الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of algeria
وزارة التعليم العالي والبحث العلمي
Ministray of higher education and scientific research
جامعة محمد البشير الإبراهيمي- برج بوعريريج-
University of mohammed Al-bachir Al –Ibrahimi-BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون الاعلام اللآلي والأنترنت

الموسومة بـــ:

الجريمة الالكترونية في التشريع الجزائري

إعداد الطالبتين:

- شريح رانية
- خضري نبيلة

إشراف الأستاذ:

د. خصري محمد

لجنة المناقشة

(اللقب والاسم)	(الرتبة)	(الصفة)
• دوادي عبد الله	أستاذ مساعد قسم –أ–	رئيسا
• خصري محمد	أستاذ محاضر قسم –أ–	مشرفا
• رياح لخضر	أستاذ مساعد قسم –أ–	ممتحنا

السنة الجامعية: 2025/2024

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): شريح رانية الصفة: طالب، أستاذ، باحث جامعة

الحامل(ة) لبطاقة التعريف الوطنية رقم 118333417 والصادرة بتاريخ 20/05/2020

المسجل(ة) بكلية / معهد كلية الحقوق والعلوم السياسية قسم حقوق

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: الحريصة الإلكترونية في التشريع الجزائري

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: .....

توقيع المعني(ة)

الشهود لأجل التصديق
السيد: شريح رانية
بطاقة التعريف الوطنية رقم: 1
مستخرج بتاريخ:
العناصر في:

2025 ماي 2
ع/رئيس المجلس الشعبي البلدي
و بتفويض منه
عون رئيسي للإدارة العامة
بلواحرث فيصل

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

انا الممضي أسفله،

السيد(ة): حمصي نبيلة الصفة: طالب، أستاذ، باحث حالة

الحامل(ة) لبطاقة التعريف الوطنية رقم 107047176 والصادرة بتاريخ 2017-12-24

المسجل(ة) بكلية / معهد حقوق علوم سياسية قسم حقوق

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: الحريات الاشتراكية في تشريع الجزائري

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: .....

توقيع المعني (*)

توقيع السيد:
بطاقة التعريف رقم:
بتاريخ:
للمصادقة على تطابق التوقيع مع بوعريريج في 20 ماي 2021
رئيس المجلس الشعبي البلدي
عن رئيس المجلس الشعبي البلدي
بتفويض منه عون الإدارة الإقليمية
هداجي عبد الكريم


بسم الله الرحمن الرحيم

شكر وتقدير

بداية نحمد الله ونشكره الذي وفقنا في انجاز هذا العمل

قال رسول الله صلى الله عليه وسلم من لا يشكر الناس لا يشكر الله

وانطلاقا من هذا التوجه النبوي الكريم نتقدم بأرقى عبارات الشكر والامتنان للدكتور **خضري محمد** التي شرفنا بقبوله الإشراف على انجاز هذا البحث العلمي والذي أفاض علينا بعلمه ولم يبخل علينا بنصيحة أو معلومة فله مني فائق الاحترام والتقدير.

وفي الختام نشكر كل من ساعدنا وساهم في هذا العمل سواء من قريب أو من بعيد ولو بكلمة طيبة أو ابتسامة عطرة.

مقدمة

لقد شهدت السنوات الأخيرة تطورا هائلا في مجال تكنولوجيا المعلومات، حيث مثلت هذه الأخيرة الابتكار الأعظم في عصرنا الراهن لما لهامن ايجابيات كثيرة، حيث ساهمت في تطور المعارف والانتاج والخدمات، ورغم كل هذا إلا أنها ظهرت سلوكات لاأخلاقية بينت الجانب السلبي لهذا التطور.

وفي هذا السياق ظهرت الجرائم الالكترونية والتي تعتبر بأنها نشاط أجرامي يتم عن طريق الحواسيب والشبكات الرقمية ، وتشمل مجموعة واسعة من الأنشطة كسرقة المعلومات، والاحتيال المالي، والتجسس الالكتروني، كل هذا أصبح من أبرز التحديات التي تواجه الأفراد والمؤسسات والحكومات على مستوى العالم، ولكن لم يلبث معظم المشرعين أن تصدى لها عن طريق تجريمها وتقرير الجزاءات لمرتكبيها.

بدأ الاهتمام بالجريمة الالكترونية دوليا منذ سبعينيات القرن الماضي، أما على الصعيد الوطني فإن المشرع الجزائري ورغبة للتصدي لهذه الجرائم ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال فقد عمد إلى تعديل القوانين الوطنية بما فيها قانون العقوبات لجعلها تتجاوب مع التطورات الاجرامية في مجال تكنولوجيا المعلومات والاتصال.

تهدف هذه الدراسة إلى فهم طبيعة هذه الجرائم وتبيان الأركان اللازمة لقيامها، كما تهدف إلى تقديم رؤية شاملة حول كيفية مواجهة هذه التهديدات من خلال استراتيجية والملاحقة والتحقيق في هذه الجرائم.

كما يكتسي موضوع الجريمة الالكترونية أهمية كبيرة في وقتنا الراهن،ويرجع ذلك إلى الانتشار الواسع للتكنولوجيا والاهتمام الكبير لها من طرف الحكومات والافراد، مما دفعنا إلى فك الغموض عنها والبحث عن الأسلوب الأمثل لمكافحة هذه الظاهرة.

يرجع سبب اختيار هذا الموضوع إلى الاهتمام الشخصب بالتكنولوجيا والأمن الرقمي ورغبة إلى كشف الغموض على مثل هذه الجرائم.

أما بالنسبة للأسباب الموضوعية فترجع إلى البحث في هذه الجرائم باعتبارها جريمة مستحدثة وغامضة لما لها علاقة بالعالم الافتراضي.

ومما لا شك فيه أن كل بحث علمي تعترضه جملة من الصعوبات، ومن بين هذه الصعوبات قلة المراجع المتخصصة في الموضوع وخاصة في الجزائر، كما لم يتسنى لنا الاستعانة بالاجتهادات القضائية المحلية لسبب ندرتها.

من خلال ما سبق ذكره يمكن طرح الاشكالية التالية:

هل وفق المشرع الجزائري في وضع آليات كافية للحد من الجرائم الالكترونية؟

وتتفرع عن هذه الاشكالية التساؤلات الفرعية التالية:

- ما مفهوم الجريمة الالكترونية؟
- ما هي الأركان التيتقوم عليها الجريمة الالكترونية؟
- كيف نظم المشرع الجزائري اجراءات اللملاحقة والتحيقيق في الجريمة الالكترونية؟

للاجابة عن الاشكالية المطروحة اعتمدنا على المنهج الوصفي التحليلي، وذلك بوصف الجريمة وبيان المفاهيم القانونية الخاصة بها، وتحليل المفاهيم وشرحها.

تم تقسيم هذه الدراسة إلى فصلين، بحث تناولنا في الفصل الأول النظام القانوني للجريمة الالكترونية والذي تم تقسيمه إلى مبحثين، تناولنا في المبحث الأول مفهوم الجريمة الالكترونية، أما المبحث الثاني فتناولنا أركان الجريمة الالكترونية.

بالنسبة للفصل الثانيفقد خصصناه إلى الملاحقة والتحقيق في الجرائم الالكترونية، والذي قسمناه بدوره إلى مبحثين، تناولنا في المبحث الأول إجراءات الملاحقة، أما المبحث الثاني فقد خصصناه إلى اجراءات التحقيق في الجرائم الالكترونية .

الفصل الاول: الإطار المفاهيمي للجريمة الالكترونية

مع التطور المتسارع لتكنولوجيا المعلومات والاتصالات وانتشار استخدام الإنترنت في مختلف مناحي الحياة، ظهرت أنماط جديدة من الجرائم تختلف في طبيعتها وأساليب ارتكابها عن الجرائم التقليدية، هذه الجرائم المستحدثة، والتي أصبحت تعرف بالجرائم الإلكترونية، باتت تشكل تحديا كبيرا للمنظومة القانونية والأمنية في مختلف دول العالم.

يتناول هذا الفصل الإطار المفاهيمي للجريمة الإلكترونية من خلال تسليط الضوء على ماهيتها وأركانها ودوافع ارتكابها، حيث سنعمل على تحديد مفهوم الجريمة الإلكترونية والوقوف على خصائصها التي تميزها عن الجرائم التقليدية، كما سنتطرق إلى أنواعها المختلفة سواء تلك الواقعة بواسطة النظام الالكتروني أو الواقعة عليه.

كما يهدف هذا الفصل إلى دراسة الأركان الأساسية للجريمة الإلكترونية من ناحية الركن الشرعي والمادي والمعنوي، مع التركيز على السمات الخاصة لهذه الأركان في البيئة الرقمية، وأخيرا سنتناول الفئات المختلفة لمرتكبي هذه الجرائم ودوافعهم المتنوعة، مما يساعد على فهم أعمق لظاهرة الإجرام الإلكتروني وآليات مكافحته.

إن فهم الإطار المفاهيمي للجريمة الإلكترونية يعد خطوة أساسية نحو تطوير استراتيجيات فعالة لمواجهتها، خاصة في ظل التحديات القانونية والتقنية التي تفرضها الطبيعة العابرة للحدود لهذه الجرائم وتطور أساليب ارتكابها بشكل مستمر.

المبحث الاول: ماهية الجريمة الالكترونية

أدى الانتشار الواسع للتكنولوجيا الرقمية إلى ظهور أنماط مستحدثة من الجرائم تتطلب فهما دقيقا لماهيتها ومختلف جوانبها، نتطرق من خلال هذا المبحث إلى دراسة ماهية الجريمة الإلكترونية من خلال مطلبين أساسيين: يتناول المطلب الأول مفهوم الجريمة الإلكترونية بتحديد تعريفها وخصائصها المميزة، بينما يركز المطلب الثاني على تصنيف أنواع الجرائم الإلكترونية إلى تلك الواقعة بواسطة النظام الالكتروني وتلك الواقعة عليه.

المطلب الاول: مفهوم الجريمة الالكترونية

في ظل التطور التكنولوجي المتسارع وانتشار استخدام الإنترنت والأجهزة الذكية في شتى مناحي الحياة، ظهرت أنماط جديدة من السلوكيات الإجرامية التي تستهدف البيئة الرقمية أو تستخدمها كوسيلة لارتكاب الجرائم، هذه الظاهرة التي أصبحت تعرف بالجريمة الإلكترونية تشكل تحديا كبيرا للأمن القومي والاقتصادي والمجتمعي، مما يستدعي دراسة مفهومها بدقة وتحديد خصائصها المميزة، سعيا لفهم طبيعتها وآليات مكافحتها بفعالية.

الفرع الأول: تعريف الجريمة الالكترونية

نتناول في هذا الفرع التعريف الفقهي (أولا)، ثم نتطرق إلى التعريف القانوني (ثانيا)، ثم نتطرق إلى التعريف المحدد من طرف المشرع الجزائري (ثالثا).

أولا: التعريف الفقهي للجريمة الإلكترونية

بالنظر إلى الجهود المبذولة لمواجهة ظاهرة الإجرام الالكتروني، يلاحظ وجود تباين واضح في المصطلحات المستخدمة للتعبير عن هذه الظاهرة، إذ لم يتوصل الفقه

الجنائي إلى اتفاق على تسمية موحدة لها، فقد أطلق عليها بعض الفقهاء تسمية جرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات، في حين استخدم آخرون مصطلح جرائم الكمبيوتر والإنترنت، وهناك من يفضل تسميتها ب الجرائم المستحدثة، كما لم يتم التوصل إلى تعريف تشريعي جامع وشامل لهذا النوع من الجرائم، وقد تعددت آراء الفقهاء في تعريف الجريمة الإلكترونية، ويرجع هذا التباين إلى التطور المتسارع والمستمر في مجال تكنولوجيا المعلومات والاتصالات، مما حال دون صياغة تعريف فقهي موحد يغطي مختلف جوانبها، وقد انقسمت الاتجاهات الفقهية في هذا السياق بين من يتبنى مفهوما واسعا للجريمة الإلكترونية، ومن يفضل تضييق نطاقه.[1] وسنحاول إبراز هذين الاتجاهين وفقا لما يلي:

1-الاتجاه الضيق لمفهوم الجريمة الإلكترونية

سعى هذا الاتجاه إلى تحديد مفهوم الجريمة الإلكترونية استنادا إلى معايير متعددة، سواء من منظور شخصي يتمثل في مدى توفر المعرفة والخبرة التقنية لدى الجاني، أو من منظور موضوعي يتعلق بطبيعة الجريمة ذاتها، إضافة إلى المعايير المرتبطة بالبيئة التي ترتكب فيها الجريمة، وفي هذا السياق، قدم عدد من فقهاء القانون الجنائي تعريفات مختلفة للجريمة الإلكترونية؛ فقد عرفتها الدكتورة هدى قشقوش بأنها: كل سلوك غير مشروع أو غير مسموح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها، كما عرفها الأستاذ *Rosen Blat* بأنها: كل نشاط غير مشروع يستهدف نسخ المعلومات المخزنة في

[1] نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، مذكرة مقدمة لنيل درجة الماجيستر، في القانون العام، بكلية الدراسات العليا في جامعة النجاح الوطنية، نابلس، فلسطين، 2017، ص 03.

الحاسب أو تغييرها أو حذفها أو الوصول غير المصرح به إليها، سواء كانت مخزنة في الجهاز أو تمر من خلاله.[1]

يعاب على هذا التعريف استبعاده لعدد كبير من الأفعال غير المشروعة التي يتم فيها استخدام الحاسوب كأداة رئيسية لارتكاب الجريمة، مثل الاحتيال الالكتروني، وفي هذا السياق، تبنت وزارة العدل الأمريكية تعريفا للجريمة الإلكترونية في تقرير أصدرته عام 1989 يتعلق بجرائم الالكترونية، حيث عرفتها بأنها: كل فعل غير مشروع يتطلب القيام به درجة كبيرة من المعرفة بتكنولوجيا الحواسيب من جهة، ويحتاج إلى هذه المعرفة أيضا لملاحقته وتحقيق الإثبات عليه من جهة أخرى.[2]

يتضح من هذا التعريف أن ارتكاب الجريمة الإلكترونية لا يتطلب فقط معرفة متقدمة بتكنولوجيا الحاسبات، بل أيضا يحتاج إلى خبرة كبيرة في هذا المجال لمتابعتها والتحقيق فيها، مما يعني ضرورة امتلاك كل من الجناة والمسؤولين عن ملاحقتهم مستوى عالٍ من الإلمام بهذه التكنولوجيا.

2- الاتجاه الموسع لمفهوم الجريمة الإلكترونية

على عكس الرأي السابق، يرى بعض الفقهاء ضرورة توسيع مفهوم الجريمة الإلكترونية أو الالكترونية ليشمل نطاقا أوسع من مجرد الحاسوب أو موضوع الجريمة أو شخص المستخدم، والتركيز بدلا من ذلك على التقنية المستخدمة في مختلف الأجهزة الالكترونية والإلكترونية، ويعرفونها بأنها: أي فعل إجرامي متعمد، مهما كانت علاقته بالالكترونية، يؤدي إلى إلحاق ضرر بالمجني عليه أو تحقيق مكسب للجاني.

[1] محمد علي قطب الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، وزارة الداخلية، الأكاديمية الملكية للشرطة، مملكة البحرين، 2010، ص 09.

[2] – سفيان سوير، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية، وعلوم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد تلمسان، الجزائر، 2011، ص 12.

أما منظمة التعاون الاقتصادي والتنمية، فقد عرفت الجريمة الإلكترونية بأنها: كل فعل أو امتناع يفضي إلى انتهاك الأموال المادية أو المعنوية، ويكون ناتجا بشكل مباشر أو غير مباشر عن استخدام التقنية الالكترونية. [1]

اعتمد مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا للجريمة الإلكترونية جاء فيه أنها: كل جريمة يمكن ارتكابها باستخدام نظام حاسوبي أو شبكة حاسوبية، موضحا أن هذا المفهوم يشمل – من حيث المبدأ – جميع أنواع الجرائم التي يمكن تنفيذها ضمن بيئة إلكترونية. [2]

نحن نؤيد هذا التعريف، لأنه يعتبر الأكثر شمولا في تناوله للأشكال المختلفة للجريمة الإلكترونية، فهو يشمل الجرائم التي قد تحدث من خلال النظام الالكتروني أو تلك التي تستهدف النظام ذاته، بما في ذلك البيانات والبرامج والمعلومات، كما يمتد ليتناول الجرائم التي يمكن أن تقع ضمن بيئة إلكترونية، هذا التعريف لم يركز على الفاعل أو مهاراته التقنية، ولم يحدد وسيلة ارتكاب الجريمة أو الأهداف والنتائج المرجوة منها، بل سعى إلى تجنب الحصر الضيق الذي قد يؤدي إلى إفلات العديد من صور الجرائم الإلكترونية من نطاق المساءلة والعقوبة.

يتبين من خلال استعراضنا للتعريفات الفقهية السابقة لمفهوم الجريمة الإلكترونية، أنها ركزت بوجه عام على عناصر محدودة تمثلت في ارتباطها بجهاز الحاسوب والبيانات، دون الخوض في التفاصيل الدقيقة التي تواكب تطور هذه الظاهرة، ويلاحظ أن الفقهاء الذين تبنوا اتجاها موسعا في تعريف الجريمة الإلكترونية قد أبدوا قدرا أكبر من

[1] بن سعيد صبرينة، الجريمة المستحدثة، دار الباحث، ط1، 2022، ص 104.

[2] نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، مذكرة مقدمة لنيل درجة الماجيستر، في القانون العام، بكلية الدراسات العليا في جامعة النجاح الوطنية، نابلس، فلسطين، 2017، ص 05.

البصيرة، نظرا للطبيعة المتسارعة والمتغيرة للعالم الرقمي، حيث إن تضييق نطاق التعريف من شأنه أن يقيد فهمنا للجريمة الإلكترونية ويحد من القدرة على مكافحتها.

وبالنظر إلى مختلف التعريفات، نجد أن تعريف منظمة التعاون الاقتصادي والتنمية يتميز بوضوحه وشموليته، وذلك لعدة أسباب:

1. أنه يحدد طبيعة السلوك الإجرامي بدقة، حيث لم يقتصر على الأفعال الإيجابية، بل شمل أيضا صور الامتناع أو التقاعس التي يمكن أن تشكل سلوكا إجراميا؛

2. اعتماده مفهوما واسعا يتيح تغطية أكبر قدر ممكن من أنماط الجرائم التقنية، من خلال الربط بين الجريمة وكل تدخل في التقنية الالكترونية، سواء تم ذلك بشكل مباشر أو غير مباشر؛

3. إبراز الطابع التقني الخاص الذي يعد سمة مميزة لأغلب صور الجريمة الإلكترونية.

يتيح إمكانية التعامل مع التطورات المستقبلية التقنية، [1]

يمكن تعريف الجريمة الإلكترونية بأنها تتألف من ثلاثة عناصر أساسية: السلوك، وصفه، والنص القانوني الذي يجرم هذا السلوك ويحدد العقوبة المترتبة عليه، يضاف إلى ذلك محل الاعتداء في الجريمة، والذي يتمثل في معطيات الحاسوب، وهو ما يميزها عن الجرائم التقليدية.

فهي تعد سلوكا غير قانوني يعاقب عليه وفقا للقانون، وينبع من إرادة جرمية، ويكون محل الجريمة دائما مرتبطا بمعطيات الحاسوب بمعناها الواسع، يشمل السلوك هنا كلا من الفعل الإيجابي والامتناع عن العمل، مع الأخذ بعين الاعتبار أن وصف الفعل

[1] سفيان سوير، مرجع سابق، ص 15.

بالصفة الجرمية لا يتحقق في المجال الجنائي إلا إذا جاء بناء على نص قانوني صريح صادر عن المشرع، [1]

بعد استعراض مختلف التعاريف، نجد أن التعريف الذي قدمه الأستاذ هلالي عبد الله أحمد هو الأكثر شمولا ودقة، حيث يعرف الجريمة الإلكترونية بأنها كل عمل أو امتناع عن عمل يرتكبه الإنسان ويتسبب في الإضرار بمكونات الحاسب الآلي وشبكات الاتصال، والتي يتم حمايتها بموجب قانون العقوبات الذي يفرض عقوبات على مرتكبي هذه الجرائم.[2]

ثانيا: التعريف القانوني :

تجنب معظم المشرعين الخوض في مسألة وضع تعريف تشريعي لنظام المعالجة الآلية للبيانات، وتركو مهمة ذلك للفقه والقضاء، ومع ذلك، اتجه بعض المشرعين إلى وضع تعاريف لنظام المعلومات بدلا من نظام المعالجة الآلية للمعلومات، ومن بين التشريعات التي قدمت تعريفا لنظام المعلومات، نذكر....

قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لعام 1996، عرف نظام المعلومات في الفقرة (و) من المادة الثانية بأنه:

كل نظام يستخدم في إنشاء رسائل البيانات، أو إرسالها، أو استلامها، أو تخزينها، أو معالجتها بأي طريقة كانت.[3]

---

[1] إدريس النوازلي، موقف القضاء من الجريمة الإلكترونية، سلسلة الندوات والأيام الدراسية، التجارة الإلكترونية أية حماية ؟ أشغال الندوة الوطنية التي نظمها مكتب الدراسات الجنائية وهيئة المحامين بمراكش المغرب، أيام 29، 30 ماي 2009، ص: 91.

[2] – عبد الله أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ، دار النهضة العربية، 1 القاهرة، 2000، ص105–106.

[3] نشناش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية، جامعة بسكرة 2015 – 2016، ص 3.

يعرف قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001، وفقا لنص المادة 2 الفقرة 10، نظام معالجة المعلومات بأنه النظام الإلكتروني الذي يستخدم لإنشاء رسائل المعلومات أو إرسالها أو استلامها أو معالجتها أو تخزينها أو تجهيزها بأي شكل من الأشكال.[1]

قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكترونية رقم 02 لسنة 2002، عرف في المادة 2 فقرة 6، ضمن سياق تعريف المصطلحات، نظام المعلومات الإلكتروني بأنه: نظام إلكتروني يستخدم لإنشاء أو استخراج أو إرسال أو استقبال أو تخزين أو عرض أو معالجة المعلومات والرسائل إلكترونيا. [2]

يلاحظ أن التعريفات الثلاثة المتقدمة تطبق بدرجة أكبر على نظام المعالجة الآلية للمعطيات، وليس على نظام المعلومات بمفهومه الشامل، كما أنها تتبنى منهجا موحدا في تعريف نظام المعلومات، يرتكز على تعداد الوظائف التي يضطلع بها هذا النظام، والتي تمثل في جوهرها أساليب المعالجة الالكترونية، في حين أن المعالجة الآلية لا تعدو كونها مجرد وظيفة من ضمن هذه الوظائف.

وعلى الرغم من أن مفهوم المعالجة الآلية أوسع نطاقا من مفهوم المعالجة الالكترونية، فإن هذه التعريفات تخلو من الإشارة إلى الشرطين الأساسيين اللذين أكد مجلس الشيوخ الفرنسي ضرورة توافرهما في النظام.

ثالثا: موقف المشرع الجزائري

اعتمد المشروع الجزائري مصطلح المساس بأنظمة المعالجة الآلية للمعطيات في تعريف الجريمة، حيث اعتبر أن النظام الالكتروني ذاته، بما يشمله من مكونات غير

[1] قانون رقم 35 لسنة 2001، الجريدة الرسمية للمملكة الأردنية الهاشمية رقم 4524 الصادر بتاريخ 31/12/2001، ص 610.

[2] قانون إمارة دبي رقم 02 لسنة 2002 متعلق بالمعاملات والتجارة الإلكترونية، صادر بتاريخ 12 فبراير 2002

مادية، يمكن أن يكون محلا للجريمة، ويشكل نظام المعالجة الآلية للمعطيات العنصر الأساسي أو الشرط الأولي الذي يجب توفره للنظر في إمكانية تحقق أركان الجريمة المتعلقة بالاعتداء على هذا النظام، فإذا لم يتحقق هذا الشرط الأولي، لا يكون هناك مجال لمواصلة البحث في الجريمة.[1]

حيث أنه عرف من خلال نص المادة 2 من الفقرة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مسميا إياه المنظومة الالكترونية وهي أي نظام منفصل ومجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين. [2]

بالتأثر بالثورة الالكترونية وما أفرزته من أنماط جديدة من الإجرام لم تعرفها البشرية من قبل، قام المشرع الجزائري بتجريم الأفعال التي تمس بأنظمة الحاسب الآلي، وذلك من خلال تعديل قانون العقوبات بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، الذي جاء مكملا للأمر رقم 156/66 المتضمن قانون العقوبات، وقد خصص هذا التعديل قسما سابعا مكررا تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وتضمن ثماني مواد تبدأ من المادة 394 مكرر إلى المادة 394 مكرر 03/07.

وفي إطار تعريفه لنظام المعالجة الآلية للمعطيات، ميز المشرع الجزائري نفسه عن بعض التشريعات الأخرى، حيث اشترط وجود ترابط بين مكونات أو أجهزة النظام أو

[1] قانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ح ر ع 47 صادر بتاريخ 16/08/2009 ، ص 5.

[2] بن سعيد صبرينة، المرجع السابق، ص 104.

بين الأنظمة المختلفة، كما أولى أهمية لوظيفة المعالجة الآلية للمعطيات، موسعا بذلك نطاق الحماية القانونية ليشمل جميع أشكال المعالجة الإلكترونية للمعلومات، [1]

يستنتج من موقف المشرع الجزائري تجاه الجريمة الإلكترونية أنه أدرك أهمية التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة وما نتج عنهما من ظهور أشكال جديدة من الجرائم، ولسد الفراغ القانوني في هذا المجال، قام المشرع بتعديل قانون العقوبات بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، والذي أضاف القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

ركز المشرع الجزائري على حماية الأنظمة الالكترونية وأساليب المعالجة الآلية للمعطيات، حيث اقتصرت التجريم على الأفعال التي تستهدف النظام الالكتروني كمحلا للجريمة، دون أن يشمل الجرائم التي يستخدم فيها النظام الالكتروني كوسيلة لارتكابها، وبذلك، خرجت الجرائم التي يكون النظام الالكتروني مجرد وسيلة لارتكابها من نطاق التجريم، مركزا بذلك على حماية النظم الالكترونية ذاتها.

أقر المشرع الجزائري بأهمية المعطيات التي يتم إدخالها إلى الحاسب الآلي، حيث تتحول إلى معلومات بعد معالجتها وتخزينها، الأمر الذي دفعه إلى اتخاذ تدابير لحمايتها من مختلف أشكال الاعتداء، وفي إطار تطوير التشريعات، اختار المشرع مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لوصف الجرائم الالكترونية، كما جاء في القانون رقم 09-04 الذي يهدف إلى مكافحتها[2].

[1] نشناش منية، المرجع نفسه ص04.

[2] قانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ح ر ع 47 صادر بتاريخ 16/08/2009

وتناول المشرع الجزائري في المادة 2 من هذا القانون تعريف الجريمة التي تستهدف أنظمة المعالجة الآلية للمعطيات، كما تم تجريم الأفعال التي تمس بهذه الأنظمة ضمن المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات، [1]

الفرع الثاني: خصائص الجريمة الإلكترونية

تعد جرائم الالكترونية نتاجا مباشرا لتطور تقنية المعلومات، إذ إنها ترتبط بها ارتباطا وثيقا وتعتمد عليها، وهو ما منحها طابعا قانونيا خاصا يميزها عن الجرائم التقليدية أو المستحدثة الأخرى، حيث تنفرد بسمات معينة قد تتقاطع مع خصائص بعض الجرائم الأخرى من جهة، لكنها من جهة أخرى تختلف عنها اختلافا جوهريا من حيث طبيعة الأفعال الإجرامية، مما أكسبها خصوصية فريدة.

ويعد تعقب جرائم الحاسب الآلي والإنترنت والكشف عنها من المهام الصعبة، نظرا لكونها لا تترك آثارا مادية ملموسة، فلا توجد أموال أو مجوهرات مفقودة، وإنما مجرد أرقام تتغير في سجلات رقمية، وغالبا ما يتم اكتشاف هذه الجرائم بالصدفة وبعد مرور وقت طويل على ارتكابها، كما أن الجرائم التي لم تكتشف تفوق بكثير تلك التي تم كشفها، وترجع صعوبة إثبات جرائم الحاسب الآلي إلى خمسة أسباب رئيسية وهي:

1.تتميز هذه الجريمة بعدم تركها لأي آثار مادية واضحة عقب ارتكابها.

2.حتى في حال وجود آثار، فإن من الصعب الاحتفاظ بها فنيا لفترة طويلة.

3.تتطلب هذه الجريمة خبرة تقنية متقدمة، ما يجعل من الصعب على المحقق التقليدي التعامل معها بفعالية.

4.ترتكب بأساليب خداعية، ويستخدم فيها التضليل لإخفاء هوية الجاني.

[1] سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجستير في علوم القانونية، جامعة الحاج لخضر باتنة 2012 2013، ص 41 وما بعدها.

5.تعتمد في تنفيذها على قدر عالٍ من الذكاء والمهارة.[1]

تعد الجريمة الالكترونية مرتبطة بشكل وثيق بالحاسوب وشبكة الإنترنت، مما منحها ميزات خاصة تميزها عن الجرائم التقليدية، ومن أبرز هذه الميزات:

– تنفيذها عبر الإنترنت: ترتكب الجرائم الالكترونية من خلال شبكة الإنترنت، التي تمثل الرابط الأساسي بين جميع الأهداف المحتملة، مثل البنوك والشركات، والتي غالبا ما تكون ضحية لهذه الجرائم.

– طبيعتها العابرة للحدود: لا تعترف الجرائم الالكترونية بالحدود الجغرافية، فالمجتمع الرقمي منفتح عبر شبكات تتجاوز قيود الزمان والمكان دون الحاجة إلى إجراءات حدودية، وهذا يجعل نطاق ارتكاب الجرائم الالكترونية عالميا، مما يثير العديد من الإشكاليات المتعلقة بتحديد الدولة صاحبة الاختصاص القضائي، وتحديد القوانين الواجب تطبيقها، إضافة إلى التحديات المرتبطة بإجراءات الملاحقة القضائية وغيرها من المسائل القانونية المرتبطة بالجرائم العابرة للحدود.[2]

– تتمثل صعوبة إثبات الجريمة الإلكترونية في كونها ترتكب بشكل خفي، دون ترك أي أثر مادي أو إيجابي للأفعال الإجرامية التي تحدث أثناء تنفيذها، فالمعلومات يتم نقلها إلكترونيا، مما يجعل تتبعها أمرا معقدا، بالإضافة إلى ذلك، يتردد مجتمع الأعمال في الإبلاغ عن هذه الجرائم لتجنب الإضرار بسمعته أو زعزعة الثقة في كفاءة المؤسسات

[1] – محمد عبد الله منشاوي: جرائم الانترنت من منظور شرعي وقانوني، ص 11، الجمعية الدولية للمترجمين www.wata.cc تاريخ التصفح 2025/03/16

[2] رصاع فتيحة، الحماية الجنائية للمعلومات علي شبكة الانترنت، مذكرة ماجستير منشورة، تخصص القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان 2011–2012، ص 43.

والمنظمات التي تعرضت للجريمة، كما أن المعلومات التي قد تستخدم كأدلة يمكن تدميرها بسهولة في أقل من ثانية واحدة، مما يزيد من تعقيد عملية الإثبات، [1]

– الخسائر الناجمة عن الجرائم الالكترونية تتجاوز بكثير تلك الناتجة عن الجرائم التقليدية، وفقا لشركة انتل سكيوريتي المتخصصة في أمن المعلومات، تتكبد قطاعات الأعمال العالمية خسائر سنوية ضخمة تصل إلى 400 مليار دولار أمريكي، والأكثر من ذلك، أن الهجمات الإلكترونية أصبحت صناعة متنامية بذاتها، حيث تقدر قيمتها بين 2 إلى 3 تريليون دولار سنويا، مما يشكل نسبة 15 إلى 20% من القيمة الاقتصادية الناتجة عبر الإنترنت.[2]

تشهد الهجمات الإلكترونية تأثيرات مدمرة على الشركات والمؤسسات المالية، حيث تكبدت شركة بريطانية خسارة هائلة بلغت 1.3 مليار دولار جراء هجوم إلكتروني واحد، بينما خسر مصرفان في الخليج 45 مليون دولار في فترة زمنية قصيرة جدا، وفي سياق متصل، كشفت الهند عن تعرض عدد كبير من المواقع الإلكترونية للاختراق، حيث بلغ العدد الإجمالي أكثر من 308371 موقعا خلال الفترة بين 2011 و2013.[3]

– تكاد الصورة النمطية التقليدية للمجرم أن تتلاشى في الجرائم الالكترونية؛ بل إن مرتكب هذا النوع من الجرائم غالبا ما ينتمي إلى طبقة اجتماعية مرتفعة مقارنة بغيره من المجرمين، ونادرا ما يكون ذا سجل إجرامي أو من العائدين إلى الإجرام، كما لا ينظر

[1] محمد علي العريان الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، 2004، ص 53.

[2] إنتل سكيوريتي: خسائر قطاعات الأعمال من الهجمات الإلكترونية تصل إلي 400 مليار دولار سنويا، البوابة العربية للأخبار التقنية، www.aitnews.com، تاريخ التصفح 2025/03/16

[3] – عبد الإله مجيد القراصنة يفضلون استهداف الدول الغنية الجريمة الالكترونية تكلف العالم 400 مليار دولار سنويا،http://elaph.com/Web/News/10/06/2014/، تاريخ التصفح، 2025/03/16.

إليه على أنه مجرم بالمعنى المتعارف عليه، نظرا لاختلاف الدوافع والعوامل التي تقف خلف الجريمة الالكترونية عن تلك المرتبطة بالجريمة التقليدية.[1]

– يعد الإبلاغ عن الجرائم الالكترونية أمرا نادرا لعدة أسباب، أبرزها:

– الخوف من التشهير: يتردد العديد من الضحايا في الكشف عن تعرضهم لجريمة إلكترونية خشية من المساس بسمعتهم، مما يؤدي إلى أن معظم هذه الجرائم لا تكتشف إلا عن طريق الصدفة أو بعد مرور وقت طويل على وقوعها.

– عدم إدراك الضحية للجريمة: في كثير من الحالات، لا يدرك الضحية أنه وقع ضحية لجريمة معلوماتية، مما يعني أن عدد الجرائم غير المكتشفة يفوق بكثير تلك التي تم كشفها، [2]

الجريمة الإلكترونية تعد من أحدث أشكال الجرائم، حيث يمتد مسرحها إلى العالم الافتراضي البعيد عن أي مظاهر ملموسة للجريمة التقليدية، وهي جريمة عابرة للحدود، تنفذ على أيدي مجرمين بارعين يتميزون بالذكاء والمهارة العالية، مما يجعل تتبعهم أو التحري عنهم أمرا معقدا، هذا الواقع يؤدي إلى تشتيت الجهود الدولية في محاولات تعقب هذه الجرائم أو الوصول إلى مرتكبيها.

المطلب الثاني: أنواع الجرائم الإلكترونية

بعد أن تناولنا مفهوم الجريمة الإلكترونية وحددنا تعريفها وخصائصها الأساسية، ننتقل الآن إلى استعراض أنواع هذه الجرائم وتصنيفاتها المختلفة، تتنوع الجرائم الإلكترونية وتتعدد أشكالها بتعدد الدوافع والوسائل والأهداف التي يسعى إليها مرتكبوها، مما يجعل تصنيفها ضرورة ملحة لفهم أبعادها وتطوير استراتيجيات فعالة لمواجهتها، في

[1] سوير سفيان جرائم المعلوماتية، مذكرة ماجستير منشورة، تخصص العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2010-2011، ص 18-19.

[2] خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، مصر، ط1، 2008، ص 51.

هذا المطلب، سنقدم عرضا منهجيا لأبرز أنواع الجرائم الإلكترونية وفقا لمعايير مختلفة، مع التركيز على خصائصها وآثارها، مما يساهم في بناء رؤية شاملة حول طبيعة هذه الظاهرة وتداعياتها على الفرد والمجتمع.

الفرع الأول: الجرائم الواقعة بالوسائل الالكترونية

في سياق الجرائم الالكترونية، يستخدم الحاسب الآلي كوسيلة لتسهيل وتسريع النتائج الإجرامية، مع تضخيم حجم الأضرار الناجمة عنها، يهدف الجاني من وراء هذه الأفعال إلى تحقيق مكاسب مالية غير مشروعة، ويتم ذلك من خلال استخدام النظام الالكتروني أو البرامج كأدوات لتنفيذ الجريمة، وتنقسم هذه الجرائم بدورها إلى عدة فئات، تشمل....[1]

أولا: الجرائم الواقعة على الأشخاص:

تتمتع الحياة الشخصية بخصوصية وحرمة لا يجوز المساس بها أو التعدي عليها من أي شخص كان، ومن صور هذا التعدي، الاعتداء على البيانات والمعلومات الإلكترونية الخاصة ببعض المهنيين، كالمحامين أو الأطباء أو المحاسبين وغيرهم، وقد تتحقق هذه الجريمة من خلال الاطلاع غير المشروع على تلك المعلومات، أو عبر تسجيل مكالمات أو مقاطع فيديو، أو حتى من خلال مراقبة الشخص المستهدف.

أما فيما يتعلق بجريمة نشر المواد الإباحية، فيتمثل ركنها المادي في السلوك الإجرامي الذي يقوم به الفاعل، من خلال إعداد أو تهيئة صفحات إلكترونية تتضمن محتوى منافيا للآداب العامة، ثم نشره عبر شبكة الإنترنت، بينما يتمثل الركن المعنوي في القصد

[1] نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر الجرائم الإلكترونية، مركز جيل البحث العلمي، طرابلس، 24-25 مارس 2017،، ص 102.

الجنائي، أي توافر الإرادة والعلم لدى الجاني بما يقوم به، مع قصدٍ واضح في نشر تلك المواد المخلة،

ثانيا: الجرائم الواقعة على الأموال

مع ظهور شبكة الإنترنت، شهدت مختلف المجالات تطورات كبيرة، حيث أصبحت المعاملات التجارية تعتمد عليها بشكل أساسي، مثل عمليات البيع والشراء، وقد أدى ذلك إلى تطور وسائل الدفع الإلكتروني، مما جعلها جزءا لا يتجزأ من هذه المعاملات، وفي ظل هذا التداول المالي عبر الإنترنت، استغل بعض المجرمين هذه الفرصة للقيام بعمليات سطو إلكترونية، حيث ابتكروا طرقا متعددة لتنفيذ جرائمهم، مثل السرقة الإلكترونية، والتحويل غير المشروع للأموال، وقرصنة بيانات البطاقات المصرفية الممغنطة.[1]

مع التحول المتنامي من المعاملات التجارية التقليدية إلى المعاملات الإلكترونية، وما رافقه من تطور في وسائل الدفع والتسوية المالية، بالإضافة إلى زيادة حجم التداول المالي عبر الإنترنت، أصبحت هذه المعاملات عرضة لمختلف أنواع الجرائم، ومن أبرزها:

- السطو على أرقام بطاقات الائتمان والقيام بتحويلات إلكترونية غير قانونية.
- ممارسة القمار وغسيل الأموال باستخدام شبكة الإنترنت.
- السرقة الإلكترونية واستهداف أموال البنوك.
- تجارة المخدرات عبر المنصات الإلكترونية.[2]

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، جامعة مولود معمري – تيزي وزو – كلية الحقوق والعلوم السياسية، 2013، ص 44.

[2] حفوظة الأمير عبد القادر وغرداين حسام الجريمة الإلكترونية وآليات التصدي لها، الملتقي الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 93.

ج الجرائم الواقعة على أمن الدولة

استغلت العديد من الجماعات المتطرفة الطبيعة الاتصالية للإنترنت لنشر معتقداتها وأفكارها، بل تجاوز ذلك إلى ممارسات تهدد أمن الدول المستهدفة، مثل الإرهاب والجريمة المنظمة، التي اكتسبت أبعادا جديدة من خلال استخدام الإنترنت، وقد أتاح هذا الوسيط لهذه الجماعات ارتكاب جرائم خطيرة بحق المجتمعات والدول.

الأمر الأكثر خطورة هو أن الإنترنت وفرت لبعض الدول إمكانية التجسس على دول أخرى، من خلال الوصول إلى أسرارها العسكرية والاقتصادية، خاصة في الدول التي تشهد نزاعات، كما أن المساس بالأمن الفكري يعد من أخطر الجرائم المرتكبة عبر الإنترنت، حيث تتيح هذه الشبكة فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها، مما يسهل خلق الفوضى.[1]

الفرع الثاني: الجرائم الواقعة على النظام الالكتروني

إلى جانب الجرائم الالكترونية التي ترتكب باستخدام النظام الالكتروني كأداة، هناك فئة أخرى من الجرائم الالكترونية التي تتركز على النظام الالكتروني نفسه، وتشمل هذه الفئة الجرائم التي تستهدف المكونات المادية للنظام، مثل الأجهزة والشبكات، أو المكونات المنطقية، مثل البرامج والبيانات، أو المعلومات المخزنة داخل النظام، مما قد يؤدي إلى أضرار كبيرة بالنظام نفسه.

أولا: الجرائم الواقعة على المكونات المادية للنظام الالكتروني:

[1] ناصر محمد البقهي، اثر التحويل مجتمع معلوماتي علي الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات كرسي الأمير نايف بن عبد العزيز الدراسات الأمن الفكري بجامعة الملك سعود المملكة السعودية 22 25 جمادي الأولي 1430 ه، ص 18

المكونات المادية للنظام الالكتروني تشير إلى الأجهزة والمعدات المرتبطة به، مثل الأسطوانات والشرائط والكابلات، التي تستخدم لتشغيل النظام، وبسبب الطبيعة المادية لهذه المعدات، فإن الجرائم التي تستهدفها غالبا ما تكون تقليدية، مثل السرقة، خيانة الأمانة، الإتلاف العمد، الحرق، أو العبث بمفاتيح التشغيل، وينتج عن هذه الجرائم خسائر مادية كبيرة، ومن الأمثلة على ذلك ما حدث في فرنسا، حيث تعرضت معدات إحدى المؤسسات الكبرى المتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية للتلف، مما أدى إلى خسائر قدرت بخمسة ملايين فرنك فرنسي، [1]

ثانيا: الجرائم الواقعة على المعلومات المدرجة بالنظام الالكتروني

لا شك أن هذه الصورة تعد من أكثر صور الجرائم الالكترونية شيوعا وخطورة، حيث يستخدم أسلوب الاحتيال لإدخال بيانات في نظم المعالجة الآلية للمعلومات، أو لتخريبها أو حذفها أو تعديل المعطيات المخزنة فيها بشكل غير مشروع، [2]

عالج المشرع الجزائري هذا النوع من الجرائم من خلال نص المادة 394 مكرر من قانون العقوبات، الذي ينص على معاقبة كل من أدخل بطرق احتيالية معطيات في نظام المعالجة الآلية للمعلومات، أو قام بإزالة أو تعديل تلك المعطيات بطرق الغش، العقوبة تشمل الحبس لمدة تتراوح بين ستة أشهر وثلاث سنوات، بالإضافة إلى غرامة مالية تتراوح بين 5000 دينار جزائري و20,000 دينار جزائري.

ولمعالجة عناصر هذه الجريمة، يتعين تحديد مفهوم الإتلاف والوسائل التي يتم بها تحقيقه، ويعرف بعضهم الإتلاف بأنه الفعل الذي يؤدي إلى جعل الشيء غير صالح

[1] نمديلي رحيمة، مرجع سابق، ص 103-104.

[2] سومية عكور، الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانوني والأمني، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، الأردن، 02-04/09/2014، ص 12.

للاستعمال، سواء بإبطال صلاحيته أو تعطيله كليا أو جزئيا، مما يؤثر على عمله بشكل مباشر.

يقصد بالإتلاف، بوجه عام، إحداث تلف أو ضرر يؤدي إلى فناء مادة الشيء أو هلاكه كليا، بحيث يفقد تماما قدرته على أداء وظيفته، أو حتى إذا لم تفنَ مادته بشكل كامل، فإن التوقف الجزئي عن العمل بما يمنع تحقق المنفعة المرجوة يعد كذلك إتلافا، متى أصبح الشيء غير صالح للاستعمال أو عاجزا عن أداء وظيفته بالشكل المطلوب.

أما فيما يتعلق بإتلاف برامج الحاسوب ومحتوياته، فيقصد به محو أو تخريب التعليمات البرمجية أو البيانات المخزنة ضمن نظام الحاسوب، وهو ما يعرف اصطلاحا بتدمير نظم المعلومات، وغالبا لا يكون هدف الجاني من هذا الفعل تحقيق مكسب مالي، وإنما يهدف إلى عرقلة النظام أو تعطيله عن أداء وظيفته.

يتحقق الإتلاف ليس فقط بالتأثير على مادة الشيء، بل أيضا بالانتقاص من قيمته الاقتصادية، حيث يكمن جوهر الإتلاف في مدى المساس بالقيمة المالية للشيء، وليس مجرد تعرضه لمادته، فالفعل الذي يؤدي إلى فقدان الشيء لقيمته أو تقليلها يعد اعتداء يعاقب عليه القانون.

وقد استخدم المشرع الجزائري عدة مصطلحات للدلالة على الإتلاف، مثل أدخل، أزال، وعدل، رغم اختلاف مدلولاتها، إلا أنها تندرج جميعا ضمن مفهوم الإتلاف، وهو ما أكدته بعض التشريعات المقارنة، مثل التشريع الفرنسي، كما أن المشرع الجزائري ذكر صورا للإتلاف في القانون على سبيل المثال لا الحصر، مما يعني إمكانية تحقق الإتلاف بطرق أخرى غير محددة قانونيا.

في سياق الجرائم الالكترونية، يشمل الإتلاف الجانب المنطقي والمعنوي للحاسب الآلي، نظرا لقيمته الاقتصادية العالية، حيث يؤدي إتلاف البرامج والمعلومات الرقمية إلى فقدانها لمنفعتها[1].

ثالثا: الجرائم الواقعة على البرامج الإلكترونية

فيما يتعلق بالجرائم الواقعة على البرامج التطبيقية، يتمثل الفعل الإجرامي في تحديد البرنامج أولا ثم التلاعب به أو تعديله، ومن الأمثلة على ذلك، ما قام به أحد المبرمجين في أحد البنوك الأمريكية، حيث قام بتعديل برنامج بحيث يضيف دولارا واحدا إلى كل حساب يزيد رصيده عن عشرة دولارات، وتم توجيه هذه المبالغ الزائدة إلى حساب خاص به تحت اسم.zzwick

أما الجرائم التي تستهدف برامج التشغيل، وهي البرامج المسؤولة عن إدارة النظام الالكتروني وضبط ترتيب العمليات فيه، فتتحقق من خلال إدخال مجموعة من التعليمات الإضافية إلى البرنامج، تتيح هذه التعليمات للمجرم الوصول إلى جميع المعطيات الموجودة في النظام الالكتروني عبر شيفرة خاصة، ومن الأمثلة على هذا النوع من الجرائم، تصميم برنامج وهمي لتنفيذ الأفعال غير المشروعة، على سبيل المثال، قامت إحدى شركات التأمين في مدينة لوس أنجلوس، بالتعاون مع مبرمجها، بتصميم برنامج يقوم بتوليد وثائق تأمين وهمية لأكثر من 46,000 شخص غير موجودين في الواقع، كان الهدف من هذه العملية الاحتيالية هو الحصول على عمولات غير مستحقة من اتحاد شركات التأمين، [2]

[1] أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الألية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد العاشر، العدد الأول، ص 486-487.

[2] نمديلي رحيمة، مرجع سابق، ص 104.

المبحث الثاني: أركان الجريمة الالكترونية ودوافع ارتكابها

بعد أن استعرضنا في المبحث الأول ماهية الجريمة الإلكترونية من حيث مفهومها وخصائصها وأنواعها المختلفة، نتناول في المبحث الثاني أركان الجريمة الالكترونية ودوافع ارتكابها، سنعالج في هذا المبحث الجهود التشريعية المبذولة للتصدي لهذه الظاهرة من خلال مطلبين أساسيين:

المطلب الأول: سنتناول فيه أركان الجريمة الإلكترونية، حيث سنقوم بتحليل الركن المادي بعناصره المختلفة ، والركن المعنوي بصورتيه ، بالإضافة إلى الركن القانوني المتمثل في النصوص التشريعية المجرمة للأفعال الإلكترونية.

المطلب الثاني: سنخصصه لدراسة دوافع ارتكاب الجرائم الإلكترونية، حيث سنستعرض الدوافع المختلفة التي تحرك مرتكبي هذه الجرائم.

من خلال هذا المبحث، سنسعى إلى تقديم فهم عميق للبنية القانونية للجريمة الإلكترونية والعوامل المحركة لها، مما يساهم في تعزيز القدرة على التصدي لها بفعالية، من خلال استهداف أركانها الأساسية ومعالجة الدوافع الكامنة وراء ارتكابها.

المطلب الأول: أركان الجريمة الالكترونية

تقوم الجريمة الإلكترونية، شأنها شأن أي جريمة تقليدية، على أركان أساسية يتطلب القانون توافرها مجتمعة لاكتمال البنيان القانوني للجريمة وقيام المسؤولية الجنائية، غير أن الطبيعة الخاصة للجريمة الإلكترونية وارتباطها بالبيئة الرقمية تضفي خصوصية على هذه الأركان وتطرح تحديات قانونية وعملية في تحديدها وإثباتها.

في هذا المطلب، سنتطرق إلى تحليل الأركان الثلاثة للجريمة الإلكترونية: والركن الشرعي المتمثل في النصوص التشريعية التي تجرم الأفعال الماسة بالنظم المعلوماتية

وبيانات الحاسب الآلي، والركن المادي بما يشمله من سلوك إجرامي ونتيجة وعلاقة سببية، والركن المعنوي بصورتيه من قصد جنائي وخطأ غير عمدي.

الفرع الأول: الركن الشرعي

استنادا إلى مبدأ الشرعية الوارد في المادة الأولى من قانون العقوبات الجزائري، التي تنص على أنه لا جريمة ولا عقوبة أو تدابير أمن بغير قانون، جاء القانون رقم 04-15 ليجرم بعض أشكال الجرائم الالكترونية، محددا العقوبات المقررة بحق مرتكبيها في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، ضمن الفصل الثالث الجنايات والجنح ضد الأموال، من الباب الثاني المتعلق بالجنايات والجنح ضد الأفراد، وذلك في المواد من 394 مكرر إلى 394 مكرر 08 من قانون العقوبات المعدل والمتمم.

أما القانون رقم 09-04، فقد تضمن قواعد خاصة تهدف إلى الوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها، من خلال اتخاذ إجراءات وقائية تحد من وقوع الجرائم الالكترونية، وذلك عبر وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وتسجيل وتجميع محتواها بشكل فوري، بالإضافة إلى تنفيذ عمليات التفتيش داخل المنظومة الالكترونية[1].

عندما يقنن المشرع الجرائم بشكل صريح ويجعلها خاضعة لمبدأ الشرعية، فإن ذلك يحظر على القاضي الجنائي اللجوء إلى القياس، وهذا يعني أنه لا يجوز للقاضي أن يوسع نطاق التجريم ليشمل أفعالا لم ينص عليها بشكل صريح في القانون، بحيث يقيس فعلا

[1] القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، صادرة بتاريخ 2009/08/16.

غير مجرم على فعل آخر تم تجريمه صراحة، ويطبق عليه نفس العقوبة بسبب التشابه بين الفعلين.[1]

الفرع الثاني: الركن المادي للجريمة الالكترونية

الركن المادي للجريمة يعرَف بأنه السلوك الإجرامي الذي يحدد بوضوح في القانون كأساس للعقاب على هذه الجريمة، ويتطلب هذا الركن أن يترتب على السلوك الإجرامي ضرر مادي أو معنوي، وأن يكون هذا الضرر شرطا ضروريا لتوقيع العقاب عليه بموجب القانون، بالإضافة إلى ذلك، يجب أن تكون هناك علاقة سببية مباشرة بين السلوك الإجرامي والنتيجة الضارة، بحيث يكون السلوك هو السبب المباشر للضرر الحاصل.

أولا: السلوك الإجرامي

يتجسد السلوك الإجرامي في الجرائم الإلكترونية من خلال الأفعال الخارجية التي يرتكبها المجرم الإلكتروني، حيث يشمل أي تصرف مادي يؤدي إلى إلحاق الضرر، بغض النظر عن نية الفاعل في وقوع هذا الضرر، ويتميز هذا السلوك بأنه ينفذ عبر الإنترنت، مما يمنح هذه الجرائم طابعا موحدا من حيث النشاط المادي.

وقد أدى هذا التطور إلى تعزيز الذكاء الإجرامي لدى الفاعلين، مما مكنهم من تجاوز الأساليب التقليدية للسلوك الجرمي والانتقال إلى مستويات أكثر تعقيدا، وهو ما تسبب في ظهور العديد من التحديات والصعوبات في مكافحتها.

من الواضح أن ارتكاب الجريمة عبر الإنترنت يعتمد بشكل أساسي على وجود البنية التحتية التكنولوجية والوسائل التقنية اللازمة، وبدونها يستحيل على الفرد الاتصال بشبكة

[1] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي للنشر والتوزيع، مصر، 2006، ص 10.

الإنترنت والقيام بالأنشطة الإجرامية، وتبرز أهمية النشاط التقني في هذا السياق، حيث يصبح شرطا ضروريا لارتكاب الجريمة، وبدونه تفقد الجريمة عناصرها الأساسية وخصائصها التي تميزها.

ثانيا: النتيجة الإجرامية

يقصد بالنتيجة الإجرامية الأثر المادي الناتج عن السلوك الإجرامي، وهو التغيير الذي يحدث في الواقع الخارجي كنتيجة لهذا السلوك، ويترتب عليه أحكام قانونية يحددها المشرع، وتنقسم النتيجة الضارة إلى مفهومين: الأول هو المفهوم المادي، الذي يشير إلى الآثار المترتبة على الجريمة في الواقع الخارجي، بينما الثاني هو المفهوم القانوني، الذي يعني أن القانون يفرض عقوبة على هذه الآثار بمجرد تحققها، [1]

حتى تتم معاقبة الجريمة، يجب أن تكون لها طبيعة مادية ملموسة في المحيط الخارجي، ومع ذلك، هناك بعض الجرائم التي لا يترتب عليها نتيجة مادية واضحة، وتعرف هذه بالجرائم السلبية، ومن هنا تبرز أهمية الاعتراف بالمعنى أو المدلول القانوني للنتيجة، دون التركيز على حدوث ضرر فعلي، فمجرد الإخلال بالمصلحة المحمية قانونا يعتبر كافيا لتحقق الجريمة من الناحية القانونية.

على سبيل المثال، إذا قام مجرم في فرنسا باختراق جهاز خادم (Server) لأحد البنوك الأمريكية، وكان هذا الخادم موجودا في إيطاليا، فإن تحديد وقت وقوع الجريمة يصبح أمرا معقدا، هل يتم اعتماد توقيت البلد الذي ينتمي إليه المجرم (فرنسا)، أم توقيت جهاز الخادم الموجود في إيطاليا؟ هذا السؤال يفتح الباب أمام العديد من التحديات المتعلقة بتحديد الزمان والمكان لتحقق النتيجة الجرمية في جرائم الإنترنت.

[1] حنان ريحان، مبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، الطبعي الأولي منشورات الحلبي الحقوقية، بيروت، 2014، ص 88-87.

علاوة على ذلك، تطرح هذه القضايا إشكاليات قانونية معقدة حول القانون الواجب التطبيق، نظرا للأبعاد العالمية لهذه الجرائم، فالاختلافات الزمنية والجغرافية بين الأطراف المعنية تجعل من الصعب تحديد الإطار القانوني المناسب لمعالجة مثل هذه الجرائم، [1]

ثالثا: العلاقة السببية

العلاقة السببية هي الرابط الذي يربط بين الفعل والنتيجة، حيث تؤكد أن ارتكاب الفعل هو السبب المباشر في حدوث النتيجة، وتكمن أهمية هذه الرابطة في أنها شرط أساسي لإسناد المسؤولية إلى مرتكب الفعل، إذ لا يمكن محاسبته قانونيا دون إثبات هذا الارتباط، كما أن العلاقة السببية تعد ضرورية في جميع الجرائم العمدية.

ومع ذلك، قد يحدث في بعض الحالات أن يرتكب النشاط الإجرامي دون أن تتحقق النتيجة المتوقعة، مما يؤدي إلى اعتبار الفعل مجرد شروع في ارتكاب الجريمة، أما في الجرائم السيبرانية، فتظهر تحديات أكبر عند محاولة إثبات العلاقة بين النشاط الجرمي والنتائج الضارة الناتجة عنه، نظرا لطبيعة هذه الجرائم المعقدة، حيث يمكن أن يؤدي فعل إجرامي واحد إلى عدة أضرار مختلفة، [2]

الفرع الثالث: الركن المعنوي للجريمة الإلكترونية

الركن المعنوي في الجرائم الإلكترونية يقوم على توافر نية إجرامية واضحة لدى الفاعل، تتجسد في إرادته لارتكاب فعل غير مشروع يعاقب عليه القانون، مثل انتحال هوية مزود خدمة عبر الإنترنت أو سرقة بيانات بطاقات الائتمان. هذه النية لا تكون

[1] عماد مجدي عبد المالك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، مصر 2001، ص 37.

[2] حنان ريحان مبارك المضحكي، المرجع السابق ص 90.

مجردة، بل ترتبط بنتيجة جرمية محددة تنشأ عن الفعل، مما يضفي على إرادة الجاني صفة إجرامية واضحة نابعة من علمه بأثر فعله الضار. [1]

وتتباين صورة هذا الركن المعنوي بحسب نوع الجريمة المعلوماتية. فمثلا، في حالة الدخول غير المصرح به إلى نظام معلوماتي، يشترط القانون توفر قصد جنائي عام، وهو علم الجاني بأنه يدخل إلى النظام دون إذن. إذا حدث هذا الدخول عن طريق الخطأ أو دون قصد، وزال بمجرد تنبه الجاني إلى الوضع، فإن القصد الجنائي ينتفى.

أما في جريمة الاحتيال الإلكتروني، فهي جريمة عمدية بطبيعتها، وتتطلب توافر القصد الجنائي بنوعيه: العام والخاص. فالجاني يكون مدركا لمخالفته القانونية، وتتجه نيته لتحقيق مكسب غير مشروع، سواء له أو لغيره، أو لسلب شخص آخر ممتلكاته دون وجه حق. [2]

المطلب الثاني: مرتكبو الجريمة الالكترونية ودوافعهم لارتكابها

تعد الجرائم الإلكترونية من الظواهر المستحدثة التي رافقت التطور التكنولوجي وانتشار الوسائط الرقمية، حيث بات من السهل ارتكاب أفعال غير مشروعة عبر الفضاء الرقمي دون الحاجة إلى التواجد المادي أو الاتصال المباشر، وللتصدي لهذا النوع من الجرائم، لا بد من فهم من يقف وراءها والدوافع التي تحركهم.

وانطلاقا من ذلك، يتناول هذا المطلب محورين أساسيين:

- الفرع الأول: مرتكبي الجريمة الإلكترونية.

[1] خالد عياد الحلبي اجراءات التحري والتحقيق في جرائم الحاسوب والانترنات الطبعة الأولي دار الثقافة للنشر والتوزيع، عمان 2011، ص 73 .74

[2] احمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية، 2006 ،ص112-113

- الفرع الثاني: نبرز فيه الدوافع التي تقف وراء ارتكاب الجريمة الإلكترونية.

الفرع الأول: مرتكبو الجرائم الإلكترونية

في العالم الإلكتروني، لا يوجد مكان للأصدقاء، فالصغير من المجرمين كالكبير، والمازح قد يكون كالحاقد، لضمان أمن المعلومات وتجنب التعرض للمساءلة القانونية، يجب التعامل مع الجميع على أنهم مصدر محتمل للخطر، المسألة ليست مسألة ثقة أو حسن نية، بل هي ضرورة أساسية لضمان الحماية من مخاطر جسيمة قد تؤدي إلى مسؤوليات وخسائر فادحة يتعذر تقديرها أو تجاوزها.[1]

كشفت الدراسات المتعمقة في مجال الجريمة الالكترونية عن وجود سبعة أنماط مميزة من المجرمين، ويمكن أن يمتلك الفرد الواحد صفات متعددة من هذه الفئات، وتتمثل هذه الفئات فيما يلي، وت وفر رؤية شاملة حول تنوع وتعدد أشكال الجريمة الالكترونية.

أولا: (Pranksters) المخادعون: تشمل هذه الفئة الأشخاص الذين يرتكبون جرائم معلوماتية بدافع التسلية أو المزاح مع الآخرين، دون أن تكون لديهم نية لإلحاق أي ضرر بالمجني عليهم، ويشمل ذلك بشكل خاص صغار مرتكبي الجرائم الالكترونية (الأحداث).[2]

ثانيا:(Hackers) القراصنة: ويقصد بالهاكر الشباب الشغوف بالالكترونية والحاسوب يتميز بقدرات استثنائية على اختراق الشبكات واستكشاف عالم البيانات، متجاوزين الحواجز مثل كلمات المرور والشفرات، ومع ذلك، فإن ما يميز هذه الفئة هو غياب النية أو القصد لإتلاف المعلومات أو تخريب أنظمة الحاسوب وشبكات الاتصال، بل إن دافعهم

[1] – محمد دباس الحميد وماركو إبراهيم نينو حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، الاردن، عمان، ط1، 2007،ص70.

[2] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية – دراسة نظرية وتطبيقية – منشورات الحاتي الحقوقية، ط1، 2005، ص 30

الأساسي يكمن في حب الاستكشاف، والبحث عن الجديد في هذا العالم الرقمي المثير، مع ميلهم إلى المغامرة والتحدي، ونادرا ما تكون أفعالهم المحظورة غير نزيهة.[1]

ثالثا: القراصنة الخبيثون (Malicious Hackers) أو (Crackers): هناك أشخاص يهدفون إلى إلحاق الأضرار بالمجني عليهم دون السعي لتحقيق أي مكاسب مالية من وراء ذلك، ويندرج تحت هذه الفئة العديد من مطوري وموزعي فيروسات الحواسيب الآلية.

رابعا: (Personnel Problem Solvers) تعد فئة الأفراد الذين يلجأون إلى جرائم الالكترونية لحل مشكلاتهم المالية ظاهرة شائعة بين مجرمي الالكترونية، هؤلاء الأفراد يرتكبون جرائم معلوماتية تسبب خسائر فادحة للمجني عليهم، وتهدف في الأساس إلى إيجاد حلول لمشكلات مالية مستعصية، والتي لا يمكن حلها بالطرق المشروعة أو حتى باللجوء إلى الجريمة التقليدية، وغالبا ما تكون المؤسسات المالية، مثل الب نوك والشركات المالية، هي المستهدفة بهذه الجرائم، مما يؤدي إلى خسائر مالية كبيرة.[2]

خامسا: (Career Criminals) المجرمون الموظفون يعد مجرمو الالكترونية الذين يسعون لتحقيق ربح مادي بطرق غير مشروعة من فئة الجرائم المنظمة، حيث تنطبق على أفعالهم صفات الجريمة المنظمة أو على الأقل يشترك أكثر من شخص في تنفيذ النشاط الإجرامي، ويتشابه المجرم الالكتروني في هذه الفئة إلى حد كبير مع المجرم التقليدي في سماته وأسلوب ارتكابه للجريمة.

سادسا: (Extreme Advocates) دعاة متطرفون: تعد الجماعات الإرهابية أو المتطرفة من بين الفئات التي تسعى إلى فرض معتقداتها وأفكارها الاجتماعية أو السياسية أو الدينية، وأحيانا تلجأ إلى النشاط الإجرامي لتحقيق ذلك، ويرتكز نشاط هذه الجماعات

[1] رصاع فتيحة، مرجع سابق، ص 56.

[2] نائلة عادل محمد فريد قورة، مرجع سابق، ص 32.

بشكل عام على استخدام العنف ضد الأفراد والممتلكات بهدف جذب الانتباه إلى قضاياها وأفكارها.

ونظرا لاعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسوب في تنفيذ أعمالها، ولأهمية المعلومات التي تحتويها هذه الأنظمة، أصبحت هدفا مغريا لهذه الجماعات، ومن الأمثلة البارزة على ذلك، قيام جماعة إرهابية تعرف في أوروبا باسم الألوية الحمراء (The Red Brigades) خلال الثمانينات بتدمير أكثر من 60 مركزا للحاسوب، في محاولة للفت الأنظار إلى معتقداتها وأفكارها، [1]

سابعا: المقصرون جنائيا: وتشمل هذه المشكلات واحدة من أبرز القضايا المرتبطة بإساءة استخدام الحواسيب الآلية، وهي الإهمال، في مجال الحواسيب، قد يؤدي الإهمال في كثير من الأحيان إلى نتائج كارثية، قد تصل حد فقدان الأرواح، على سبيل المثال، في نيوزيلندا قام اثنان من مبرمجي الحواسيب بإجراء تعديل على أحد البرامج الذي يحدد...

وقع حادث مأساوي عندما تم تغيير خط سير إحدى الطائرات، ولكن للأسف لم يتمكن الطاقم من إبلاغ قائد الطائرة بهذا التغيير الهام، مما أدى إلى كارثة عندما اصطدمت الطائرة بأحد الجبال، ونتج عن ذلك تحطمها ومقتل 60 راكبا كانوا على متنها، وقد خضع المتهمون فيما بعد للمحاكمة بتهمة القتل الخطأ، في إطار التحقي قات التي أجريت لتحديد المسؤولية عن هذا الحادث المأساوي.[2]

وهكذا، يختلف المجرم الإلكتروني بمختلف تصنيفاته عن المجرم التقليدي، إذ لا يقتصر نشاطه على مجرد الاحتيال أو السرقة، بل يتسم بذكاء حاد وقدرة تقنية عالية تمكنه

[1] سوير سفيان، مرجع سابق، ص 31

[2] – نائلة عادل محمد فريد قورة، مرجع سابق، ص 63.

من إخفاء هويته وبصماته الرقمية باستخدام وسائل إلكترونية متطورة، مما يصعب من عملية تعقبه وكشفه.

الفرع الثاني: دوافع ارتكاب الجريمة الإلكترونية

تتميز المفاهيم القانونية للدافع والغرض والغاية بمعانٍ اصطلاحية مختلفة في إطار القانون الجنائي، وترتبط ارتباطا وثيقا بمفهوم القصد الخاص في الجريمة، وتحظى هذه المسألة باهتمام واسع في الأوساط الفقهية والقضائية، حيث تثير جدلا واسعا حول دور الدافع في تحديد القصد الجرمي، وتقرر القاعدة القضائية بشكل عام أن الدافع لا يعد عنصرا أساسيا من عناصر القصد الجرمي، مما يفتح المجال لمزيد من النقاش والتحليل في هذا السياق.[1]، ولا يلعب الدافع دورا في تحديد وجود القصد الجنائي، وعلى الرغم من أن هذه التعبيرات غالبا ما تستخدم بشكل متبادل في اللغة اليومية، إلا أن لها معانٍ مختلفة في السياق القانوني وتنتج عنها آثار قانونية مهمة، فالدافع يعرَف بأنه العامل الذي يحرك الإرادة ويوجه السلوك الإجرامي، مثل الحب أو الشفقة أو الكراهية أو الانتقام، ويلعب دورا مهما في فهم دوافع الجريمة وآثارها القانونية[2]، يعرَف الدافع بأنه قوة نفسية داخلية تدفع الإرادة نحو ارتكاب الجريمة بهدف تحقيق غاية معينة، ويتفاوت هذا الدافع من جريمة إلى أخرى، حيث يتأثر بمجموعة من العوامل الفردية مثل السن والجنس والتعليم والمستوى الاجتماعي وغيرها من المؤثرات النفسية والاجتماعية، كما يختلف الدافع

[1] محمود نجيب حسني، شرح قانون العقوبات – القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، 1989 ، ص 1052.

[2] كامل السعيد ، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، الطبعة الثانية، دار الفكر للنشر والتوزيع ، عمان، 1983، ص 226.

بالنسبة للجريمة الواحدة من شخص لآخر، مما يعكس تعقيدا في فهم الدوافع والخلفيات النفسية للأفراد الذين يرتكبون الجرائم.[1]

أما الغرض، فيقصد به الهدف المباشر والفوري للسلوك الإجرامي، ويتمثل في تحقيق النتيجة التي توجه إليها القصد الجنائي، أو في الاعتداء على الحق الذي يحميه قانون العقوبات [2] ، أما الغاية، فهي الهدف البعيد أو النهائي الذي يسعى الجاني إلى تحقيقه من خلال ارتكاب الجريمة، مثل إشباع رغبة الانتقام أو الاستيلاء على مال المجني عليه في حالة جرائم القتل.

الأصل أن الباعث والغاية لا يؤثران قانونيا على وجود القصد الجنائي، الذي يعتمد على عنصرين أساسيين: علم الجاني بعناصر الجريمة، واتجاه إرادته لتحقيق هذه العناصر أو قبولها، وبالتالي، لا يؤثر الباعث أو الغاية على قيام الجريمة أو العقاب عليها، حيث تتحقق الجريمة بمجرد اكتمال عناصرها، بغض النظر عن كون الباعث نبيلا أو دنيئا، أو كون الغاية شريفة أو غير ذلك.

ومع ذلك، قد يمنح القانون في بعض الحالات أهمية قانونية خاصة للباعث أو الغاية، مما يبرز استثناء لهذه القاعدة، [3]

تعددت الدوافع التي تدفع الجناة إلى ارتكاب مختلف أفعال الاعتداء المتعلقة بجرائم الكمبيوتر والإنترنت، ومن خلال استعراض الحالات التطبيقية، يمكن تحديد الدوافع الرئيسية التالية:

---

[1] فوزية عبد الستار، شرح قانون العقوبات – القسم العام، بدون ذكر رقم الطبعة دار النهضة العربية، القاهرة، 1992، ص79.

[2] كامل السعيد، المرجع السابق، ص 226.

[3] نجيب محمود حسني، المرجع السابق، ص 480.

أولا: السعي الى تحقيق الكسب المالي:

يعد الدافع الرئيسي لارتكاب الجرائم الإلكترونية هو السعي وراء تحقيق مكاسب مالية، حيث تشجع طبيعة هذه الجرائم وإمكانية تحقيق أرباح كبيرة من خلالها، خاصة في حالات غش الحاسوب والاحتيال الإلكتروني، على انتشارها.

ومنذ ظهور هذه الظاهرة، أكدت الدراسات أن الهدف الأساسي وراء عمليات احتيال الكمبيوتر، والتي امتدت لاحقا إلى احتيال الإنترنت، هو الربح المالي، ففي دراسة قديمة أجراها الفقيهParker ، تبين أن 43% من حالات الغش المرتبط بالحاسوب المعلن عنها كانت تهدف إلى اختلاس الأموال، وهي النسبة الأعلى مقارنة بجرائم أخرى شملتها الدراسة، مثل **سرقة المعلومات (32%)، الأفعال التخريبية (19%)، وسرقة وقت استخدام الحاسوب لأغراض شخصية (15%)**، [1]

إذا انتقلنا إلى الدراسات الحديثة، سنلاحظ أن هذا الدافع يتصدر باقي الدوافع، مما يعكس استمرارية توجه مجرمي التقنية نحو السعي لتحقيق مكاسب مادية شخصية، ومن أبرز هذه الدراسات والتقارير الإحصائية تلك الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية (NFIC).

ثانيا: الانتقام من رب العمل وإلحاق الضرر به

لقد تم ملاحظة أن العاملين في قطاع التقنية أو أولئك الذين يستخدمونها ضمن مجالات عمل أخرى، يتعرضون بشكل كبير لضغوط نفسية ناتجة عن ضغوط العمل، المشكلات المالية، وعلاقات العمل غير المستقرة أو المنفرة في بعض الحالات، هذه

[1] سامي الشوا: في الواقع فان المحرك لاقتراف فعل الغش المعلوماتي يمكن أن ينطلق من مجرد النجاة من غرق الديون المستحقة أو من المشاكل العائلية الراجعة الي النقد، أو من الخسائر الضخمة لألعاب القمار أو من ادمان المخدرات، وقد تكون جميع الوسائل مشروعة في هذه المرحلة وبالنسبة للبعض فالغاية تبرر الوسيلة

العوامل قد تدفع البعض نحو السعي لتحقيق الربح كما ذكرنا سابقا، لكنها في كثير من الأحيان تمثل دافعا رئيسيا لبعض العاملين لارتكاب جرائم الحاسوب، حيث يكون الانتقام من المؤسسة أو من رب العمل هو الباعث الأساسي.

وفي هذا السياق، تحتل أنشطة زرع الفيروسات في أنظمة الكمبيوتر مكانة بارزة كوسيلة شائعة بين فئة الأشخاص الذين تحركهم مشاعر الكراهية والانتقام ضد أصحاب العمل.

ثالثا: الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية:

يرى البعض إن الدافع لارتكاب الجرائم في الطائفة الأولى (جرائم الحاسوب) يغلب عليه الرغبة في قهر النظام أكثر من الرغبة في تحقيق الربح، ومع أن الدراسات لا تؤكد هذه الحقيقة بشكل مطلق، حيث يظهر أن السعي لتحقيق الربح يشكل دافعا أكثر تحريكا لجرائم الحاسوب مقارنة بالرغبة في قهر النظام، إلا أن هذا الأخير يظل الدافع الأبرز في نسبة معتبرة من جرائم الحاسوب، خاصة تلك المرتبطة بأنشطة المتطفلين الدخلاء (Hackers)، [1] تتجسد هذه الجرائم في أفعال مثل التوصل إلى أنظمة الحاسوب عن بعد، الاستخدام غير المصرح به لنظام الحاسوب، واختراق مواقع الإنترنت، ويميل مرتكبو هذه الجرائم إلى إظهار تفوقهم وبراعتهم العالية، لدرجة أنه مع كل تقنية جديدة، يشعرون بشغف كبير تجاهها ويحاولون إيجاد طرق لتحطيمها أو التفوق عليها، ويبدو هذا الدافع أكثر شيوعا بين فئة صغار السن من مرتكبي جرائم الحاسوب، الذين يمضون وقتا طويلا أمام حواسيبهم الشخصية في محاولات مستمرة للتغلب على حواجز الأمان الخاصة بأنظمة الحواسيب.

[1] حسب ترجمة غرفة التجارة العربية البريطانية، والحاذق المأجور حسب ترجمة أستاذنا كامل السعيد.

ويتمثل هذا الدافع أيضا في الرغبة في إظهار التفوق على وسائل التقنية، خاصة في مجال شبكات المعلومات، وقد استعرضنا في الفصول السابقة العديد من الأمثلة الواقعية التي تظهر هذا النوع من الدوافع، ويمكن التأكيد هنا على أن هذا الدافع هو الأكثر شيوعا في استخدامه من قبل المنظمات الإجرامية، مثل مجموعات الجريمة المنظمة، حيث يتم استغلاله لاستدراج المحترفين في مجال الاختراق للمشاركة في أنشطة اعتداء معقدة أو لتوظيفهم في تنفيذ الجرائم، مما يعزز قدرات هذه المنظمات في تنفيذ أنشطتها الإجرامية.

خلاصة الفصل:

تناول هذا الفصل الإطار المفاهيمي للجريمة الإلكترونية بتحليل شامل لماهيتها وأركانها ودوافع ارتكابها، من خلال دراسة التعريفات المختلفة للجريمة الإلكترونية، تبين أنها تتميز بمجموعة من الخصائص الفريدة التي تميزها عن الجرائم التقليدية، كطبيعتها العابرة للحدود، وصعوبة اكتشافها وإثباتها، واعتمادها على المهارات التقنية المتقدمة، كما أظهرت الدراسة تنوع الجرائم الإلكترونية بين تلك التي تقع بواسطة النظام الالكتروني كوسيلة لارتكاب الجريمة، وتلك التي تستهدف النظام الالكتروني ذاته، هذا التنوع يعكس تعقيد الظاهرة الإجرامية في البيئة الرقمية وتشعب أساليبها.

أما فيما يتعلق بأركان الجريمة الإلكترونية، فقد تم تحليل الركن الشرعي الذي يواجه تحديات التكييف القانوني، والركن المادي بعناصره، إضافة إلى الركن المعنوي.

وفي سياق البحث في مرتكبي الجريمة الإلكترونية، تم تحديد فئات متنوعة من المجرمين الإلكترونيين تختلف بحسب خبراتهم ومهاراتهم وأهدافهم، كما تم استعراض الدوافع المتعددة وراء ارتكاب هذه الجرائم.

الفصل الثاني: الملاحقة والتحقيق في الجرائم الإلكترونية

تمهيد:

إن تطور تكنولوجيات الإعلام والاتصال لم يقتصر على تغيير أنماط الحياة فحسب، بل أدى أيضا إلى بروز أنماط جديدة من الإجرام، باتت تشكل تحديا حقيقيا للأنظمة القانونية والأمنية في مختلف دول العالم، ومنها الجزائر. فالجرائم الإلكترونية ترتكب غالبا عبر الفضاء الافتراضي، ما يجعل كشفها والتحقيق فيها يخرج عن الأطر التقليدية المعروفة في الجرائم الكلاسيكية، ويستدعي تكيفا مؤسساتيا وتشريعيا يتماشى مع طبيعتها المعقدة وسرعة تنفيذها وطابعها العابر للحدود.

وبناء على ذلك، فقد أصبح من الضروري تسليط الضوء على مختلف الآليات التي تعتمدها الدولة لملاحقة هذا النوع من الإجرام، بدءا بالوحدات المختصة التي تعهد إليها مهام البحث والتحري، سواء كانت هيئات إدارية مثل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أو أجهزة أمنية تابعة للشرطة والدرك الوطني، مرورا بالإجراءات القانونية والفنية المعتمدة في عملية التحري والكشف، كالإجراءات المادية والخبرة التقنية، وصولا إلى الوسائل القانونية لإثبات الجريمة وتحديد المسؤولية، سواء تعلق الأمر بالأشخاص أو بالأموال المتحصلة من النشاط الإجرامي. ومن هذا المنطلق، سنعالج في هذا الفصل محورين أساسيين: نخصص أولهما لدراسة الجهات المختصة بملاحقة الجرائم الإلكترونية، بينما نفرد المبحث الثاني للوقوف على الإجراءات القانونية المعتمدة في الكشف عن هذا النوع من الجرائم.

المبحث الأول: الوحدات المختصة التي تتولى اجراءات البحث والتحقيق في الجريمة المعلوماتية

لمواجهة الجريمة المعلوماتية، كان من الضروري إنشاء وحدات متخصصة تمتلك الكفاءة التقنية والقانونية اللازمة للتحري والتحقيق في هذا النوع من الجرائم. وتتمثل أبرز هذه الوحدات في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التي تتميز ببنية تنظيمية محددة واختصاصات متعددة، إلى جانب الأجهزة الأمنية، سواء تلك التابعة للأمن الوطني أو للدرك الوطني، التي تلعب دورا ميدانيا فعالا في التصدي لهذه الجرائم.

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعالم والاتصال

حرص المشرع الجزائري على معرفة المزيد عن الأحداث العالمية في مجال مكافحة الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات ، أنشأ المكتب الوطني لمنع الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات.

الفرع الأول: تشكيلة الهيئة

لكي تقوم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بدورها على أكمل وجه وتحقق الفعالية المطلوبة[1]، لابد أن تتكون من جهاز إداري تنفيذي وهذا فمن أجل نجاعة وفعالية الهيئة الوطنية في أداء الاختصاصات المنوطة بها، حيث منحها القانون مجموعة من الوسائل القانونية التي تضمن تأدية مهامها، حيث نص المشرع

[1] المادة 04 من المرسوم الرئاسي رقم 19-172، مؤرخ في 14 جوان 2019، يتعلق بالسلطات الإدارية المستقلة.

بأن الهيئة تتكون من مجلس توجيه ومديرية عامة [1]، حيث يرأس مجلس التوجيه وزير الدفاع الوطني أو ممثله وتتشكل من الوزارات الآتية :

- وزارة الدفاع الوطني.
- وزارة العدل.
- الوزارة المكلفة بالداخلية.
- الوزارة المكلفة بالمواصلات السلكية واللاسلكية. [2]

غير أنه وما يجب التأكيد عليه أن مثل هذه الهيئات لا تعمل بمعزل عن الأهداف الحكومية الكبرى أو خارج السياسة العامة للدولة [3]، لأن الهدف من إنشائها هو تحقيق سياسة الدولة في المجالات المعنية لذلك، ومن أجل إنجاح هذه المهمة تعمد الدولة إلى منح هذه الهيئات نوعا من الاستقلالية كقوة دفع لها، بغية إتاحة الفرصة لها للعمل بنجاعة .

الفرع الثاني: مهام الهيئة:

تزود الهيئة بأمانة عامة توضع تحت سلطة وزارة الدفاع الوطني [4]، ويكلف مجلس التوجيه على الخصوص بما يأتي:

التداول حول استراتيجية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[1] المادة 04 من المرسوم الرئاسي رقم 19-172، مؤرخ في 14 جوان 2019، يتعلق بالسلطات الإدارية المستقلة.

[2] المادة 05 من المرسوم الرئاسي رقم 19-172، مؤرخ في 14 جوان 2019، يتعلق بالسلطات الإدارية المستقلة.

[3] حنفي عبد الله حنفي عبد الله السلطات الإدارية المستقلة، دراسة مقارنة دار النهضة العربية، القاهرة، مصر، 2000، 09 ص

[4] المادة 7/01 المرسوم الرئاسي رقم 19-172، مؤرخ في 14 جوان 2019، يتعلق بالسلطات الإدارية المستقلة.

التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة[1].

اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- الموافقة على عمل الهيئة.
- دراسة التقرير السنوي للهيئة
- إبداء رأيه في كل مسألة تتصل بمهام الهيئة .
- المساهمة في ضبط المعايير القانونية في مجال اختصاصه.
- دراسة مشروع الهيئة.

وقد نص المشرع على أن سير مجلس التوجيه تحدد بموجب قرار من وزير الدفاع. [2]

وهذا يدل على شيء واحد وهو سيطرة وزير الدفاع على الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حتى وبالتالي تبعية هذه الهيئة لوزارة الدفاع فلا يمكن القول باستقلاليتها. والمقصود بالاستقلالية بأنها عدم خضوع تلك السلطة الإدارية المستقلة لأية رقابة سلمية ولا لرقابة الوصاية، سواء كانت السلطة المعنية تتمتع

[1] المادة 06 من المرسوم الرئاسي رقم 19-172، مؤرخ في 14 جوان 2019، يتعلق بالسلطات الإدارية المستقلة.

[2] المادة 07 من المرسوم الرئاسي رقم 19-172، مؤرخ في 14 جوان 2019، يتعلق بالسلطات الإدارية المستقلة.

بالشخصية المعنوية أو لا تتمتع بها على أساس أن الشخصية المعنوية لا تعد معيارا أو عاملا فعالا لقياس درجة الاستقلالية.[1]

المطلب الثاني: اختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إن التطور التقني في العصر الحالي أدى إلى تغير كبير إن لم يكن جذريا في المفاهيم السائدة حول الدليل، ويقود مثل هذا القول إلى إعلان انضمام الخبرة التقنية إلى عالم الخبرة المتميز بتصنيف التعامل مع موضوع الدعوى من حيث ضرورة الاستعانة بالمتخصص في مجال النزاع وبالضرورة، فإن ذلك لا بد أن ينعكس على آليات تتلاءم اختصاصاتها في البحث والتحري عن هذه الأدلة، وتتولى مهمة الخبرة التقنية، وفي سياق ذلك تم استحداث الهيئة محل الدراسة وتمكينها من اختصاصات دقيقة يخولها احتلال مكانة الخبير العلمي والفني بما تتمتع به من مقومات في مجال الأمن الإلكتروني[12].

الفرع الأول: اختصاصات مجلس التوجيه:

يجتمع مجلس التوجيه في دورة عادية مرتين في السنة بناء على استدعاء من رئيسه ويمكنه أن يجتمع في دورة غير عادية كلما كان ضروريا بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أومن المدير العام للهيئة[13].

يكلف مجلس التوجيه على الخصوص بما يلي: [14]

-التداول حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

---

[1] ZOUAIMIA Rachid, Les autorités administratives indépendantes et la régulation économique en Algérie, édition distribution HOUMA, Alger, 2005,p25…

-التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

-القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين المراقبة الواجب القيام بها والأهداف المنشودة بدقة،

-اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

- الموافقة على برنامج عمل الهيئة،

- إعداد نظامه الداخلي والمصادقة عليه أثناء أول اجتماع له،

-دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه،

- إبداء رأيه في كل مسألة تتصل بمهام الهيئة،

- تقديم كل اقتراح يتصل بمجال اختصاص الهيئة،

- المساهمة في ضبط المعايير القانونية في مجال اختصاصه،

-دراسة مشروع ميزانية الهيئة والموافقة عليه.

الفرع الثاني: اختصاصات المديرية العامة:

يدير المديرية العامة مدير عام، وتتولى على الخصوص الصلاحيات الآتية[15]:

-السهر على حسن سير الهيئة،

- إعداد مشروع ميزانية الهيئة،

- إعداد وتنفيذ برنامج عمل الهيئة،

- تنشيط وتنسيق ومتابعة ومراقبة أنشطة هياكل الهيئة،

[1] القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، صادرة بتاريخ 2009/08/16.

تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

-تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم،

- تحضير اجتماعات مجلس التوجيه،

-إعداد التقرير السنوي لنشاطات الهيئة.

المدير العام هو الآمر بصرف ميزانية الهيئة، ويعين المدير العام، الآمر بصرف ميزانية هذه الأخيرة ،وكذا مستخدموها طبقا للتنظيم المعمول به في وزارة الدفاع الوطني، كما يعاد إدماج القضاة والمستخدمين التابعين للدوائر الوزارية الأخرى العاملين بالهيئة في هياكلهم الأصلية.

وتضم المديرية العامة مديرية تقنية تتكفل على وجه الخصوص بمهمة المراقبة الوقائية للاتصالات الالكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة إضافة إلى مساعدة السلطات القضائية ومصالح الشرطة، بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتلك التي تتطلب اللجوء إلى أساليب التحري للهيئة.[1]

وإلى جانب هذا، تضم المديرية العامة مديرية للإدارة والوسائل، توكل لها مهمة تسيير الموارد البشرية والوسائل المالية الخاصة بالهيئة، الإسناد التمويني والتقني، صيانة العتاد والوسائل والمنشآت القاعدية وكذا إعداد احتياجات الهيئة في إطار تحضير تقديرات الميزانية.

[1] المادة 12 من القانون رقم 18-04 المؤرخ في 10 مايو 2018، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 27، ص 11

وتفصل المادة 16 من المرسوم في الأحكام المالية المتعلقة بالهيئة سيما الإعانات التي تمنحها الدولة، عائدات كل النشاطات المرتبطة بموضوعها، نفقات التسيير والتجهيز.

و عليه، أمكن القول أن المهام العامة للهيئة تتنوع بين ٍ كونها هيئة استشارية، وهيئة تحري، ومرصد لجمع وتسجيل وحفظ المعطيات الرقمية، وهي مساعدة للضبط القضائي ولجهاز القضاء، بالإضافة إلى أنها، هيئة تكوين للمحققين في مجال الأمن الإلكتروني، حيث أنه بمقتضى المادة14من القانون04/09المؤرخ في05أوت2009المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها، أوكل المشرع لهذه الهيئة مهمتان رئيسيتان تتمثلان فيما يلي[1]:

1) ا لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إنَ إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الالكترونية، التلاعب بحسابات العملاء أو ببطاقات ائتمانهم، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية[19].إلخ.

2) مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

بحسب نص المادة 14 من القانون 04/09 ،هناك نوعان من المكافحة تقوم بهما هذه الهيئة:

[1] القانون رقم 09–04 المؤرخ في 5 أغسطس 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، صادرة بتاريخ 2009/08/16.

في مجال التدخل مع السلطات المختصة

-مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وا نجاز الخبرات القضائية المادة 14 فقرة ب من القانون 04/09 السالف الذكر،

-تنشيط وتنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين والمشتركين في ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

-القيام بإذن من السلطات القضائية بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة مصالح الشرطة القضائية المختصة بالتحقيقات في جرائم خاصة ارتكبت أو سهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال، ولكن دون المساس باختصاص باقي الهيئات الوطنية المختصة بمكافحة جرائم معينة نص عليها القانون،

-تقديم المساعدة لمصالح الأمن والدرك الوطنيين، ولجميع إدارات ومصالح الدولة المركزية (المديريات العامة المختلفة) فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح،

,-التدخل من تلقاء نفسها بعد موافقة السلطات القضائية المسبقة (المادة 4 فقرة 2 من القانون 04/09) في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به[1]،

-من أجل القيام بمهامها فلها تركيز، تحليل، استقراء كل المعلومات المتعلقة بأفعال أو جرائم متصلة بتكنولوجيات الإعلام والاتصال، والاتصال بكل من مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة)، وكذلك كل الإدارات والمصالح العامة للدولة المعنية للقيام بمهامها.

[1] القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، صادرة بتاريخ 2009/08/16.

– يحب على مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة) في أقرب الآجال إخطار الهيئة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال فيما تسمح به القوانين– وخاصة منها ما يتعلق بالسر المهني– بما كشفته أو وصل إلى علمها من جرائم متصلة بتكنولوجيات الإعلام والاتصال.

في مجال تحري المعلومة

– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم: في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية، ومن ثم تشاركها مع المنظمات المماثلة لها على مستوى الدول، بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم.

هذا وتمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني، وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من معالجة أكثر من 1000 جريمة الكترونية منها 30 بالمائة على مواقع التواصل الاجتماعي، هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016 وجود 11 قضية متعلقة بالإرهاب الالكتروني، أغلبها خاصة بتهديدات إرهابية باسم تنظيم داعش الإرهابي،لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخص متورط في قضايا إرهاب الكتروني تمت إحالتهم على القضاء.

هذا وقد استطاع الجيش الالكتروني الجزائري من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق وسوريا وليبيا، كما تمكن من فك

شفرات الرسائل المتبادلة، وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجنيده عبر مواقع الانترنت ومنصات التواصل الاجتماعي خاصة الفيس بوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة، وتلقيها معلومات تفيد بوجود منشورات إرهابية تدعو للمشاركة في منتديات إرهابية إلى جانب اتصالات محلية ودولية.

وررغم كل الجهود المبذولة من قبل هذه الهيئة لكبح الجريمة المعلوماتية، إلا أن النتائج الملموسة في الميدان تبقى ضعيفة، لذلك أوعز الخبراء قرار الحكومة بسحب هذه الهيئة من وصاية وزارة العدل وإلحاقها بوزارة الدفاع الوطني بعد ثلاث سنوات من تنصيبها إلى فشل هذه الأخيرة في محاربة الجريمة الالكترونية واختراق الأنظمة المعلوماتية للقطاعات الحساسة، كما أن تغيير إدارة هذه الهيئة قد يعود إلى كون وزارة الدفاع الوطني تحوز على تجهيزات جد متطورة في مجال مكافحة الجوسسة والتصنت لاسيما بعدما استرجعت الضبطية القضائية، ولها أجهزة متقدمة في التحقيقات لاسيما الدرك الوطني وجهاز الاستخبارات.

و عليه، نأمل أن تكون المردودية أكبر لهذه الهيئة بعد إلحاقها بوزارة الدفاع الوطني، وعلى القضاء الجزائري متابعة الأشخاص المتورطين في مثل هذه الجرائم، وتكتفي الهيئة تحت وصاية الدفاع الوطني بتقديم مساهماتها التقنية في كشفهم.

المطلب الثاني: الأجهزة الأمنية

لقد عملت كل من المديرية العامة للأمن الوطني وقوات الدرك الوطني على تعزيز قدراتها لمكافحة الجرائم الحديثة، خاصة الجرائم المعلوماتية، ومن ضمنها الجرائم المرتبطة باستخدام الذكاء الاصطناعي. وفي هذا الإطار، تم إنشاء وحدات متخصصة ومراكز بحثية مكلفة بالتحقيق في هذه النوعية من الجرائم، كما تم تكوين كوادر بشرية مؤهلة للعمل في هذا المجال، سواء على المستوى الداخلي أو الخارجي.

كما يمتلك الجهازان مختبرات علمية متخصصة في الشرطة التقنية والعلمية، مزوَدة بأحدث التكنولوجيا المتقدمة التي تمكن من كشف وتحليل هذا النوع من الجرائم الرقمية. [1]

الفرع الأول: الوحدات التابعة لسلك الأمن الوطني

ضمن إطار وضع سياسة أمنية شاملة وفعالة، تسخِر المديرية العامة للأمن الوطني جميع الإمكانيات البشرية والتقنية المتاحة لديها لمواجهة مختلف أنواع الجرائم، وبخاصة الجرائم الحديثة مثل جرائم الذكاء الاصطناعي. وتأتي هذه الجهود استجابة للتحديات الناتجة عن التأخر المسجل على المستوى الوطني في مجال تكنولوجيا الإعلام والاتصال، خاصة فيما يتعلق بتطبيقات الذكاء الاصطناعي، وذلك بهدف حماية المصلحة العامة، بالإضافة إلى المصالح الخاصة المرتبطة باستخدام هذه التكنولوجيات. [2]

الوحدات المكلفة بالبحث والتحقيق في الجرائم المعلوماتية تنقسم إلى:

- المخبر المركزي للشرطة العلمية والتقنية الواقع بمدينة الجزائر العاصمة.
- المخبر الجهوي للشرطة العلمية والتقنية بولاية قسنطينة.
- المخبر الجهوي للشرطة العلمية والتقنية بولاية وهران.

وبهدف تعزيز قدرات الشرطة القضائية على المستوى المحلي، أقدمت المديرية العامة للأمن الوطني سنة 2010 على إنشاء ما يقارب 23 خلية متخصصة في مكافحة الجرائم المعلوماتية عبر ولايات الوطن (في المناطق الوسطى والشرقية والغربية والجنوبية)، ثم

[1] محمد السعيد زناتي،الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية،مجلة إليزا للبحوث والدراسات،المركز الجامعي إليزي، العدد الثاني،ديسمبر2017، ص34–35.

[2] سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري،مجلة العلوم الانسانية،كلية الحقوق جامعة الاخوة منتوري، قسنطينة،المجلد ب، عدد52، ديسمبر2019،ص53.

امتدت هذه الخلايا لتشمل كافة الولايات والمصالح الأمنية المنتشرة عبر التراب الوطني لاحقا.[1]

الفرع الثاني: الوحدات التابعة للقيادة العامة للدرك الوطني.

في إطار تنفيذ مهامه المتعلقة بالحفاظ على الأمن الوطني، وصون النظام العام، ومكافحة مختلف أشكال الجريمة، يتوفر جهاز الدرك الوطني على مجموعة متنوعة من الوحدات المنتشرة على مستوى القيادة العامة، وكذا على مستوى القيادات الجهوية والمحلية. ومن بين هذه الوحدات نذكر على وجه الخصوص:

- المصالح والمراكز العلمية والتقنية.
- هياكل التكوين.
- المصلحة المركزية للتحريات الجنائية.
- المعهد الوطني لعلم الجرائم.[2]

ويعد المعهد الوطني للأدلة الجنائية وعلم الإجرام الواقع ببوشاوي، والتابع للقيادة العلمية للدرك الوطني، من أبرز المراكز المتخصصة، حيث يضم قسما للإعلام والإلكترونيك يعنى بالتحقيق في الجرائم الإلكترونية، بما في ذلك الجرائم المرتبطة بالذكاء الاصطناعي. ويتولى هذا القسم مهام تحليل الأدلة الرقمية، بما يشمل تحليل الوسائط الإلكترونية، والتقاطع الهاتفي، وتحسين جودة التسجيلات الصوتية والمرئية والصور، بهدف تيسير استخدامها في مجريات التحقيق.

---

[1] سعيدة بوزنون ، المرجع نفسه، ص54.

[2] وشن لبني،نباش مراد،دور رجال الضبطية القضائية في مكافحة الجريمة الالكترونية،مذكرة تخرج لنيل شهادة الماستر،تخصص قانون إعلام آلي والانترنت،كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي،2022/2021،ص59.

إضافة إلى ذلك، يجري العمل على إنشاء مركز متخصص في مكافحة جرائم الإعلام الآلي والجرائم المعلوماتية ببئر مراد رايس، وهو تابع لمديرية الأمن العمومي للدرك الوطني. وتكمن المهمة الأساسية لهذا المركز في دعم العدالة وتعزيز قدرات وحدات التحري، ضمن إطار مهام الشرطة القضائية، لا سيما في مجال مكافحة الجرائم الإلكترونية وجرائم الذكاء الاصطناعي. كما يضم هذا المركز قسما خاصا بالإعلام الآلي والإلكترونيك، مكلفا بالتحقيق الفني في هذا النوع من الجرائم.[1]

*المرسوم الرئاسي رقم 15–261 المؤرخ في 8 أكتوبر 2015، المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال،الجريدة الرسمية للجمهورية الجزائرية العدد 53الصادرة في 8–10–2015.

[1]. يوسف جفال،التحقيق في الجريمة الالكترونية، مذكرة مقدمة لنيل شهادة الماستر،كلية الحقوق جامعة محمد بوضياف، لمسيلة،2017/2016،ص20.

المبحث الثاني: الاجراءات القانونية للكشف عن الجرائم المعلوماتية

إن خصوصية الجريمة المعلوماتية تفرض اتباع إجراءات قانونية وتقنية دقيقة للكشف عنها، تختلف في كثير من جوانبها عن تلك المعتمدة في الجرائم التقليدية. وتشمل هذه الإجراءات وسائل التحري الكلاسيكية، كالضبط والمعاينة والخبرة التقنية، إلى جانب قواعد الإثبات والمتابعة الجنائية التي تراعي طبيعة هذا النوع من الإجرام، سواء تعلق الأمر بالأشخاص أو بالأموال المتحصلة منه.

المطلب الأول: اجراءات التحري الكالسيكية للكشف عن الجريمة المعلوماتية

رغم الطبيعة المستحدثة للجريمة المعلوماتية، فإن التحري بشأنها لا يستغني عن بعض الإجراءات الكلاسيكية المعروفة في قانون الإجراءات الجزائية. وتشمل هذه الإجراءات الوسائل المادية المعتمدة في البحث والتتبع، إلى جانب الاستعانة بالخبرة التقنية لفهم الجوانب الفنية المرتبطة بالجريمة، مما يسمح بتكييف الأدلة وفقا للقانون وتحقيق الفعالية في ملاحقة الجناة.

الفرع الأول: الاجراءات المادية لمواجهة الجريمة المعلوماتية

تشكل الإجراءات المادية أولى خطوات التحري في الجريمة المعلوماتية، حيث تهدف إلى جمع الأدلة من مسرح الجريمة الرقمية، وضبط الأجهزة والوسائط المستخدمة، وتتبع الآثار التقنية التي يتركها الجاني. ورغم اختلاف البيئة التي ترتكب فيها هذه الجرائم، إلا أن المبادئ العامة في التحري الميداني تظل حاضرة، مع ضرورة التكيف مع طبيعة الفضاء السيبراني.

أولا: التفتيش وضبط الأدلة

1- تفتيش المنظومات المعلوماتية

يعد التفتيش في قضايا الجرائم المعلوماتية من أصعب أنواع التفتيش، وذلك نظرا للتطور التكنولوجي المتسارع الذي يشهده مجال الاتصالات وتكنولوجيا المعلومات.

1.مفهوم التفتيش

يمكن تعريف التفتيش بأنه إجراء من إجراءات التحقيق تنفَذ بواسطة جهة تحددها القوانين النافذة، ويهدف إلى البحث والتحري عن الأدلة المادية المتعلقة بجناية أو جنحة، وذلك داخل مكان خاص يتمتع بحماية قانونية، وبغض النظر عن رغبة مالكه أو مستخدمه. [1]

ويرى بعض الفقه أن التفتيش يعد من الإجراءات التحقيقية التي يقوم بها موظف مختص وفقا للإجراءات المنصوص عليها قانونا، داخل مكان يخضع لحرمة قانونية، بهدف العثور على أدلة مادية تثبت وقوع الجريمة ونسبتها إلى المتهم.

ويتميز هذا الإجراء بأهميته الكبيرة، حيث يرتبط مباشرة بحقوق الأفراد الأساسية، خاصة الحق في الخصوصية، ولذلك تم حمايته بعدة ضمانات قانونية. [2]

كما يعرفه البعض على أنه وسيلة فعالة من وسائل جمع الأدلة – سواء كانت مادية أو معنوية – في موقع الجريمة أو خارجه، ويهدف إلى كشف الحقيقة وتوثيقها عبر جمع

[1] سامي حسني الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة، 1972، ص36.

[2] عوض محمد عوض، قانون الإجراءات الجنائية، ج1، مؤسسة الثقافة الجامعية، 1989، ص475.

الدلائل المؤدية إلى إثبات ارتكاب الجريمة وتحديد مرتكبيها، إذ لا يمكن الحديث عن إدانة أو توقيع عقوبة دون وجود دليل قاطع. [1]

2 .شروط التفتيش في الأنظمة المعلوماتية

تنقسم الشروط التي يجب توافرها عند إجراء التفتيش في المجال المعلوماتي إلى نوعين :شروط شكلية وشروط موضوعية ، وهي تتمثل فيما يلي: [2]

أ- الشروط الشكلية:

•توقيت إجراء التفتيش:

في حالة الأنظمة الآلية للمعطيات (أنظمة المعالجة الإلكترونية)، يجوز القيام بإجراءات التفتيش والمعاينة والحجز في أي مكان، سواء كان سكنيا أم غير سكني، وفي أي ساعة من ساعات النهار أو الليل، شريطة الحصول مسبقا على إذن قضائي من وكيل الجمهورية المختص إقليميا.

حضور الأشخاص المعنيين أثناء التفتيش:

نص المشرع الجزائري صراحة على ضرورة حضور المتهم أثناء تفتيش المنزل، ويعد هذا الحضور من الضمانات الجوهرية لحماية حقوقه أثناء سير الإجراءات. وفي حال تعذر حضور المتهم لأي سبب من الأسباب، يتوجب على ضابط الشرطة القضائية أن يطلب منه تعيين ممثل ينوب عنه. أما إذا امتنع المتهم عن ذلك أو كان في حالة فرار،

[1] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد05، جوان 2012، ص162.

[2] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد04، جانفي 2018، ص57-58.

فتلزم الإجراءات بحضور شاهدين لا تربطهما أي علاقة وظيفية بضابط الشرطة القضائية القائم بالتفتيش، لضمان شفافية العملية.

أ– محضر التفتيش في الجرائم المتعلقة بالمعطيات الآلي:

تعد محاضر الشرطة القضائية، والتي يطلق عليها محاضر البحث الابتدائي، من أهم وسائل الإثبات في الجريمة، نظرا لما تتمتع به من قوة قانونية في تأكيد وقوع الجريمة ونسبتها إلى الفاعل. كما تكتسب هذه المحاضر أهمية خاصة لما تمنحه من صلاحيات واسعة لضابط الشرطة القضائية في إطار تنفيذ إجراءات التحقيق.

ب– الشروط الموضوعية للتفتيش: [1]

- **سبب التفتيش :**يرتبط التفتيش بوقوع جريمة معلوماتية، ويشكل ذلك الدافع الأساسي المباشر لتنفيذ الإجراء.

- **محل التفتيش :**في الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال، يعتبر الحاسوب أو أي وسيلة إلكترونية مماثلة هو محل التفتيش الرئيس، باعتباره الأداة التي تستخدم في ارتكاب الجريمة، والوسيلة التي تمكن من الاتصال بالعالم الخارجي.

- **الجهة المخولة بالتفتيش :**تخول مهمة التفتيش في الأصل إلى النيابة العامة أو قاضي التحقيق بحسب مقتضيات القانون. وقد تسند هذه الصلاحية استثنائيا إلى ضباط الشرطة القضائية في حالات معينة. أما في حال وقوع جريمة من صنف الجنايات أو الجنح، وكان قاضي التحقيق المختص غير متوفر في حينه، فإن الجهة المكلفة بالتحقيق تتولى اتخاذ الإجراء الفوري اللازم، ويعرض الأمر لاحقا على أقرب قاضٍ مختص ضمن دائرة

[1] عز الدين عثماني، مرجع سابق، ص58–59.

الاختصاص أو من دائرة مجاورة، مع وجوب إحالة الملف إلى قاضي التحقيق المختص في أقرب وقت ممكن لاستكمال الإجراءات.

2- ضبط الأدلة في الجريمة الإلكترونية

يعد الضبط من الإجراءات الأساسية في جمع الأدلة الجنائية، وهو النتيجة التي تنتهي إليها عملية التفتيش. ويتمثل الضبط في وضع اليد على الأشياء أو الوسائل التي استخدمت في ارتكاب الجريمة ، والتي يمكن أن تسهم في كشف الحقيقة وتقديمها أمام القضاء كأدلة إثبات. [1]

وفي هذا السياق، قد تكون المضبوطات ذات طبيعة مادية ، أي مرئية وملموسة، مثل: أجهزة الحاسوب وأجزاؤها (الأقراص الصلبة، الطابعات)، أو الأشرطة المغناطيسية، وبطاقات الدفع الإلكتروني، والمعدات المستخدمة في شبكات الإنترنت مثل المودم.

كما يمكن أن تتخذ المضبوطات طبيعة غير مادية ، أي معنوية، مثل البيانات الرقمية والبرمجيات المعالجة آليا، والمراسلات الإلكترونية، ورسائل البريد الإلكتروني،[2] وغيرها من المعلومات الرقمية التي تحمل دلالة على ارتكاب الجريمة.

وعليه، وفي حال تم العثور على دليل رقمي خلال التحقيق، فإن الإجراء التالي الذي يجب اتخاذه هو الحجز ، وقد نص المشرع الجزائري على ذلك صراحة في المادة 06 من القانون رقم 09/04 المؤرخ في 15 يوليو 2004، المتضمن للإجراءات المتعلقة بالتفتيش والحجز في المنظومات المعلوماتية.

---

[1] خالد عياد الحلبي، ، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، دار الثقافة للنشر والتوزيع، عمان،2011، ص169.

[2] جمال نجيمي، ، إثبات الجريمة علي ضوء الإجتهاد دراسة مقارنة، دار هومة، الجزائر، 2011، ص46.

وتشير هذه المادة إلى أنه:

عندما تكتشف الجهة المختصة أثناء عملية تفتيش في منظومة معلوماتية بيانات مخزنة تعتبر ذات فائدة في الكشف عن الجريمة أو مرتكبيها، فإنه ليس من الضروري حجز المنظومة بأكملها ، بل يكتفى بنسخ البيانات محل البحث، بالإضافة إلى البيانات اللازمة لفهمها، على وسيلة تخزين إلكترونية قابلة للحجز، وتوضع ضمن أحراز رسمية.

كما يؤكد القانون على أن الجهة التي تقوم بالتفتيش والحجز ملزمة بضمان سلامة البيانات داخل المنظومة المعلوماتية التي يتم التعامل معها، وذلك طوال مدة إجراء العملية.

وفي حالة كانت هناك صعوبات تقنية تمنع القيام بالحجز الفعلي ، يتعين على الجهة المختصة استخدام تقنيات مناسبة لمنع الوصول إلى تلك البيانات أو إلى نسخها الاحتياطية، حتى لا تتعرض للتغيير أو الاستخدام غير المشروع.

أما إذا كانت البيانات المضبوطة تحتوي على معلومات يشكل محتواها جريمة ، فإن القانون يمنح الجهة المكلفة بالتحقيق الحق في اتخاذ جميع الإجراءات الضرورية لمنع الإطلاع عليها من طرف الغير .

وأخيرا، سواء كانت البيانات محل شك أو كان محتواها مجرما، فلا يجوز استعمالها لأي غرض آخر غير التحري أو التحقيق أو العمل القضائي ، وإلا عرض الشخص المسؤول للمساءلة الجنائية.

ثانيا: المعاينة الالكترونية.

يعد مكان ارتكاب الجريمة هو الإطار الأساسي الذي يحتوي على أبرز الأدلة الجنائية، إذ يخلف الجاني في أعقاب ارتكابه الفعل الإجرامي آثارا مادية قد تشي به، خاصة في لحظة يكون فيها تحت تأثير اضطراب نفسي وعصبي شديد، ما يمنعه غالبا من

التفكير المنظم أو التخلص من تلك الآثار. ومن ثم، لا يكاد يوجد مجرم، مهما بلغت دقته وحنكته، إلا ويترك خلفه ما قد يدل على هويته. [1]

لذا، يصبح من واجب ضابط الشرطة القضائية الانتقال الفوري إلى مسرح الجريمة لمعاينة الموقع وتوثيق حالته المادية والأشخاص والأشياء المرتبطة به، والعمل على حفظ الأدلة التي قد تساعد في كشف الحقيقة. ويجب عليه كذلك إشعار النيابة العامة فورا، خصوصا في حالات الجنايات المتلبس بها، لتنتقل بدورها إلى مكان الجريمة لمباشرة إجراءاتها.

والمقصود بالمعاينة هو الاطلاع المباشر بالعين على مكان أو شخص أو شيء معين بغرض إثبات حالته الراهنة وضبط ما يفيد في التحقيق. وتكمن أهمية هذه المعاينة في أنها تمثل الخطوة الأولى في سلسلة إجراءات الاستدلال، حيث يتم من خلالها جمع الأدلة والقرائن، وتكوين تصور أولي حول ظروف وملابسات الجريمة. [2]

وتزداد أهمية المعاينة كونها تقدم لجهات التحقيق والمحاكمة صورة واضحة وشاملة عن مسرح الجريمة، من حيث تفاصيله المكانية والفيزيائية، وما يحتويه من آثار مادية، مما يسهم في تكوين تصور موضوعي عن كيفية وقوع الجريمة واستنباط الأدلة من الوقائع المثبتة. [3]

---

[1] نبيه صالح ،.الوسيط في شرح مبادئ الاجراءات الجزائية.د ط.منشاة المعارف القانونية للنشر، عمان، ص .30.

[2] عبد العال الديري ومحمد صادق اسماعيل، .الجرائم الالكترونية.ط .01 ،المركز القومي للإصدارات القانونية،:القاهرة، 2012.ص 264.

[3] نبيه صالح ،.الوسيط في شرح مبادئ الاجراءات الجزائية، ص 31.

وفي سبيل ضمان سلامة المعاينة وصدقيتها، نصت بعض التشريعات الجنائية على معاقبة كل من يعبث بمسرح الجريمة أو يجري تغييرات على حالته قبل وصول السلطات المختصة بالتحقيق أو الاستدلال، بصرف النظر عن هوية من قام بذلك. [1]

أما في الجرائم المعلوماتية، فإن المعاينة تتم على مستويين:

1 -المسرح التقليدي:

وهو الموقع المادي خارج بيئة الحاسوب، ويشمل جميع **المكونات الفيزيائية** المرتبطة بالجريمة، مثل وحدات الحفظ (الأشرطة والأقراص)، الكابلات، شاشة العرض، لوحة المفاتيح، ومفاتيح التشغيل وغيرها من المعدات التقنية. ويعد هذا المستوى قريبا من مسرح الجريمة التقليدية، إلا أنه يرتبط هنا بأجهزة تكنولوجية تشكل جسد الجريمة الإلكترونية. [2]

لا توجد أي صعوبة مادية في تحديد صلاحية مسرح الجريمة ومعاينته من قبل ضباط الشرطة العلمية، حيث يمكنهم التحفظ على الأدلة المادية التي تثبت وقوع الجريمة وربطها بشخص معين. وتشمل هذه الإجراءات وضع الأختام في الأماكن التي تم فحصها، إلى جانب ضبط كافة الأدوات والوسائل التي استخدمت في ارتكاب الجريمة، مع ضرورة إبلاغ النيابة العامة بذلك لضمان سير التحقيق وفق الأطر القانونية.

[1] عبد العال الديري ومحمد صادق اسماعيل، المرجع السابق، ص 265.

[2] المادة 03/42 من قانون رقم 86 –05 ، المؤرخ في 04 مارس 1986 ،جريدة رسمية عدد 10 ،مؤرخ في 05 مارس 1986 ،يعدل ويتمم الأمر رقم 66 –155 المتضمن قانون الإجراءات الجزائية.

2-المسرح الافتراضي

يعرف المسرح الافتراضي بأنه البيئة الرقمية التي تتم فيها الجرائم الإلكترونية، ويتألف أساسا من البيانات الرقمية المخزنة داخل الحواسيب، ولا سيما في ذاكرة الأقراص الصلبة .تتنوع هذه الجرائم بين الاعتداء على البرامج والبيانات الإلكترونية، وارتكاب جرائم التزوير المعلوماتي والتخريب، خاصة عبر الإنترنت. [1]

صعوبات المعاينة في العالم الافتراضي

تواجه عمليات التحقيق في الجرائم الإلكترونية تحديات كبيرة، أبرزها:

- **ندرة الآثار المادية** التي تتركها الجرائم الرقمية، مما يجعل إثباتها أكثر تعقيدا مقارنة بالجرائم التقليدية.

- **عدد الأشخاص الهائل** الذين قد يترددون على المسرح الافتراضي خلال فترة زمنية قصيرة،[2] مما يصعب تتبع الجناة.

ولكي يتمكن ضباط الشرطة القضائية من معاينة الجرائم في العالم الافتراضي، فإن عليهم دخول البيئة الرقمية من خلال مكاتبهم، أو الاستعانة بمقاهي الإنترنت، أو طلب مساعدة خبراء في المجال، وكلها وسائل تساهم في كشف الحقيقة.

[1] عبد العال الديري ومحمد صادق اسماعيل، المرجع نفسه، ص 266.

[2] نظرا لكون الجريمة المعلوماتية صعبة الاثبات واكتشاف من قام بها خاصة في مقاهي الانترنت لتوافد عدد كبير جدا من الأشخاص علي مسرح الجريمة .

أساليب المعاينة في جرائم الإنترنت والمعلوماتية

تختلف طرق المعاينة حسب نوع الجريمة الإلكترونية، لكن هناك أساليب عامة متوافقة مع طبيعة الاتصال بالإنترنت، من بينها:

– تصوير شاشة الحاسوب(Capture d'écran) ، سواء عبر آلة تصوير تقليدية أو باستخدام برامج متخصصة تتيح التقاط صورة للمحتوى المعروض على الشاشة.

– **تقنية تجميد مخرجات الشاشة(Frozen Output)** ، التي تمكن المحققين من حفظ الأدلة الرقمية دون التلاعب بها. [1]

مع تطور التكنولوجيا وانتشار الجرائم الإلكترونية، أصبح من الضروري اعتماد أساليب حديثة ومتطورة في المعاينة لضمان جمع الأدلة بكفاءة وملاحقة الجناة بفعالية.

الفرع الثاني: الخبرة التقنية

أحدث التطور الهائل في تكنولوجيا الإعلام والاتصال تغييرا جوهريا في المفاهيم المتعلقة بالدليل الجنائي، مما عزز من دور الإثبات العلمي وجعل الخبرة التقنية جزءا لا يتجزأ من الخبرة القضائية. وأصبح اللجوء إلى خبراء متخصصين في فحص الأدلة التقنية، تقييم عملية الإثبات الرقمي، وتحليل الجرائم الإلكترونية أمرا لا غنى عنه، نظرا لتعقيد هذه القضايا وحاجتها إلى تخصص دقيق، إذ يصعب على القاضي الفصل فيها دون الاستناد إلى الخبرة التقنية، تحقيقا لمبدأ التخصص، الذي يضمن دقة الأحكام ويحول دون وقوعها في الأخطاء القانونية.

[1] زيدان نبيل ودواقي يزيد،.مذكرة تخرج لنيل شهادة القيادة والاركان الدفعة 18 تحت عنوان الجريمة المعلوماتية ودور الدرك الوطني 2014 –2015 . ص .48.

1- دور الخبرة التقنية

تعرف الخبرة الفنية بأنها أحد إجراءات التحقيق التي يتم من خلالها الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية متخصصة، لا تتوفر لدى جهات التحقيق أو القضاء، وذلك بهدف الكشف عن دليل أو قرينة تساعد في معرفة الحقيقة بشأن وقوع الجريمة أو تحديد هوية مرتكبها، فهي بمثابة استشارة فنية يلجأ إليها القاضي أو المحقق لمساعدته في تكوين قناعته القضائية حول مسائل ذات طبيعة تقنية معقدة لا يستطيع تقديرها دون معرفة فنية متخصصة

.2--دور الخبرة التقنية في إثبات الجرائم الإلكترونية

تلعب الخبرة الفنية دورا محوريا في إثبات الجرائم الإلكترونية، حيث تساعد في:

- تمكين سلطات التحقيق والقضاء من فهم الأدلة الرقمية وضبطها.
- الوصول إلى الحقيقة وتعزيز العدالة الجنائية[1] عبر فحص البيانات الإلكترونية بدقة.
- كشف غموض الجرائم الإلكترونية عبر تحليل الأدلة التقنية وربطها بالمتهمين.

وفي ظل الانتشار المتزايد للجرائم الإلكترونية، أصبح من الضروري أن تستعين جهات التحقيق والمحاكم بخبراء في التقنية الرقمية، بهدف:

- تفكيك الأدلة الإلكترونية وتجميعها بصورة قانونية سليمة.
- المساعدة في التحقيقات المتعلقة بالجرائم الإلكترونية المعقدة.
- توضيح الأبعاد التقنية للجريمة، خاصة فيما يتعلق بالبرمجيات والشبكات.

[1] بوكر رشيدة، جرائم الاعتداء علي أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، 2012 ، ص 424.

شهدت السنوات الأخيرة تزايدا ملحوظا في الحاجة إلى الخبرة الفنية في مجال التحقيق في الجرائم الإلكترونية، وذلك نتيجة للتحولات التكنولوجية العميقة التي طرأت على وسائل الإعلام والاتصال. فقد تنوعت أنواع الحواسيب ونماذجها، وتوسعت شبكات الاتصال بينها، إلى جانب التطور المتسارع في العلوم والتقنيات المرتبطة بها، مما جعل هذه المجالات تنتمي إلى تخصصات علمية وفنية دقيقة ومعقدة يصعب الإلمام بها بالكامل.

بل يمكن القول إن الواقع التقني قد بلغ من التعقيد حدا لا يوجد معه خبير يمتلك معرفة شاملة بكل أنواع الحواسيب، أو البرامج، أو الشبكات، أو يتمكن من التعامل مع مختلف أنماط الجرائم الإلكترونية بكفاءة مطلقة. ولهذا السبب، منح المشرع الجزائري سلطة التحقيق الحرية التامة، وفي أي مرحلة من مراحل التحقيق، في ندب الخبير الذي يراه كفؤا فنيا للاستعانة بخبرته في المجال المطلوب.[1]

ويلاحظ أن القانون لم يلزم جهة التحقيق أو الحكم بالاستجابة لطلب المتهم أو أي طرف من الخصوم في هذا الشأن. وقد أكدت الفقرة الثانية من المادة 143 من قانون الإجراءات الجزائية على أنه :إذا رأى قاضي التحقيق أنه لا موجب لطلب الخبرة، فعليه أن يصدر في ذلك قرارا مسببا ....ورغم ذلك، فإن الاستعانة بالخبرة الفنية – التي قد تكون اختيارية في الجرائم التقليدية – تعد ضرورة ملحة في سياق الجرائم الإلكترونية، نظرا لارتباطها الوثيق بمسائل فنية دقيقة ومعقدة لا يمكن تفسيرها أو التحقق منها إلا من خلال خبير متخصص وذو كفاءة عالية.[2]

وتتجلى أهمية الخبير الفني بوضوح في حالة غيابه، إذ قد تفشل جهات التحقيق والاستدلال في فك رموز الجريمة الإلكترونية، أو في جمع الأدلة التقنية الدالة عليها،

[1] سليمان احمد فضل، مرجع سابق ، ص 134.

[2] فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية ، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق بجامعة القاهرة 2012، ص 640.

نتيجة نقص الكفاءة أو غياب التخصص اللازم، مما قد يؤدي إلى ضياع الأدلة أو إتلافها دون قصد نتيجة للجهل الفني أو الإهمال.

وقد تنبه المشرع الجزائري إلى هذه الإشكالية، حيث نص في الفقرة الأخيرة من المادة 5 من القانون رقم 04-09، المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، على ما يلي:

يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية معطيات المعلومات التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

- وعليه، فإن المشرع أقر صراحة إمكانية الاستعانة بالخبراء والمتخصصين لدعم أجهزة التحقيق، بما يضمن إنجاز المهام الموكلة إليها على نحو فني سليم، ويجنب ضياع الأدلة أو إفسادها. [1]

يلاحظ أن المشرع الجزائري عند صياغته للنص المتعلق بالمساعدة القضائية في مجال مكافحة الجرائم الإلكترونية، عمد إلى استعمال عبارة عامة وموسعة كل شخص له دراية، وهو تعبير مقصود يهدف إلى توسيع نطاق الأشخاص المؤهلين لتقديم الدعم الفني للسلطات القضائية، بحيث لا يقتصر الأمر فقط على الخبراء، بل يشمل أيضا كافة المختصين والعاملين في مجال تكنولوجيات الإعلام والاتصال، مثل مهندسي الإعلام الآلي، الحاصلين على الشهادات العليا في المجال، ومقدمي خدمات الاتصال الإلكتروني ك مزودي خدمة الإنترنت، ومزودي خدمات الإيواء، والحوسبة السحابية، وكل من يمتلك كفاءة تقنية أو معرفة فنية متخصصة.

[1] القانون 09-04 المؤرخ في 05-8-2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ولم يكتف المشرع الجزائري بهذا التوسع النظري، بل عزز جهوده على أرض الواقع من خلال إنشاء هيئات وأجهزة متخصصة في مجال مواجهة الجرائم الإلكترونية، زودت بتقنيات حديثة ووسائل متطورة، وأسندت إليها مهمة تقديم الدعم الفني وإنجاز الخبرات التي تطلبها الجهات القضائية .ومن بين هذه الهيئات:

- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، الذي أنشئ سنة 2009 تحت إشراف قيادة الدرك الوطني.

- المعهد الوطني للبحث في علم التحقيق الجنائي، المحدث بموجب المرسوم الرئاسي رقم 04–432 المؤرخ في 20 ديسمبر 2004، والمنظم هيكليا وفق قرار وزاري مشترك صادر بتاريخ 14أبريل 2007، والذي يضم مصلحة متخصصة في الخبرات المتعلقة بالأدلة التكنولوجية.

- القسم الرقمي التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية على مستوى المديرية العامة للأمن الوطني، والذي يقدم الخبرة الفنية في القضايا ذات الطابع الرقمي، وتنتشر مصالحه على مستوى بعض ولايات الوطن.

- ثلاثة مخابر جنائية جهوية أنشئت مؤخرا في شمال البلاد، تابعة للأمن الوطني، وتضم عدة أقسام متخصصة، من بينها قسم الأدلة الإلكترونية والرقمية، ومن المتوقع أن تستَكمل هذه الجهود بإنشاء ثلاث مخابر مماثلة في الجنوب،[1] وفقا لما صرحت به السيدة هودة رشيدة، ملازم أول للشرطة ورئيسة فرقة مكافحة الجرائم المعلوماتية بأمن ولاية وهران.

[1] القرار الوزاري المؤرخ في 14/04/2007 المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، جريدة رسمية عدد 36 ، صادر بتاريخ 03 جويلية 2009.

وفي السياق نفسه، نص المرسوم الرئاسي رقم 15–261 المؤرخ في 8 أكتوبر 2015 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،[1] وقد أسندت إليها مهمة دعم السلطات القضائية ومصالح الشرطة القضائية في مجالات البحث والتحري، وتقديم المساعدة الفنية، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المتخصصة في الجرائم ذات الصلة بالتكنولوجيات الرقمية.[2]

[1] مرسوم رئاسي رقم 15 – 261 مؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015 ، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 53 ، صادر بتاريخ 8 أكتوبر 2015.

[2] أنظر الفقرة ب من المادة 13 من القانون رقم 09–04 المؤرخ في 05/08/2009.

المبحث الثاني: الاجراءات القانونية للكشف عن الجرائم المعلوماتية

يعد الكشف عن الجرائم المعلوماتية من المسائل المعقدة التي تستوجب إجراءات قانونية دقيقة تتماشى مع طبيعة هذا النوع من الإجرام. فإلى جانب التحري التقليدي، تبرز الحاجة إلى وسائل متطورة في جمع الأدلة وتثبيتها قانونا، وهو ما يفرض على الجهات المختصة اعتماد إجراءات خاصة تجمع بين الطابع المادي والتقني، والإطار القانوني الذي ينظم عملية المتابعة والتحقيق.

المطلب الأول: اجراءات التحري الكالسيكية للكشف عن الجريمة المعلوماتية

رغم الطابع المستحدث للجريمة المعلوماتية، إلا أن إجراءات التحري الكلاسيكية لا تزال تحتفظ بأهميتها في الكشف عنها، حيث تعد خطوة أولى في جمع المعلومات وتحديد الجناة. وتشمل هذه الإجراءات الوسائل المادية التي تعتمدها السلطات المختصة، إضافة إلى الاستعانة بالخبرة التقنية لفهم وتحليل المعطيات الرقمية المرتبطة بالجريمة.

الفرع الأول: الاجراءات المادية لمواجهة الجريمة المعلوماتية

تعد الإجراءات المادية من أبرز الوسائل التي تعتمدها السلطات المختصة في مواجهة الجريمة المعلوماتية، حيث تشمل عمليات التفتيش، الحجز، وضبط الأجهزة والوسائط الإلكترونية المستخدمة في ارتكاب الجريمة. وتكتسي هذه الإجراءات أهمية بالغة نظرا لطبيعة الأدلة الرقمية التي تتطلب سرعة ودقة في المعالجة للحفاظ على سلامتها وقيمتها القانونية.

أولا: المعاينة الالكترونية.

هي المكان الذي ارتكبت فيه الجريمة، الوعاء الأساسي الذي يحتوي على اخطر الأدلة الجنائية التي يخلفها الجاني وراءه في اعقاب اقترافه الجريمة، وفي لحظة يكون فيها

اضطرابه العصبي والذهني قد بلغ قمة الانفعال بصورة لا تتيح المراجعة الدقيقة لأعماله وإزالة الاثار التي يخلفها في مكان الحادث (مجرم مهما كانت دقته سوف يترك وراءه ما قد يشير الى شخصيته[1] ولذلك كان من الواجب على ضباط الشرطة القضائية الانتقال الى ذلك المكان لمعاينة واثبات الاثار المادية للجريمة والمحافظة عليها واثبات حالة الاماكن والاشخاص وكل ما يفيد في كشف الحقيقة، وكذا اخطار النيابة فورا بانتقاله، لكي تنتقل بدورها الى محل الجريمة في حالة الجناية الملتبس بها[2]. ويقصد بالمعاينة رؤية بالعين لمكان او شخص او شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة، وهي تقتضي في ذلك سرعة الانتقال الى محل تلك الواقعة حيث يقوم ضابط الشرطة القضائية بجمع الدلائل والقرائن التي يستدل بها عن الجريمة والتثبيت المباشر لحالة الأشخاص والاشياء والأماكن ذات الصلة بالحادث، وهي المرحلة الأولى للاستدلال حول ملابسات اية جريمة ونظرا لاختلاف الجريمة المعلوماتية كثيرا عن الجرائم التقليدية نظرا لكون مسرحها الاجرامي قد يتعدى حدود الدولة فان المعاينة التقنية تتم بإتباع مجموعة من الإجراءات الخاصة التي سنوردها فيما بعد.[3]

وتظهر أهمية المعاينة في انها تنقل لجهات التحقيق والمحاكمة صورة مجملة لموقع الجريمة بكل ما يحتويه هذا الموقع من تفصيلات سواء تعلقت هذه التفصيلات بمكانه او وصفه من الداخل او الاثار الموجودة به، والتي تنقلها بالجريمة واجمالا كل ما يمكن

[1] نبيه صالح ، الوسيط في شرح مبادئ الاجراءات الجزائية.د ط.منشاة المعارف القانونية للنشر،عمان.ص .30.

[2] المادة 31 قانون إ.ج المصري... الانتقال فور الي مكان الجريمة...

[3] عبد العال الديري ومحمد صادق اسماعيل، الجرائم الالكترونية، ط01 ، المركز القومي للإصدارات القانونية، القاهرة، 2012.ص 264.

جهات الشرطة والقضاء من وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة من المادة التي تم جمعها.[1]

وحتى تحقق المعاينة ثمارها وتفي بأغراضها المشهودة، نجد ان بعض التشريعات قد قررت جزائيات جنائية على كل من يقوم بإجراء أي تغيير على حالة الأماكن التي فيها الجريمة او ينزع أي شيء منها او يحدث تعديلا في مكان وقوع الجريمة قبل قيام سلطة التحقيق او الاستدلالات بإجراء المعاينة الأولى أيا كان مرتكبه.[2]

إذا كانت المعاينة في الجرائم التقليدية تتم في مسرح الجريمة العادي فان الجريمة المعلوماتية تتم المعاينة فيها على مستويين:

1-المسرح التقليدي:

المسرح التقليدي هو المسرح الذي يقع عادة خارج بيئة الحاسوب ويتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة وهو قريب من مسرح الجريمة التقليدية، ومن امثلة هذه الجرائم تلك الواقعة على اشرطة الحاسب d.f والكابلات الخاصة به وشاشة العرض الملحق به ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب الالي ذات الطابع المادي المحسوس.[3]

وليس هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل ضباط الشرطة العلمية والتحفظ على الأشياء التي تعد ادلة مادية على ارتكاب الجريمة ونسبها الى شخص معين، وكذلك وضع الاختام في الأماكن

[1] نبيه صالح ، الوسيط في شرح مبادئ الاجراءات الجزائية، ص 31.

[2] عبد العال الديري ومحمد صادق اسماعيل، المرجع السابق، ص 265.

[3] المادة 03/42 من قانون رقم 86 -05 ، المؤرخ في 04 مارس 1986 ،جريدة رسمية عدد 10 ،مؤرخ في 05 مارس 1986 ،يعدل ويتمم الأمر رقم 66 -155 المتضمن قانون الإجراءات الجزائية.

التي تمت المعاينة فيها، وضبط كل الأدوات والوسائل التي استخدمت في ارتكاب الجريمة مع وجوب اخطار النيابة العامة بذلك.

2-المسرح الافتراضي:

المسرح الافتراضي يقع عادة داخل البيئة الالكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله وفي مقدمة هذه الجرائم الواقعة على برامج الحاسب الالي او بياناته او تتم بواسطتها، وكذلك الجرائم التي تتم بطريق الانترنت ومنها جرائم التزوير المعلوماتي والتخريب.[1]

وتتميز المعاينة في العالم الافتراضي بالصعوبة تتمثل في:

_ ندرة الاثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلومات.

_ الاعداد الهائلة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة زمنية[2]
وحتى يمكن لضابط الشرطة القضائية القيام بالمعاينة في العالم الافتراضي لابد عليه ان ينتقل، الى العالم الافتراضي لمعاينة من مكتبه او اللجوء الى مقهى الانترنت او الى الخبراء وغيرها من الأماكن التي تساعده في اظهار الحقيقة.

وللمعاينة في جرائم الانترنت والحاسوب (المعلوماتية) اشكال مختلفة تختلف بحسب نوعية الجريمة المرتكبة على ان هناك طرقا عامة تتوافق مع طبيعة الاتصال بالانترنت او الوسيلة التي تستخدم مثلا: وسيلة تصوير شاشة الحاسوب écran'd captures de impression والتي تكون بواسطة الة تصوير تقليدية او عن طريق استخدام برمجة

[1] عبد العال الديري ومحمد صادق اسماعيل، المرجع نفسه، ص 266.

[2] نظرا لكون الجريمة المعلوماتية صعبة الاثبات واكتشاف من قام بها خاصة في مقاهي الانترنت لتوافد عدد كبير جدا من الأشخاص علي مسرح الجريمة .

حاسوب متخصصة في اخذ صورة لما يظهر على الشاشة وهذا ما يصطلح عليه تجميد مخرجات الشاشة frozen وغيرها.[1]

ثالثا: تفتيش المنظومات المعلوماتية

يعتبر التفتيش عن الجريمة المعلوماتية من أصعب أنواع التفتيش، وهذا راجع إلى التطور التكنولوجي في وسائل الاتصال.

1- مفهوم التفتيش

يعرف التفتيش بأنه إجراء من إجراءات التحقيق، تقم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه[2].

وهناك من يعرف الرقابة بأنها من أنشطة التحقيق التي يقوم بها الموظف المختص وفق الإجراءات التي يحددها القانون، في محل يتمتع بحرمته، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها، لإثبات ارتكابها ونسبها إلى المتهم، وقد أحاط إجراء التفتيش _نظرا لمساسه بالحريات الخاصة للأفراد بضمانات عديدة[3].

[1] زيدان نبيل ودواقي يزيد،.مذكرة تخرج لنيل شهادة القيادة والاركان الدفعة 18 تحت عنوان الجريمة المعلوماتية ودور الدرك الوطني 2014 -2015 . ص .48.

[2] سامي حسني الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة، 1972، ص36.

[3] عوض محمد عوض، قانون الإجراءات الجنائية، ج1، مؤسسة الثقافة الجامعية، 1989، ص475.

وهناك من يعرفه بأنه وسيلة من وسائل التحري عن مختلف الأدلة المعنوية والمادية للجريمة، يهدف إلى جمع الأدلة التي تؤدي إلى كشف الحقيقة وضبطها والوصول غلى دليل حاسم، لأنه لا إدانة ولا جزاء دون دليل[1].

2- شروط التفتيش في المنظومات المعلوماتية

وتنقسم إلى شروط شكلين وشروط موضوعية تتمثل في الآتي:

أ- **الشروط الشكلية** وهي كالآتي:[2]

وقت إجراء التفتيش: عندما يتعلق الأمر بأنظمة المعالجة الآلية للمعطيات فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل من ساعة من ساعات النهار أو الليل وهذا بناء على إذن مسبق من وكيل الجمهورية المختص.

حضور الأشخاص المعنيين أثناء التفتيش: واشترط المشرع الجزائري أن يتم تفتيش المنزل بحضور المتهم وفي حالة منعه من ذلك أثناء الإجراءات، كان على ضابط الشرطة القضائية أن يكلفه بتعيين ممثل له وإذا امتنع عن ذلك أو كان هاربا كان من الواجب أن ينوبه عنه شاهدين غير الموظفين الخاضعين له.

1. **محضر التفتيش:** في الجرائم الماسة بالمعطيات الآلية: تسمى محاضر الشرطة القضائية محاضر البحث الابتدائي وتكمن أهميتها في قيمتها الممنوحة لها كوسيلة إثبات على وقوع الجريمة ونسبتها إلى فاعلها من جهة، ومن خطورة الصلاحيات الواسعة الممنوحة بموجبها لضابط الشرطة القضائية.

[1] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد05، جوان 2012، ص162.

[2] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد04، جانفي 2018، ص57-58.

ب- الشروط الموضوعية: وتتمثل في[1]:

سبب التفتيش: ارتكاب الجريمة المعلوماتية بشكل عام.

محل التفتيش: محل التفتيش بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها على العالم.

السلطة الخاصة بالقيام بالتفتيش: تتمثل الجهة القضائية التي تم إسنادها مهمة التفتيش في قاضي التحقيق أو النيابة العامة باختلاف التشريعات كسلطة أصلية، أو استثناء في رجال الضبط القضائي. وفي حالة وقوع جريمة من نوع الجنايات أو الجنح ولم يكن قاضي التحقيق المختص موجودا فإن على المسؤول عن التحقيق عندما تقتضي الضرورة إصدار قرار أو إجراء فوري في التحقيق عرض الأمر على أي قاضي في منطقة اختصاص قاضي التحقيق أو أي منطقة قريبة لاتخاذ ما يلزم على أن تعرض الأوراق على قاضي التحقيق المختص في أقرب وقت.

ثالثا: ضبط الأدلة في الجريمة الإلكترونية

يعد الضبط من الإجراءات الأساسية في جمع الأدلة الجنائية، وهو النتيجة التي تنتهي إليها عملية التفتيش. ويتمثل الضبط في وضع اليد على الأشياء أو الوسائل التي استخدمت في ارتكاب الجريمة ، والتي يمكن أن تسهم في كشف الحقيقة وتقديمها أمام القضاء كأدلة إثبات. 2

[1] عز الدين عثماني، مرجع سابق، ص58-59.

[2] خالد عياد الحلبي، 2011، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، دار الثقافة للنشر والتوزيع، عمان،ص169.

وفي هذا السياق، قد تكون المضبوطات ذات طبيعة مادية ، أي مرئية وملموسة، مثل: أجهزة الحاسوب وأجزاؤها (الأقراص الصلبة، الطابعات)، أو الأشرطة المغناطيسية، وبطاقات الدفع الإلكتروني، والمعدات المستخدمة في شبكات الإنترنت مثل المودم.

كما يمكن أن تتخذ المضبوطات طبيعة غير مادية ، أي معنوية، مثل البيانات الرقمية والبرمجيات المعالجة آليا، والمراسلات الإلكترونية، ورسائل البريد الإلكتروني،[1] وغيرها من المعلومات الرقمية التي تحمل دلالة على ارتكاب الجريمة.

وعليه، وفي حال تم العثور على دليل رقمي خلال التحقيق، فإن الإجراء التالي الذي يجب اتخاذه هو الحجز ، وقد نص المشرع الجزائري على ذلك صراحة في المادة 06 من القانون رقم 09/04 المؤرخ في 15 يوليو 2004، المتضمن للإجراءات المتعلقة بالتفتيش والحجز في المنظومات المعلوماتية.

وتشير هذه المادة إلى أنه:

عندما تكتشف الجهة المختصة أثناء عملية تفتيش في منظومة معلوماتية بيانات مخزنة تعتبر ذات فائدة في الكشف عن الجريمة أو مرتكبيها، فإنه ليس من الضروري حجز المنظومة بأكملها ، بل يكتفى بنسخ البيانات محل البحث، بالإضافة إلى البيانات اللازمة لفهمها، على وسيلة تخزين إلكترونية قابلة للحجز، وتوضع ضمن أحراز رسمية.

كما يؤكد القانون على أن الجهة التي تقوم بالتفتيش والحجز ملزمة بضمان سلامة البيانات داخل المنظومة المعلوماتية التي يتم التعامل معها، وذلك طوال مدة إجراء العملية.

[1] جمال نجيمي، 2011 ، إثبات الجريمة علي ضوء الإجتهاد دراسة مقارنة، دار هومة، الجزائر،ص46.

وفي حالة كانت هناك صعوبات تقنية تمنع القيام بالحجز الفعلي ، يتعين على الجهة المختصة استخدام تقنيات مناسبة لمنع الوصول إلى تلك البيانات أو إلى نسخها الاحتياطية، حتى لا تتعرض للتغيير أو الاستخدام غير المشروع.

أما إذا كانت البيانات المضبوطة تحتوي على معلومات يشكل محتواها جريمة ، فإن القانون يمنح الجهة المكلفة بالتحقيق الحق في اتخاذ جميع الإجراءات الضرورية لمنع الإطلاع عليها من طرف الغير .

وأخيرا، سواء كانت البيانات محل شك أو كان محتواها مجرما، فلا يجوز استعمالها لأي غرض آخر غير التحري أو التحقيق أو العمل القضائي ، وإلا عرض الشخص المسؤول للمساءلة الجنائية.

الفرع الثاني: إجراءات إثبات الجريمة الإلكترونية.

يقوم قاضي التحقيق في مجال الكشف والبحث والتحري عن الجريمة المعلوماتية وكشف الغموض عنها والقبض على فاعلها باتخاذ الكثير من الإجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه، ومن بينها:

أولا: الاستجواب الالكتروني: الاستجواب هو مناقشة المتهم بالتهم والوقائع المنسوبة إليه ومواجهته بالأدلة القائمة ضده والمتهم حر في الإجابة عن الأسئلة الموجهة عليه ولا يعد امتناعه قرينة ضده، وهو وسيلة تمحيص للتهم أو لنفيها عنه فهو طريق من طرق تقصي الحقيقة ومصدر من مصادر الإثبات وليس وسيلة إثبات.

يعتبر الاستجواب اجراء من الإجراءات العامة في التحقيق لأن نجاح المحقق في اسناد الواقعة إلى الجاني واعترافه بارتكابها.

إذ اعتبر الاستجواب ذو طبيعة مزدوجة فهو أداة اتهام ووسيلة دفاع في آن واحد بحيث يسمح للمتهم أن يحاط بالتهم والوقائع المنسوبة إليه وبكل ما يوجد بالملف من أدلة التي تساعد على كشف براءته[1].

قبل أن يقوم المحقق بإجراء الاستجواب والمواجهة عليه أن يستعد لها وذلك بإتباع القواعد العامة التالية :

- الإلمام الكامل بفهم أقوال الشهود وسائر المتهمين أن يحدد النقاط الجوهرية التي سيتم ايضاحها من المتهم.
- فهم فحوى التقارير الفنية التي وضعها الخبراء عن نتائج عملهم في الآثار المستخلصة.
- وضع خطة لنفسه يسير عليها في استجواب المتهم.[2]

ثانيا: الشهادة الالكترونية.

إن مصطلح الشهادة الالكترونية يطلق على نوع من الشهادة التي لا يكون فيها الشاهد حاضرا فقد تتم مثلا عن طريق وسائل الكترونية أو رقمية من خلال شبكة الإنترنت.

المطلب الثاني: الإجراءات الجنائية المقررة للجريمة الالكترونية

تستلزم الجرائم الإلكترونية اعتماد إجراءات جنائية خاصة تتناسب مع طبيعتها التقنية المعقدة وأثرها الواسع على الأفراد والمجتمع. وتتضمن هذه الإجراءات قواعد وضوابط قانونية تهدف إلى ضمان ملاحقة الجناة بفعالية، مع احترام الحقوق والحريات الأساسية، سواء فيما يتعلق بالأشخاص المتهمين أو الأموال المتصلة بالجريمة، مما يضمن تحقيق العدالة وفرض الردع القانوني.

[1] علي حسن محمد الطوالبة،المرجع السابق، ص 61.

[2] هدي حامد قشقوس، المرجع السابق، ص 58.

الفرع الأول: الإجراءات الجنائية المقررة للجريمة الالكترونية المطبقة على الأشخاص.

تتطلب الجرائم الإلكترونية إجراءات جنائية خاصة عند التعامل مع الأشخاص المتهمين، نظرا للطابع المعقد لهذه الجرائم والتحديات التي تفرضها التكنولوجيا الحديثة على عملية التحقيق والمحاكمة. لذلك وضعت القوانين ضوابط دقيقة تحكم حقوق المتهمين وضمانات سير العدالة، مع مراعاة خصوصية الأدلة الرقمية وطرق جمعها وإثباتها.

أولا: الترصد الالكتروني.

1- تعريف الترصد الالكتروني :

استحدث المشرع الجزائري آلية **الترصد الإلكتروني** كأحد أساليب التحري الخاصة بجرائم الفساد، وذلك بموجب المادة 56 من القانون رقم 06/01 المتعلق بالوقاية من الفساد ومكافحته. غير أن المشرع لم يضمن نص هذه المادة تعريفا دقيقا لهذا الإجراء أو يوضح كيفية تطبيقه.

وقد تم تدارك هذا النقص لاحقا عبر القانون رقم 06/22 المعدل والمتمم لقانون الإجراءات الجزائية، حيث أدرج فصلٌ خاص تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، تناول فيه المشرع الترصد الإلكتروني بشكل مفصل من خلال المواد من 65 مكرر 5 إلى 65 مكرر 10، مع تعميم هذا الإجراء على مختلف الجرائم الخطيرة، بما في ذلك جرائم الفساد.

ورغم هذا التفصيل في الإجراءات، إلا أن المشرع الجزائري لم يقدم تعريفا صريحا للترصد الإلكتروني، وهو ما دفع الفقه القانوني إلى محاولة تحديد مفهومه من خلال تحليل مظاهره وتطبيقاته، والتي تتمثل أساسا في اعتراض المراسلات، تسجيل

المحادثات الصوتية، والتقاط الصور بهدف توثيقها واستغلالها في سياق التحري والتحقيق الجنائي[1] وعليه، يمكن تعريف الترصد الإلكتروني بأنه:

عملية فنية تستخدم فيها وسائل تكنولوجية متطورة لاعتراض الاتصالات، أو تسجيل الأصوات، أو التقاط الصور، من أجل جمع الأدلة التي تسهم في كشف الجرائم والتعرف على مرتكبيها.

كما أن هناك تعريفات فقهية أخرى تناولت الترصد الإلكتروني من زاوية وظيفية، منها من عرفه بأنه عملية تتبع منهجي ومستمر لشخص مشتبه به، سواء قبل أو بعد ارتكاب الجريمة، بقصد ضبطه في حالة تلبس، ومنها من عرفه بأنه إجراء يتمثل في تسجيل المحادثات باستخدام أجهزة خاصة، ويعد التصنت أو الاكتفاء بالتسجيل الصوتي من بين الوسائل المعتمدة، على أن يدون مضمون هذه التسجيلات في محاضر رسمية تعد لهذا الغرض[2].

2- أشكال الترصد الالكتروني :

-اعتراض المراسلات

يتمثل اعتراض المراسلات في نسخها أو تسجيلها، وهي تشمل جميع الرسائل التي ترسل عبر وسائل الاتصال المختلفة، سواء كانت سلكية مثل الهاتف الثابت، والبرقية (التلغراف)، والفاكس، أو لاسلكية مثل الهاتف الجوال، الإنترنت، البريد الإلكتروني، الوسائل التقنية الحديثة.

[1]-عبد العالي حاجة وآمال، يعيش تمام مجلة كلية القانون الكويتية العالمية – أبحاث المؤتمر السنوي الدولي الخامس 9 – 10 350 مايو

[2]خرشي عثمان، الترصد الالكتروني كآلية لمكافحة الجرائم المعلوماتية مجلة الدراسات الحقوقية المجلد 7 العدد 3 سبتمبر 2020، ص –804

-تسجيل الأصوات:

تقصد بهذه العملية مراقبة المحادثات الشفوية وتسجيلها، سواء أجرتها شخص واحد أو مجموعة من الأشخاص بشكل خاص أو سري في أماكن متعددة، سواء كانت عامة كالمقاهي والمطاعم والحانات، أو خاصة كالمحلات والمكاتب والمساكن.

-التقاط الصور:

يشير هذا الإجراء إلى استخدام التصوير الفوتوغرافي أو المرئي (الفيديو) كوسيلة للبحث والتحري عن الجرائم. وقد أصبحت الكاميرات واحدة من أهم الأدلة التي تستخدم لإثبات الواقعات، لما توفره من صور دقيقة وحية تعكس مكان الحادثة أو الزمان أو الشخص بدقة عالية، وقد رأى المشرع أنها أداة فعالة لا غنى عنها لخدمة العدالة وكشف الحقيقة.

ثانيا: التسرب (الاختراق)

في ظل التطور المتسارع الذي يشهده مجتمعنا اليوم، خاصة على مستوى أنواع الجرائم وأساليب ارتكابها، كان لا بد من تكيف المشرع مع هذه المستجدات، وذلك من خلال اعتماد طرق جديدة وفعالة لمواجهة هذا النوع من الإجرام.

وهو ما ظهر بوضوح في آخر تعديل لقانون الإجراءات الجزائية ، حيث تم استحداث مفهوم التسرب باعتباره أحد الأساليب الحديثة المساعدة في إجراء التحريات وجمع الأدلة المتعلقة بالجرائم. وتهدف هذه الآلية إلى تعزيز فعالية البحث الجنائي ومواكبة التعقيدات التي تكتنف بعض القضايا.

وسنتناول في هذا السياق مفهوم التسرب، بالإضافة إلى بيان الشروط والإجراءات التي وضعها المشرع الجزائري في هذا المجال من خلال مطلبين:

1- مفهوم التسرب

لغة، كلمة التسرب مشتقة من الفعل تسرب، أي دخل خفية أو انتقل بطريقة سرية. ويقصد به عمليا الولوج أو الاختراق بطريقة غير مباشرة إلى مكان معين أو إلى مجموعة أو تنظيم، بهدف جمع المعلومات أو الأدلة حول نشاط إجرامي[1].

أدرج المشرع الجزائري تقنية التسرب أو الاختراق ضمن تعديل قانون الإجراءات الجزائية لسنة 2006، كوسيلة خاصة للتحري والتحقيق، تستخدم عند الضرورة في بعض الجرائم المنصوص عليها في المادة 65 مكرر 05 .ويجوز لوكيل الجمهورية أن يأذن، تحت إشرافه، بتنفيذ هذه التقنية وفق شروط محددة.[2]

يعد التسرب أو الاختراق أحد أساليب التحري الخاصة، حيث يتيح لضباط أو أعوان الشرطة القضائية التوغل داخل جماعات إجرامية بهدف مراقبة المشتبه بهم وكشف أنشطتهم، وذلك من خلال إخفاء الهوية الحقيقية والتظاهر بأنهم فاعلون أو شركاء في الجريمة. تتم هذه العملية تحت مسؤولية ضابط شرطة قضائية مكلف بتنسيق المهمة.[3]

أ-التعريف القانوني للتسرب

حدد المشرع الجزائري هذا المفهوم في المادة 65 مكرر 12 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، حيث يعرف التسرب بأنه قيام ضابط أو عون شرطة قضائية، تحت إشراف مسؤول مكلف بالتنسيق، بمراقبة المشتبه بهم عبر إيهامهم بأنه شريك أو فاعل معهم في الجريمة .الجدير بالذكر أن المشرع استخدم مصطلح التسرب في قانون الإجراءات الجزائية، في حين ورد مصطلح الاختراق في المادة 56 من القانون

[1] سهيل حسيب سماحة، معجم اللغة العربية، الطبعة الأولي، مكتبة سمير ، 1984، ص 130

[2] نعيمي جمال النبات الجريمة علي ضوء الاجتهاد القضائي دراسة مقارنه دار هومة للطباعة والنشر والتوزيع، الجزائر 451 2011

[3] حريزي ربيحة، إجراءات جمع الأدلة ودورها في الكشف عن الجريمة، رسالة ماجد طير، جامعة الجزائر، 2001، ص 59

رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته، إلا أن كلا المصطلحين يحملان ذات المفهوم والهدف.

أهمية وآليات التسرب

يعتبر التسرب تقنية ميدانية معقدة تستخدم في عمليات التحري لجمع الأدلة والوقائع من داخل الجماعة الإجرامية، مما يستدعي احتكاكا مباشرا بالمشتبه بهم والمتهمين. ونظرا لما تنطوي عليه هذه العملية من خطورة بالغة، فإنها تتطلب دقة عالية في التنفيذ، تخطيطا محكما، وتركيزا شديدا لتجنب كشف هوية المتسرب.

طبيعة عملية التسرب

يعد التسرب أحد أخطر وأكثر أساليب التحري تعقيدا، حيث يتوجب على ضابط الشرطة القضائية وأعوانه اتخاذ تصرفات توحي بكونهم جزءا من العصابة الإجرامية، في حين أن هدفهم الحقيقي هو الاحتيال على المجرمين، الاطلاع على أسرارهم من الداخل، وجمع الأدلة الكافية لإثبات تورطهم، تمهيدا لتقديمها إلى السلطات المختصة وضبط المجرمين[1].

أهداف عملية التسرب

لضمان نجاح عملية التسرب، لا بد من تحليل شامل للوسط المستهدف عبر:

- الحصول على صورة دقيقة عن طبيعة الجماعة الإجرامية وأهدافها.
- دراسة تاريخ نشأتها وطريقة عملها.
- تحديد اختصاصات كل فرد داخل التنظيم.

[1] روزو زوليخة، جرائم الصفقات العمومية، رسالة ماجستير جامعة محمد خيضر بسكرة 2011، ص 72.

- معرفة وسائل النقل والاتصال المستخدمة.
- كشف نقاط القوة والضعف داخل الجماعة الإجرامية.

بناء على هذه الدراسة، يتم اختيار العناصر المناسبة لتنفيذ العملية، لضمان تحقيق الأهداف دون تعريض المتسربين للخطر أو كشف هويتهم[1].

2- شروط وإجراءات التسرب

نظرا لما تنطوي عليه عملية التسرب من حساسية بالغة وخطورة قانونية، فقد أحاطها المشرع بمجموعة من الشروط والإجراءات الشكلية والموضوعية التي تكفل قانونية تنفيذها، وهو ما يمكن تفصيله في فرعين رئيسيين:

أ- شروط التسرب:

تنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية على أن اللجوء إلى التسرب يجب أن يكون مبررا بضرورات التحري أو التحقيق .ويفهم من ذلك، وبمفهوم المخالفة، أنه إذا توفرت أدلة كافية تعزز الاشتباه أو تدعم توجيه الاتهام، فإن اللجوء إلى هذا الأسلوب يصبح غير مبرر، بل غير مشروع. وعليه، فإن التسرب يشكل إجراء استثنائيا يلجأ إليه فقط عند تعذر أو صعوبة تحصيل الأدلة بوسائل أخرى.

كما قيد المشرع استعمال هذا الأسلوب بطبيعة الجرائم المرتكبة، إذ لا يجوز استخدامه إلا في مواجهة جرائم محددة ذات طابع خطير ومعقد، تم حصرها على سبيل القطع في المادة 65 مكرر 5 من نفس القانون. وتشمل هذه الجرائم:

- جرائم المخدرات،

[1] محمد خريط، مذكرات في القانون الإجراءات الجزائية الجزائري، الطبعة الرابعة، دار هومة للطباعة والنشر والتوزيع، 134 الجزائر.

- الجريمة المنظمة العابرة للحدود الوطنية،
- الجرائم التي تمس أنظمة المعالجة الآلية للمعطيات،
- جرائم تبييض الأموال،
- الإرهاب،
- الجرائم المتعلقة بالتشريع الخاص بالصرف،
- وجرائم الفساد.

بالتالي، فإن أي استعمال لأسلوب التسرب في غير هذه الجرائم المحددة يعد باطلا، وهو ما يؤكد حرص المشرع على حصر نطاق تطبيق هذا الإجراء، نظرا لما تشكله تلك الجرائم من تهديد حقيقي لأمن الدولة ومصالحها الاقتصادية. [1].

ب- إجراءات التسرب:

حرصا على ضمان شرعية الدليل المستخلص من عمليات التسرب، فرض المشرع جملة من الإجراءات القانونية الدقيقة التي تؤطر هذه العملية، وذلك في ظل مبدأ المشروعية الذي يعد مرتكزا أساسيا لأي إجراء سليم.

ومن أبرز هذه الإجراءات، أن يتم تنفيذ عملية التسرب بناء على إذن مسبق يصدر عن وكيل الجمهورية المختص إقليميا، وتتم تحت إشرافه ومراقبته المباشرة .وإذا ما تولى قاضي التحقيق مسؤولية إصدار الأمر بالتسرب، فإنه يكون ملزما أولا بإخطار وكيل الجمهورية، ثم منح إذن كتابي صريح يسلم إلى ضابط الشرطة القضائية المكلف بتنفيذ العملية، على أن يحدد هذا الإذن هوية الضابط المعني بوضوح[2] .

[1] محمد خريط، قاضي التحقيق في النظام القضائي الجزائري، الطبعة الثانية، دار هومه الجزائر، 2009، ص 115

[2] المادة 65/03/02 مكرر 15 من الأمر رقم 66-155 ملمم بموجب المادة 14 من القانون رقم 05-22 يتضمن قانون الإجراءات الجزائية

ينبغي أن يكون الإذن القضائي المتعلق بعملية التسرب مكتوبا ومسببا، بحيث يتضمن بيان الجريمة التي تستدعي اللجوء إلى هذا الإجراء، إضافة إلى تحديد هوية ضابط الشرطة القضائية الذي تنفذ العملية تحت مسؤوليته. كما يجب أن يتضمن الإذن مدة العملية، والتي لا يجوز أن تتجاوز أربعة (04) أشهر،[1] مع إمكانية تجديدها وفق نفس الشروط الشكلية إذا اقتضت ذلك متطلبات التحري أو التحقيق.[2]

ويجوز للقاضي الذي منح الإذن أن يقرر في أي وقت إيقاف العملية قبل انتهاء المدة المحددة، وتودَع الرخصة في ملف الإجراءات بعد إتمام العملية.

وتنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية على أنه يمكن لوكيل الجمهورية أو قاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يمنح هذا الإذن **تحت رقابته**، حسب الحالة، وذلك في إطار التحري في الجرائم المتلبس بها أو التحقيق الابتدائي في جرائم مثل:

المخدرات، الجريمة المنظمة العابرة للحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الإرهاب، الجرائم المتعلقة بتشريع الصرف، وجرائم الفساد.

وتشترط هذه المادة أن تتم عملية التسرب تحت رقابة مباشرة من القاضي، الذي يتولى الإشراف على كل مراحلها تفاديا لأي تجاوز للقانون، على أن يكون الإذن مكتوبا ومسببا، تحت طائلة البطلان، وفقا لما تنص عليه المادة 65 مكرر 15.

[1] المادة 65/04 مكرر 15 من الأمر رقم 66–155 مقدم بموجب المادة 14 من القانون رقم 06–22، يتضمن قانون الإجراءات الجزائية

[2] المادة 65 مكرر 11 من الأمر رقم 66–155 متمم بموجب المادة 14 من القانون رقم 06–22، ينحسن قانون الإجراءات الجزائية

ويترتب عن بطلان الإذن القضائي بطلانٌ لكل الإجراءات المتخذة بناء عليه، ولهذا يلزم أن يتضمن الإذن تحديد الجريمة المبررة للعملية، واسم ضابط الشرطة القضائية المسؤول عنها، إضافة إلى تحديد مدتها (التي لا تتجاوز 4 أشهر) مع إمكانية تجديدها عند الحاجة، كما يمكن للقاضي الأمر بإيقاف العملية في أي وقت قبل انتهاء أجلها، وتودع نسخة من الإذن في ملف الإجراءات بمجرد انتهاء المهمة.

وبموجب المادة 65 مكرر 14، يسمح لضباط وأعوان الشرطة القضائية، في إطار هذه العمليات، باستعمال هويات مستعارة، وارتكاب بعض الأفعال الضرورية لمصلحة التحري، من بينها:

اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصلة من الجريمة أو تستخدم في ارتكابها، بالإضافة إلى استخدام أو توفير الوسائل القانونية أو المالية، وكذا وسائل النقل أو التخزين أو الإبداع أو الحفظ أو الاتصال، لفائدة مرتكبي الجريمة.

يرى بعض الفقهاء أن الأعمال التي تنجز في إطار التسرب تمثل خروجا عن مبدأ نزاهة ومشروعية الدليل الجنائي، غير أنهم يقرون بأنها تهدف إلى غاية أسمى، وهي حماية المجتمع، خاصة في الحالات التي تعجز فيها الوسائل التقليدية للتحري والتحقيق عن التصدي لبعض أنواع الجرائم المعقدة أو الخطيرة[1] .

ويحرر ضابط الشرطة القضائية المكلف بالتنسيق تقريرا يتضمن كل العناصر الضرورية لمعاينة الجرائم، باستثناء تلك التي قد تشكل خطرا على سلامة العون المتسرب

[1] عبد الرحمان خلفي السلطات الإدارية المستقلة، دراسة مقارنة دار النهضة العربية، القاهرة، مصر 2000، ص ص 74-74

أو الأشخاص المسخرين للعملية، وذلك وفقا لأحكام المادة 65 مكرر 13 من قانون الإجراءات الجزائية.

وفي حال تقرر إنهاء العملية، أو عند انتهاء المهلة المحددة في الإذن دون تجديدها، يمكن للعون المتسرب الاستمرار مؤقتا في أداء مهمته بالقدر الضروري لتوقيف نشاطه في ظروف تضمن سلامته، دون أن يسأل جزائيا عن هذا التمديد، شريطة ألا تتجاوز هذه الفترة أربعة (04) أشهر.

وفي حال تعذر عليه التوقف الآمن خلال هذه المهلة، يتوجب إبلاغ القاضي المختص، الذي يمكنه الترخيص بتمديد إضافي لا يتجاوز أيضا أربعة أشهر كحد أقصى.

ويلاحظ أن القانون يمنع سماع أي شخص بشأن عملية التسرب سوى ضابط الشرطة القضائية المسؤول عنها، باعتباره الشاهد الوحيد المقبول قانونا على مجرياتها. كما يترتب على الكشف عن هوية ضباط أو أعوان الشرطة القضائية الذين نفذوا العملية بهوية مستعارة، عقوبات جزائية، وذلك في أي مرحلة من مراحل الإجراءات، بموجب المادة 65 مكرر 16.

أما عن الجهات المخولة بإجراء عمليات التسرب، فهي تلك الواردة في المادة 15 من قانون الإجراءات الجزائية، والتي تشمل ضباط الشرطة القضائية، باستثناء بعض الفئات لاعتبارات ميدانية مثل الولاة ورؤساء المجالس الشعبية البلدية.

ويشار أيضا إلى أن أعوان الشرطة القضائية، المنصوص عليهم في المادة 19 من نفس القانون، يمنحون صلاحية المساهمة في العمليات تحت مسؤولية ضباط الشرطة القضائية المكلفين بالتنسيق، وتحرر محاضرهم باسم هؤلاء الضباط.

الفرع الثاني: الإجراءات الجنائية المقررة الإجراءات الجنائية المقررة للجريمة الالكترونية المطبقة على الأموال

تتطلب الجرائم الإلكترونية إجراءات جنائية مخصصة تتعلق بالأموال المتصلة بهذه الجرائم، سواء كانت أموالا متحصلة من نشاط إجرامي أو أموالا مستخدمة في ارتكاب الجريمة. وتهدف هذه الإجراءات إلى تحديد وتتبع وحجز الأموال المشبوهة، بما يضمن حماية الحقوق المالية للدولة والأطراف المتضررة، ويعزز فاعلية مكافحة الجرائم الإلكترونية المالية.

أولا: التسليم المراقب للعائدات الإجرامية

1- تعريف التسليم المراقب

جاء ذكر مصطلح التسليم المراقب لأول مرة في اتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع بالمخدرات والمؤثرات العقلية لسنة 1988[1]، حيث عرف بأنه ذلك الأسلوب الذي يسمح بعبور شحنات المخدرات والمؤثرات العقلية غير المشروعة عبر إقليم دولة أو أكثر، سواء أكان ذلك عبر البر أو البحر أو الجو، وبإشراف مباشر من السلطات المعنية وتحت رقابتها. ويمكن أن يتم هذا العبور مع وجود أشخاص مصاحبين للشحنات أو بدونهم، ويشمل حتى الشحنات البريدية والمراسلات.

وتنص المادة (11) من هذه الاتفاقية على أن التسليم المراقب هو منهج يتيح استمرار حركة الشحنات غير القانونية من المخدرات والمؤثرات العقلية، وكذلك المواد المدرجة في الجدول الأول والثاني المرفقين بالاتفاقية (أو ما يحل محلها)، داخل إقليم دولة

[1] للاطلاع علي تفاصيل هذه الاتفاقية يرجي العودة إلي موقع الأمانة العامة للأمم المتحدة https://www.unodc.org: تاريخ الولوج :تاريخ الاطلاع 15-04-2025 علي الساعة 11:45.

أو عبره أو خارجه، وذلك بعلم الجهات المختصة وتحت مراقبتها الضرورية ، بهدف الوصول إلى كشف هوية الأفراد المتورطين في ارتكاب الجرائم المرتبطة بهذه المواد. [1]

كما نصت الفقرة الرابعة من المادة 50 من اتفاقية الأمم المتحدة لمكافحة الفساد على مبدأ التسليم المراقب على الصعيد الدولي وهو تطوير قانوني يواكب طبيعة الجرائم الحديثة ذات الطابع العابر للحدود.

وفي ظل تنامي الجرائم المنظمة التي أصبحت تتخذ طابعا دوليا واضحا وتنتشر فروعها عبر العديد من الدول، مثل: الاتجار بالمخدرات والإرهاب، والاتجار غير المشروع بالأسلحة، والاتجار بالبشر، والاتجار بالأعضاء البشرية، وتبييض الأموال، والتهريب وغيرها، برزت الحاجة الملحة إلى تعزيز آليات التعاون الدولي بين الدول، من أجل التعرف على هويات العصابات الإجرامية، وكشف أماكن تمركزها وتحركاتها، ومن ثم القبض على عناصرها والتصدي لها أينما وجدت.

ولا يمكن تحقيق هذا الهدف إلا من خلال وضع نصوص تشريعية داخلية تتيح مرور المواد المحظورة ضمن الحدود الوطنية تحت إشراف وإدارة السلطات المختصة،[2] وذلك عملا بما جاء في المادة 11 من اتفاقية فيينا لعام 1988 المشار إليها سابقا.

يعد يعد التسليم المراقب أو المرور المراقب أحد أساليب التحري الحديثة التي استحدثها المشرع الجزائري بموجب المادتين 02 و56 من قانون الوقاية من الفساد

[1] اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية الموقعة بفيينا في 20 ديسمبر 1988. انظر: موقع الأمانة العامة للأمم المتحدة، https://www.unodc.org.

[2] مجراب الدوادي، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق جامعة الجزائر 1 ، 2015–2016، ص 56.

ومكافحته .[1] وفقا للمادة 2فقرة ك، يعرف هذا الإجراء بأنه السماح بمرور شحنات غير مشروعة أو مشبوهة داخل الإقليم الوطني أو عبره، تحت مراقبة السلطات المختصة، بغية التحري عن الجرائم وكشف المتورطين فيها، دون أن يحدد القانون شروطه أو إجراءات تطبيقه.[2]

في وقت لاحق، جاء القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية لتوضيح كيفية تطبيق هذا الأسلوب، لكنه استخدم مصطلحا مختلفا وهو مراقبة الأشخاص أو مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات إجرامية، وذلك في سياق توسيع اختصاص ضباط الشرطة القضائية، وفقا للمادة 16مكرر من الباب الأول، رغم أن هذا الأسلوب تم استحداثه وتخصيص فصلين مستقلين له في الباب الثاني المتعلق بأساليب التحري الجديدة.

إشكالية تصنيف أساليب التحري الخاصة

كان من الأفضل للمشرع الجزائري أن يجمع جميع أساليب التحري الخاصة، مثل التسليم المراقب، الترصد الإلكتروني، والتسرب، ضمن الباب الثاني، بحيث يتم تخصيص فصل مستقل لكل تقنية تحري على حدة، مما يسهل فهم تطبيقاتها القانونية.

[1] القانون 06-01 المؤرخ في 21 محرم 1427 ه، الموافق ل 20 فبراير 2006 المتعلق بالوقاية من الفساد ومكافحته المعدل والمتمم، ج. ر. ج. ج، رقم 14 المؤرخة في 08 صفر 1427 ه الموافق ل: 08 مارس 2006 م انظر الموقع الإلكتروني للجريدة الرسمية للجمهورية الجزائرية.

[2] المادة 2 من القانون رقم 06-01 المؤرخ في 21 محرم عام 1427 الموافق 20 فبراير سنة 2006 ، المتعلق بالوقاية من الفساد ومكافحته، المعدل والمتمم.

كما جاء في المادة 56 من القانون 06-01 ما يلي: من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلي التسليم المراقب أو اتباع أساليب تحر خاصة كالترصد الإلكتروني والاختراق علي النحو المناسب وبإذن من السلطة القضائية المختصة.....

لكن الإشكال الحقيقي يظهر في المادة 16مكرر من قانون الإجراءات الجزائية، حيث يقتصر اعتماد هذا الأسلوب على الجرائم الخطيرة المنصوص عليها في المادة 16، والتي تشمل:

- جرائم المخدرات
- الجريمة المنظمة عبر الحدود الوطنية
- الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات
- تبييض الأموال
- الإرهاب
- الجرائم المرتبطة بالتشريع الخاص بالصرف

إغفال إدراج جرائم الفساد ضمن نطاق التسليم المراقب

رغم أن المادة 56 من قانون الوقاية من الفساد ومكافحته رقم 06-01 نصت على اعتماد التسليم المراقب كإحدى تقنيات التحري الجديدة، فإن المادة 16مكرر من قانون الإجراءات الجزائية لم تشر إلى إدراج جرائم الفساد ضمن الجرائم التي يطبق عليها هذا الأسلوب.

من المحتمل أن يكون هذا إغفالا تشريعيا، حيث لم يدرج المشرع جرائم الفساد ضمن نطاق المادة 16 مكرر، رغم أنها من الجرائم التي تستدعي استخدام هذه التقنية في التحري وكشف المتورطين .قد يعود هذا الإغفال إلى الموقع والفحوى العامة للمادة، والتي جاءت بأحكام جديدة لم تشمل جرائم الفساد، مما أدى إلى التباس في التطبيق واستبعاد هذه الجرائم من نطاق توسيع اختصاص ضباط الشرطة القضائية في التحري.

يعد التسليم المراقب أداة فعالة في كشف الجرائم، إلا أن عدم إدراج جرائم الفساد ضمن نطاق المادة 16مكرر يمثل قصورا تشريعيا قد يؤثر على فعالية التحري في هذه القضايا. من هنا، قد يكون من الضروري إعادة النظر في تعديل التشريع بحيث تشمل المادة 16مكرر جرائم الفساد، لضمان تكامل النظام القانوني في مكافحة الجرائم المختلفة، وخاصة الجرائم المتعلقة بالفساد الإداري.

نصت المادة 40 من الأمر رقم 05-06 المتعلق بمكافحة التهريب[1] على تعريف إجراء التسليم المراقب، حيث جاء فيها :يمكن للسلطات المختصة بمكافحة التهريب أن ترخص، بعلمها وتحت رقابتها، بمرور البضائع غير المشروعة أو المشبوهة أو السماح بخروجها أو دخولها إلى الإقليم الجزائري، وذلك بهدف البحث عن أفعال التهريب ومحاربتها، بناء على إذن من وكيل الجمهورية المختص.[2]

ويفهم من هذا النص أن التسليم المراقب هو إجراء استثنائي يباشره ضباط الشرطة القضائية تحت إشراف مباشر وبترخيص من وكيل الجمهورية، ويهدف إلى تتبع مسار شحنة ممنوعة – مهما كان نوعها – انطلاقا من مصدرها حتى نقطة الوصول، وذلك بقصد الكشف عن الشبكات الإجرامية المتورطة وأبرز العناصر الفاعلة فيها،[3] بما في ذلك القيادات المحركة والممولة لهذه الشبكات.

وتبرز التعاريف المختلفة للتسليم المراقب مجموعة من الضوابط المسبقة التي تعد ضرورية لاعتماد هذا الإجراء، من أبرزها:

---

[1]- الأمر رقم 05/06 المؤرخ في 18 رجب 1426 ه الموافق ل: 23 غشت سنة 2005 المتعلق بمكافحة التهريب، ج ر ج ج ، رقم: 59 المؤرخة في 23 رجب 1426 ه الموافق ل 28 أوت 2005 م. انظر الموقع الإلكتروني للجريدة الرسمية للجمهورية الجزائرية: .https://www.joradp.deتاريخ الاطلاع: 15/05/2025 14:36

[2]المادة 40 من الأمر: 05-06 المتعلق بمكافحة التهريب، المصدر نفسه

[3]صرياك مسعودة زرارة لخضر دور نظامي التسليم المراقب وتسليم المجرمين في تحقيق التعاون الدولي لمكافحة الفساد في الجزائر. مقال منشور بمجلة الباحث للدراسات الأكاديمية، المجلد 08 العدد 01. سنة 2021، ص 89

1. وجود معلومات دقيقة ومسبقة بحوزة الجهات المختصة، تفيد بأن هناك شحنات مشبوهة أو غير مشروعة يخطط لنقلها أو تهريبها من مكان إلى آخر، سواء داخل حدود الدولة أو عبرها إلى الخارج.

2. أن تكون السلطات المكلفة بالمكافحة على دراية تامة بوقوع الجريمة وبالتحركات المرتبطة بها، لا سيما تحركات الأشخاص المشتبه في تورطهم.

3. أن لا يقتصر الهدف من هذا الإجراء على توقيف الأشخاص الظاهرين في الجريمة فحسب، بل يتجاوز ذلك إلى الكشف عن أكبر عدد ممكن من المتورطين، وصولا إلى العناصر الأساسية المدبرة والممولة والمستفيدة من الفعل الإجرامي. [1]

ويمثل أسلوب التسليم المراقب كذلك أداة فعالة لتتبع حركة الأموال غير المشروعة، إذ يمكن السلطات من مراقبة مسار العائدات الإجرامية، سواء الناتجة عن الصفقات العمومية المشبوهة، أو رشوة الموظفين العموميين، أو الاختلاس وسرقة المال العام، وذلك حتى يتم تحديد أماكن إيداعها داخل أو خارج الوطن، خاصة في الحسابات البنكية الوطنية أو الأجنبية. [2]

ثانيا: تجميد الأموال وحجزها

تنص الفقرة الأولى من المادة 51 من القانون المتعلق بالوقاية من الفساد ومكافحته بأنه يمكن تجميد أو حجز العائدات والأموال غير المشروعة الناتجة عن ارتكاب جريمة

[1] عادل عبد العزيز السن، غسيل الأموال من منظور قانوني واقتصادي وإداري المنظمة العربية للتنمية الإدارية 2008، ص 226 227

[2] الحاج علي بدر الدين، المرجع السابق، ص 236

أو أكثر من الجرائم المنصوص عليها في القانون المتعلق بالوقاية من الفساد ومكافحته، وذلك بقرار قضائي أو بأمر من السلطة المختصة كإجراء تحفظي.[1]

[1] احسن بوسقيعة، الوجيز في القانون الجزائي العام. دار هومه للطباعة والنشر والتوزيع، الطبعة الرابعة 310 الجزائر، 2007 ، ص33.

خلاصة الفصل:

يستعرض هذا الفصل الوحدات المختصة بإجراءات البحث والتحقيق في الجرائم المعلوماتية، حيث يسلط الضوء على الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بتشكيلتها ومهامها واختصاصاتها، بالإضافة إلى دور الأجهزة الأمنية كالشرطة والدرك الوطني في ملاحقة هذه الجرائم. كما يتناول الفصل الإجراءات القانونية اللازمة للكشف عن الجرائم الإلكترونية، مشيرا إلى أهمية الجمع بين التحري الكلاسيكي والإجراءات التقنية الحديثة مثل الخبرة الفنية، وأدوات إثبات الجريمة الإلكترونية. وأخيرا، يبرز الفصل الإجراءات الجنائية المقررة لملاحقة مرتكبي الجرائم الإلكترونية، سواء على المستوى الشخصي أو المالي، مع التركيز على ضمان التوازن بين تحقيق العدالة وحماية الحقوق القانونية.

خاتمة

من خلال ما تم تناوله في هذا البحث، يتضح أن موضوع الجريمة المعلوماتية يعد من المواضيع ذات الأهمية البالغة، نظرا لما تشكله من تهديدات خطيرة تمس الأفراد والدول على حد سواء، وهو ما يستوجب دراسة دقيقة ومعمقة لهذا النوع من الجرائم المستحدثة.

وقد تبين لنا أن المشرع الجزائري، إدراكا منه لخطورة هذا النوع من الإجرام، وحرصا على سد الفراغ التشريعي الذي كان قائما، قد بادر إلى تعديل قانون العقوبات، وإصدار القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك ضمن مجهودات الدولة لمواجهة هذه الجرائم العابرة للحدود والمرتبطة بتطور الوسائل التكنولوجية.

وفي ضوء الدراسة، توصلنا إلى جملة من النتائج المهمة، نوجز أبرزها فيما يلي:

النتائج:

- لم يجمع الفقهاء على تعريف موحد وشامل للجريمة الإلكترونية، وذلك بسبب طبيعتها المعقدة والمتغيرة باستمرار، مما يجعل من الصعب وضع إطار دقيق وثابت لها.
- ورغم سعي المشرع الجزائري للتصدي لهذا النوع من الجرائم، إلا أنه لم يخصص لها إلى اليوم قانونا مستقلا ومتكاملا يضمن التحكم الصارم في مختلف أبعادها، الأمر الذي يضعف فعالية المواجهة القانونية لهذه الظاهرة المستحدثة.
- وتتميز الجريمة الإلكترونية بعدد من الخصائص التي تميزها بشكل جوهري عن الجريمة التقليدية، سواء من حيث الوسائل أو من حيث الفاعلين أو حتى من حيث طبيعة الأضرار والضحايا.
- وفي هذا السياق، يلاحظ أن النصوص القانونية الحالية، خاصة تلك المتعلقة بحماية حقوق المؤلف والحقوق المجاورة، تبقى غير كافية لمجابهة الانتهاكات التي تتعرض لها هذه الحقوق عبر شبكة الإنترنت، وهو ما يبرز قصور القوانين التقليدية أمام الجرائم الإلكترونية التي فرضتها التطورات التكنولوجية الحديثة.

التوصيات:

- تعزيز التعاون مع شركات التقنية والإنترنت من خلال إلزامها باتخاذ إجراءات أمنية ملائمة، سواء على مستوى حماية البنية التحتية والمنشآت، أو عبر تطوير أنظمة فعالة لحماية الأجهزة والبرمجيات من الهجمات الإلكترونية.
- الاستفادة من التجارب الدولية الرائدة في هذا المجال، وذلك لاكتساب الخبرات والمهارات الضرورية التي تسمح بتطوير آليات وطنية فعالة لمكافحة هذا النوع من الجرائم المستحدثة.
- الاعتماد على خبراء ومختصين قادرين على تحليل وتشخيص طبيعة الجريمة الإلكترونية، مع العمل على تكوين فرق متخصصة من عناصر الضبطية القضائية والقضاة، وتوفير الإمكانات المادية والتقنية الكفيلة بتمكينهم من أداء مهامهم بأعلى درجات الكفاءة.
- ضرورة انضمام الجزائر إلى الاتفاقيات الدولية والإقليمية ذات الصلة بمكافحة الجريمة الإلكترونية، قصد تعزيز أطر التعاون وتبادل المعلومات مع باقي الدول.
- تكثيف حملات التوعية الرقمية بين أفراد المجتمع، وتثقيف المستخدمين حول سبل حماية بياناتهم الشخصية، وتوعيتهم بخطورة الإهمال الرقمي، وما قد يترتب عليه من تهديدات لأمنهم المعلوماتي.

قائمة المراجع

قائمة المصادر والمراجع:

أولا: النصوص القانونية

- القانون رقم 06-01 المؤرخ في 21 محرم عام 1427 الموافق 20 فبراير سنة 2006 ، المتعلق بالوقاية من الفساد ومكافحته، المعدل والمتمم.
- الأمر رقم 05-06 المؤرخ في 18 رجب 1426 ه الموافق ل: 23 غشت سنة 2005 المتعلق بمكافحة التهريب، ج ر ج ج ، رقم: 59 المؤرخة في 23 رجب 1426 ه الموافق ل 28 أوت 2005 م.
- القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، صادرة بتاريخ 2009/08/16.
- القانون رقم 18-04 المؤرخ في 10 مايو 2018، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 27.

ثانيا: المراسيم:

- المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، عدد 53.
- المرسوم الرئاسي رقم 19-172، مؤرخ في 14 جوان 2019، يتعلق بالسلطات الإدارية المستقلة.

القوانين الأجنبية:

- قانون إمارة دبي رقم 02 لسنة 2002 متعلق بالمعاملات والتجارة الإلكترونية، صادر بتاريخ 12 فبراير 2002.

- القانون رقم 35 لسنة 2001، الجريدة الرسمية للمملكة الأردنية الهاشمية، عدد 4524، صادرة بتاريخ 2001/12/31، ص 6010.

ثانيا: الكتب

- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط2، 2006.
- جمال نجيمي، إثبات الجريمة على ضوء الاجتهاد دراسة مقارنة، دار هومة، الجزائر، 2011.
- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية: دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014.
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2011.
- سامي حسني الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة، 1972.
- عبد العال الديري، محمد صادق إسماعيل، الجرائم الإلكترونية، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012.
- عبد الله أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة دار النهضة العربية، القاهرة، 2000.
- عماد مجدي عبد المالك، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، مصر، 2001.
- عوض محمد عوض، قانون الإجراءات الجنائية، ج1، مؤسسة الثقافة الجامعية، 1989.
- فوزية عبد الستار، شرح قانون العقوبات – القسم العام، دار النهضة العربية، القاهرة، 1992.

- كامل السعيد، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، ط2، دار الفكر، عمان، 1983.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، 2004.
- محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، وزارة الداخلية، الأكاديمية الملكية للشرطة، البحرين، 2010.
- محمود نجيب حسني، شرح قانون العقوبات – القسم العام، ط6، دار النهضة العربية، القاهرة، 1989.
- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية – دراسة نظرية وتطبيقية، منشورات الحاتي الحقوقية، ط1، 2005.
- نبيه صالح، الوسيط في شرح مبادئ الإجراءات الجزائية، منشأة المعارف القانونية للنشر، عمان، بدون تاريخ.

ثالثا: الرسائل الجامعية

- إدريس النوازلي، موقف القضاء من الجريمة الإلكترونية، أشغال ندوة وطنية، مراكش، المغرب، ماي 2009.
- رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة ماجستير، جامعة تلمسان، 2011–2012.
- سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر، باتنة، 2012–2013.
- سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير، جامعة أبو بكر بلقايد، تلمسان، 2010–2011.
- صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، جامعة مولود معمري، تيزي وزو، 2013.

- نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، مذكرة ماجستير، جامعة النجاح الوطنية، فلسطين، 2017.
- نشناش منية، الركن المفترض في الجريمة المعلوماتية، جامعة بسكرة، 2015–2016.
- وشن لبنى، نباش مراد، دور رجال الضبطية القضائية في مكافحة الجريمة الإلكترونية، مذكرة ماستر، جامعة محمد البشير الإبراهيمي، 2021–2022.
- يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة ماستر، جامعة محمد بوضياف، المسيلة، 2016–2017.
- زيدان نبيل، دواقي يزيد، الجريمة المعلوماتية ودور الدرك الوطني، مذكرة تخرج، المدرسة العليا للقيادة والأركان، 2014–2015.
- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 2012.

رابعا: المقالات العلمية

- أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد 10، العدد 1.
- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد 5، جوان 2012.
- عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد 4، جانفي 2018.
- سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوة منتوري، قسنطينة، العدد 52، ديسمبر 2019.

- محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إليزا للبحوث والدراسات، المركز الجامعي إليزي، العدد 2، ديسمبر 2017.

خامسا: الندوات والمؤتمرات

- حفوظة الأمير عبد القادر، غرداين حسام، الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017.
- سومية عكور، الجرائم المعلوماتية وطرق مواجهتها: قراءة في المشهد القانوني والأمني، الملتقى العلمي حول الجرائم المستحدثة، كلية العلوم الاستراتيجية، الأردن، 02-04 سبتمبر 2014.
- نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المؤتمر الدولي الرابع عشر الجرائم الإلكترونية، مركز جيل البحث العلمي، طرابلس، 24-25 مارس 2017.

سادسا: المواقع الإلكترونية

- www.aitnews.com
- http://elaph.com/Web/News/10/06/2014/

المراجع الأجنبية:

- ZOUAIMIA Rachid, *Les autorités administratives indépendantes et la régulation économique en Algérie*, Édition Distribution Houma, Alger, 2005.

فهرس المحتويات

فهرس المحتويات:

Contenu

ملخص:

شهد المجتمع الجزائري، شأنه شأن باقي المجتمعات، تطورًا متسارعًا في مجال تكنولوجيا المعلومات والاتصال، ما أدى إلى بروز جرائم جديدة تُعرف بالجرائم الإلكترونية، والتي تُعد من أبرز الانعكاسات السلبية للتطور الرقمي. وتتنوع هذه الجرائم بين اختراق الحسابات الشخصية، والهجمات على الأنظمة المعلوماتية للمؤسسات الكبرى، بل وحتى استهداف الأجهزة الاستخباراتية، مما يجعلها تشكل تهديدًا فعليًا للأمن الفردي والمؤسسي على حد سواء.

ولمواجهة هذه الظاهرة، تدخل المشرّع الجزائري بإصدار جملة من النصوص القانونية الموضوعية والإجرائية، في محاولة لمواكبة هذا النوع المستحدث من الإجرام. وقد أفضى تحليل هذه الجهود إلى جملة من النتائج، أهمها تبني سياسة مزدوجة في التصدي للجرائم المعلوماتية، واستحداث قوانين خاصة تتناسب مع طبيعة هذه الجرائم. كما أوصت الدراسة بضرورة تعزيز التعاون القضائي والأمني مع الدول العربية والغربية ذات الخبرة، من أجل الاستفادة من تجاربها في التصدي الفعال للجرائم الإلكترونية.

الكلمات المفتاحية: الجريمة التقليدية ، الجريمة الإلكترونية ، التشريع الجزائري ،الثورة التكنولوجية ،وسائل الإتصال والإعلام.

Abstract

The Algerian society, like other societies, has witnessed rapid development in the field of information and communication technology, which has led to the emergence of new types of crimes known as cybercrimes. These crimes are considered among the most significant negative consequences of digital advancement. They range from hacking personal accounts to attacks on information systems of major institutions, and even targeting intelligence agencies, thus posing a real threat to both individual and institutional security.

In response to this phenomenon, the Algerian legislator has intervened by enacting a series of substantive and procedural legal texts in an attempt to keep pace with this emerging type of crime. An analysis of these efforts has led to several findings, most notably the adoption of a dual policy in combating cybercrime and the introduction of special laws that align with the complex nature of such offenses. The study also recommends strengthening judicial, security, and legislative cooperation with Arab and Western countries that possess greater expertise in combating cybercrime, in order to benefit from their advanced experiences in this field.

Keywords: traditional crime, cybercrime, Algerian legislation, technological revolution, media and communication tools.