، وإلا كان الإجراء باطلاً. في هذا الصدد، يثور التساؤل حول أمرين:

-**الأول:** الإجراءات التي تتخذ قبل بدء التحقيق الابتدائي لكشف الجريمة.

-**الثاني:** إجراءات الضبط الإداري التي تُتخذ لمنع وقوع الجريمة.[1]

ومن المؤكد أن لدى ضـابط الشـرطة القضـائية الحق في بدء إجراءات جمع الأدلة والتحريات للبحث عن دلائل تثبت وجود الجريمة.

بالنسبة لتحقق صور الجريمة في مجال التكنولوجيا، يعتقد البعض أنه يمكن تحقيقها في حال اكتشاف ضابط الشرطة القضائية أو المجني عليه أثناء اختراق الجاني للشبكة أو النظام المعلوماتي، حيث يتوفر لديهم الوسائل التقنية لتتبع الجاني والقبض عليه.

ومن الأمثلة على ذلك، قيام شركة خدمات الإنترنت (ISP) في الولايات المتحدة الأمريكية بالكشف عن أنشطة دعارة وترتيب لقاءات جنسية مع الأطفال أثناء مراقبتها لأنشطة

[1] نصيرة بوحزمة، المرجع السابق، صفحة 36.

المشتركين لديها. وفور اكتشافها لهذه الأنشطة، قامت بتقديم أسماء المشتبه فيهم للشرطة الفيدرالية الأمريكية التي نجحت في القبض على العديد منهم بعد مراقبتها لأنشطتهم. [1]

ويمكن أيضًا مشاهدة الجريمة حال حدوثها من خلال الإنترنت إذا شاهد ضابط الشرطة القضائية أو غيرها الجريمة حال ارتكابها. في مثل هذه الحالة، تتحقق صورة الجريمة المتلبس بها بالمشاهدة عن بعد وعبر موجات كهرومغناطيسية، مثلها مثل المشاهدة المادية الملموسة التي نصت عليها القوانين التقليدية.

ومثال على ذلك هو ملاحظة صاحب مقهى الإنترنت (Cyber café) لشخص يقوم ببث صورًا إباحية لفتاة عبر الإنترنت مستخدمًا حاسوب آلي في المقهى، فيقوم على الفور بإخطار السلطات المعنية بوجود جريمة ترتكب داخل مقهى الإنترنت المملوك له.

ومع ذلك، تعترض حالات الجريمة المتلبس بها بعض المشكلات، منها ضرورة كشف حالة التلبس بشكل مشروع، حيث يجب أن يتم الإجراء اللازم لكشف التلبس بطريقة قانونية. هذا يمثل تحديًا في حالات الجرائم الإلكترونية نظرًا لحداثتها وعدم وجود تشريعات محددة لتنظيمها. بالإضافة إلى ذلك، يتداخل القيام بالإجراءات مع موضوع الحرية الشخصية، والتي يجب أن تكون محمية بشكل كافٍ للحفاظ على حقوق الأفراد وحرياتهم. وبناءً عليه، ينبغي أن يكون الإجراء محددًا ومنصوصًا عليه في القانون.[2]

وفيما يتعلق بهذه المسألة، تظهر مشكلة مشروعية التخفي عبر الإنترنت من قبل جهات التحري، سواء للكشف عن جريمة محددة قد وقعت، أو للبحث العام عن الجرائم ومرتكبيها. غالبًا ما يقوم عناصر التحري بالتخفي واستخدام أسماء وهمية للولوج إلى الإنترنت، والانضمام إلى غرف المحادثات والمنتديات لتبادل الحديث مع الآخرين بهدف الوصول إلى نتائج غير محددة تتعلق بمرتكبي الجرائم.

---

[1] فايز محمد رجب غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، كلية الحقوق، فرع القانون الجنائي والعلوم الجنائية، جامعة الجزائر 1، 2010-2011، صفحة 288.

[2] فايز محمد رجل غلاب، المرجع السابق، صفحة 290.

وهناك مشكلة أخرى تتعلق بتقدير الزمن اللازم لحالة التلبس، حيث يترك تحديدها عادة لضابط الشرطة القضائية، مع الحرص على عدم تجاوز مدة محددة. وبينما يمكن تقدير مدة التلبس في الجرائم التقليدية بسهولة، فإن ذلك يصعب في الجرائم الإلكترونية خاصة في حالات المطاردة.

ومن أجل توضيح كيفية المطاردة عبر الإنترنت، يتم استخدام برمجيات دقيقة لتعقب المتورطين في الجرائم الإلكترونية، حيث يمكن لهذه البرمجيات تحديد هوية المجرمين بفاعلية عالية، نظرًا لأنهم يتركون بصمات إلكترونية خلفهم.

لقد شهدت تقنية المطاردة والتتبع عبر الإنترنت تطورًا ملحوظًا، حيث تم تطوير برمجيات تسمح بتتبع أولى محاولات المجرمين المعلوماتيين. على سبيل المثال، برمجية "أتسيديTC" تمكن من تحديد أولى البصمات الإلكترونية للمجرمين عبر الإنترنت.

بعد تحديد الجهاز المستخدم في ارتكاب الجريمة الإلكترونية، يمكن الوصول إلى مكان ومحل إقامة مستخدمه عن طريق استخدام تقنيات التتبع والمعلومات الإلكترونية المتاحة عن طريق (IP Adresse).[1]

يمكن العثور على رقم (IP) الخاص بكل جهاز متصل بالإنترنت في خانة (Header) في البريد الإلكتروني. يقوم رجال الضبط القضائي بفحص الرسالة والانتقال إلى (Mail option)، ثم (General préférence)، ثم إضافة (Header)، واختيار (Show all Header on incoming message). بعد ذلك، يمكنهم العثور على الـ (IP) المرسل، الذي يتكون من أربعة (04) أرقام مفصولة بنقطة في X-originating-IP. بعد التوصّل إلى الـ (IP)، يتم استخدامه

[1] بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، مصر، 2012، صفحة 45.

لتحديد الموقع الجغرافي، ومزود الخدمة وخط التليفون الأرضي أو شبكة (ADSL) لمستخدم الجهاز. هذا يمكن من تحديد محل إقامة مالك الجهاز.[1]

ثالثا: أن يجري التحقيق في مواجهة متهم معين بارتكاب الجريمة أو للبحث عنه

يتطلب ذلك تحديد هوية المتهم بارتكاب الجريمة، سواء كانت إلكترونية أو تقليدية ويشير مصطلح "المتهم" إلى الشخص الذي يوجه إليه الاتهام بارتكاب إحدى الجرائم المنصوص عليها في قوانين العقوبات أو في التشريعات الجنائية الخاصة مثل قانون مكافحة الجرائم التقنية، سواء كان بوصفه فاعلاً أو شريكًا.

الفرع الثاني: خصائص التحقيق في الجرائم الإلكترونية

اولا: الكتابة أو التدوين

تدوين إجراءات التحقيق في الجرائم الإلكترونية يُعتبر جزءًا أساسيًا من ضمانات التحقيق، وتتطلب القواعد العامة وجوب توثيق التحقيق. يجب أن تُسجَّل هذه الإجراءات كتابةً حيث يمكن للأطراف المعنية الرجوع إليها للدفاع عن أنفسهم. يعكس ذلك أهمية توثيق الإجراءات لإثبات ما تم تحقيقه، بما في ذلك النتائج التي تم الوصول إليها. من المهم أن يكون توثيق التحقيقات كتابيًا لضمان مصداقية ما تم توثيقه، بينما يتمكن المحققون من التركيز على مهامهم الفنية دون الانشغال بالجوانب الإدارية. [2]

[1] خط الانترنت الرقمي غير المماثل (ADSL) هو عبارة عن تقنية الشبكة التي تنقل البيانات بسرعة على خطوط الهواتف الحاسوبية التناظرية ANALOGUE وبشكل غير مماثل، حيث تتحرك البيانات في اتجاه واحد وبسرعة أكبر من الاتجاهات الأخرى.

[2] حسين بن سعيد الغافري، "التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت"، دار النهضة العربية، القاهرة، 2009، صفحة 170.

فغاية التحقيق الابتدائي ليست كافية في ذاتها، وقد يؤثر تقديمها بعد الانتهاء منها على قرار القضاء في القضايا المتعلقة بها. لذا، يهدف تدوين التحقيق إلى توثيق جميع الإجراءات والقرارات المتخذة، حيث يتم إثباتها في محضر معد خصيصًا لذلك. إن الكتابة تلعب دورًا حاسمًا في تثبيت الإجراءات، حيث لا يعتد بالإجراءات غير الموثقة كتابيًا. ويُقصد بتدوين التحقيق توثيق جميع الأوامر والقرارات الصادرة بشأنه بحيث يكون الإجراء المكتوب هو الذي يُعتمد، فالإجراء غير المكتوب في ملف التحقيق لا يُعتد به.[1] وتُثبت تلك الإجراءات في محضر واحد أو في محاضر متعددة، وفقاً لما ينص عليه القانون. فقد جاء في المادة 24 بالفقرة الثانية من قانون الإجراءات الجنائية المصري أنه "يجب أن تثبت جميع الإجراءات التي يقوم بها مأمورو الضبط القضائي في محاضر موقع عليها منهم يبين بها وقت اتخاذ الإجراءات ومكان حصوله، ويجب أن تشمل تلك المحاضر زيادة على ما تقدم توقيع الشهود والخبراء الذين سمعوا، وتُرسل المحاضر إلى النيابة العامة مع الأوراق." [2]

ومبدأ تدوين التحقيق ينطبق على جميع الإجراءات التي يقوم بها المحقق، مثل سماع الشهود واستجواب المشتكى عليه والمعاينة والانتقال وضبط الأشياء المضبوطة. يُثبت كل إجراء تم القيام به ونتائجه في المحضر، وبالتالي لا يمكن إثبات حصول الإجراء إلا في المحضر الذي يُدون فيه.[3] لا يمكن استبعاد طرق الإثبات الأخرى في هذا الشأن. ومن

[1] فاروق الكيلاني، "محاضرات في قانون أصول المحاكمات الجزائية الأردني والمقارن"، جزء 2، طبعة 2، دار المروج، بيروت، 1995، صفحة 124.

[2] د. حسن جوخدار، "التحقيق الابتدائي في قانون أصول المحاكمات الجزائية – دراسة مقارنة"، دار الثقافة للنشر والتوزيع، عمان، 2008، صفحة 56.

[3] المحضر هو الوثيقة الرسمية التي يدون فيها مأمور الضبط القضائي ما تم وما سوف يتم من إجراءات التحقيق، وهو يحتوي على الوقائع التي حدثت مرتبطة بالزمن (التاريخ – الوقت) سواء كانت هذه الوقائع مرتبطة بالأشخاص (مبلغ، شاهد، مجني عليه، خبراء، متهم، أو مشتبه فيه) أو الأماكن، أو الأشياء حسب طبيعتها. انظر د. مصطفى محمد موسى، "التحقيق الجنائي في الجرائم الإلكترونية"، دار الكتب القانونية، المحلة، مصر، 2005م. صفحة 330.

الأساسيات في الإجراءات الجنائية أن يكون هناك كاتب يرافق المحقق لتدوين الإجراءات فالتوثيق الكتابي يعزز مصداقية العملية ويسهل استعراض الأدلة والشهادات في المحاكمة.[1]

تنص المادة 201 من تعليمات النيابة العامة على ضرورة تحرير محاضر التحقيق بواسطة كاتب من موظفي القلم الجنائي بالنيابة المختصة، حيث يتحمل الكاتب مسؤولية التحقق من الدقة والوضوح والنظافة في تدوين المحضر. لذا، فإن حضور كاتب التحقيق مع المحقق أمر لازم في جميع الإجراءات التي تتطلب تحرير محاضر، سواء كان ذلك لسماع الشهود أو إجراء المعاينات أو التفتيش أو الاستجواب. ويترتب على ذلك بداهة إثبات الإجراءات في محاضر يتم جمعها في ملف الدعوى، الذي يُعرض لاحقًا أمام المحكمة. ومع ذلك ينصرف وجوب تدوين الإجراءات بمشاركة كاتب التحقيق إلى الإجراءات التي يلزم لها تحرير محضر يثبت القيام بها، بينما لا تتطلب أوامر التحقيق تحرير محضر، ويمكن أن تُصدر بمعرفة المحقق نفسه، كما هو الحال في أوامر التفتيش.[2]

وعلى الرغم من أن بعض الإجراءات قد تتطلب توقيع الكاتب عليها، إلا أنها ليست من المحاضر المنصوص عليها في المادة 73 من قانون الإجراءات الجنائية. يتضح أيضًا أن ما فرضه القانون من حضور كاتب مع المحقق وتوقيعه على المحضر ينطبق فقط على الإجراءات التي تستوجب تحرير محاضر، مثل سماع الشهود وإجراء المعاينات. بالرغم من ذلك، فإن عدم توقيع الكاتب على محاضر التحقيق لا يجعلها باطلة وتحولها إلى مجرد جمع استدلالات حيث لم ينص المشرع صراحة على ذلك.[3]

---

[1] نصت المادة (73) من قانون الإجراءات الجنائية المصري على أنه: "يستصحب قاضي التحقيق في جميع إجراءاته كاتبًا من كتبة المحكمة يوقع معه المحاضر وتحفظ هذه المحاضر مع الأوامر وباقي الأوراق في قلم كتاب المحكمة" صفحة 49.

[2] د. مأمون محمد سالمة، "الإجراءات الجنائية في التشريع المصري"، الجزء الأول، دار النهضة العربية، القاهرة، 2008م. صفحة 661.

[3] أحمد أبو الروس، "التحقيق الجنائي والتصرف فيه والأدلة الجنائية"، المكتب الجامعي الحديث، الإسكندرية، 1998م، صفحة 17.

إذا لم يتم استعمال كاتب مختص، سواء كتب المحضر بنفسه أو تم استعمال كاتب غير مختص، فإن المحضر يعتبر باطلاً كمحضر تحقيق، ولكن يمكن أن يُعتبر كإجراء استدلالي، حيث لا يشترط القانون وجود كاتب لتحرير الإجراءات الاستدلالية. وعلى الرغم من ذلك، يتمتع عضو النيابة بصلاحياته كرئيس للضبط القضائي وفقًا للمواد 31 و 24 من قانون الإجراءات الجنائية المصري، مما يسمح له بإثبات الوقائع قبل حضور كاتب التحقيق.[1]

وعلاوة على ذلك، فإن القاعدة العملية في تحرير محاضر التحقيق تقتضي أن تكون خالية من أي تعديل أو تحريف، وفي حال وجود أي تعديل يجب على المحقق المصادقة عليه، وإلا فإنه يُعتبر باطلاً. وتنص المادة 203 من تعليمات النيابة العامة على ذلك بأن محاضر التحقيق يجب أن تُحرر بخط واضح دون أي تعديلات، مع ترقيم الصفحات بأرقام متتابعة. ويشدد على هذا المبدأ أيضًا المادة 73 من قانون أصول المحاكمات الجزائية الأردني التي تنص على ضرورة مصادقة المدعي العام والكاتب والمستجوب على أي تعديلات تُجرى على المحضر، سواء كانت شطبًا أو إضافة.

ثانيا: سرية التحقيق

ينبغي على المحقق الالتزام بالسرية في سير التحقيقات، حيث تُعتبر إجراءات التحقيق والنتائج المستنتجة منها معلومات سرية.[2] ينبغي الحرص على الحفاظ على سرية التحقيقات وعدم الكشف عنها لوسائل الإعلام المختلفة، سواء الصحف أو الإذاعات أو وكالات الأنباء وذلك حرصًا على المصلحة العامة وتجنب أي تأثير سلبي يمكن أن يطرأ على التحقيقات خاصة فيما يتعلق بالجوانب التي تؤثر على الاقتصاد الوطني أو تهدد الثقة العامة بالنظام القانوني وتعرض العدالة للخطر.[3]

---

[1] نقض 20/5/1961، مجموعة أحكام النقض، س12، ق 140، صفحة 2.

[2] وفي ذلك قضت محكمة النقض المصرية على أنه: "مقتضى نص المادة 75 من قانون الإجراءات الجنائية أن إجراءات التحقيق من الأسرار التي لا يجوز لمن شاء إليهم إفشاؤها" الطعن رقم 961 لسنة 29 ق – جلسة 9/11/1959.

[3] د. محمد أنور عاشور، "المبادئ الأساسية في التحقيق الجنائي العملي"، عالم الكتب، القاهرة، 1987م، صفحة 28.

ركز المشرع على أهمية الحفاظ على سرية التحقيقات، حيث نصت المادة 75 من قانون الإجراءات الجنائية المصري على أن إجراءات التحقيق والنتائج التي تنتج عنها يجب أن تُعتبر سرية، ويتعين على جميع أعضاء القضاء والنيابة العامة والمساعدين والكتاب والخبراء وغيرهم الذين يشاركون في التحقيق أو يحضرونه بسبب وظيفتهم أو مهمتهم عدم الكشف عنها، ومن ينتهك هذا الحظر يعاقب وفقًا للمادة 310 من قانون العقوبات.[1]

المشرع حدّد من لهم الحق في حضور إجراءات التحقيق، مما يعني أنه ليس من الجمهور أو العامة الحق في الحضور، حيث أن التحقيق ليس علنيًا وليس من الصواب أن يحضره أي شخص بغض النظر عن شأنه. وفي المادة 193 من نفس القانون، جرم المشاركة في نشر أخبار بشأن تحقيق جنائي قائم بشكل علني دون موافقة السلطة المختصة، مع مراعاة للنظام العام والآداب أو لضمان ظهور الحقيقة.

السرية في إجراءات التحقيق خارج الأضواء العامة تضمن حسن سير العمل وتحافظ على مصالح الأفراد، مما يحميهم من التأثيرات الضارة التي قد تؤثر على سير التحقيق وتجعل المتهم عرضة للظلم. ينبغي على الجميع، سواء كانوا مشاركين في التحقيق أو لا، احترام هذه السرية، فالنهي يمتنع عن نقل أو نشر معلومات التحقيق بشكل علني. يتعين على المحققين أن يحترموا هذا السر وأن يمتنعوا عن كشف المعلومات التي يتعرفون عليها خلال أداء واجباتهم، فإشاعة تلك المعلومات قد تؤدي إلى فشل التحقيقات وتعرضها للخطر.[2]

السرية في التحقيقات الجنائية تقيّد انتشار الشائعات بين الناس، مما يمنع التنبؤ غير المنطقي بمجريات القضية وتضخيم الوقائع المتهم بها. بالمقابل، يُسمح لأطراف الدعوى بالوصول إلى المعلومات بشكل علني، ما يمنح المتهمين فرصة للتحضير للدفاع عن أنفسهم

---

[1] نصت المادة (310) من قانون العقوبات المصري على أنه: "كل من كان من الأطباء أو الجراحين أو الصيادلة أو القوابل أو غيرهم مودعًا إليه بمقتضى صناعته أو وظيفته سرًا خصوصيًا اؤتمن عليه فأفشاه في غير الأحوال التي يلزمه القانون فيها بتبليغ ذلك يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بغرامة 500 جنيه".

[2] د. عمار عباس الحسيني، "التحقيق الجنائي والوسائل الحديثة في كشف الجريمة"، منشورات الحلبي الحقوقية، لبنان، 2015م، صفحة 61.

بشكل مناسب ويزيل عنصر المفاجأة بالنسبة للأدلة المقدمة ضدهم، مما يحقق العدالة ويضمن لهم حق الرد وتقديم الدفوع.[1]

المبدأ العام هو عدم وجود سرية بالنسبة للخصوم، إلا أن المشرع قد أدرج استثناءات تعود فيها إلى مبدأ السرية، وهي حالات الضرورة والاستعجال.[2]

المبحث الثاني: مفهوم الجريمة الالكترونية

الجريمة الإلكترونية تُعد واحدة من النتائج السلبية للتقنية العالية، حيث أصبحت موضوعًا محوريًا في الدراسات لتحديد طبيعتها، مما أدى إلى تطوير عدة مصطلحات للإشارة إليها، مثل جرائم الحاسب، وجرائم التقنية العالية، وجرائم الغش الإلكتروني، مع تعقيد وضع مفهوم دقيق لهذه الظاهرة.

المطلب الأول: أساسيات حول الجريمة الالكترونية

الجريمة الإلكترونية تُعتبر ظاهرة حديثة نتيجة لارتباطها بتكنولوجيا المعلومات والاتصالات، وقد أثارت الكثير من الغموض في تعريفها، حيث تم تبني مصطلحات مختلفة لوصفها. بينما يُفضل البعض عدم تحديد تعريف دقيق لها، ويعتبرها مجرد جرائم يتم ارتكابها بواسطة وسائل إلكترونية، في حين يتم تعريف الجرائم التقليدية بشكل أكثر دقة ولها تعريفات قانونية معترف بها.[3]

الفرع الأول: تعريف الجريمة الالكترونية

أولاً: التعريف اللغوي

---

[1] د. فايز الضفيري، "المعالم الأساسية لقضية العدالة في مرحلة الاستدلالات والتحقيق الجسدي"، مجلس النشر العلمي، جامعة الكويت، 2001، صفحة 98.

[2] د. عمر محمد سالم، الوجيز في شرح قانون الإجراءات الجنائية، الجزء الأول، مركز جامعة القاهرة للتعليم المفتوح، 2007، صفحة 185.

[3] خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، مصر، 2019، صفحة 73.

تُعــرّف الجريمــة لغويًــا علــى أنهــا ســلوك متعمــد غيــر مشــروع ينطــوي علــى انتهــاك لحقــوق أو مصــالح محميــة قانونيًــا، ويتضــمن تلــك الانتهاكــات العدوانيــة علــى الممتلكــات أو الحقــوق الشخصــية للآخــرين، ويكــون مرتكبهــا مسؤولًا جنائيًا عن أفعاله في غير حالات الشرعية أو الاستثنائية.[1]

تم تعريف الجريمة أيضًا على أنها فعل غير مشروع يعاقب عليه القانون، وتتضمن الجرائم التي تنشأ عن استخدام غير مشروع لشبكة الإنترنت بشكل أساسي. يُستخدم مصطلح "الإلكترونية" (Cyber) لوصف فكرة أو جزء من التكنولوجيا المتعلقة بالحواسيب أو المعلومات.[2]

ثانيًا: التعريف الاصطلاحي

لفهم مفهوم الجريمة الإلكترونية، يتعين علينا النظر في التعريف الفقهي لهذا المصطلح ومن ثم التعمق في التعريف القانوني المعتمد.

أ- التعريف الفقهي للجريمة الإلكترونية:

الفقه بذل جهوداً كبيرة في محاولة تحديد تعريف دقيق للجريمة الإلكترونية، حيث انقسمت الآراء بين من يحاول تضييق مفهومها ومن يسعى لتوسيعه.[3]

من بين التعاريف التي وضعها أنصار الاتجاه المضيق، يُعرّفون الجريمة الإلكترونية على أنها أي فعل غير مشروع يتطلب معرفة واسعة بتكنولوجيا الكمبيوتر لارتكابه ومعرفة لازمة لملاحقته، ويصفونها هذا الاتجاه على أنها الجرائم التي تتعلق بجهاز الكمبيوتر.

---

[1] هبة نبيلة هروال، جرائم الإنترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013، صفحة 12.

[2] يوسف صغير، الجرائم المرتكبة عبر الإنترنت، رسالة لنيل شهادة الماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر، 2013، صفحة 7.

[3] عادل محمد فريد نائلة، جرائم الحاسوب الاقتصادية، الطبعة 1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، صفحة 27.

يُمكن تصوير الجريمة الإلكترونية على أنها "نشاط غير مشروع يستهدف نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل أو مرسلة عبر أنظمة الكمبيوتر".[1]

أما أصحاب الاتجاه الموسع، فقد عرفوا الجريمة الإلكترونية بأنها "كل سلوك إجرامي ينطوي على استخدام الكمبيوتر"، أو ببساطة هي "كل جريمة ترتكب في سياق الأجهزة الحاسوبية".

وفقًا لهذا التعريف، تُعرف الجريمة الإلكترونية كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو ينقلها. يشير هذا التعريف إلى أن الجريمة المعلوماتية تشمل أي نشاط إجرامي يشتمل على دور أو تأثير للكمبيوتر في ارتكابه، سواء كان الكمبيوتر أداة لإتمام الجريمة أو كان محلاً لها. ومع ذلك، عند وضع تعريف دقيق للجريمة المعلوماتية، يجب مراعاة عدة اعتبارات هامة[2]:

1. أن يكون هذا التعريف مقبولًا ومفهومًا على المستوى العالمي، بما في ذلك توافقه مع المعايير الدولية.

2. أن يأخذ في الاعتبار التطور السريع والمتلاحق لتكنولوجيا المعلومات والاتصالات أثناء وضع التعريف.

3. أن يشير التعريف بوضوح إلى الدور الذي يلعبه جهاز الكمبيوتر في تنفيذ الأنشطة الإجرامية.

ب-التعريف التشريعي للجريمة الإلكترونية

المشرع الجزائري على عكس العديد من التشريعات الأخرى، لم يقدم تعريفًا دقيقًا لنظام المعالجة الآلية للمعطيات، وترك هذه المهمة للفقهاء والقضاة لفهم هذا الأمر بشكل أفضل دعونا نلقي نظرة على تعريفاته المذكورة في القوانين 04-15 و 09-04 على التوالي:

[1] خالد ممدوح إبراهيم، المرجع السابق، صفحة 75.

[2] عادل محمد فريد نائلة، المرجع السابق، صفحة 32.

أ- تعريف الجريمة الإلكترونية حسب القانون 04-15:

باستعراض قواعد القانون 04-15، والنظر إلى المادة 394 مكرر 1 وثم المادة 394 مكرر 2، نجد تعريفًا لمفهوم المساس بأنظمة المعالجة الآلية للمعطيات، حيث جاء في المادة 394 مكرر ما يلي:

• الدخول والاحتفاظ بالغش في أي جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك.

• حذف أو تغيير المعطيات في المنظومة إذا نشأ ذلك نتيجة للدخول غير المشروع أو الابقاء بهدف تخريب نظام عمل المنظومة.

أما المادة 394 مكرر 1 فقد أشارت إلى ما يلي:

تجميع أو توفير أو نشر أو تصحيح أو بحث في المعطيات التي تم تخزينها أو معالجتها أو إرسالها عبر نظام معلوماتي، والتي يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.[1]

-حيازة أو إفشاء أو نشر أو استخدام المعطيات التي تم الحصول عليها من أحد الجرائم المنصوص عليها في هذا القسم، لأي غرض من الأغراض.

ب-تعريف الجريمة الإلكترونية في حسب القانون 09-04:

حددت المادة (02) منه الجريمة الإلكترونية بقولها: " يقصد في مفهوم هذا القانون بما يأتي:

-الجرائم المتصلة بتكنولوجيات الاعلام والاتصال:

[1] القانون رقم 04-15 المؤرخ في 10 نوفمبر يعدل ويتمم الأمر 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 71 الصادر في 10 نوفمبر 2004.

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، بالإضافة إلى أي جريمة أخرى يتم ارتكابها أو تسهيل ارتكابها عن طريق نظام معلوماتي أو نظام للاتصالات الإلكترونية.

-منظومة معلوماتية:

أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، حيث يقوم واحد أو أكثر من هذه الأنظمة بمعالجة آلية للمعطيات تنفيذًا لبرنامج محدد.

معطيات معلوماتية:

أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل نظام معلوماتي، بما في ذلك البرمجيات المناسبة التي تمكّن المنظومة المعلوماتية من أداء وظائفها.[1]

الفرع الثاني: خصائص الجريمة الالكترونية

تتميز الجرائم الإلكترونية بعدة خصائص تميزها عن الجرائم العادية، وهذه الخصائص تنعكس أيضًا على مرتكبيها، ويتضح ذلك فيما يلي:

أولا: الجريمة الإلكترونية عابرة للحدود (الزمان والمكان).

الجرائم الإلكترونية لا تقتصر على الحدود الجغرافية للدول ولا بين القارات، بل مع انتشار شبكة الاتصالات بين دول العالم وأقاليمه، يصبح من الممكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة. وبما أن الجريمة الإلكترونية تتسم غالبًا بالطابع الدولي نظرًا للطابع العالمي لشبكة الإنترنت واتصالاتها المستمرة، فإنها تُسهِّل

[1] القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادرة في 16 أوت 2009.

ارتكاب الجريمة من دولة إلى دولة أخرى، مما يجعلها عابرة للحدود بين الدول والقارات، وهو ما يمثل شكلاً جديدًا من أشكال الجرائم العابرة للحدود الإقليمية.[1]

الجرائم الإلكترونية لا تقتصر على الحدود الجغرافية للدول ولا بين القارات، بل مع انتشار شبكة الاتصالات بين دول العالم وأقاليمه، يصبح من الممكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة. وبما أن الجريمة الإلكترونية تتسم غالبًا بالطابع الدولي نظرًا للطابع العالمي لشبكة الإنترنت واتصالاتها المستمرة، فإنها تُسهّل ارتكاب الجريمة من دولة إلى دولة أخرى، مما يجعلها عابرة للحدود بين الدول والقارات، وهو ما يمثل شكلاً جديدًا من أشكال الجرائم العابرة للحدود الإقليمية.[2]

ثانيا: صعوبة إثبات الجريمة الإلكترونية

الجرائم الإلكترونية تتميز بالخفاء، حيث لا تترك آثارًا مادية يمكن تتبعها، مما يجعلها صعبة وخطيرة للكشف عنها وصعبة في تحديد مكان وقوعها. نظرًا لاتساع نطاقها المكاني وضخامة البيانات المتورطة، يصعب تحديد مكان التعامل معها. إثبات الجرائم الإلكترونية يعتبر صعبًا لأنها غالبًا ما تُكتشف بالصدفة وبعد فترة طويلة من ارتكابها، وتفتقر إلى الدليل المادي التقليدي. بالإضافة إلى ذلك، فإن تعقبها يتطلب خبرة فنية تصعب تواجدها لدى المحققين العاديين.[3]

وتتميز الجرائم الإلكترونية عن الجرائم التقليدية بطابع خاص لا يوجد له مثيل في الجرائم الأخرى، خاصة الجرائم التقليدية، ويتمثل هذا الطابع في صعوبة اكتشافها وإثباتها نظرًا لعدة أسباب، تتمثل في[4]:

---

[1] خالد ممدوح ابراهيم، المرجع السابق، صفحة 77.

[2] هبة نبيلة هروال، المرجع السابق، صفحة 45.

[3] خالد ممدوح ابراهيم، المرجع السابق، صفحة 79.

[4] هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة، العدد الثاني، 1999، صفحة 11.

- فضاء الجريمة: في الجريمة الإلكترونية، غالبًا ما تكون منتشرة وخفية، حيث لا يلاحظها المجني عليه بسبب عدم ترك آثار خارجية واضحة بعد ارتكابها، نتيجة لعدم وجود دليل مرئي ملموس. بينما في الجريمة التقليدية، تكون الجريمة واضحة وملحوظة مثل وجود جثث للقتلى أو آثار اقتحام لعمليات سرقة الممتلكات.[1]
- صعوبة الاحتفاظ بآثار الجريمة: في الجرائم الإلكترونية، تكون الأدلة غير مرئية حيث تتمثل في نبضات إلكترونية تنتقل عبر أجزاء الحاسوب والشبكة، مما يساعد الجاني في محوها بسرعة. وعادةً ما تكون الأدلة مرمزة أو مشفرة، حيث لا يمكن للشخص قراءتها إلا عند ظهورها على شاشة الحاسوب. بينما في الجرائم التقليدية، تكون الأدلة مرئية وصعبة المحو في وقت قصير، ويمكن للشخص قراءتها بدون الحاجة إلى الآلات أو الحواسيب.

ثالثاً: قلة الإبلاغ عن الجريمة الإلكترونية

ويرجع السبب في ذلك إلى أن معظم الجرائم الإلكترونية يتم اكتشافها بمحض الصدفة نظرًا لبقاء الجريمة في طي الكتمان، مما يعبر عنه علماء الإجرام بمصطلح "الرقم الأسود" أو "الرقم الخفي". ومن بين أسباب اختفاء هذه الجرائم، يأتي إحجام المجني عليه عن الإبلاغ عنها، حيث تكتفي معظم الجهات التي تتعرض لانتهاك أنظمتها المعلوماتية باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة، تجنبًا للإضرار بسمعتها ومكانتها، خاصة إذا كان المجني عليه هو مؤسسة مالية مثل البنوك والمؤسسات الادخارية.

حيث يخشى مجالس إدارة المؤسسات الاقتصادية عادةً من أن يؤدي اتخاذ الإجراءات القضائية حيال الجرائم الإلكترونية إلى تضاؤل الثقة فيها من قبل المتعاملين معها، مما قد يؤدي إلى انصرافهم عنها. في المقابل، يتم الإبلاغ عن الجرائم التقليدية بكثرة لأنها من السهل

[1] هبة نبيلة هروال، المرجع السابق، صفحة 48.

اكتشافها، كما أن المجني عليه في الجريمة التقليدية ملزم بالإبلاغ عن الجرائم، وإلا فسيتابع بجريمة عدم التبليغ.[1]

رابعاً: نقص خبرة الشرطة والقضاء

يتطلب كشف جرائم الإنترنت وتعقب مرتكبيها ومحاكمتهم استراتيجيات تحقيق وتدريب خاصة، أي خبرة تقنية تتماشى مع طبيعة هذا النوع من الجرائم، مما يتيح فهم ومواجهة الخصوصيات التي يعتمد عليها المجرم، والأساليب التي يستخدمها في ارتكابها. ولذلك، وجدت أجهزة العدالة أنفسها غير قادرة على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذا النوع المستحدث والفريد من الإجرام، مما جعلها فاشلة في مواجهته. ويختلف هذا عن الجريمة التقليدية، حيث يتمتع رجال الشرطة والقضاء بالتخصص والتدريب والخبرة في هذا المجال مع التركيز على القدرات البدنية.[2]

الفرع الثالث: أطراف الجريمة الإلكترونية

لابد للجريمة الإلكترونية كغيرها من الجرائم أن يكون لها طرفان: فاعل وضحية.

أولاً: الفاعل في الجريمة الإلكترونية

بالإضافة إلى الشروط العامة المطلوبة في مرتكب الجريمة الإلكترونية، مثل سلوك منحرف وعلم وإرادة في نتائج هذا السلوك، يجب أن يكون هذا الشخص ماهرًا ومتخصصًا في مجال علوم الحاسوب وتقنية المعلومات. وقد وُصف بعضهم بالمجرم الإلكتروني أو المجرم المعلوماتي لهذا الغرض. ومن هذا المنظور، فإن الجاني في الجريمة الإلكترونية يجب أن يكون شخصًا طبيعيًا قادرًا على تحمل العقوبة، مما يستبعد وجود الجنسيات الاعتباطية. كما يجب أن يكون الجاني ذو خبرة ومعرفة في مجال علوم الحاسوب سواء كان مستخدمًا عاديًا

[1] هشام فريد رستم، الجوانب الإجرامية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، مصر، 1994، صفحة 25.

[2] هبة نبيلة هروال، المرجع السابق، صفحة 50.

أو مبرمجًا أو هاويًا أو محترفًا في جرائم الحاسوب وتقنية المعلومات. ومن الأهمية بمكان أن يكون لدى هذا الشخص معرفة جيدة بالمسائل المعلوماتية وآلية عمل الحاسوب الآلي، لأن الإجرام المعلوماتي ينبعث من تقنيات التدمير الهادئة التي تشمل التلاعب بالمعلومات والكيانات المنطقية.[1]

الجاني في جرائم الإنترنت يختلف عن مثيله في الجرائم التقليدية، حيث يُطلق عليه في غالب الأحيان مصطلحات مثل "مجرم تقني"، "هاكر"، أو "مجرم معلوماتي". ويتميز هذا الشخص غالبًا بمستوى عالٍ من العلم والمعرفة التقنية، مما يجعله يتساوى في بعض السمات مع مجرمي الياقات البيضاء. وتتميز شخصيته بالتنوع، حيث يكون في بعض الأحيان فردًا فريدًا بقدرته على اختراق الأنظمة وارتكاب أعمال تقنية في العالم الافتراضي بطريقة لا يمكن للأشخاص العاديين أو العامة القيام بها.[2]

ومن ناحية أخرى، يتميز هؤلاء المجرمون بالاختلاف عن المجرمين التقليديين؛ حيث يمضون فترات طويلة أمام أجهزة الحاسوب. وتكمن قوتهم ليست في الأسلحة النارية أو الأدوات الحادة، بل في العقل والبرمجيات والفيروسات التي يستخدمونها لاختراق الأنظمة والبرمجيات بطرق جاسوسية.[3]

ثانياً: الضحية في الجرائم الإلكترونية

مع تعدد أصناف المجرمين، يتنوع أيضًا نوع الضحايا، ولكن الاختلاف يكمن في أنه ليس بنفس درجة تعدد المجرمين الإلكترونيين. فالضحية قد يكون شخصًا طبيعيًا، مثل الأفراد

---

[1] عبد الله دغش العجمي، العلمية والقانونية للجرائم الإلكترونية (دراسة مقارنة)، رسالة ماجستير، القانون العام، جامعة الشرق الأوسط، عمان، الأردن، 2014، صفحة 32.

[2] علي أحمد عبد الزعبي، حق الخصوصية، منشور على الموقع الإلكتروني: https://almerja.net/reading.php?idm=77368 تاريخ الاطلاع 2024/04/25، الساعة 22:30.

[3] هبة نبيلة هروال، المرجع السابق، صفحة 59.

أو المؤسسات، أو قد يكون شخصًا معنويًا، مثل الشركات أو الحكومات أو المؤسسات غير الربحية.

ويُمكن أن تكون الضحية فردًا عاديًا في المجتمع، أو مؤسسة اقتصادية مثل شركات التأمين. ومن الخطورة أن تشمل الضحايا الدول أو الجهات ذات الاهتمام العسكري، حيث يمكن أن تتعرض لعمليات تجسس مستهدفة.[1] المشرع الجزائري لم يتجاهل تلك النقاط، بل اتخذ إجراءات خاصة للوقاية من جرائم تكنولوجيا الإعلام والاتصال، بما في ذلك مراقبة الاتصالات الإلكترونية كإجراء وقائي ضمن إطار الضبط الإداري وفقاً للمادة 04 من القانون 04-09.[2]

في جرائم التكنولوجيا والجرائم بشكل عام، يمكن أن يكون الضحية شخصًا طبيعيًا أو معنويًا الذي تم انتهاك حقوقه المحمية قانونًا، مما يتسبب في أضرار مادية أو معنوية. يجب ملاحظة أن هذه الضحية قد تكون أيضًا سببًا في ارتكاب الجريمة، سواء بسبب جهله بالجريمة وارتكابها، أو عدم اتخاذ التدابير الأمنية اللازمة لحماية نظامه المعلوماتي، أو حتى بسبب الإهمال في رقابة وتوجيه الأطفال في استخدام الإنترنت والأجهزة المتصلة بها.[3]

في الجرائم الإلكترونية، يختلف المجني عليه أو الضحية عن تلك في الجرائم التقليدية في مسألة الإبلاغ عن الجريمة. فعادةً ما يلعب الضحية دورًا سلبيًا بسبب تكتمهم وخوفهم على سمعتهم، مما يمنعهم من الإبلاغ عن الجريمة. وفي حالة المؤسسات الاقتصادية التجارية فمن المؤكد أنها لن تكشف عن نفسها في حالة اختراق موقعها الإلكتروني أو وجود ثغرات أمنية ما لم تُعفَ من المسؤولية القانونية في حالات محددة.[4]

---

[1] بلال محمد الزعبي، أسامة أحمد مناغسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة، عمان، الأردن، 2010، صفحة 77.

[2] دلال موالي ملياني، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، أطروحة دكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018/2017، صفحة 41.

[3] بلال محمد الزعبي، أسامة أحمد مناغسة، المرجع السابق، صفحة 78.

[4] بلال محمد الزعبي، أسامة أحمد مناغسة، المرجع السابق، صفحة 80.

المطلب الثاني: الأحكام الخاصة بالجرائم الإلكترونية

لفهم أي جريمة، سواء كانت تقليدية أو إلكترونية، يتعين التطرق إلى أركانها والدوافع التي أدت إلى وقوعها، بالإضافة إلى استعراض أنواع هذه الجرائم. سنتناول هذه النقاط في هذا النص.

الفرع الأول: أركان الجريمة الإلكترونية

لتعريف جريمة ما، يلزم وجود ركنين: ركن مادي وركن معنوي، حيث يشمل الركن المادي النشاط المادي والعلاقة السببية والنتيجة الإجرامية، بينما يتضمن الركن المعنوي القصد الجنائي والخطأ غير العمدي والتجاوز في القصد، ويمكن أيضًا أن يكون بصورة القصد الاحتمالي وفقًا لتقدير المشرع في كل حالة.

أولاً: الركن المادي في الجريمة الإلكترونية

الركن المادي في الجريمة يشير إلى وجود فعل ملموس ينطوي على تحريك الحواس ويتضمن السلوك المادي الذي يُجرمه القانون والذي يكون له طبيعة مادية تلمسه الحواس وهو أساسي لوقوع الجريمة حيث لا يُعترف بجرائم بدون ركن مادي. في الجرائم المعلوماتية، يتطلب السلوك المادي وجود بيئة رقمية وجهاز كمبيوتر واتصال بالإنترنت، ويتطلب أيضًا معرفة ببداية النشاط وشروعه ونتائجه. على سبيل المثال، يقوم مرتكب الجريمة بتجهيز الكمبيوتر لتنفيذ الجريمة عن طريق تحميل برامج اختراق أو إعدادها بنفسه، وقد يقوم بتهيئة صفحات تحمل مواد مخلة بالآداب وتحميلها على الخادم، ويمكن أيضًا أن يقوم بإعداد برامج فيروسات قبل بثها.[1]

إن النشاط أو السلوك المادي في الجريمة الإلكترونية يثير العديد من التساؤلات فيما يتعلق ببداية أو الشروع في ارتكاب الجريمة. يختلف هذا النشاط عما هو عليه في العالم المادي، حيث إن ارتكاب الجريمة عبر الإنترنت يتطلب بالضرورة منطلقًا تقنيًا. بدون هذا

[1] خالد ممدوح إبراهيم، المرجع السابق، من صفحة 98 إلى صفحة 99.

المنطلق، لا يمكن للشخص الاتصال بالإنترنت، سواء كان ذلك بقصد ارتكاب جريمة أو لمجرد التصفح أو الدخول في الاتصال المباشر وغير ذلك.[1]

حيث إن الفقه القانوني اشترط لقيام الركن المادي ثلاثة عناصر هي:

-**الفعل** : وقد يكون السلوك الإجرامي إيجابياً بارتكاب الجريمة عبر حركة إرادية يقوم بها الجاني لتنفيذ الجريمة المنسوبة إليه. إذا كانت هذه الحركة خالية من الإرادة المسيطرة عليها فإن السلوك الإجرامي يفقد صفته الإرادية، وهو أحد عناصر الركن المادي. كما يمكن أن يكون الفعل الإجرامي سلبياً بالامتناع، عندما يحجم الشخص عن اتخاذ سلوك إيجابي محدد يتوجب عليه قانونياً القيام به في ظروف معينة.[2]

-**النتيجة الإجرامية:** كان الفقه يشترط حدوث نتيجة جرمية لقيام الركن المادي للجرم، إلا أن التوجه الحديث في التجريم لم يعد يتطلب حدوث النتيجة الجرمية لقيام الجريمة في نوع معين من الجرائم، والتي تُعرف حالياً بجرائم الخطر. من بين هذه الجرائم الجريمة المنظمة، كما هو منصوص عليه في اتفاقية الأمم المتحدة لعام 2000، التي تعاقب على مجرد الاتفاق لارتكاب إحدى الجرائم المنصوص عليها، حتى لو لم تتحقق النتيجة الجرمية.

-**العلاقة السببية** : إذا كان القانون يشترط حصول نتيجة جرمية لقيام الجريمة، فلا بد من وجود علاقة سببية بين الفعل والنتيجة حتى يستكمل الركن المادي عناصره. تلعب علاقة السببية دورًا هامًا في تحديد حدود المسؤولية الجنائية، حيث تتحقق هذه المسؤولية عندما يمكن إسناد النتيجة التي وقعت إلى مرتكب السلوك الذي أدى إليها، وتستبعد المسؤولية عندما لا تكون النتيجة مرتبطة بالفعل ارتباطًا سببيًا.

---

[1] حجازي عبد الفتاح بيومي، جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2004، صفحة 113.

[2] مؤيد محمد القضاة، شرح قانون العقوبات الاتحادي الإماراتي، مكتبة الجامعة، الشارقة، الإمارات العربية المتحدة، 2014، صفحة 173.

هذه هي عناصر الركن المادي التي يجب توافرها مجتمعة حتى يستكمل عناصره. يختلف الركن المادي في الجريمة الإلكترونية عن الجريمة التقليدية، حيث يمكن رؤية السلوك الإجرامي في الجرائم التقليدية بالعين والتأكد منه، مثل القتل أو السرقة أو التزوير.[1]

ثانياً: الركن المعنوي في الجريمة الإلكترونية

الركن المعنوي هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني. في تحديد الركن المعنوي للجريمة، يتنقل المشرع الأمريكي بين مبدأ الإرادة ومبدأ العلم. يستخدم مبدأ الإرادة في بعض الحالات، مثل قانون العلامات التجارية في القانون الفيدرالي الأمريكي، بينما يأخذ بمبدأ العلم في حالات أخرى، مثل قانون مكافحة الاستنساخ الأمريكي.[2]

ويتوفر القصد الجنائي في حق الجاني في حالات ثلاثة هي:

– **الأولى:** إذا كان الجاني يتوقع ويريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر الذي حدث والذي يعلق عليه القانون وجود الجري

–**الثانية** : إذا نجم عن الفعل أو الامتناع ضرر أو خطر أكثر جسامة مما كان يقصده الفاعل وذلك في حالة جواز القصد التي ينص عليها القانون صراحة على إمكان ارتكابها بهذا الوصف.

–**الثالثة:** الحالات التي يعزى فيها القانون الفعل إلى الفاعل نتيجة لفعله أو امتناعه، أي الحالات التي يفترض فيها القانون توافر القصد الجنائي لدى الجاني افتراضًا. ويستند القانون

[1] سبع زيان، سلمى المفتي، صور وأركان الجريمة المنظمة، دراسة مقارنة في القانون الإماراتي والقانون الجزائري، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 13، العدد 3، 2020، صفحة 233.

[2] خالد ممدوح إبراهيم، المرجع السابق، صفحة 100.

في ذلك إلى أن النتيجة الجسيمة التي تحققت نشأت عن فعل الجاني، وبالتالي يجب على الجاني أن يتحمل نتائجها سواء توقعها أم لم يتوقعها.[1]

إن توافر الركن المعنوي في الجرائم الإلكترونية يعد أمرًا هامًا في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص القانونية التي يجب تطبيقها. بدون الركن المعنوي، لن يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع. على سبيل المثال التمييز بين جريمة الدخول غير المشروع على نظم المعالجة الآلية للبيانات وجريمة تجاوز الصلاحيات في الدخول يعد تمييزًا دقيقًا. في جريمة تجاوز صلاحية الدخول، يلزم توافر صلاحية الدخول على نظام ما، ولكن يجب أن يكون هناك داخل هذا النظام أنظمة معينة لا يملك هذا الشخص الحق في الدخول عليها، فيقوم بالدخول عليها. في هذه الحالة، لا تتوافر سوى جريمة واحدة حيث إن الشخص يملك صلاحية الدخول على النظام الأساسي ولكن ليس على الأنظمة الداخلية. تكوين النشاط المادي هنا يتطلب أن يكون السلوك "الإجرامي" مرتكبًا في إطار نشاط ثانٍ وليس النشاط الأول. مثل هذا الأمر يجعل جريمة تجاوز صلاحيات الدخول من الجرائم التي لا يتطلب فيها ركنًا معنويًا، وهذا الأمر محرم قانونًا.[2]

وتختلف الجريمة الإلكترونية عن الجريمة التقليدية من حيث الركن المادي، حيث يتكون في القانون الجنائي من ثلاثة عناصر وهي السلوك الإجرامي أو النشاط الإجرامي، والنتيجة وعلاقة السببية. يختلف النشاط الإجرامي في جرائم الإنترنت عن الجرائم التقليدية، إذ يعتبر في الجرائم التقليدية عملاً ملموساً، بينما في الجرائم الإلكترونية يكون النشاط الإجرامي ذا طبيعة افتراضية للغاية.

هذا من جهة، ومن جهة أخرى، يجب أن يشمل النشاط الإجرامي في الجرائم الإلكترونية نشاطًا تقنيًا محددًا يتمثل في استخدام الحاسوب والإنترنت. أي أنه لارتكاب جرائم الإنترنت

[1] محمد الجبور، الوسيط في قانون العقوبات القسم العام، الطبعة 1، دار وائل، عمان، الأردن، 2021، صفحة 238.

[2] عبد الله دغش العجمي، المرجع السابق، صفحة 30.

يجب توفر منطلق تقني، على عكس الجرائم التقليدية التي يتكون فيها النشاط الإجرامي من فعل مادي لا يحتاج إلى التقنية العالية المطلوبة في الجرائم الإلكترونية.[1]

الفرع الثاني: دوافع ارتكاب الجريمة الإلكترونية

الدافع أو الباعث أو الغرض أو الغاية هي مصطلحات لها دلالتها الاصطلاحية في القانون الجنائي، وترتبط بما يُعرف بالصد الخاص في الجريمة. وتتعدد الدوافع التي قد تدفع لارتكاب الجرائم الإلكترونية؛ فبعضها قد يرجع إلى دوافع شخصية، ومنها ما قد ينبع من دوافع خارجية، وأخرى قد تكون خاصة بالمؤسسات. وتُعدّ الرغبة الإجرامية مصدرًا محتملاً لجميع هذه الدوافع، وسنستعرض كل دافع في النقاط التالية:

أولاً: الدوافع الشخصية

ويمكن تصنيف الدوافع الشخصية لمرتكبي الجرائم المعلوماتية إلى دوافع مالية وذهنية أو نمطية.

ثانيا: الدوافع المادية

السعي إلى تحقيق الكسب المالي يعد واحدًا من أبرز الدوافع التي تحرك الجناة لارتكاب الجرائم الإلكترونية، حيث تتطلب خصائص هذه الجرائم حجمًا كبيرًا من الربح المالي المحتمل ويزيد من تعزيز هذا الدافع خاصة في الجرائم مثل غش الحاسوب أو الاحتيال المعقد، حيث يمكن تحقيق ثروة فاحشة. كمثال، في فرنسا في عام 1986، كان العائد من جريمة سرقة مع معمل سلاح هو 70,000 فرنك فرنسي، بينما حصل الجاني على 670,000 فرنك فرنسي من جريمة الغش في مجال المعالجة الآلية للبيانات، أي أكثر من 38 مرة.[2]

وتشير الدراسات الحديثة إلى أن الدافع الرئيسي وراء جرائم التقنية يتمثل في الرغبة في تحقيق مكاسب مالية شخصية، وهذا يعكس اتجاه مستمر للمجرمين نحو هذا الهدف. تشمل

[1] هبة نبيلة هروال، المرجع السابق، صفحة 58.

[2] خالد ممدوح إبراهيم، المرجع سابق، من صفحة 37 إلى صفحة 38.

هذه الدراسات التحليلية والإحصائية التقارير التي تصدرها مراكز الأبحاث الرائدة مثل مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية (N.F.I.C).

هناك أيضًا فئة من مرتكبي الجرائم الإلكترونية يعود ارتكابهم إلى المشاكل المالية نتيجة للمشاكل العائلية أو الخسائر الكبيرة من القمار أو إدمان المخدرات. بالنسبة لبعضهم، قد تبدو جميع الوسائل مبررة في هذه الحالات، حيث يكون الهدف مبررًا لاختيار الوسيلة.

ب-الدوافع الذهنية أو النمطية

غالبًا ما يكون الدافع وراء ارتكاب الجرائم الإلكترونية هو الرغبة في إثبات الذات وتحقيق النجاح في التحدي مع التقنيات الحديثة، دون أن يكون لهم نوايا شريرة. يعود هذا إلى وجود ثغرات في التقنيات التي يستغلها محترفو برمجيات النظام لتنفيذ هذه الجرائم. وبناءً على ذلك يعتقد البعض أن دافع ارتكاب الجرائم الإلكترونية يكمن في الرغبة في تحديد وقهر النظام بدلاً من الرغبة في الربح.[1]

وعلى الرغم من أن الدراسات لا تثبت هذه الحقيقة تمامًا، حيث تشير إلى أن الرغبة في تحقيق الربح تعتبر الدافع الرئيسي وراء جرائم الحواسيب بشكل عام، فإن الدافع الثاني يظهر بوضوح في العديد من جرائم الحواسيب، خاصة فيما يتعلق بأنشطة المتطفلين الداخليين على النظام، والتي تشمل جرائم التوصل إلى أنظمة الحاسوب عن بُعد والتي تعتبر من أشهر أنواع جرائم الحواسيب.

ثانيًا: الدوافع الخارجية

في بعض الحالات، يتأثر الأفراد ويستجيبون للمؤثرات الخارجية بشكل يؤدي إلى ارتكاب بعض الجرائم الإلكترونية، وذلك نتيجة لوجودهم في بيئة المعالجة الآلية للمعلومات وتوافر بعض المؤشرات. وفي النهاية، يمكن أن يؤدي هذا الوضع إلى ارتكاب جرائم إلكترونية. تتنوع

[1] أحمد خليفة ملط، الجرائم المعلوماتية، طبعة 1، دار الفكر الجامعي، الإسكندرية، مصر، 2006، من صفحة 89 إلى صفحة 90.

المؤثرات التي تدفع الأفراد نحو ارتكاب مثل هذا السلوك، سواء كانت نتيجة للانتقام، الجنون العظمة، التعاون والتواطؤ مع الآخرين، أو التهديدات الخارجية.[1]

أ-دافع الانتقام وإلحاق الضرر برب العمل

قد يكون الانتقام دافعًا قويًا لارتكاب الجرائم، كما حدث في حالة محاسب شاب قام بتلاعب بالبرمجيات في منشأة معينة، ثم بعد مغادرته تم تدمير بيانات المنشأة. يظهر أن العاملين في مجال التقنية أو غيرهم يتعرضون لضغوطات نفسية نتيجة الضغط المالي والعمليات اليومية. في بعض الحالات، يمكن أن تكون هذه الضغوطات دافعًا لتحقيق الربح ولكن في حالات أخرى، قد تدفع إلى الانتقام من رب العمل. بالتالي، يُعتبر زرع الفيروسات في نظام الكمبيوتر من الأنشطة الرئيسية التي يتخذها البعض كوسيلة للانتقام.

ب-الرغبة في قهر النظام والتفوق على تعقيد رسائل التقنية

مرتكبو الجرائم الإلكترونية يسعون إلى إظهار تفوقهم وارتفاع مستواهم، فعندما تظهر تقنية جديدة، يتحمسون لاستكشافها وغالبًا ما يجدون الطريقة لاختراقها. يزداد انتشار هذا الدافع بين الشباب الذين يقضون وقتًا طويلاً أمام أجهزتهم بحثًا عن ثغرات في أنظمة الحواسيب والشبكات لإظهار مهاراتهم التقنية. يُعتبر هذا الدافع واحدًا من أكثر الدوافع استغلالًا من قبل منظمات الجريمة، حيث يتم استقطاب خبراء الاختراق للمشاركة في أنشطة جريمة معقدة أو توظيفهم لتنفيذ هذه الجرائم، وهذا هو الحل الذي يُفضله.

الدوافع المختلفة، بما في ذلك الإرهاب الإلكتروني والصراعات الأيديولوجية، قد تتداخل في أنشطة الجريمة الإلكترونية. بالإضافة إلى ذلك، تحرك أنشطة الاستيلاء على الأسرار التجارية دوافع المنافسة. في بعض الأحيان، يمكن أن تتشابك هذه الدوافع وتتعاون في الفعل الواحد، مما يجعل من الصعب التمييز بينها.

وتتميز الجريمة الإلكترونية عن الجريمة التقليدية في أنها تشمل العنف وسفك الدماء بينما تعتمد جرائم الإنترنت على الذكاء والحيلة. في جرائم الإنترنت، كما سبق الذكر، تُعتبر

1 خالد ممدوح إبراهيم، المرجع السابق، صفحة 39.

جرائم الإغراء والتلاعب مما يحتاج إلى ذكاء، ولا يوجد فيها عنف أو سفك للدماء، ولا آثار للاقتحام لسرقة الأموال.[1]

وعادةً ما تُرتكب الجرائم التقليدية بواسطة مجهولين، وعندما يتم اكتشافها، يكون من الصعب إثباتها ومحاكمة المتهمين بها. وعلى الرغم من ذلك، يُحتمل أن يتردد المجتمع في الإبلاغ عن هذه الجرائم خشية التأثير على السمعة والثقة في فعالية القضاء. في حالة الجرائم الإلكترونية، قد تُرتكب ضد مجهول أو تكون متعلقة بمعلومات قابلة للتعقب.[2]

الفرع الثالث: أهم أنواع وأشكال الجريمة الالكترونية.

من الصعب تحديد أنواع الجريمة الإلكترونية بدقة، حيث تتنوع وتتزايد تلك الأشكال مع زيادة استخدام الحاسوب وشبكة الإنترنت. يتضمن أهم أهدافها الحصول على المعلومات، سواء كانت مخزنة على الأجهزة الحاسوبية أو تنتقل عبر الإنترنت، إضافة إلى الاستيلاء على الأموال، واستهداف الأفراد أو الجهات الخاصة. تقسمها الفقه إلى طائفتين رئيسيتين هما:

أولاً: الجرائم الموجهة ضد نظم المعلوماتية.

الجرائم الموجهة ضد النظام المعلوماتي قد تشمل الضرر بالمكونات المادية للنظام مثل الأجهزة والبرمجيات، أو الإخلال بالمعلومات المسجلة عليه، وسنعرض بعضها كما يلي:

أ. الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

وتعتبر هذه الجرائم من الجرائم التي تدخل في نطاق الجرائم التقليدية. وتندرج هذه الجرائم ضمن الجرائم العادية التي تستهدف المال، باعتبار أن المكونات المادية للحاسوب هي أموال منقولة تصلح للاعتداء عليها، والجرائم الموصوفة بأنها تقع على المال، وجرائم التدمير

[1] محمود صالح العادلي، الفارغ التشريعي في مجال مكافحة الجرائم المعلوماتية، بحث منشور على الإنترنت، الموقع DRLADLY.COM، صفحة 38، تاريخ الإطلاع: 2024/04/23، على الساعة: 16:00.

[2] هبة نبيلة هروال، مرجع سابق، صفحة 58.

والتخريب، ولا ترتبط بالمعلومات. التكنولوجيا باستثناء استخدام الأجهزة المادية التي تكون موضوع الجريمة. في تشغيل نظام المعلومات.

ومن الجرائم المرتكبة ضد المكونات المادية لنظام المعلومات جريمة سرقة وقت الآلة كما كانت تسمى في الفقه الفرنسي – vol du tempsmachine أو سرقة وقت الآلة vol du temps – ordinur أو جريمة السرقة من الوقت والخدمات.[1]

ب-الجرائم الواقعة على المكونات المنطقية للنظام المعلوماتي

وتحدث جريمة التعدي على المكونات غير الملموسة لنظام المعلومات عندما تكون مكونات المعلومات غير الملموسة للحاسوب، مثل البرامج المستخدمة والبيانات المخزنة في ذاكرة الحاسوب، هي محل الجريمة أو محلها. والمقصود بالبرنامج المنطقي أو الكيان المنطقي هو مجموعة الأوامر التي تسمح بتشغيل الحاسوب أو أنظمة المعلومات المخصصة لمعالجة المعلومات بهدف إتمام عملية معينة أو إعطاء نتائج محددة.[2]

وتتخذ جرائم مهاجمة برامج الكمبيوتر شكلين:

أولا: بشكل مهاجمة البرامج التطبيقية والثاني بشكل مهاجمة برامج التشغيل. وفيما يتعلق بالبرامج التطبيقية، يشكل هذا النوع من الجرائم نسبة تقدر بحوالي 15% من إجمالي قضايا الجرائم الإلكترونية. أما بالنسبة لتشغيل البرامج، فإن الجريمة في هذه الحالة تتم من خلال تزويد البرنامج بمجموعة إضافية من التعليمات التي يمكن الوصول إليها بسهولة من خلال كود يسمح بالحصول على كافة البيانات الموجودة في نظام المعلومات.

الجرائم ضد المعلومات المسجلة في نظام المعلومات: يركز هذا النوع من الجرائم على المعلومات باعتبارها المحور الأساسي الذي تدور حوله تكنولوجيا المعلومات والذي يمثل

[1] خالد ممدوح ابراهيم، المرجع السابق، صفحة 116.

[2] هدى حامد قشقوش، جرائم الحاسوب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، صفحة 15.

المعالجة الآلية للبيانات والمعلومات. والحقيقة أن المعلومات هي أساس عمل نظام المعلومات ومن أشكال هذه الجرائم التلاعب بالمعلومات وإتلافها.

ثانياً: الجرائم المرتكبة بواسطة نظام المعلومات. وتتنوع الجرائم التي ترتكبها أنظمة المعلومات إلى جرائم اقتصادية، أو قرصنة معلوماتية، أو ذات طبيعة سياسية أو تتعلق بالأمن القومي. أو قد تحدث هذه الجرائم ضد الأشخاص الطبيعيين أو الاعتباريين. وهذه الجرائم هي[1]:

أ- الجرائم الإلكترونية الواقعة على الأشخاص

تستهدف معظم الجرائم المرتكبة في مجال تكنولوجيا المعلومات إما أفراداً أو جهات محددة، وغالباً ما تكون هذه الجرائم جرائم مباشرة، ترتكب في شكل ابتزاز أو تهديد أو تشهير وعبر وسائل التواصل الاجتماعي مثل فيسبوك، وفايبر، وواتساب. ومن أهم الجرائم التي تقع على الأشخاص جرائم التصنيع والنشر. تتخذ المواد الإباحية والجنس، سواء للبالغين أو الأطفال، أشكالًا مختلفة، بدءًا من الصور وحتى تسجيلات الفيديو والصوت التي تتم عبر الإنترنت.[2]

ب- الجرائم الإلكترونية المتعلقة بالأموال

وتستهدف أغلب هذه الجرائم أعضاء الخدمة المالية على وجه التحديد، ويكون الجشع وراء ارتكابها هو الحصول على تلك الأموال والاستيلاء عليها، كما أن فكرة الكسب السريع تدفع مرتكبيها. وقد يكون ارتكابها في بعض الأحيان مجرد إخضاع نظام مؤسسة (مؤسسة)

[1] فريحة حسين، الجرائم الالكترونية والأنترنت، مقال منشور بمجلة المعلوماتية، السعودية، العدد 36، أكتوبر 2011، صفحة 4.

[2] يوسف صغير، الجريمة الإلكترونية المرتكبة عبر الإنترنت، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، 2013. صفحة 50.

مثلاً، وتجاوز حواجز الحماية أو انتقاماً من مالك تلك المؤسسة أو أحد أعضائها.[1] مثل جرائم السطو والسرقة والتحويل الإلكتروني غير القانوني للأموال، وجريمة غسيل الأموال الإلكترونية والاختراق غير القانوني للحسابات المصرفية.[2]

ج- الجرائم الواقعة على أمن الدولة

وهي من أخطر الجرائم الإلكترونية ومن أهمها الإرهاب الإلكتروني والتجسس الإلكتروني، اللذين يهددان الأسرار العسكرية والاقتصادية للدول، مما يسهل خلق الفوضى والإضرار بأمنها الداخلي.

ثالثًا: أنواع الجرائم الإلكترونية في التشريع الجزائري

تناول المشرع الجزائري أشكال التعدي على أنظمة المعالجة الآلية للبيانات من خلال قانون العقوبات، وهي:

أ-جريمة الدخول والبقاء بطريقة غير مشروعة في نظام معالجة البيانات الآلي منصوص عليها في المادة 394 مكرر من قانون العقوبات، حيث يعاقب على مجرد الدخول إلى النظام أو البقاء بشكل غير قانوني في نظام المعلومات دون علم المجني عليه.[3]

ب-جريمة التلاعب بالبيانات في أنظمة المعالجة الآلية للبيانات منصوص عليها في المادة 3/323 من قانون العقوبات الجزائري. وهذه الجريمة لها ثلاثة أشكال: المحو، والتعديل، والإدخال.

أما فيما يتعلق بجريمة عرقلة أو تشويه تشغيل أنظمة المعالجة الآلية للبيانات فلم يرد لها نص محدد واقتصر المشرع على جريمة التلاعب بالبيانات في أنظمة المعالجة الآلية والعرقلة التي تدخل في إطار حجب المعلومات النظام بأي وسيلة.

[1] حكيم سياب، المرجع السابق، صفحة 221.

[2] خالد ممدوح ابراهيم، المرجع السابق، صفحة 76.

[3] المرجع نفسه، صفحة 115.

الفصل الثاني: آليات التحقيق في الجرائم الإلكترونية

تمهيد:

إن طبيعة الجرائم الإلكترونية بعناصرها ووسائل ارتكابها قد تدفع المشرع الجنائي إلى إعادة النظر في كثير من المسائل الجزائية، خاصة فيما يتعلق بمسألة الإثبات، لأن الأدلة التي تقوي الإثبات في هذا النوع من الجرائم يجب أن تكون من ذات طبيعة إلكترونية، وهو ما يقودنا إلى المناقشة. فيما يتعلق بمسألة مدى قبول هذه الأدلة أمام القضاء ومدى تعبيرها عن الحقيقة، نظراً لما قد تتعرض له من تزوير وأخطاء، فضلاً عن مصداقيتها ومشروعيتها.

وقد تم تقسيم هذا الفصل إلى قسمين. القسم الأول بعنوان "إجراءات التحقيق للحصول على الأدلة الإلكترونية"، بينما المبحث الثاني بعنوان "القواعد الإجرائية للحصول على الأدلة الإلكترونية".

المبحث الأول: إجراءات التحقيق في الحصول على الدليل الرقمي الإلكتروني

إن التطور التقني لنظام المعالجة الآلية، فضلا عن الطبيعة الخاصة للأدلة الرقمية سيؤدي حتما إلى تغيير العديد من المفاهيم السائدة حول إجراءات وطرق الحصول عليها الأمر الذي يتطلب بالضرورة إعادة تقييم المنهج المتبع لدى البعض. الإجراءات التقليدية في قانون الإجراءات الجنائية، فضلا عن تطوير القواعد الإجرائية. والبعض الآخر يتوافق مع طبيعة البيئة التقنية. إن تطوير الأدلة ووسائلها أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم. وهذا هو الأمر الذي سنتناوله من حيث دراسة القواعد الإجرائية التقليدية ومدى إمكانية الاعتماد عليها في الحصول على الأدلة الرقمية في المطلب الأول. ثم نقدم القواعد. الإجراءات الحديثة لاستخراج الأدلة الإلكترونية في المطلب الثاني.

المطلب الأول: القواعد الإجرائية التقليدية في الحصول على الدليل الإلكتروني

ولا شك أن المشرع لم يجيز استخراج الأدلة دون ضوابط تحكم ذلك من خلال قواعد إجرائية معينة أهمها التفتيش وضبط الأشياء والتجربة والتفتيش، وهو ما سنتناوله في هذا المطلب.

الفرع الأول: التفتيش وضبط الأدلة

أولًا: التفتيش

ولم يقدم المشرع الجزائري تعريفا محددا ودقيقا للتفتيش بقدر ما اعتبره إجراء تحقيقيا وأحاطه بضوابط صارمة نظرا لأهميته في كشف الأدلة من جهة، وخطورته من حيث ما يترتب على ذلك من مخالفة للقانون. وحرية الناس وكرامتهم من جهة أخرى.[1] وخير دليل على ذلك اهتمام الدستور الجزائري بأهمية هذا الإجراء من خلال نص المادة 40 منه التي نصت على ما يلي: "لا يجوز التفتيش إلا وفقا للقانون وفي إطار احترامه، ولا يجوز التفتيش إلا بموجب أمر كتابي صادر عن السلطة القضائية المختصة.

تنص المادة 15 من القانون 04-09، الذي يتضمن قواعد خاصة لمنع ومكافحة الجرائم المتعلقة بالتكنولوجيا العالمية والاتصالات، على ما يلي: "تتولى السلطات القضائية المختصة، وكذلك أفراد الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي إطار قانون في الحالات المنصوص عليها في المادة 04 أعلاه، يجوز، لغرض التفتيش، ولو عن بعد الدخول إلى نظام المعلومات أو جزء منه، وكذلك البيانات المخزنة فيه ونظام تخزين المعلومات.[2]

يمكن تعريف التفتيش بأنه ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي، ولا يجوز إجراؤه إلا من قبل النيابة العامة وقاضي التحقيق.[3]

---

[1] خالد ممدوح ابراهيم، مرجع سابق، صفحة 212.

[2] القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا العالم والاتصال ومكافحتها، المؤرخ في 14 شعبان 1430 الموافق لـ 5 أغسطس 2009، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادر بتاريخ 25 شعبان 1430 الموافق 16 أغسطس 2009، صفحة 6.

[3] مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها، كلية الحقوق والإدارة العامة، جامعة بيرزيت، رام الله، فلسطين، المجلد 4، العدد 2018، الصفحة 289.

أ. القواعد الموضوعية لتفتيش الحاسوب

وتلخص هذه القواعد كالتالي:

– حدوث جريمة إلكترونية.

–توافر أدلة إلكترونية قوية أو أدلة على وجود أشياء أو أجهزة أو معدات معلوماتية أو إلكترونية تفيد في كشف الجريمة.

–أن يكون موضوع التفتيش هو جهاز الكمبيوتر بكافة مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به.

ب. القواعد الشكلية لتفتيش نظام الحاسوب

تتضمن عدة قواعد منها:

– أن يتم التفتيش بشكل آلي من خلال أجهزة مخصصة.

– أن يتم التفتيش بعد التخطيط المسبق.

– تشكيل فريق تفتيش يضم خبراء وفنيين متخصصين في الحواسيب والأنظمة الإلكترونية.[1]

ثانيًا: الضبط

تتمثل عملية الضبط في العثور على أدلة الجريمة التي يجري التحقيق فيها وضبطها. تعتبر الضبطية هدف التفتيش والنتيجة المباشرة والمستهدفة. ولذلك يجب عند إجرائها أن تكون لها نفس القواعد المطبقة في التفتيش، وعدم التفتيش يؤدي إلى فشل الحجز.

تختلف مكافحة جرائم المعلوماتية عن مكافحة الجرائم الأخرى من حيث المكان، لأن الجرائم الإلكترونية تنطوي على السيطرة على أشياء ذات طبيعة غير ملموسة من بيانات

[1] عيدة بلعايد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، جامعة مولاي الطاهر، سكيكدة، 2011، المجلد 06، العدد 143، صفحة 143.

ومراسلات واتصالات إلكترونية، وأشياء ذات طبيعة مادية مثل الكمبيوتر وملحقاته والأجهزة الخارجية. الأقراص والأقراص المرنة.[1]

الفرع الثاني: المعاينة

يعد التفتيش من أهم مراحل التحقيق في الجرائم الجديدة لما يمكن أن يقدمه من أدلة لإثبات الجريمة، وتتزايد أهميته في إثبات الجرائم الإلكترونية عبر الإنترنت، حيث يقوم على التفتيش على عدد من البرامج أو الأقراص وكل ما يتعلق بالحاسوب الشخصي، وذلك لطبيعة الفحص الخاصة في هذا المجال. ولذلك فإن جوهر التفتيش هو الملاحظة والفحص الجسدي المباشر لمكان أو شخص أو أي شيء له علاقة بالجريمة من أجل الوقوف على حالتها والتحفظ على كل ما يفيد في كشف الحقيقة. ويجوز اللجوء إلى التفتيش في جميع الجرائم.[2]

إلا أن أغلبية التشريعات، بما فيها التشريع الجزائري، تقتصر على الجنايات والجنح الكبرى، حيث تعتبر إجراء واجبا في الجنايات ومباحا في الجنح، ويمكن إجراؤها في مكان عام أو خاص. وإذا كان في مكان عام فلا يحتاج مأمور الضبط القضائي إلى إذن أو تفويض. ويجب إجراء التحقيق لإجرائه، أما إذا كان في مكان خاص فيجب أن تكون صحته إما برضا صاحب المكان أو وجود إذن مسبق من سلطة التحقيق بإجرائه.

لتحقيق الفحص، يجب مراعاة خطوات وإرشادات محددة، بما في ذلك:

– تتضمن عملية التصوير الفوتوغرافي للكمبيوتر وملحقاته، بالإضافة إلى تشغيل وقت التقاط الصور. ويتم تطبيق سياسة عدم نقل أي معلومات قبل إجراء الاختبارات اللازمة للتأكد من خلو الموقع من أي مجالات مغناطيسية قد تؤدي إلى محو أو تلف البيانات.[3]

– الحفاظ على سلة مهملات الأوراق الممزقة والأوراق المستعملة والأشرطة والأقراص المغناطيسية والغير صحية لفحصها وإزالة بصمات الأصابع.

–إعداد خطة تفصيلية للمنشأة التي وقعت فيها الجريمة.

---

[1] خالد ممدوح ابراهيم، مرجع سابق، صفحة 221.

[2] عيدة بلعابد، مرجع سابق، صفحة 140.

[3] عيدة بلعابد، مرجع سابق، صفحة 141.

-جعل التفتيش الإلكتروني سرياً ومقتصراً على الباحثين والمحققين المؤهلين تأهيلاً عالياً وذوي الخبرة الفنية.

الفرع الثالث: الخبرة

الاستعانة بالخبراء هي أحد الإجراءات التي تلجأ إليها كل من السلطة القضائية وسلطات التحقيق عندما يتعذر عليهم الأمر. ومن هذه المجالات التي تتطلب اللجوء إلى الخبرة نجد الجرائم الإلكترونية، إذ لا يستطيع التعامل مع هذه الجريمة إلا من لديه المعرفة والخبرة في مجال الإلكترونيات.

أولًا: أنواع الخبراء الإلكترونيين

الخبير في الجرائم الإلكترونية هو فني متخصص لديه خبرة في مجال التكنولوجيا الإلكترونية وشبكاتها. ويكون قد رأى أو سمع أو أدرك بحواسه معلومات مهمة ضرورية للدخول إلى نظام معالجة البيانات الرقمية الآلي إذا كانت مصلحة التحقيق تقتضي البحث عن أدلة رقمية إلكترونية داخله. ويعتبر الخبراء الالكترونيون هم:

- المبرمجون
-المحللون هم الأشخاص الذين يحددون خطوات العمل ويجمعون البيانات لنظام معين
-مهندسي الصيانة والاتصالات
-مشغلي الكمبيوتر
-مدير نظام المعلومات[1]

ثانيًا: أهمية الخبرة في البحث عن الدليل الإلكتروني

وتكمن أهمية الخبرة في الأدلة التي تقدمها إلى جهات التحقيق والقضاء والجهات الأخرى المختصة بالدعوى الجزائية. ولذلك اهتم المشرع الجزائري بتنظيم عمل الخبرة في المواد من 143 إلى 156 من قانون الإجراءات الجزائية واعتبره أحد إجراءات البحث عن الأدلة. ونصت المادة 143 على أنه "لجهة التحقيق أو الحكم، عند عرض عليها مسألة ذات طبيعة فنية، أن

[1] يوسف صغير، مرجع سابق، صفحة 89.

تأمر بندب خبير إما من تلقاء نفسها أو بناء على طلب النيابة العامة أو بناء على طلب الخصوم".[1]

كما أشار المشرع الجزائري في المادة 05 الفقرة الأخيرة من القانون رقم 04-09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه "يمكن للسلطة المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".[2]

المطلب الثاني: القواعد الإجرائية الحديثة في الحصول على الدليل الإلكتروني

وقد شهد تطور أساليب ارتكاب الجرائم السيبرانية منحنى تصاعديا بين الجرائم المرتكبة في الجزائر، مما اضطر المشرع إلى الاعتماد على قواعد إجرائية خاصة في سبيل مكافحة الجرائم السيبرانية، وهو ما جاء في القانون عدد 06-22 الصادر في ديسمبر 2006 بتعديل وتتميم الأمر العدد 155-66 المؤرخ في 08 جويلية 1966 المتضمن قانون الإجراءات الجزائية.

الفرع الأول: التسرب الإلكتروني

وقد تناول المشرع الجزائري تعريف التسرب من خلال نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية بعد أن تم تعديله بالقانون 06-22 والذي نص على ما يلي: "التسرب يعني أن أحد ضباط أو أعوان الشرطة القضائية، تحت مسئولية ويقوم ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم. يجوز لمأمور الضبط القضائي أو أعوانه، عند ارتكاب جناية أو جنحة بإيهامهم أنه فاعلها أو شريك فيها، أن يستعمل لهذا الغرض اسما مستعارا وأن يرتكب عند الاقتضاء الأفعال المنصوص عليها في المادة 69

[1] القانون رقم 66-155 المؤرخ في 8 يونيو 1966، المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 48، المعدل والمتمم للأمر 15-02 المؤرخ في 23 يوليو 2015، العدد 4.

[2] القانون 04-09 السالف الذكر.

مكررا 14 أدناه. ولا يجوز أن تشكل هذه الأفعال تحريضاً على ارتكاب جرائم تحت طائلة البطلان.[1]

التسرب هو عندما يقوم ضابط أو وكيل الشرطة القضائية بمراقبة الأشخاص المشتبه في ارتكابهم الجريمة من خلال إظهار أنه شارك معهم أو كان شريكا، ويستخدم الضابط أو الوكيل هوية مزورة إذا كان مرتبطا بإحدى هذه الجرائم:

- جرائم المخدرات
-الجريمة المنظمة العابرة للحدود الوطنية
-الجرائم المتعلقة بأنظمة معالجة البيانات الآلية
-جرائم غسيل الأموال
-الجرائم الموصوفة بالأعمال الإرهابية
-الجرائم المتعلقة بالتشريعات المتعلقة بجرائم الصرف والفساد.[2]

الفرع الثاني: اعتراض المراسلات والمراقبة الإلكترونية

أولًا: مفهوم اعتراض المراسلات

مع تطبيق المادة 65 مكررا إلى 65 مكرر 10 من قانون الإجراءات الجزائية، يجوز لقاضي التحقيق أن يأمر أحد أعوان الضابطة العدلية، بإذن كتابي وتحت إشرافه المباشر بالتنصت على المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، ووضع الترتيبات الفنية دون موافقة الشخص المعني من أجل تنفيذ عملية الالتقاط والتركيب. التسجيل والبحث سرا وفي أي مكان عام عن طريق وسائل الاتصال السلكية أو اللاسلكية واتخاذ

[1] المادة 65 مكرر 5 من قانون الإجراءات الجزائية، أمر رقم 66-156 مؤرخ في 8 جوان 1966، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد 84 معدل ومتمم وفقا للقانون 06-22 المؤرخ في 20 جويلية 2006.

[2] فالح عبد القادر، آيت عبد المالك نادية، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، خميس مليانة، مجلد 04، العدد 02، 2019، صفحة 98.

الترتيبات الفنية دون إشراف ذوي الصلة لالتقاط الصور وتثبيت والبحث وتسجيل الكلام المنطوق سرا أو سرا من قبل شخص أو أكثر في الأماكن العامة أو أماكن خاصة.[1]

وهذا ما جاء في القانون 04-09 المتضمن القواعد الخاصة لمنع ومكافحة الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات، في المادة 2 من فقرة، في تعريفه للاتصالات الإلكترونية بأنها مراسلات أو إرسال أو استقبال إشارات أو إشارات. أو كتابات أو صور أو أصوات أو معلومات مختلفة بأي وسيلة كانت.

وتجدر الإشارة في هذا الصدد إلى أن الاتصالات التي يمكن اعتراضها يجب أن تتم في خصوصية، ولكي يتم ذلك لا بد من توافر عنصرين أساسيين:

– عنصر موضوعي يتعلق بموضوع الرسالة ومحتواها، أي أن الرسالة يجب أن تكون ذات طبيعة شخصية وسرية.

–عنصر شخصي ويعني إرادة المرسل في تحديد هوية المرسل إليه ورغبته في عدم السماح للآخرين بالاطلاع على محتوى الرسالة.

وعندما يتواجد هذان العنصران في الرسالة، فإنها توصف بأنها مراسلة خاصة لها خصوصيتها وسريتها المحمية قانونا، ولا يهم شكل الرسالة أو طريقة إرسالها وتسليمها إلى المرسل إليه. لا يجوز لمأموري الضبط القضائي اللجوء إلى اعتراض المراسلات إلا بعد الحصول على إذن كتابي مسبب من النائب العام أو القاضي. التحقيق إذا تم فتح تحقيق قضائي.

ثانيا: المراقبة الإلكترونية

تعد مراقبة الاتصالات الإلكترونية أو كما يطلق عليها "رصد الاتصالات الإلكترونية" من أهم المصادر التحقيقية المستخدمة في التحقيق في الجرائم المختلفة، بما في ذلك الجرائم المتعلقة بالتقنيات الحديثة، خاصة في ظل لجوء مرتكبيها إلى وسائل الاتصال التكنولوجية

[1] المادة 65 مكرر، قانون سالف الذكر من قانون الإجراءات الجزائية.

الحديثة. في تنفيذ مخططاتهم الإجرامية والتواصل. بينهم. تعد مراقبة الاتصالات الإلكترونية أيضًا مصدرًا للأدلة الرقمية.[1]

أ. مفهوم مراقبة الاتصالات الإلكترونية

ونجد أن المشرع الجزائري كغيره من المشرعين لم يحدد عملية مراقبة الاتصالات الإلكترونية، بل عرفتها بعض التشريعات مثل التشريع الأمريكي الذي عرفها على أساس أنها "عملية الاستماع إلى محتويات الأسلاك أو أي اتصالات شفهية باستخدام جهاز إلكتروني أو أي جهاز آخر. [2]

ولكن يمكننا تعريفها على أساس أنها تحقيق يتم بشكل سري ويتم فيه انتهاك سرية المحادثات الخاصة، بأمر من السلطة القضائية على الوجه المحدد قانونا بهدف الحصول على أدلة غير مادية على وقوع الجريمة المعلوماتية، والذي يتضمن من ناحية التنصت على المحادثات، ومن ناحية أخرى حفظها بواسطة أجهزة متخصصة لذلك.[3]

بينما حدد القانون 04-09 في المادة 3 منه كيفية مراقبة الاتصالات على النحو التالي: "مع مراعاة الأحكام القانونية التي تشمل سرية المراسلات والاتصالات، ومتطلبات حماية النظام العام، والمتطلبات، والتحقيقات، أو يجوز إجراء التحقيقات القضائية الجارية وفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية، ويضع هذا القانون الترتيبات الفنية لمراقبة الاتصالات الإلكترونية وجمع وتسجيل محتواها في الوقت المناسب، والقيام بإجراءات التفتيش والضبط خلال مدة زمنية محددة. نظام معلومات.[4]

ولذلك فإن مراقبة الاتصالات تحددها القوانين كاستثناء وحصرا في الحالات المنصوص عليها في المادة 04 من قانون منع الجرائم المتعلقة بالتكنولوجيا العالمية والاتصالات.

---

[1] عيدة بلعابد، مرجع سابق، صفحة 145

[2] فالح عبد القادر، آيت عبد المالك نادية، مرجع سابق، صفحة 99.

[3] بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية، مذكرة ماجستير، جامعة عبد الرحمن ميرة، بجاية، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، 2018-2017، صفحة 8.

[4] المادة 04 من القانون 04-09 المذكور أعلاه، صفحة 6.

المبحث الثاني: القيمة القانونية للدليل الإلكتروني

أثارت مسألة الأدلة الرقمية العديد من التساؤلات حول ما إذا كانت تعبر عن الحقيقة أم لا تعكسها، لما يمكن أن تتعرض له من تزييف وتحريف وتلاعب، مما يثير مسألة مشروعية النظر فيها، فالأدلة الجنائية بشكل عام هي ويشترط أن تكون مشروعة من حيث وجودها وإيصالها.

إن مجرد وجود دليل يثبت وقوع الجريمة وإسنادها إلى شخص معين لا يكفي ليكون دليلاً، إذ يجب أن تكون لهذا الدليل قيمة قانونية، وتتوقف قيمة الدليل الجنائي على مسألتين أساسيتين، الأولى هي الشرعية من الأدلة والثاني هو سلطة الأدلة المراد إثباتها.

المطلب الأول: مشروعية الدليل الإلكتروني

وتعرف الشرعية بأنها المطابقة والالتزام بأحكام القانون في إطاره ومحتواه العام. ويهدف إلى إرساء ضمانة أساسية وجادة للأفراد لحماية حقوقهم وحرياتهم الشخصية ضد تعسف السلطة وضد الاستغلال في غير الحالات التي يجيزها القانون، وذلك حماية للنظام الاجتماعي وبالقدر نفسه تحقيق حماية مماثلة. للفرد نفسه.[1]

ولذلك فإن صحة الإجراءات التي تقوم بها سلطة التحقيق يجب ألا تخل بمبدأ الشرعية للحصول على الأدلة الصحيحة والسليمة التي يبني عليها القضاء أحكامه. والحقيقة أن مشروعية الأدلة الإلكترونية هي مشروعية وجودها ومشروعية الحصول عليها.[2]

[1] عبد الله بن حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014، صفحة 55.

[2] سعيد علي نعيم، آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2013-2012. صفحة 207.

الفرع الأول: ماهية الدليل الإلكتروني

أولاً: تعريف الدليل الإلكتروني

هناك العديد من التعريفات التقليدية للأدلة الرقمية، رغم أنها في مجملها تلتقي على نقطة محددة تتعلق بالبيئة الإلكترونية لهذا الدليل الحديث. الأدلة الرقمية هي الأدلة المأخوذة من أجهزة الكمبيوتر على شكل موجات ونبضات مغناطيسية أو كهربائية يمكن جمعها وتحليلها باستخدام برامج تطبيقية وتقنيات خاصة. وهو مكون رقمي لتوفير المعلومات. بأشكال مختلفة مثل النصوص المكتوبة أو الصور أو الأصوات أو الرسومات حتى يتم اعتمادها من قبل جهات إنفاذ القانون.[1]

وتعرف أيضًا بالدليل الذي يجده الفرد في العالم الافتراضي والذي يقوده إلى الجريمة أو تلك المعلومات التي يقبلها المنطق والعقل ويقرها العلم، ويتم الحصول عليها من خلال الإجراءات القانونية والعلمية من خلال ترجمة البيانات الحسابية المخزنة في أجهزة الكمبيوتر الآلية وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو التحقيق. المحاكمة لإثبات حقيقة الفعل أو الشيء المتعلق بالجريمة أو المجني عليه.[2]

كما يمكن تعريف الأدلة الرقمية بأنها تلك الأدلة التي تشمل البيانات الإلكترونية المخزنة في جهاز الكمبيوتر والموجودة في البيئة الافتراضية، والتي من خلالها يتم الكشف عن الجريمة أو إثبات العلاقة بين وقوع الجريمة ومرتكبها.

ثانيا: خصائص الدليل الإلكتروني

تتمتع الأدلة الرقمية بمجموعة من الخصائص التي تميزها عن الأدلة الجنائية الأخرى. هذه الخصائص هي كما يلي[3]:

---

[1] محمد الأمين البشيري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، صفحة 3.

[2] عبيدة بلعابد، مرجع سابق، صفحة 153.

[3] سعيداني علي نعيم، مرجع سابق، صفحة 208.

1. الدليل الرقمي دليل علمي وتقني:

تتكون الأدلة الرقمية بشكل أساسي من مجموعة من البيانات والمعلومات ذات الطبيعة الإلكترونية غير الملموسة، والتي يتم إدراكها عن طريق الأجهزة والمعدات وأدوات المحاسبة الآلية واستخدام أنظمة البرمجيات الحاسوبية. وهذا ما يجعل الدليل الرقمي أحد الأدلة العلمية والتقنية الحديثة نظرا لبنيته التقنية في المجال الافتراضي. وهو أيضًا دليل يعتمد بشكل أساسي على التقنيات.[1]

2. الدليل الرقمي ذو طبيعة متطورة:

ويتميز الدليل الرقمي بتطوره العفوي نتيجة تطور البيئة الرقمية التي تعتمد بشكل أساسي على الابتكار. ويرجع ذلك إلى تقدم الثورة التكنولوجية وخاصة في مجال الاتصالات وأجهزة الاتصالات.[2]

3. صعوبة اتلاف الدليل الرقمي

قد يتم تدمير الأدلة الرقمية، سواء كليًا أو جزئيًا، من خلال عملية المسح. ومع ذلك فإن تدميرها لا يمنع من استرجاع محتوى الأدلة الرقمية من ذاكرة الحاسوب أو استخدام نسخ منها.[3]

ثالثًا: تقسيمات الدليل الإلكتروني

لم يتناول معظم فقهاء القانون الجنائي دراسة شاملة ودقيقة للأدلة الجنائية الرقمية بسبب حداثة هذا النوع من الأدلة وبيئته المتطورة باستمرار. ولكننا نشير إلى محاولة فقهية قسمت الأدلة الرقمية إلى أربعة أقسام[4]:

---

[1] عيدة بلعابد، مرجع نفسه، صفحة 154.

[2] مرجع نفسه، صفحة 155.

[3] محمد الامين البشرى، مرجع سابق، صفحة 136

[4] محمد الامين البشرى، مرجع سابق، صفحة 137.

-الأدلة الرقمية لأجهزة الكمبيوتر وشبكاتها، والتي تكون الأخيرة عبارة عن مقتطفات من برامج الكمبيوتر.

-الأدلة الرقمية عبر الإنترنت.

-الدليل الرقمي لبروتوكولات تبادل المعلومات بين الأجهزة في شبكة المعلومات العالمية.

-الأدلة الرقمية لشبكة المعلومات العالمية.

الفرع الثاني: مشروعية الدليل الإلكتروني في الوجود

إن مشروعية وجود الدليل الإلكتروني تقتضي أن يكون المشرع قد قبل هذه الأدلة كجزء من أدلة الإثبات الجنائي. ومشروعية الوجود تعني الاعتراف بالدليل، أي أن القانون يسمح للقاضي بالاعتماد عليه والاستدلال به لتكوين اعتقاده وقناعته ليقرر الإدانة أو البراءة، وربما المعيار الذي يتم تحديده على أساسه. موقف القوانين. وفيما يتعلق بسلطة القاضي الجزائري في قبول الأدلة الإلكترونية، فهي تتمثل في نظام الأدلة السائد في البلاد، حيث يختلف النظام القانوني في موقفه من حيث الأدلة التي يمكن قبولها في الأدلة، وهناك ثلاث فئات نذكرها سوف تناقش في هذا الفرع.

أولاً: نظام الإثبات المقيد

فيه يحدد المشرع سلفا وحصرا الأدلة التي يجوز للقاضي قبولها واستخدامها في الإثبات كما يحدد القوة الاستدلالية لكل دليل بناء على اقتناعه بها، بينما في هذا النظام ليس للقاضي الجزائري أي حق في الإثبات. دوره في تقييم الأدلة أو البحث عنها. [1] بل يقتصر دوره على فحص الأدلة للتأكد من مشروعيتها ومطابقتها للشروط التي يفرضها القانون. وإذا تم اختيار الشروط التي يقتضيها القانون في الأدلة، فلا يجوز للقاضي أن يحكم بالإدانة حتى ولو كانت لديه قناعة يقينية بأن المتهم ارتكب الجريمة المنسوبة إليه.[2]

ومن هنا، فمن الواضح أن نظام الإثبات المقيد يقوم على مبدأين أساسيين. الأول هو الدور الإيجابي للمشرع في عملية الإثبات، حيث ينظم قبول الأدلة، سواء بالتحديد المسبق

[1] فالح عبد القادر، آيت عبد المالك نادية، مرجع سابق، صفحة 100.

[2] مرجع نفسه، صفحة 101.

للدليل المقبول للحكم بالإدانة، أو باستبعاد الأدلة الأخرى، أو بإخضاع كل دليل لشروط معينة. شروطها، ولأنها تحدد القيمة المقنعة لكل دليل أنها تعطي سلطة قاطعة لبعض الأدلة، وحجة نسبية لبعض الأدلة الأخرى. أما المبدأ الثاني فيتمثل بالدور السلبي للقاضي الجزائي في الإثبات، إذ يلتزم بشدة بما يفرضه عليه المشرع من الأدلة الاستدلالية بما يفقده سلطته في الحكم بما يتفق مع الوقائع، وكثيراً ما يحكم بما يخالف قناعته التي كوَّنها من الأدلة التي يعترف بها ذلك النظام، فيصبح القاضي كالعبد في طاعته لنصوص القانون.[1]

ثانيًا: نظام الإثبات الحر

وهو نظام يسود فيه مبدأ حرية الإثبات، حيث لم يحدد المشرع طرقا معينة لإثباتها ولغزها أمام القضاء، بل يترك ذلك للقاضي الجزائري الذي له دور إيجابي في البحث عن المناسب الأدلة وتقدير قيمتها الإثباتية بحسب اقتناعه بها. ويجب عليه قانوناً أن يعتمد على أدلة محددة في تكوين إدانته، وله أن يبني هذه الإدانة على أي دليل يقدم في الدعوى، ولو لم يكن منصوصاً عليه فيها. بل إن المشرع في مثل هذا النظام لا يملك صلاحية اشتراط أدلة الإثبات، فكل دليل يستحق قيمته في نظر المشرع، والقاضي هو الذي يختار من بين ما يعرض عليه. من الأدلة التي يراها مفيدة للوصول إلى الحقيقة، له الحرية المطلقة في قبول الأدلة أو رفضها إذا لم يطمئن إليها، دون أن يطلب منه تعليل قناعته.[2]

ويجد هذا النظام مبرره في أن الإثبات في المواد الجنائية لا يركز على الوقائع الجسدية أو النفسية الخاصة بالجريمة، ولا على الأفعال القانونية التي وافق عليها المشرع سلفا من خلال تحديد وسائل إثباتها ومدى السلطة. التي يتمتع بها كل منهم. كما يركز الإثبات على

[1] نداء نائل فايز المصري، "خصوصية الجرائم المعلوماتية"، جامعة النجاح الوطنية، كلية الدراسات العليا، رسالة ماجستير، فلسطين، 2017، صفحة 95.

[2] فالح عبد القادر، آيت عبد المالك نادية، المرجع السابق، صفحة 103.

الوقائع الجنائية التي ينوي مرتكبوها، قدر الإمكان، إزالة آثارها ومحو آثارها، مما يحتم على القضاء استخدام كافة الوسائل المتاحة والممكنة لكشف الجريمة وتقصي الحقيقة.[1]

وعلى النقيض من نظام الإثبات المقيد، فإن فلسفة هذا النظام تقوم على مبدأين مختلفين:

الأول: يتمثل في الدور السلبي للمشرع في عملية الإثبات، حيث يمتنع المشرع من خلاله عن التحديد المسبق للأدلة الصالحة للإثبات، مما يفتح المجال أمام قبول جميع الأدلة حسب تقدير القاضي. القاضي وليس المشرع. أما المبدأ الثاني: فهو الدور الإيجابي للقاضي الجزائي في الإثبات، ويظهر ذلك من جانبين: الأول من خلال الحرية المطلقة التي يتمتع بها القاضي الجزائي في إثبات حقيقة الجريمة بجميع وسائل الإثبات والإثبات. وسلطته الواسعة في اتخاذ كافة الإجراءات، ومن جهة أخرى يمنح نظام الإثبات الحر للقاضي الجزائي. تقدير كبير في قبول الأدلة ووزنها وتقدير قيمتها الاستدلالية، استنادا إلى ثقافته وخبرته القانونية.

ثالثًا: نظام الإثبات المختلط

وهو نظام وسط بين نظام الإثبات المقيد ونظام الإثبات الحر، وقد تناولت فيه الانتقادات الموجهة إلى نظام الإثبات الحر بشأن خوف القاضي الجزائي من التعسف وابتعاده عن طريق الحق، وذلك بتحديد له وسائل الإثبات التي يلجأ إليها في إثبات حكمه.[2]

وفي ضوء ما سبق نستنتج أن مسألة مشروعية الدليل الإلكتروني في وجوده تطرح بالدرجة الأولى في الأنظمة القانونية التي تعتمد نظام الإثبات المقيد، والذي بموجبه لا يمكن اعتبار الدليل الإلكتروني ذا أي قيمة إثباتية ما لم ينص القانون على ذلك صراحة ضمن قائمة الأدلة الإثباتية المقبولة، وبالتالي لا يجوز للقاضي الجنائي أن يعتمد عليها في تكوين إدانته، بغض النظر عن توافر شروط اليقين.[3]

---

[1] براهيمي جمال، "التحقيق الجنائي في الجرائم الإلكترونية"، أطروحة دكتوراه، قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2018، صفحة 139.

[2] براهيمي جمال، مرجع سابق، صفحة 142.

[3] براهيمي جمال، المرجع السابق، صفحة 143.

وفي هذا الصدد نجد أن المشرع الجزائري، كغيره من التشريعات التابعة لنظام الأدلة الحرة، لم يحدد نصوصا خاصة تملي على القاضي الجزائي مسبقا قبول أي دليل من عدمه بما في ذلك الأدلة الإلكترونية.[1]

الفرع الثالث: مشروعية الدليل الإلكتروني في التحصيل

ولا بد من وضع ضوابط وأطر محددة يجب أن تتم ضمنها عملية البحث عن الأدلة وجمعها والتحقيق فيها حتى لا تحيد عن الغرض الذي قصده المشرع وآراؤه وهو الوصول إلى الحقيقة الفعلية. في الدعوى، وهو الهدف الأسمى لقانون الإجراءات الجزائية، ويعني مبدأ مشروعية الحصول على الأدلة. إن المفاهيم الإلكترونية بما فيها المفاهيم الإلكترونية تتطلب إجراءات تتوافق مع القواعد والأنظمة القانونية المتبعة في وحدات المجتمع المتحضر، أي أن قاعدة مشروعية الأدلة الجنائية لا تقتصر فقط على مجرد مطابقتها للقواعد القانونية، بل يجب أن تأخذ في الاعتبار مع مراعاة المبادئ السامية لحقوق الإنسان، وقواعد النظام، وآداب المجتمع.[2]

لكي يتم قبول الأدلة الجنائية كأدلة، يشترط عموماً أن يتم الحصول عليها بطريقة مشروعة، وهذا يتطلب أن تلتزم الجهة المسؤولة عن جمع الأدلة بالشروط التي حددها القانون في هذا الشأن. ونحن إذ نبحث عن مشروعية الأدلة الإلكترونية، فإننا نقتصر على ما يثير جمع الأدلة الإلكترونية من حيث مشروعية الحصول عليها، وهو ما يتركز بشكل أساسي على إجراءات التفتيش للبحث عن هذه الأدلة، ويتم ذلك من خلال النقاط التالية:

-حالة الشخص الذي يقوم بالتفتيش

-مدى مشروعية البحث عن الأدلة الإلكترونية وضبطها في البيئة الافتراضية.

[1] خالد عياد الحلبي، "إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت"، دار الثقافة للنشر والتوزيع، عمان، الطبيعة الاولى، 2012، صفحة 235.

[2] المرجع نفسه، صفحة 2.

ويشترط أن تكون الإدانة في أي جريمة مبنية على أدلة مشروعة يتم الحصول عليها وفقا لقواعد الأخلاق والنزاهة واحترام القانون من قبل الجهة المختصة بجمع الأدلة الجنائية بما في ذلك الأدلة التي تحتوي عليها والمستخرجة من الوسائل الإلكترونية.[1] ولا يحدث ذلك إذا تم البحث عنها أو الحصول عليها، أو كانت عملية تقديمها للقضاء وإحالتها أمامها بالطرق المنصوص عليها في القانون. ومتى تم الحصول على الأدلة خارج هذه القواعد القانونية، فلا تؤخذ قيمتها بعين الاعتبار، مهما كانت أهميتها الحقيقية، لعدم مشروعيتها. وعلى هذا الأساس فإن إجراءات جمع الأدلة الإلكترونية التي يتم الحصول عليها من الوسائل الإلكترونية، إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها، تكون باطلة، وبالتالي فإن الأدلة المستمدة منها تكون باطلة ولا يجوز الاستناد إليها كدليل للإدانة المسائل الجنائية.[2]

المطلب الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي

فمجرد الحصول على الأدلة الإلكترونية وتقديمها للقضاء لا يكفي للاعتماد عليها كدليل للإدانة، إذ إن الطبيعة الفنية للدليل الإلكتروني تمكن من التلاعب به. وبالإضافة إلى ذلك فإن معدل الخطأ في إجراءات الحصول على أدلة موثوقة في إعداد التقارير عن الحقيقة فتبدو عادية في مثل هذا النوع من الأدلة، لذلك تثور فكرة الشك في مصداقيتها كأدلة الإثبات الجنائي.[3]

الفرع الأول: شروط اكتساب الدليل الإلكتروني حجية الإثبات الجنائي

إن مسألة تقييم الأدلة الجنائية في إثبات الوقائع الجنائية هي مسألة موضوعية بحتة يمارسها القاضي لسلطته التقديرية.

أولاً: تقييم الدليل الإلكتروني من حيث سلامته من التزوير

[1] خالد عياد الحلبي، مرجع سابق، صفحة 239.

[2] مرجع نفسه، صفحة 240.

[3] خالد عياد الحلبي، المرجع السابق، صفحة 246.

يمكن التأكد من سلامة الدليل الإلكتروني من التزوير بعدة طرق، منها:

– فكرة التحليل التخاطري الرقمي، حيث تتم مقارنة الأدلة الرقمية المقدمة للقضاء مع الأصل المدرج في الآلة الرقمية، ومن ثم التأكد من مدى التزوير في النسخة المستخرجة.[1]

– استخدام عمليات حسابية خاصة تسمى الخوارزميات، والتي من خلالها يمكن التأكد من سلامة الأدلة الرقمية من التحريف والتغيير في حالة عدم الحصول على النسخة الأصلية من الأدلة الرقمية.[2]

إن استخدام الأدلة المحايدة، وهي نوع من الأدلة الرقمية المخزنة في البيئة الافتراضية والتي لا علاقة لها بموضوع الجريمة، يساعد على التأكد من سلامة الأدلة الرقمية المقصودة وعدم تعرضها لأي تعديل في النظام الحاسوبي. تشير الشكوك إلى أن الخبرة الفنية تلعب دورًا مهمًا في ضمان سلامة الأدلة الرقمية. وإذا كانت للخبرة الفنية أهمية كبيرة في استخلاص الأدلة الرقمية، فإنها لا تقل أهمية في تقييم مصداقيتها واعتمادها في مجال المعالجة الآلية للمعلومات وتحقيق اليقين. وقد يتطلب ذلك من القاضي الجنائي الاستعانة بخبراء للتأكد من موضوعية الأدلة ومصداقيتها.[3]

ثانيا: تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المتبعة في الحصول عليه.

وسبق أن ذكرنا أنه يتم الحصول على الأدلة الرقمية باتباع مجموعة من الإجراءات الفنية، والتي قد تتعرض لخطأ يلقي بظلال من الشك على سلامة نتائجها. وهذا يتطلب منا إخضاعها للاختبارات كوسيلة للتأكد من سلامة هذه الإجراءات من حيث إنتاج أدلة تتمتع بالمصداقية لقبولها كأدلة. ويتبع ذلك مجموعة من الخطوات:

– إخضاع الآلة المستعملة لعدة تجارب للتأكد من دقتها في إعطاء النتائج، وذلك من خلال إتباع اختبارين أساسيين يتم من خلالهما التأكد من أن الدليل المستخدم يعرض

[1] ياسين بن عمر، المعالجة القانونية الإلكترونية في القانون الجزائري والتشريعات المقارنة، جامعة باتنة، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 2019، صفحة 720.

[2] خالد عياد الحلبي، المرجع السابق، صفحة 249.

[3] خالد عياد الحلبي، المرجع السابق، صفحة 250.

كافة البيانات المتعلقة بالدليل الرقمي، وفي نفس الوقت لن يتم إضافة أي بيانات جديدة. مضاف إليه مما قد يعطي للنتائج المقدمة مصداقية في الأدلة. وعلى الوقائع فإن هذين الاختبارين هما:

- اختبار السلبيات الكاذبة، ويعني أن الأدلة المستخدمة للحصول على الأدلة تخضع للاختبار لبيان مدى قدرتها على عرض جميع البيانات المتعلقة بالدليل الرقمي، وذلك لم يتم التغاضي عن أي بيانات مهمة. أما الاختبار الثاني، والذي يتم عن طريق اختبار الإيجابيات الكاذبة، فيعني إخضاع الأداة المستخدمة للحصول على الأدلة الرقمية للاختبار للتأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة.[1]
- الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل، حيث أظهرت الدراسات العلمية والأبحاث المنشورة في مجال تكنولوجيا المعلومات الطرق الصحيحة التي يجب اتباعها في الحصول على الأدلة الرقمية. ومن ناحية أخرى، أظهرت هذه الدراسات أيضاً أدوات ذات كفاءة مشكوك فيها، مما يساهم في تحديد مدى مصداقية المخرجات المستمدة من تلك الأدوات.[2]

ومما سبق يمكن تحديد مدى سلامة الأدلة الإلكترونية. فإذا كانت الأدلة الإلكترونية مستوفية للشروط العامة لما يمكن أن يشكل أساساً لتأكيد الثقة بها، فيبدو من غير المعقول أن يعيد القاضي تقييم هذه الأدلة ويقدمها مرة أخرى للتحقيق. الدليل الإلكتروني كدليل علمياً أهميته قاطعة بالنسبة للحادثة المذكورة منه. وإذا سبق أن قبلنا إمكانية التشكيك في سلامة الأدلة الإلكترونية لقابليتها للتلاعب ونسبة الخطأ في إجراءات الحصول عليها، فهذه مسألة فنية لا يستطيع القاضي إبداء رأي حاسم فيها، حتى ولو كان القاضي قد وافق على ذلك. المتخصصين لا يؤكدون ذلك.[3]

[1] خالد عياد الحلبي، المرجع السابق، صفحة 251.

[2] بوضياف، إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 11، 2018، صفحة 46.

[3] فالح عبد القادر، آيت عبد المالك نادية، المرجع السابق، صفحة 105.

إذا كان الدليل الإلكتروني مستوفياً للشروط السابقة فيما يتعلق بسلامته من التلاعب والخطأ، فلا يمكن إرجاع هذا الدليل بناء على سلطة القاضي التقديرية. وإذا كانت سلطة القاضي في رفض الدليل مبنية على فكرة الشك، فلا بد أن يكون هناك ما يصل إلى درجة الشك في الدليل، وهو ما لا يستطيع القاضي التأكد منه ما دام هذا الدليل مستوفيا لشروط الصحة. لذلك يقتصر دور القاضي على فحص ارتباط الأدلة بالجريمة، ولا شك أن الخبرة تلعب دوراً مهماً في التأكد من صحة هذه الأدلة كأساس لتكوين اعتقاد القاضي، كما أن فحص الأدلة هي جوهر تجربة القاضي.[1]

الفرع الثاني: موقف المشرع الجزائري من الدليل الإلكتروني في إثبات الجنائي

ومن واجب القاضي الجنائي، سواء كان قاضي التحقيق أو غرفة الاتهام أو محكمة الجنايات، تقييم الأدلة ضد المتهم. ولا يجوز محاكمة المتهم وإدانته على أساس الأدلة فقط. بل يجب أن يكون هذا الدليل مكملاً لبقية الأدلة المادية الأخرى. كما يجب أن تتصف إجراءات جمع الأدلة بالمشروعية، احتراما للحرية الشخصية للمتهم، فهو بريء حتى تثبت إدانته بحكم.[2]

إثبات الجنايات هو كل ما يؤدي إلى كشف الجريمة وإقامة الأدلة على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل وأن هناك أدلة على ذلك. تعتبر الأدلة الوسيلة القانونية التي يستخدمها القاضي للوصول إلى الحقيقة وكشف الجريمة ونسبتها إلى المتهم. لقد وضع الفقه الإجرائي نظامين إجرائيين في مجال الأدلة الجنائية، من حيث الأسس التي يقوم عليها كل منهما، وقد سبق بيان ذلك. تنتمي الجزائر إلى مجموعة الدول التي تعتمد نظام الأدلة الحرة في مجال الإثبات الجنائي. وهي تتبع الأنظمة اللاتينية مثل فرنسا وبلجيكا والأردن وسوريا، وهو ما نصت عليه المادة 212 من قانون الإجراءات الجزائية التي نصت على أنه "يجوز إثبات الجرائم بأي وسيلة من طرق الإثبات". فيما عدا الأحوال التي ينص فيها القانون

[1] فالح عبد القادر، آيت عبد المالك نادية، المرجع السابق، صفحة 107.

[2] بوضياف، إسمهان، المرجع السابق صفحة 48.

على خلاف ذلك، يجوز للقاضي أن يصدر حكمه بناء على اقتناعه، ولا يجوز للقاضي أن يبني حكمه إلا على الأدلة التي قدمت له أثناء المرافعة والتي نوقشت في حضوره أمامه.[1]

إن قرار المشرع الجزائري بتقديم الأدلة المقنعة بحرية في شخص قاضي الموضوع هو تعزيز لإثبات قرينة البراءة، وتعزيز ممارسة حقوق الدفاع الفردية. إلا أن هذا التطبيق دون تخصيص وتخصيص يعد قصورا تشريعيا واضحا، إذ لا نجد ضمن قانون الإجراءات الجزائية ما يدل على أن الدليل الإلكتروني هو دليل. ومن نوع خاص كالجرائم الإلكترونية، فإن غياب أدنى نص قانوني في هذا الشأن يؤدي إلى ظهور إشكاليات تتعلق بطبيعة الأدلة المقدمة أمام الجهات القضائية، بحيث تقوم هذه الأخيرة في حال عدم توفرها فالإلمام بتكنولوجيا المعلومات يمكنه أن يدحض هذه الأدلة ولا يأخذها بعين الاعتبار، حتى لو كان لها قوة تشريعية ومتوفرة. جميع الحالات الصحية والعكس.[2]

أما بالنسبة لسلطة القاضي الجزائري في تقييم الأدلة الإلكترونية، فإن المادة العلمية للأدلة الإلكترونية جعلت من سلطة القاضي في تقييم هذه الأدلة محل خلاف فقهي. هناك من يرى أن الأدلة العلمية، بما فيها الأدلة الإلكترونية، لها قوة إثباتية ملزمة حتى للقاضي، مستندين في رأيهم على أن هذه الأدلة تتميز بالدقة العلمية التي تصل إلى درجة اليقين. وهناك من يرى أن مبدأ حرية القاضي التقديرية يجب أن يبسط سلطته على كل الأدلة دون استثناء، حتى الأدلة الرقمية، معتبراً أن إعطاء الأدلة الرقمية سلطة ثبوتية لا يستطيع القاضي مناقشتها أو تصديرها هو بمثابة العودة إلى القانون المقيد. عقيدة الإثبات. لقد أجاز المشرع الجزائري، كما سبق بيانه، إثبات الجرائم بأي وسيلة من وسائل الإثبات، باستثناء الجرائم التي يحتاج إثباتها إلى دليل خاص، ومنح القاضي الجزائي سلطة تقدير الأدلة وحرية تكوين إدانته من أي دليل يراه مريح.[3]

---

[1] المادة 12 من قانون الإجراءات الجزائية.

[2] بوبكر، رشيدة، "جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن"، منشورات الحلبي الحقوقية، بيروت، لبنان، طبعة1، لبنان 2012، صفحة 67.

[3] بوبكر رشيدة، مرجع سابق، صفحة 69.

الخاتمة

خاتمة:

وفي ختام هذه دراستنا لموضوع اجراءات التحقيق والتفتيش في الجرائم الإلكترونية نجد أنها تسلط الضوء على العديد من الجوانب التي تتطلب الاهتمام والتفكير. وأظهرت الدراسة أن التحقيق والتفتيش في هذا النطاق يمثل تحدياً قانونياً وفنياً معقداً، حيث يتطلب مواكبة التطورات التكنولوجية وفهم القوانين الجديدة المتعلقة بالجرائم الإلكترونية. ومن هنا فإن تطوير إجراءات التحقيق والتفتيش أمر حيوي للغاية للحفاظ على الأمن السيبراني وتحقيق العدالة.

ونظراً للتحديات المستمرة التي تواجه المحققين في هذا المجال، يجب علينا كمجتمع قانوني وتكنولوجي أن نبذل جهوداً متواصلة لتطوير القدرات والمهارات اللازمة لمواجهة هذه التحديات. وبالإضافة إلى ذلك، ينبغي العمل على تعزيز التعاون بين الجهات المعنية، بما في ذلك الشرطة والقضاء والقطاع الخاص، من أجل تبادل المعرفة والخبرات وتطوير الأدوات والتقنيات اللازمة لتحقيق النجاح في مجال التحقيق والتفتيش في الجرائم الإلكترونية.

وفي نهاية المطاف، يجب علينا جميعا أن ندرك أن التحقيق والتفتيش في الجرائم الإلكترونية يمثل تحديا مستمرا يتطلب الالتزام والتفاني والتطوير المستمر، حفاظا على الأمن الرقمي وتحقيق العدالة.

من خلال دراسة التحقيق والتفتيش في الجريمة الإلكترونية، يمكن استخلاص عدة نتائج مهمة:

- موضوع التحقيق الجنائي المعلوماتي هو المعلومات والبيانات الموجودة في البيئة الإلكترونية.
- يواجه التحقيق الجنائي المعلوماتي صعوبات قد ترجع إلى طبيعة الجريمة المعلوماتية أو الأطراف المتضررة أو جهات التحقيق.
- تعتبر الأدلة الرقمية وسيلة مثالية لإثبات الجرائم الإلكترونية وتحديد مرتكبيها.
- التفتيش الإلكتروني، المراقبة الإلكترونية والضبط الإلكتروني هي إجراءات تحقيقية للحصول على الأدلة الرقمية.

-ويرتبط نجاح إجراءات البحث والتحقيق في الجرائم المعلوماتية بمدى براعة وفعالية وجاهزية الجهات المختصة في البدء بإجراءات تتبع الأدلة الإلكترونية وجمعها وحفظها بغرض عرضها على الجهات المختصة لتقييمها.

-وعلى المستوى القانوني والتشريعي يظهر مدى الاهتمام الذي توليه الدول والحكومات لهذا المجال من خلال التحديث المستمر للنصوص القانونية لمواكبة تطور الجريمة واساليبها.

ومن خلال الملاحظات السابقة، فإنه بدا لنا ضرورة تقديم جملة من التوصيات التي نرى أنه من الممكن أن تساهم في مواجهة تحديات الموضوع قيد الدراسة، والتي تتمثل فيما يلـــــي:

-سن نصوص قانونية تتماشى و مستوى التطور الذي وصلت إليه التكنولوجيا الإلكترونية.

-حث ضحايا الجرائم الإلكترونية على الإبلاغ.

-تعديل قانون الإجراءات الجزائية بشكل عاجل بإضافة قسم خاص للبحث والتحقيق في الجرائم الإلكترونية.

-إبرام اتفاقيات التعاون الداخلي بين القضاء ومهندسي المعلومات الآلية من أجل إثراء المعرفة الفكرية في مجال المعلوماتية.

-رغم اهتمام المشرع الجزائري بالجرائم الإلكترونية والعقوبات المقررة لها (04-09)، إلا أنها لا تكفي لمواجهة الانتشار الرهيب لهذه الجرائم. بل يجب إصدار قانون خاص بشأنها وتشديد العقوبات على مرتكبيها.

قائمة المصادروالمراجع

*** المراجع:**

- الكتب:

- ابن منظور محمد بن مكرم، لســـان العرب، تحقيق: عبد الله علي الكبير، محمد أحمد حسب الله، هاشم محمد الشاذلي، دار صادر، بيروت، الطبعة الأولى، 1955، الجزء 10.

- الزركلي خير الدين، الأعلام: قاموس تراجم لأشـــهر الرجال والنســـاء من العرب والمستعربين والمستشرقين، دار العلم للملايين، بيروت، الطبعة الخامسة، 1980، المجلد 1.

- الزبيدي مرتضـــى الحســـيني، تاج العروس من جواهر القاموس، دار الهداية، القاهرة، 1965، الجزء 1.

- المرعشي عبد الكريم، أصول التحقيق في التراث العربي، دار الغرب الإسلامي، بيروت، الطبعة الأولى، 1989.

- هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، سنة 1997.

- عبد الفتاح بيومي حجاري، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي، مصر، 2006.

- مانع ســـلمى، "التفتيش كإجراء التحقيق في الجرائم المعلوماتية"، مجلة العلوم الإنســـانية، عدد 22، جامعة بسكرة، جوان 2011 .

- هميسي رضا، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، عدد 11، جامعة الوادي، جوان 2012.

- بكري يوســـف بكري، التفتيش عن المعلومات في وســـائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، مصر، 2012.

- خط الانترنت الرقمي غير المماثل (ADSL) هو عبارة عن تقنية الشـــبكة التي تنقل البيانات بســـرعة على خطوط الهواتف الحاســـوبية التناظرية ANALOGUE وبشـــكل غير مماثل، حيث تتحرك البيانات في اتجاه واحد وبسرعة أكبر من الاتجاهات الأخرى.

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

- فاروق الكيلاني، "محاضـرات في قانون أصـول المحاكمات الجزائية الأردني والمقارن"، جزء2، طبعة2، دار المروج، بيروت، 1995.

- د. مأمون محمد سـالمة، "الإجراءات الجنائية في التشـريع المصـري"، الجزء الأول، دار النهضة العربية، القاهرة، 2008م.

- أحمد أبو الروس، "التحقيق الجنائي والتصـرف فيه والأدلة الجنائية"، المكتب الجامعي الحديث، الإسكندرية، 1998م.

- د. عمار عباس الحسـيني، "التحقيق الجنائي والوسـائل الحديثة في كشـف الجريمة"، منشورات الحلبي الحقوقية، لبنان، 2015م.

- د. فايز الضـفيري، "المعالم الأسـاسـية لقضـية العدالة في مرحلة الاسـتدلالات والتحقيق الجسدي"، مجلس النشر العلمي، جامعة الكويت، 2001.

- د. عمر محمد سـالم، الوجيز في شـرح قانون الإجراءات الجنائية، الجزء الأول، مركز جامعة القاهرة للتعليم المفتوح، 2007.

- خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، مصر، 2019.

- عادل محمد فريد نائلة، جرائم الحاسـوب الاقتصـادية، الطبعة 1، منشـورات الحلبي الحقوقية، بيروت، لبنان، 2005.

- هشـام رسـتم، الجرائم المعلوماتية، أصـول التحقيق الجنائي، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة، العدد الثاني، 1999.

- هشـام فريد رسـتم، الجوانب الإجرامية للجرائم المعلوماتية، دراسـة مقارنة، مكتبة الآلات الحديثة، أسيوط، مصر، 1994.

- بلال محمد الزعبي، أسامة أحمد مناغسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة، عمان، الأردن، 2010.

- حجازي عبد الفتاح بيومي، جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصـر، 2004 .

– مؤيد محمد القضـاة، شـرح قانون العقوبات الاتحادي الإماراتي، مكتبة الجامعة، الشـارقة، الإمارات العربية المتحدة، 2014.

– محمد الجبور، الوســـيط في قانون العقوبات القســـم العام، الطبعة 1، دار وائل، عمان، الأردن، 2021.

– أحمد خليفة ملط، الجرائم المعلوماتية، طبعة 1، دار الفكر الجامعي، الإسكندرية، مصـر، 2006.

– هدى حامد قشـقوش، جرائم الحاسـوب الآلي في التشـريع المقارن، دار النهضـة العربية، القاهرة، 1992.

– مصـــطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها، كلية الحقوق والإدارة العامة، جامعة بيرزيت، رام الله، فلسطين، المجلد 4، العدد 2018.

– عيدة بلعايد، خصـــوصـــية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والســـياســـية، جامعة مولاي الطاهر، ســـكيكدة، 2011، المجلد 06، العدد 143.

–محمد الأمين البشـــيري، التحقيق في الجرائم المســـتحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

– خالد عياد الحلبي، "إجراءات التحري والتحقيق في جرائم الحاسـوب والإنترنت"، دار الثقافة للنشر والتوزيع، عمان، الطبيعة الاولى، 2012.

– ياسين بن عمر، المعالجة القانونية الإلكترونية في القانون الجزائري والتشريعات المقارنة، جامعة باتنة، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 2019.

– بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 11، 2018.

– بوبكر رشـــيدة، "جرائم الاعتداء على نظم المعالجة الآلية في التشـــريع الجزائري المقارن"، منشورات الحلبي الحقوقية، بيروت، لبنان، طبعة1، لبنان 2012.

- المقالات والمنشورات:

- علي أحمد عبد الزعبي، حق الخصـــوصـــية، منشـــور على الموقع الإلكتروني : https://almerja.net/reading.php?idm=77368تاريخ الاطلاع 2024/04/25، الساعة 22:30.

- محمود صـــالح العادلي، الفارغ التشـــريعي في مجال مكافحة الجرائم المعلوماتية، بحث منشـــور على الإنترنـت، الموقع DRLADLY.COM، ص 38، تـاريخ الإطلاع: 2024/04/23، على الساعة: 16:00.

- فريحة حسين، الجرائم الالكترونية والأنترنت، مقال منشور بمجلة المعلوماتية، السعودية، العدد 36، أكتوبر 2011.

- الأطروحات والرسائل:

- طرشـــي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجســـتير في القانون الجنائي، كلية الحقوق، جامعة الجزائر2012.

- نصيرة بوحزمة، التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، رسالة دكتوراه في العلوم القانونية، تخصـص القانون الخاص، كلية الحقوق والعلوم السـياسـية، قسـم الحقوق، جامعة الجيلالي اليابس، سيدي بلعباس، 2022.

- فوزي عمارة، قاضـــي التحقيق، أطروحة دكتوراه في العلوم، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2009-2010.

- فـايز محمـد رجـب غلاب، الجرائم المعلومـاتيـة في القـانون الجزائري واليمني، أطروحـة دكتوراه، كليـة الحقوق، فرع القـانون الجنـائي والعلوم الجنـائيـة، جـامعـة الجزائر1، 2010-2011.

- هبة نبيلة هروال، جرائم الإنترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013.

- عبد الله دغش العجمي، العلمية والقانونية للجرائم الإلكترونية (دراســـة مقارنة)، رســـالة ماجستير، القانون العام، جامعة الشرق الأوسط، عمان، الأردن، 2014.

– يوسف صغير، الجرائم المرتكبة عبر الإنترنت، رسالة لنيل شهادة الماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر، 2013.
– فالح عبد القادر، آيت عبد المالك نادية، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، خميس مليانة، مجلد 04، العدد 02، 2019.
– سبع زيان، سلمى المفتي، صور وأركان الجريمة المنظمة، دراسة مقارنة في القانون الإماراتي والقانون الجزائري، مجلة الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 13، العدد 3، 2020.
– دلال موالي ملياني، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، أطروحة دكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018/2017.
– بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية، مذكرة ماجستير، جامعة عبد الرحمن ميرة، بجاية، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، 2017-2018.
– عبد الله بن حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014.
– نداء نائل فايز المصري، "خصوصية الجرائم المعلوماتية"، جامعة النجاح الوطنية، كلية الدراسات العليا، رسالة ماجستير، فلسطين، 2017.
– براهيمي جمال، "التحقيق الجنائي في الجرائم الإلكترونية"، أطروحة دكتوراه، قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2018.

- القوانين والمراسيم:

- أمر رقم 66-155، مؤرخ في 08 يونيو سنة 1966، يتضمن قانون الإجراءات الجزائية، معدل ومتمم لاسيما بالقانون رقم 17-07 المؤرخ في 27 مارس 2017.
- نقض 20/5/1961، مجموعة أحكام النقض، س12، ق 140.
- القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا العالم والاتصال ومكافحتها، المؤرخ في 14 شعبان 1430 الموافق لـ 5 أغسطس 2009، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادر بتاريخ 25 شعبان 1430 الموافق 16 أغسطس 2009.
- القانون رقم 66-155 المؤرخ في 8 يونيو 1966، المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية، العدد 48، المعدل والمتمم للأمر 15-02 المؤرخ في 23 يوليو 2015، العدد 4.
- المادة 65 مكرر 5 من قانون الإجراءات الجزائية، أمر رقم 66-156 مؤرخ في 8 جوان 1966، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 84 معدل ومتمم وفقا للقانون 06-22 المؤرخ في 20 جويلية 2006.
- القانون رقم 04-15 المؤرخ في 10 نوفمبر يعدل ويتمم الأمر 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 71 الصادر في 10 نوفمبر 2004.
- القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادرة في 16 أوت 2009.

الفهـــرس

ملخص الدراسة

ملخص الدراسة:

تناولت هذه الدراسة إجراءات التحقيق والتفتيش في الجريمة الإلكترونية كواحدة من الظواهر الجديدة التي نتجت عن تطور التكنولوجيا ووسائل الاتصال الحديثة. تمحورت الدراسة حول تحليل الجوانب القانونية والفنية والتقنية لهذا الموضوع الذي يمثل تقاطعًا بين علوم الإنترنت والعلوم القانونية الإجرائية. تضمنت الدراسة تعريفًا للجريمة الإلكترونية وخصائصها الفقهية والقانونية، بالإضافة إلى تحليل لعمليات التحقيق الجنائي ودور المحققين فيها. كما تناولت الدراسة دور الهيئات المختصة بالبحث والتحقيق في الجرائم الإلكترونية، مع التركيز على الجهات الأمنية كالشرطة والدرك. في الختام، تم استعراض نتائج الدراسة وتقديم توصيات قانونية تهدف إلى تعزيز آليات البحث والتحقيق في هذا المجال.

الكلمات المفتاحية: الجرائم الإلكترونية، التحقيق الجنائي الإلكتروني، الإثبات الجنائي الإلكتروني، الأمن السيبراني.

Abstract :

This study examined the procedures of investigation and inspection in electronic crime as one of the emerging phenomena resulting from the advancement of technology and modern means of communication. The study focused on analyzing the legal, technical, and technological aspects of this subject, which represents a intersection between internet sciences and procedural legal sciences. The study included a definition of electronic crime and its legal and jurisprudential characteristics, as well as an analysis of criminal investigation procedures and the role of investigators. Additionally, the study addressed the role of specialized authorities in investigating electronic crimes, with a focus on security agencies such as the police and gendarmerie. In conclusion, the study reviewed the findings and provided legal recommendations aimed at enhancing the mechanisms of research and investigation in this field.

Keywords : electronic crimes, electronic criminal investigation, electronic criminal evidence, cybersecurity.