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 الالي والأنترنت

الموسومة بـ :

مجابهة الجريمة الإلكترونية في التشريع الجزائري

إعداد الطالبين:

- **خريف محمد**
- **بروري عبد العزيز**

إشراف:

درارجة عبدالجليل

لجنة المناقشة

(اللقب والاسم)	(الرتبة)	(الصفة)
• بوجادي صليحة	أستاذ محاضر قسم –أ–	رئيسا
• درارجة عبدالجليل	أستاذ محاضر قسم –أ–	مشرفا
• بن حامة فارس	أستاذ مساعد قسم –ب–	ممتحنا

السنة الجامعية : 2025/2024

2020 — 27
ملحق بالقرار رقم ....1082..... المؤرخ في ....
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

أنا الممضي أسفله، (الطالب الأول)

السيد(ة): خريف محمد الصفة: طالب، أستاذ، باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: 109663863 والصادرة بتاريخ 2018/06/18

المسجل(ة) بكلية / معهد الحقوق قسم قانون الإعلام الآلي والأنترنت

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

عنوانها: مكافحة الجريمة الإلكترونية في التشريع الجزائري .

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

شوهد لأجل التصديق
السيد :
بطاقة التعريف الوطنية رقم :
مستخرج بتاريخ :
الصادر في :

التاريخ: 2025/06/02

توقيع المعني (ة)

KHERIF

ملحق بالقرار رقم ....1082.... المؤرخ في 2020 27

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)

أنا الممضي أسفله،

السيد(ة): بوراوي عبد العزيز الصفة: طالب. أستاذ. باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم 111276356 والصادرة بتاريخ 2016/04/26

المسجل(ة) بكلية / معهد العلوم قسم قانون الاعلام الآلي والانترنت

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

عنوانها: حماية الصورة الرقمية للمؤسسة في التشريع الجزائري

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

التاريخ: 2025/06/02

شوهد قصد التصديق
الصورة
السيد:
بطاقة التعريف الوطنية رقم:
مستخرج بتاريخ:
في:

2025 جوان 02

توقيع المعني (ة)

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة العدل حافظ الأختام
المجلس القضائي لبشار
مصلحة الحالة المدنية

حروز ذهم


بسم الله الرحمن الرحيم
الأستاذ
عبدالصادق
١٤٣٩

شكر وعرفان:

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 **درارجة عبدالجليل** 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

بالنظر إلى ما يشهده العالم المعاصر من تطورات متسارعة في مجال التكنولوجيا والمعلومات، فقد أصبحت الشبكة المعلوماتية جزءا لا يتجزأ من حياة الإنسان اليومية، بما في ذلك المؤسسات الرسمية والهيئات الحكومية والمالية، بل وحتى في أبسط البيوت والأفراد، وقد أفرز هذا التقدم ما يعرف بثورة المعلومات، التي أدخلت البشرية في عصر جديد تقوم ركائزه على التقنية والسرعة والاتصال الفوري، مما ساهم في نشأة بيئة إلكترونية عالمية نشطة، تبرم فيها صفقات مالية وتجارية كبرى، وتنجز فيها تعاملات ومعاملات تتسم بالكفاءة والسهولة.

غير أن هذا التحول الرقمي، وعلى الرغم من إيجابياته العديدة، لم يكن بمنأى عن التحديات والمخاطر، حيث رافقته ظواهر إجرامية مستحدثة باتت تهدد أمن الأفراد والمجتمعات، وعلى رأسها الجرائم الإلكترونية أو ما يعرف بجرائم السيبر كرايم، وتمثل هذه الجرائم نمطا جديدا من التعدي، يتسم بالدقة والخفاء ويستهدف المعلومة في جوهرها، سواء تعلقت بالحياة الخاصة للأفراد، أو بالمؤسسات الاقتصادية والمالية، بل وقد تمتد آثارها لتطال سيادة الدول وأمنها القومي، مما يزعزع الثقة في الوسائل التكنولوجية ويهدد مكاسب الحضارة الرقمية.

ومن هذا المنطلق، تبرز أهمية إدراك الطبيعة القانونية لهذه الجرائم، والوقوف على خصائصها وأشكالها وأبعادها المختلفة، بغية بناء وعي قانوني ومجتمعي قادر على مواجهتها، وحماية الضحايا من آثارها المدمرة، لا سيما وأن مرتكبي هذه الجرائم غالبا ما يتمتعون بدرجات عالية من الذكاء والمعرفة التقنية، مما يزيد من صعوبة الكشف عنهم ومتابعتهم بالطرق التقليدية.

إزاء هذه التحديات، وجد المشرع الجزائري نفسه مدفوعا إلى ضرورة التحرك الفوري لوضع إطار قانوني فعال لمواجهة هذه الجرائم، عبر تطوير المنظومة التشريعية

الوطنية، وعلى رأسها قانون العقوبات، واستحداث نصوص خاصة تستجيب لحجم المخاطر المستجدة، وتواكب التحولات التكنولوجية المتسارعة، وقد جاءت هذه المبادرات التشريعية تعبيرا عن إرادة الدولة في ضمان الحماية القانونية الكافية للمعاملات الإلكترونية، وصون الحقوق والحريات في البيئة الرقمية، بما يحقق التوازن بين متطلبات التطور ومقتضيات الأمن والعدالة.

أهمية الموضوع

تؤدي الأنظمة المعلوماتية دورا محوريا في مختلف مجالات الحياة، غير أن هذا التطور التقني صاحبه بروز جرائم إلكترونية خطيرة باتت تتطلب مواجهة فعالة، في ظل عجز واضح للتشريعات التقليدية عن التصدي لها، وضعف كفاءة بعض السلطات في التعامل مع تعقيداتها، الأمر الذي يستدعي ضرورة إحكام الرقابة القانونية وتعزيز آليات مكافحة هذه الجرائم للحد من آثارها المتنامية.

أهداف الدراسة :

تهدف هذه الدراسة إلى تسليط الضوء على عدد من الجوانب الأساسية المرتبطة بالجريمة المعلوماتية، من خلال التعرف على ماهية هذه الجريمة وأهداف ارتكابها، ودراسة أركانها في ظل التشريع الجزائري، بالإضافة إلى إبراز دور الهيئات المختصة بمكافحتها، واستعراض إجراءات التحقيق المعتمدة في الكشف عنها وملاحقة مرتكبيها.

أسباب اختيار الموضوع:

تعود دوافع اختيار هذا الموضوع إلى أسباب ذاتية وموضوعية، فمن الناحية الذاتية، تنبع الرغبة من اهتمام شخصي عميق بفهم الجريمة الإلكترونية وتحليل مختلف أبعادها، نظرا لخطورتها المتزايدة على الفرد والمجتمع، أما من الناحية الموضوعية، فإن تنامي

هذه الظاهرة في البيئة الجزائرية، وما تحمله من تهديد للقيم الاجتماعية والاقتصادية، يفرض دراسة معمقة لموقف المشرع الجزائري منها، من خلال تحليل النصوص العقابية والتنظيمية ذات الصلة، واستقراء مدى فعاليتها في التصدي لهذه الجرائم المستحدثة، مع إبراز السبل والآليات القانونية والمؤسساتية التي تم اعتمادها للحد منها ومكافحتها بفعالية.

صعوبات الدراسة:

وكغيره من المواضيع التي تتطلب البحث والدراسة، لم يخل هذا الموضوع من جملة من الصعوبات، لعل أبرزها تمثلت في صعوبة وضع خطة متوازنة تسمح بمعالجة دقيقة وفعالة لموضوع يحمل طابعا مزدوجا يجمع بين الجانبين القانوني والفني، وهو ما شكل تحديا حقيقيا نظرا لما يتسم به من تعقيد في المصطلحات وتداخل في المفاهيم العلمية والقانونية يصعب التحكم فيها وتوظيفها بشكل متناسق ومترابط، كما تجسدت إحدى العقبات الأساسية في شح المصادر المتخصصة، خاصة تلك التي تتناول الجريمة الإلكترونية من منظور التشريع الجزائري، إذ إن أغلب المراجع المتاحة تركز على القوانين المقارنة في الدول العربية الشقيقة، بينما تبقى المؤلفات الجزائرية في هذا المجال قليلة إن لم تكن نادرة.

الاشكالية:

ما مدى نجاعة الاليات التي سنها المشرع الجزائري لمجابهة الجريمة الالكترونية؟

الاسئلة الفرعية:

- ما مفهوم الجريمة الالكترونية؟
- ما هي أركان الجريمة الاكترونية؟
- ماهي الاليات التي سنها المشرع الجزائري لمجابهة الجريمة الالكترونية؟

المنهج المتبع :

وقد ارتكزت منهجية هذه الدراسة على منهجين رئيسيين، حيث تم اعتماد المنهج الوصفي في تحليل الجانب الفني لموضوع البحث، مع الاستعانة بالمنهج التحليلي في مراحل متعددة لدراسة القواعد والسنن القانونية والتشريعية ذات الصلة بعناصر البحث، بما يضمن فهما دقيقا ومتوازنا للمضمون القانوني والفني معا.

تم تقسيم الدراسة إلى فصلين على النحو التالي:

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية

الفصل الثاني: آليات مجابهة الجريمة الإلكترونية

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية

شهد العالم في العقود الأخيرة ثورة رقمية هائلة أثرت بشكل جذري على مختلف مجالات الحياة، حيث أضحى الفضاء السيبراني مجالا واسعا للتواصل، والتعاملات التجارية، والإدارية، والتعليمية وغيرها. غير أن هذا التطور التكنولوجي، وعلى الرغم من إيجابياته المتعددة، أفرز أشكالا جديدة من الإجرام عرفت بـــالجرائم الإلكترونية، وهي جرائم تتجاوز الحدود المادية والتقليدية للجريمة، مما يطرح تحديات قانونية وأمنية معقدة.

ولفهم هذا النوع من الجرائم، لا بد أولا من تحديد الإطار المفاهيمي لها، وذلك من خلال الوقوف على تعريفها الفقهي والتمييز بينها وبين الجرائم التقليدية، ثم تسليط الضوء على خصائصها التي تميزها عن غيرها. كما يتطلب الأمر التعرف على أنواعها المختلفة، سواء تلك التي ترتكب بواسطة النظام المعلوماتي أو التي ترتكب عليه، إضافة إلى بيان أركانها القانونية وأخيرا، نعالج الإطار الجزائي الذي يؤسس لمجابهة هذه الجرائم، من حيث مبدأ الشرعية الجنائية، والخصوصيات المرتبطة بالركنين المادي والمعنوي في سياق الجريمة المعلوماتية.

المبحث الأول: مفهوم الجريمة الالكترونية

يشكل تحديد مفهوم الجريمة الإلكترونية خطوة أساسية لفهم هذا النمط الجديد من الإجرام، نظرا لحداثته وتشعب صوره واختلافه الجوهري عن الجرائم التقليدية. وفي هذا السياق، يستعرض هذا المبحث الإطار المفاهيمي للجريمة الإلكترونية من خلال التطرق أولا إلى مختلف التعريفات الفقهية التي حاولت ضبط هذا المفهوم، ثم التعرف على أهم الخصائص التي تميز هذه الجريمة من حيث وسلتها ومجالها ومرتكبيها.

المطلب الاول: تعريف الجريمة الإلكترونية

أفرز التطور التكنولوجي المتسارع نوعا جديدا من الجرائم، بات يشكل تهديدا حقيقيا للأفراد والمؤسسات على حد سواء، وهو ما يعرف بالجريمة الإلكترونية. ونظرا لحداثة هذا المفهوم وغموض حدوده القانونية، فقد حاول الفقه القانوني تقديم تعريفات متعددة لهذا النمط الإجرامي، في محاولة لتأصيله وضبط معالمه، بما يساعد على تمييزه عن غيره من الجرائم التقليدية.

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية

يقصد بهذا النوع من الجرائم تلك التي ترتكب باستخدام الحاسوب وما يحتويه من بيانات، فهي جرائم يكون موضوعها المعطيات أثناء معالجتها آليا. وبناء على ذلك، فإن أي معلومة يتم جمعها أو تخزينها أو نقلها أو نسخها إلكترونيا بصورة غير قانونية تعد جريمة معلوماتية.

تعرف بأنها: أي فعل غير مشروع يؤدي إلى الإضرار بالبيانات والمعلومات المخزنة في الأنظمة الحاسوبية[1].

من الناحية التقنية، لا تحدث الجريمة الإلكترونية إلا بوجود أجهزة كمبيوتر تحتوي على معلومات، سواء كانت متصلة بشبكة اتصالية أم لا. يمكن أن تقع الجريمة المعلوماتية أثناء انتقال البيانات أو حتى في حالتها الثابتة. وفقا لمكتب تقييم التقنية بالولايات المتحدة الأمريكية، تعرف هذه الجريمة بأنها: الجريمة التي يكون للبيانات الكمبيوترية والبرامج المعلوماتية دور أساسي فيها. [2]

كما عرّفت عند آخرين هذه الظاهرة بأنها كل سلوك غير مشروع أو غير مسموح به يهدف إلى نسخ، تعديل، حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي يتم تحويلها من خلاله. في حين عرفتها خبراء منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة بأنها كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها.

ويستند هذا التعريف إلى معيارين أساسيين: الأول يتمثل في وصف طبيعة السلوك، بينما الثاني يربط هذا السلوك بعملية المعالجة الآلية للبيانات.

يؤخذ على هذا التعريف أنه يستبعد عددا كبيرا من الأفعال غير المشروعة التي يستخدم فيها الحاسوب كأداة رئيسية لارتكاب الجريمة، مثل جرائم الاحتيال الإلكتروني. وفي هذا السياق، اعتمدت وزارة العدل الأمريكية تعريفا للجريمة الإلكترونية في تقرير صدر عام 1989، عرّفت فيه هذه الجريمة بأنها: كل فعل غير مشروع يتطلب لتنفيذه

[1] عبد الله هبد العزيز يوسف، الظواهر الاجرامية المستحدثة وسبل مواجهتها، التقنية والجرائم المستحدثة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ص 198.

[2] عبد الله عبد الكريم، جرائم المعلوماتية والأنترنت، الجرائم الالكترونية، منشورات الحلبي الحقوقية، بيروت، 2011، ص 15.

درجة عالية من الإلمام بتكنولوجيا الحواسيب، كما يحتاج إلى هذا المستوى من المعرفة أيضا في مراحل ملاحقته القانونية وإثباته.[1]

الفرع الثاني: التعريف القانوني

صدر أول تشريع جزائري خاص بجرائم المعلومات عام 2001، حيث شملت المواد 144 مكرر 1 و144 مكرر 2 و164 من قانون العقوبات تجريم القذف والسب والإهانة باستخدام الوسائل الإلكترونية والمعلوماتية. وفي عام 2004، صدر قانون جديد يتناول الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وذلك من خلال المواد 394 مكرر إلى 394 مكرر 7، التي جاءت تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

صدر القانون رقم 09-04 الذي يتضمن القواعد الخاصة بالجرائم المتعلقة بالإعلام والاتصال وآليات مكافحتها. وقد شمل هذا القانون جميع الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات كما حددها قانون العقوبات. كما جرّم كل فعل يشكل اعتداء على هذه الأنظمة، بغض النظر عن طبيعة المصالح التي قد تتأثر جراء هذه الأفعال، سواء كانت مصالح اقتصادية، أمنية، أو مالية. ويؤكد القانون على أهمية حماية النظام المعلوماتي بحد ذاته كقيمة مستقلة.[2]

من خلال التعاريف السابقة للجريمة الإلكترونية في التشريع الجزائري، يمكن استخلاص موقف المشرع من هذا النوع من الجرائم، حيث يتجلى هذا الموقف في إدراكه أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أسفرا عن ظهور أنماط جديدة من

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

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

الإجرام. وقد دفع ذلك العديد من الدول إلى سن تشريعات خاصة لمعاقبة هذا النوع من الجرائم، في محاولة منها لتوفير حماية قانونية للأنظمة المعلوماتية وطرق المعالجة الآلية للبيانات. وفي هذا الإطار، قام المشرع الجزائري بتعديل قانون العقوبات لسد الفراغ التشريعي القائم، وذلك من خلال القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، الذي عدل وأتم الأمر رقم 66-156 المتضمن قانون العقوبات، حيث أدرج القسم السابع مكررا تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات. ويلاحظ أن المشرع الجزائري استخدم مصطلحا خاصا للدلالة على المعلومات والنظام الذي تتضمنه، ما جعله يخرج من نطاق التجريم تلك الأفعال التي يستخدم فيها النظام المعلوماتي كوسيلة لارتكاب الجريمة، مقتصرا بذلك على الأفعال التي تعد اعتداء مباشرا على النظام المعلوماتي نفسه، أي تلك التي يكون فيها النظام المعلوماتي هو محل الجريمة.

قدّر المشرع الجزائري من خلال هذا التدخل، أن جوهر المعلوماتية يكمن في المعطيات التي تدخل إلى الحاسب الآلي، حيث تعالج وتخزَّن لتتحول إلى معلومات، ولذلك حرص على حماية هذه المعطيات من عدة جوانب. وفي مرحلة لاحقة، اختار المشرع الجزائري استخدام مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال للتعبير عن الجريمة المعلوماتية، وذلك بموجب القانون رقم 09/04 المتعلق بمكافحة هذا النوع من الجرائم، وقد تناول المشرع الجزائري تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات في المادة 2 من القانون ذاته، كما قام بتجريم الأفعال الماسة بهذه الأنظمة في المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات[1].

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

المطلب الثاني: خصائص الجريمة الإلكترونية

جرائم المعلوماتية هي نتاج مباشر لتطور تقنية المعلومات، حيث ترتبط بها بشكل وثيق وتعتمد عليها في وجودها. هذا الارتباط منحها طابعا قانونيا مميزا يفرقها عن الجرائم التقليدية أو المستحدثة، من خلال مجموعة من الخصائص التي قد تتشابه في بعض جوانبها مع أنواع أخرى من الجرائم، ومع ذلك فإن طبيعة الأفعال الإجرامية في الجرائم المعلوماتية تختلف جوهريا عن الجرائم التقليدية، مما يمنحها خصوصية فريدة وغير اعتيادية[1].

تعتبر متابعة جرائم الحاسب الآلي والإنترنت وكشفها من الأمور بالغة الصعوبة، حيث إن هذه الجرائم غالبا لا تترك أي أثر مادي يمكن تتبعه. فعلى عكس الجرائم التقليدية التي قد تفقد فيها أموال أو ممتلكات، فإن جرائم الحاسب الآلي تترك فقط تغييرات في الأرقام أو البيانات المسجلة، والتي قد لا يتم اكتشافها إلا بالصدفة، وربما بعد مرور فترة طويلة على ارتكابها. كما أن عدد الجرائم غير المكتشفة يفوق بكثير تلك التي تم الكشف عنها.

1. وتتمثل صعوبة إثبات هذه الجرائم في خمسة عوامل رئيسية:
2. عدم ترك هذه الجرائم لأي أثر مادي يمكن تتبعه بعد التنفيذ.
3. وجود صعوبة تقنية في الاحتفاظ بأي آثار رقمية قد تكون متبقية.
4. الحاجة إلى خبرة تقنية متخصصة، مما يجعل من الصعب على المحققين التقليديين التعامل مع مثل هذه الجرائم.
5. اعتماد مرتكبي هذه الجرائم على أساليب الخداع والتضليل لإخفاء هوياتهم وطريقة تنفيذهم لها.

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

6. استخدام مرتكبيها لمستويات عالية من الذكاء والمهارة التقنية في التخطيط والتنفيذ.

- الجريمة المعلوماتية، بفضل ارتباطها الوثيق بالحواسيب وشبكات الإنترنت، تتسم بمجموعة من الخصائص والمميزات التي تميزها عن الجرائم التقليدية، وتشمل هذه الخصائص:
- تعد الجرائم المعلوماتية من الجرائم التي ترتكب عبر شبكة الإنترنت، والتي تمثل الرابط الأساسي بين مختلف الأهداف المحتملة لهذه الجرائم، مثل البنوك والشركات وغيرها من الجهات التي غالبا ما تكون ضحايا لها.
- كما تتميز الجريمة المعلوماتية بكونها جريمة عابرة للحدود، إذ إن المجتمع المعلوماتي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح يعمل من خلال شبكات تتجاوز الزمان والمكان دون أن تقف عند حواجز أو قيود جغرافية. وهذا ما يجعل مسرح الجريمة المعلوماتية يتجاوز النطاق المحلي ليأخذ طابعا عالميا، مما يثير إشكاليات متعددة، أبرزها تحديد الدولة المختصة قضائيا، واختيار القانون الواجب التطبيق، إضافة إلى التعقيدات المرتبطة بإجراءات الملاحقة القضائية وغيرها من التحديات المرتبطة بالجرائم العابرة للحدود.[1]
- يعد إثبات الجريمة الإلكترونية أمرا بالغ الصعوبة نظرا لطبيعتها السرية وغياب أي آثار ملموسة للأفعال الإجرامية أثناء تنفيذها، حيث يتم تداول المعلومات إلكترونيا دون ترك دليل مادي واضح. بالإضافة إلى ذلك، غالبا ما يتردد مجتمع الأعمال في الإبلاغ عن هذه الجرائم تفاديا لتضرر السمعة وزعزعة الثقة في كفاءة المؤسسات المتضررة. كما أن إمكانية تدمير الأدلة الرقمية التي يمكن استخدامها

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

للإثبات في غضون أجزاء من الثانية تزيد من تعقيد عملية كشف هذه الجرائم وملاحقتها قانونيا.[1]

- الخسائر المالية الناجمة عن الجرائم المعلوماتية تتجاوز بكثير تلك الناتجة عن الجرائم التقليدية، ووفقا لتقارير شركة انتل سكيوريتي، المتخصصة في حماية المعلومات، تقدّر الخسائر السنوية للشركات العالمية بـــ 400 مليار دولار، بينما تشير تقديرات أخرى إلى أن الهجمات الإلكترونية باتت صناعة مزدهرة بقيمة تتراوح بين 2 و3 تريليون دولار سنويا، وهو ما يمثل نسبة 15% إلى 20% من إجمالي القيمة الاقتصادية المولدة عبر الإنترنت، [2] تكبدت إحدى الشركات البريطانية خسائر تقدّر بـــ 1.3 مليار دولار نتيجة هجوم إلكتروني واحد، كما خسر مصرفان في منطقة الخليج ما يقارب 45 مليون دولار خلال ساعات معدودة، في حين أعلنت الهند عن اختراق 308,371 موقعا إلكترونيا في الفترة ما بين عامي 2011 و2013.[3]
- تكاد الصورة التقليدية للمجرم أن تتلاشى في سياق الجرائم المعلوماتية، بل على العكس، غالبا ما ينتمي مرتكبو هذا النوع من الجرائم إلى فئات اجتماعية عالية مقارنة بالمجرمين التقليديين، ونادرا ما يكونون من محترفي الإجرام أو من أصحاب السوابق. كما أن النظرة العامة إليهم لا تتطابق مع المفهوم التقليدي

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

[2] إنتل سكيوريتي، خسائر قطاعات الأعمال من الهجمات الإلكترونية تصل إلى 400 مليار دولار سنويا، البوابة العربية للأخبار التقنية، www.aitnews.com، أطلع عليها بتاريخ 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/، أطلع عليها بتاريخ 2025/03/16.

للمجرم، وذلك لأن الدوافع والعوامل المؤدية إلى ارتكاب الجريمة المعلوماتية تختلف بشكل كبير عن تلك التي تقف وراء الجرائم التقليدية.[1]

- قلة الإبلاغ عن الجرائم المعلوماتية تعود إلى عاملين رئيسيين. الأول هو الخوف من التشهير، حيث يفضل العديد من الضحايا والمؤسسات تجنب الكشف عن تعرضهم لهذه الجرائم حفاظا على سمعتهم. لهذا السبب، يتم اكتشاف معظم جرائم الإنترنت بالصدفة أو بعد مرور فترة طويلة على وقوعها. أما العامل الثاني، فهو عدم إدراك الضحية لحدوث الجريمة من الأساس، مما يعني أن عدد الجرائم غير المكتشفة يفوق بكثير عدد الجرائم التي يتم الكشف عنها.[2]

الجريمة الإلكترونية تعد واحدة من أحدث أشكال الجرائم، حيث إن مسرحها هو العالم الافتراضي الذي لا يمكن لمسه أو رؤيته بشكل مباشر، مما يجعلها بعيدة كل البعد عن السمات التقليدية المرتبطة بالجرائم المعتادة. تتميز هذه الجرائم بأنها عابرة للحدود، ينفذها مجرمون بارعون يتمتعون بذكاء عالي ومهارات تقنية متقدمة. هذا الواقع يؤدي إلى تشتيت الجهود الدولية المبذولة في تتبع هذه الجرائم أو التحري عنها، فضلا عن صعوبة الوصول إلى هوية مرتكبيها الحقيقيين.

المبحث الثاني: أنواع الجرائم الإلكترونية ومجابهتها جزائيا

مع تزايد الاعتماد على النظم المعلوماتية في مختلف مجالات الحياة، تعددت صور الجريمة الإلكترونية وتطورت أساليب ارتكابها، مما أفرز أنماطا جديدة من الجرائم، منها ما يرتكب بوساطة هذه الأنظمة، ومنها ما يوجه ضدها مباشرة. كما أن تحديد الأركان القانونية لهذه الجرائم، لا سيما الركن المادي والمعنوي، يمثل خطوة أساسية في فهم

[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 19.18

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

طبيعتها وتحديد المسؤولية الجنائية عنها. ومن هنا، يهدف هذا المبحث إلى استعراض التصنيفات المختلفة للجرائم الإلكترونية وبيان أركانها، مع التركيز على الإشكاليات التي تطرحها على المستوى القانوني.

المطلب الأول: أنواع الجرائم الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة التي أثار تصنيفها جدلا واسعا في الفقه، حيث تعددت التسميات واختلفت التقسيمات، دون أن تراعي معظمها الخصائص المميزة لهذا النوع من الجرائم وموضوعها. ويكمن أبرز ما يميز الجرائم الإلكترونية عن غيرها في أنها تستهدف الكيانات المعنوية للحاسب الآلي، وترتكب باستخدام جهاز إلكتروني، في حين أن الأفعال التي تستهدف الكيانات المادية للحاسب تعد من صور الجرائم التقليدية.

ويعزى اختلاف الفقه في تصنيف الجرائم الإلكترونية إلى طبيعتها المتغيرة وظهور أنماط جديدة منها باستمرار، إذ لا يمكن حصرها أو الإحاطة بجميع أشكالها وصورها، فهي في تجدد دائم. فمع كل وسيلة جديدة لاستخدام الحاسوب أو الإنترنت، تظهر جريمة إلكترونية جديدة ترتبط بها. لم يتوصل الفقهاء إلى معيار موحد لتصنيف الجرائم الإلكترونية، وذلك بسبب تنوع هذه الجرائم وتطورها السريع. فقد اعتمد بعضهم تصنيفها استنادا إلى وسيلة ارتكاب الجريمة، بينما اعتمد آخرون على أساس محل ارتكاب الجريمة. ومن هذا المنطلق، يمكن تقسيم الجرائم الإلكترونية إلى عدة أنواع. [1]

الفرع الأول : الجرائم الواقعة بواسطة النظام المعلوماتي

[1] حفوظة الأمير عبد القادر و غرداين حسام الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 93

يعد الحاسب الآلي في هذا النوع من الجرائم أداة لتسهيل الوصول إلى النتيجة الإجرامية وزيادة حجمها، حيث يسعى الجاني من خلالها إلى تحقيق ربح مادي بطرق غير مشروعة. في هذه الحالة، يستخدم النظام المعلوماتي أو برامجه كوسيلة لتنفيذ الجريمة. وتنقسم هذه الجرائم بدورها إلى عدة أنواع.

أولا: الجرائم الإلكترونية الواقعة على الأشخاص:

تتمتع الحياة الشخصية بخصوصية وحماية لا يجوز لأي شخص انتهاكها، ومن أمثلة ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين وغيرهم من المهنيين، وقد ترتكب هذه الجريمة عبر الاطلاع غير المشروع على البيانات والمعلومات الشخصية أو تسجيل المكالمات والفيديوهات أو مراقبة الأفراد دون إذن.

أما فيما يتعلق بجريمة نشر المواد الإباحية، فإن الركن المادي لها يتمثل في السلوك الذي ينتهجه الفاعل، حيث يقوم بإنشاء صفحات تحتوي على مواد مخلة بالآداب العامة ونشرها عبر الإنترنت. بينما الركن المعنوي يتعلق بالنية والقصد الجنائي، إذ يكون الجاني مدركا لما يفعل ويملك إرادة نشر تلك المواد عن قصد.

ثانيا: الجرائم الإلكترونية الواقعة على الأموال

مع ظهور شبكة الإنترنت، شهدت مختلف المجالات تطورات ملحوظة، حيث أصبحت معظم المعاملات التجارية تتم عبر هذه الشبكة، مثل عمليات البيع والشراء. وقد رافق ذلك تطور وسائل الدفع والتسوية المالية، التي أصبحت جزءا لا غنى عنه في هذه العمليات. وفي ظل هذا التداول المالي المتنامي عبر الإنترنت، استغل بعض المجرمين الفرصة للقيام بأعمال غير قانونية تستهدف هذه المعاملات. ومن بين الأساليب التي ابتكرت لهذا

الغرض: السطو الإلكتروني، سرقة الأموال، التحويل غير المشروع للأموال عبر الإنترنت، وقرصنة بيانات البطاقات الممغنطة.[1]

في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية وما نتج عن ذلك من تطور في وسائل الدفع والوفاء، ومع تزايد التداول المالي عبر الإنترنت، أصبحت هذه المعاملات عرضة لمختلف أنواع الجرائم، بما في ذلك:

- الاستيلاء على أرقام بطاقات الائتمان والتحويلات الإلكترونية غير المشروعة.
- القمار وغسيل الأموال عبر الإنترنت.
- جريمة السرقة والسطو على أموال البنوك.
- تجارة المخدرات عبر الإنترنت.[2]

ثالثا: الجرائم الإلكترونية الواقعة على أمن الدولة

استغلت العديد من الجماعات المتطرفة الطبيعة الاتصالية للإنترنت لنشر معتقداتها وأفكارها، بل تجاوز الأمر ذلك إلى تنفيذ ممارسات تهدد أمن الدول المستهدفة، خاصة في مجالات الإرهاب والجريمة المنظمة، حيث أصبح الإنترنت وسيلة لارتكاب جرائم خطيرة بحق المجتمعات والدول. والأخطر من ذلك، أن الإنترنت أتاح لبعض الدول فرصة التجسس على دول أخرى من خلال الاطلاع على أسرارها العسكرية والاقتصادية، خصوصا في الدول التي تشهد نزاعات. كما يعد المساس بالأمن الفكري من أخطر

[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 و غرداين حسام، مرجع سابق، ص 93.

الجرائم المرتكبة عبر الإنترنت، حيث يوفر الإنترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها، مما يسهل خلق حالة من الفوضى. [1]

الفرع الثاني : الجرائم الواقعة على النظام المعلوماتي

الجرائم المعلوماتية تتنوع بين تلك التي تستخدم فيها الأنظمة المعلوماتية كأداة لارتكاب الجريمة، وتلك التي تستهدف مباشرة مكونات النظام المعلوماتي، سواء كانت مكونات مادية، برمجيات، أو البيانات والمعلومات المخزنة داخله.

أولا: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

يقصد بالمكونات المادية للنظام المعلوماتي الأجهزة والمعدات المرتبطة به والتي تستخدم في تشغيله، مثل الأسطوانات والشرائط والكابلات. وبسبب الطبيعة المادية لهذه المعدات، فإن الجرائم التي تستهدفها غالبا ما تكون تقليدية، مثل السرقة، خيانة الأمانة، الإتلاف العمدي، الإحراق، أو العبث بمفاتيح التشغيل، مما يؤدي إلى خسائر كبيرة. وقد وقع هذا النوع من الجرائم في فرنسا، حيث أسفر عن إتلاف معدات مؤسسة كبيرة ومتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية، وقدرت الخسائر بحوالي 5 ملايين فرنك فرنسي.

ثانيا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

تعد هذه الصورة بلا شك من أكثر الصور انتشارا وخطورة، حيث يتم من خلالها استخدام الاحتيال لإدخال بيانات في أنظمة المعالجة الآلية للمعطيات، أو إتلافها، أو حذفها، أو تعديل البيانات الموجودة فيها. [1]

[1] ناصر محمد البقهي، اثر التحويل مجتمع معلوماتي على 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 جمادى الأولى 1430 هـ. ص 18.

عالج المشرع الجزائري هذا النوع من الجرائم من خلال نص المادة 394 مكرر من قانون العقوبات، التي تنص على معاقبة كل من أدخل بطرق احتيالية معطيات في نظام المعالجة الآلية، أو قام بإزالة أو تعديل معطيات يتضمنها النظام ذاته باستخدام الغش. وفقا لهذا النص، تفرض عقوبة الحبس لمدة تتراوح بين ستة (6) أشهر وثلاث (3) سنوات، بالإضافة إلى غرامة مالية تتراوح بين 5000.00 دينار جزائري و20.000.00 دينار جزائري.

ولأجل تحليل عناصر هذه الجريمة ومعالجتها، يتعين أولا تحديد مفهوم الإتلاف والوسائل التي يتم بواسطتها تحقيق هذا الإتلاف.

يعرف البعض الإتلاف على أنه الفعل الذي يؤدي إلى جعل الشيء غير صالح للاستخدام أو إعدام صلاحيته أو تعطيله، سواء بشكل كامل أو جزئي. كما يقصد بالإتلاف أيضا تدمير مادة الشيء أو هلاكها تماما، مما يؤدي إلى توقفه عن أداء وظيفته، حتى وإن لم تفنى مادته بشكل كامل. ويصبح الشيء غير صالح للاستخدام عندما يفقد القدرة على أداء وظيفته المخصصة له بأكمل وجه.

وفيما يتعلق بإتلاف برامج الحاسوب الآلي ومعلوماته، فإن ذلك يعني محو أو تدمير تعليمات البرامج والبيانات، وهو ما يعرف بتدمير نظم المعلومات. وعادة ما لا يكون الهدف من هذا الاعتداء هو تحقيق فائدة مالية للفاعل، بل يكمن في إعاقة عمل نظام المعلومات فقط.

استنادا إلى هذه التعريفات، يمكن القول إن الإتلاف لا يقتصر على التأثير على مادة الشيء فقط، بل يتحقق أيضا في حال حدوث انتقاص من قيمته الاقتصادية. وبالتالي، فإن

[1] 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، ص 12.

الحكمة من الإتلاف ليست متعلقة فقط بتعرض مادة الشيء، بل تكمن العبرة في مدى تأثير الفعل على قيمته المالية. فالفعل الذي يؤدي إلى فقدان الشيء لقيمته المالية أو التسبب في انتقاص منها هو الذي يتحقق من خلاله الاعتداء الذي يعاقب عليه القانون، باعتبار أن الفعل قد أثر في أهمية الشيء بالنسبة لمالكه.

لتوضيح مدلول الإتلاف، استخدم المشرع الجزائري عدة تعابير مثل أدخل، أزال، وعدل. ورغم أن لهذه التعابير دلالات خاصة، إلا أنها تندرج تحت مفهوم الإتلاف، وهو ما أقرته بعض التشريعات المقارنة، لا سيما التشريع الفرنسي. وبالتالي، يمكن القول أن المشرع الجزائري قد ذكر هذه الصور التي يتحقق بها الإتلاف على سبيل المثال لا الحصر، وبمعنى آخر يمكن أن يتحقق الإتلاف بطرق أخرى لم يذكرها المشرع الجزائري في قانون العقوبات.

في هذا السياق، الإتلاف يعني التدمير أو الإضرار بالجوانب البرمجية والمعلوماتية للحواسيب، التي أصبحت ذات قيمة اقتصادية عالية. هذا النوع من الإتلاف يؤدي إلى فقدان البرامج والبيانات لقيمتها وفائدتها. [1]

ثالثا: الجرائم الواقعة على البرامج الإلكترونية

تتفرع هذه الجرائم إلى تلك التي تستهدف البرامج التطبيقية، حيث يتم أولا تحديد البرنامج المستهدف ثم التلاعب به أو تعديله. ومن الأمثلة على ذلك ما قام به أحد المبرمجين العاملين في بنوك أمريكية، حيث قام بتعديل برنامج بإضافة دولار واحد من كل حساب يتجاوز رصيده عشرة دولارات. وقام بتوجيه هذه المبالغ الزائدة إلى حساب خاص به، أطلق عليه اسم.zzwick

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

تشمل هذه الجرائم أيضا الأفعال التي تستهدف برامج التشغيل، وهي البرامج المسؤولة عن إدارة وتشغيل النظام المعلوماتي وتنظيم ترتيب عملياته. وتتحقق هذه الجريمة من خلال إدخال تعليمات إضافية إلى برنامج التشغيل، تمكن الجاني من الوصول إلى كافة البيانات التي يحتوي عليها النظام عبر شيفرة خاصة. ومن الأمثلة على ذلك: تصميم برنامج وهمي يستخدم كوسيلة لتنفيذ الجريمة. ومن أبرز الحالات الواقعية على ذلك، ما قامت به إحدى شركات التأمين الأمريكية في مدينة لوس أنجلوس، حيث عمد مبرمجها إلى تصميم برنامج يقوم بإنشاء وثائق تأمين لأشخاص غير حقيقيين بلغ عددهم 46,000 شخص، وذلك بهدف تمكين الشركة من الحصول على عمولات من اتحاد شركات التأمين.

المطلب الثاني: المجابهة الجزائية للجريمة الالكترونية (التجريم والعقاب)

لقد أحدث الإجرام الإلكتروني تحولا كبيرا في مجال التجريم والعقاب والإجراءات الجنائية، الأمر الذي استدعى ضرورة وضع أطر قانونية جديدة تتناسب مع هذا الواقع المستجد، أو إدخال تعديلات على القوانين القائمة بما يواكب التطورات الراهنة. وقد تحقق ذلك من خلال سن نصوص جزائية جديدة تهدف إلى حماية الأنظمة المعلوماتية، وردع أي تجاوزات أو انتهاكات في استخدامها، سواء على المستوى المحلي أو الدولي.

الإجرام المعلوماتي يمثل نوعا خاصا من الجرائم الذي يتسم بطابع التطور المستمر، مما جعل النصوص العقابية عاجزة عن استيعاب جميع صوره وأشكاله. ومع ذلك، فإن هذا لا يمنع من إمكانية توسيع نطاق التجريم والعقاب ليشمل المزيد من أبعاد وصور الإجرام المعلوماتي[1]، لقد أفرزت هذه الجرائم إشكالية تتعلق بمدى ملاءمة النصوص القانونية التقليدية مع الطبيعة الخاصة للجريمة المعلوماتية المستحدثة، إذ تعد

[1] نور الدين الواهلي، الاختصاص في الجريمة الإلكتورنية، سلسلة ندوات، محكمة الإستئناف بالرباط مطبعة الأمنية العدد07، ص117.

الجريمة المعلوماتية ظاهرة إجرامية متميزة بطبيعتها، ترتبط ارتباطا وثيقا بالقانون الجنائي المعلوماتي.

الفرع الأول: مبدأ الشرعية الجنائية في المجال المعلوماتي:

يشكل نظام المعالجة الآلية للبيانات الشرط الأساسي لجميع الجرائم المعلوماتية بموجب التشريع الفرنسي، بدون هذا النظام يستحيل البحث عن أي عنصر من عناصر الجريمة، ويعد هذا الشرط ضروريا لقيام أي جريمة معلوماتية.

مبدأ الشرعية الجنائية هو الضمان الرئيسي للحرية ويمنع المتابعة القضائية في غياب النص القانوني الذي يجرم الفعل، يكتسب هذا المبدأ أهمية خاصة في مجال الجرائم المعلوماتية، حيث يتعزز دوره في ضمان عدم المساس بالحريات دون سند قانوني واضح[1]، السبب في ذلك يعود إلى حداثة هذا النشاط، إلى جانب وجود بعض الحالات التي لم يتناولها المشرع الجزائري بنصوص خاصة تجرمها، بخلاف بعض التشريعات الأخرى التي عالجتها بشكل صريح.

سنتناول في المقام الأول الركن الشرعي للجريمة المعلوماتية، ثم نتوسع في دراسة الركنين المادي والمعنوي لها في المقام الثاني.

أولا: الركن الشرعي

يعد تجريم الأفعال وفرض العقوبات عليها من أخطر الصلاحيات التي تمارسها السلطة التشريعية، نظرا لما ينطوي عليه ذلك من مساس بحرية الأفراد والمجتمع. ويستند مبدأ الشرعية إلى الدستور المعدل لسنة 2016، بالإضافة إلى ما ورد في المادة الأولى

[1] المادة 01 من قانون العقوبات رقم 04-05، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم القانون العقوبات .

من قانون العقوبات لا جريمة ولا عقوبة ولا تدابير أمن إلا بنص، ومع ذلك، فإن مبدأ شرعية الجرائم والعقوبات يظل الركيزة الأساسية التي يبنى عليها النظام الجنائي[1].

يكتسب الإجرام المعلوماتي في الوقت الحاضر أهمية كبرى من الناحية السياسية. فمن جهة، يلعب دورا محوريا في تحديد نطاق حرية الأفراد ومدى تمتعهم بها، ومن جهة أخرى، يعمل على تقليص صلاحيات القاضي فيما يتعلق بالقضايا المرتبطة بالمجال المعلوماتي. وقد أدت العديد من الأسباب إلى عدم تجريم بعض الأفعال التي قد تنتهك حقوق الأفراد وحرياتهم، ومن بين هذه الأسباب:

1- سهولة إخفاء الجريمة المعلوماتية

تتميز الجرائم المعلوماتية بالدقة في التنفيذ وإمكانية إخفاء آثارها بسهولة، دون الحاجة إلى جهد بدني ظاهر. فهي من الجرائم التي يسهل طمس معالمها وإخفاء أدواتها، وربما لا يتطلب الأمر أكثر من ضغطة زر واحدة. كما أن نقص الخبرة لدى جهات إنفاذ القانون، مثل الشرطة والنيابة العامة والقضاء في المجال المعلوماتي، يزيد من تعقيد التعامل مع هذه الجرائم. وبالنظر إلى التطور والتعقيد الذي تتميز به الجرائم المعلوماتية، فإن اكتشافها والتعرف على مرتكبيها يستلزم مستوى عالٍ من التطور، الدقة، والخبرة في المجال الرقمي.

2-صعوبة الوصول إلى أغلب مرتكبي الجرائم الالكترونية:

كما أشرنا سابقا، فإن مرتكبي الجريمة المعلوماتية يتميزون بدرجة عالية من الذكاء، وتنفذ أفعالهم بدقة متناهية، الأمر الذي يجعلهم لا يتركون وراءهم أي أثر أو دليل يمكن أن يقود إلى كشف هويتهم أو الوصول إليهم.

[1] الإتفاقية الدولية حول الإجرام المعلوماتي أبرمت بتاريخ 20/11/2001، من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 22/11/2001 .

3-صعوبة الإثبات:

ويعزى ذلك إلى الطبيعة الخاصة للدليل في الجرائم المعلوماتية، إذ لا يكون دليلا ماديا ملموسا يسهل الوصول إليه أو الإحاطة به. ففي كثير من الحالات، يعمد المجرم المعلوماتي إلى ترك شفرات وكلمات مرور معقدة يستحيل اختراقها، كما يكون بمقدوره في أحيان أخرى محو الدليل بكل سهولة، مما يزيد من صعوبة جمع الأدلة وإثبات الجريمة.

أدى الفراغ التشريعي إلى عدم تجريم بعض الأفعال الإلكترونية الحديثة، ومن بين النماذج البارزة لذلك: تقنية التقاط البيانات عبر الحقل المغناطيسي، وفيروس البريد الإلكتروني. فالتقنية الأولى تقوم على استغلال الحقل المغناطيسي المحيط بالحاسوب لالتقاط المعلومات المخزنة فيه، باستخدام أجهزة خاصة تختلف عن الوسائل التقليدية للولوج إلى النظام، وقد اعتبرتها بعض التشريعات الدولية والمقارنة – كالسعودية والإمارات – جريمة مستقلة. أما فيروس البريد الإلكتروني، فقد تم تجريمه، نظرا لكونه يتسلل إلى الأنظمة عبر رسائل مجهولة المصدر، ثم يقوم بنسخ نفسه وتخريب البيانات، وينتقل إلى باقي الأجهزة المتصلة بالشبكة، مما يشكل تهديدا خطيرا لأمن المعالجة الآلية للمعطيات.

الفرع الثاني: توسيع نطاق الركن المادي والمعنوي للجريمة المعلوماتية:

أولا: الركن المادي للجريمة المعلوماتية:

يتجسد الركن المادي في الجرائم المعلوماتية من خلال الدخول غير المشروع إلى نظم وقواعد معالجة البيانات، دون الحاجة إلى التلاعب بهذه البيانات كي يعتبر الفعل جريمة. فبمجرد الوصول غير القانوني إلى المواقع المعلوماتية أو الأنظمة الحاسوبية، يعد النشاط الإجرامي متحققا. أما السلوك الإجرامي في هذه الجرائم، فيتمثل في ارتباط المعلومة بالنظام المعلوماتي أو الأجهزة الحاسوبية، حيث لا يتطلب ارتكاب الجريمة

إجراءات معقدة أو متعددة، بل يمكن أن يحدث بضغطة زر واحدة، مما قد يؤدي إلى تدمير النظام المعلوماتي، أو ارتكاب عمليات التزوير أو السرقة الرقمية[1].

بخصوص العواقب الإجرامية، تطرح أسئلة حول نطاق تأثيرها، سواء كانت محصورة في الفضاء الافتراضي أو امتدت إلى العالم الواقعي، وما إذا كانت مقتصرة على منطقة جغرافية معينة أو أنها تتجاوز الحدود لتشمل أقاليم متعددة.

النشاط الإجرامي في الجرائم المعلوماتية يعتمد على البيئة الرقمية والاتصال بشبكة الإنترنت، مع ضرورة توافر دراية الفاعل بالنشاط الإجرامي وعواقبه. يحدد المشرع مكونات السلوك الإجرامي لكل جريمة، وفي سياق الجرائم المعلوماتية، يرتبط هذا السلوك عادة بالتعامل غير المصرح به مع البيانات المخزنة في الأنظمة الحاسوبية.[2]، التي أدخلت به، أو سرقة صور من الهاتف الذكي.

ثانيا: الركن المعنوي للجريمة المعلوماتية:

يتحقق الركن المعنوي في الجرائم المعلوماتية من خلال علم الجاني بأن الأفعال التي يرتكبها عبر شبكة الإنترنت تشكل جريمة من الناحية القانونية، إضافة إلى توافر القصد الجنائي، أي أن تكون إرادته قد اتجهت بشكل واعٍ ومقصود إلى ارتكاب فعل غير مشروع قانونا، مما يستلزم وجود إرادة آثمة موجهة نحو السلوك الإجرامي، [3] إلى جانب ذلك، تبرز أهمية تحقق نتيجة إجرامية ناتجة عن الأفعال المرتكبة، إذ تكسب إرادة الجاني صفة التجريم عندما تصدر عن فعل إجرامي مقصود، ويكون على علم بما يترتب عليه من آثار، ويتجلى ذلك بوضوح في جرائم مثل تقليد المصنفات والبرامج الحاسوبية، أو عرض المنتجات الأدبية والفكرية على شبكة الإنترنت دون الحصول على إذن من

[1] منى شاكر فراج العسيلي، مقال على الخط http//kenanaonline.com أطلع عليه بتاريخ تاريخ 2025/03/26.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط01، دار الفكر الجامعي، الإسكندرية 2008، ص 36.

[3] المرجع نفسه، ص 36.

مؤلفيها، حيث يتجه الجاني بإرادته الكاملة نحو ارتكاب هذا الفعل مع إدراكه للعواقب القانونية المترتبة عليه.

عند استعراض نظام مكافحة الجرائم المعلوماتية والتشريعات المنظمة لهذه الجرائم حتى عام 1990، نجد أنها ركزت أساسا على السلوك الإجرامي. وهذا التركيز استدعى ضرورة تطوير القوانين والتشريعات بحيث تأخذ بعين الاعتبار الجانب المتعلق بالقصد الجنائي في الجرائم المعلوماتية، لضمان معالجة شاملة ودقيقة لهذا النوع من الجرائم.

من خلال الدراسة التي تم إجراؤها، يتضح أن طبيعة الجرائم المعلوماتية تفرض على المشرع صياغة نصوص مرنة وقابلة للتفسير الواسع، سواء في جانب التجريم أو في جانب العقوبات، ذلك لأن هذا النوع من الجرائم يهدد العديد من المصالح والمراكز القانونية المستجدة بفعل التطور التقني، والتي تتغير وتتزايد بشكل سريع. ومن غير الممكن الاعتماد على نصوص جامدة لا تتماشى مع هذا التطور ولا تتحمل التفسير. لذا، يجب التعامل مع كل جريمة على حدة بطريقة مستقلة. ومن هنا، يبرز ضرورة وجود نصوص مرنة تمنح السلطة القضائية هامشا واسعا لتقدير العقوبة المناسبة وفقا لخصوصية كل حالة في المجال المعلوماتي.

خلاصة الفصل:

يتبيّن من خلال هذا الفصل أن الجريمة الإلكترونية تمثل نمطا مستحدثا من الإجرام، فرضته التحولات الرقمية المتسارعة وانتشار استخدام نظم المعلومات والاتصالات الحديثة. وقد أظهرت الدراسة أن تحديد مفهوم الجريمة الإلكترونية لا يزال محل جدل فقهي، نظرا لتطورها المستمر وتشعب صورها، إلا أن الفقه اتفق نسبيا على اعتبارها كل فعل غير مشروع يرتكب عبر الوسائط الإلكترونية ويهدف إلى الإضرار بالأشخاص أو المؤسسات أو نظم المعلومات.

كما اتضح أن هذه الجرائم تتميز بخصائص تجعلها مختلفة عن الجرائم التقليدية، سواء من حيث طبيعة الوسيلة المستخدمة، أو طبيعة المجرم، أو حتى من حيث صعوبة اكتشافها وتتبع مرتكبيها، وقد تنوعت صور الجريمة الإلكترونية بين تلك التي تقع بواسطة النظام المعلوماتي، كجرائم الاحتيال الإلكتروني، وتلك التي تقع على هذا النظام، مثل الاختراق أو تعطيل الشبكات.

وفيما يخص المجابهة القانونية، فإن السياسة الجنائية تواجه تحديات في التعامل مع هذا النوع من الإجرام، خصوصا فيما يتعلق بتكييف الأفعال المجرّمة وضمان مبدأ الشرعية الجنائية. وهو ما دفع الفقه والقضاء إلى محاولة توسيع مفهومي الركن المادي والمعنوي للجريمة بما يتناسب مع طبيعة الجريمة المعلوماتية، دون المساس بالضمانات القانونية المعروفة.

الفصل الثانـي:

آليات مجابهة الجريمة الإلكترونية

تمثّل الجريمة الإلكترونية إحدى أبرز التحديات الأمنية والقانونية المعاصرة، نظرا لتطور أساليبها وتعدد صورها وامتداد آثارها عبر الحدود الجغرافية للدول، وهو ما أفرز ضرورة تبنّي مقاربات شاملة تتضمن جانبين أساسيين: أولهما وقائي يهدف إلى الحد من فرص ارتكاب هذه الجرائم، وثانيهما علاجي يتمثل في إجراءات التحقيق والمتابعة. وفي هذا السياق، برزت الحاجة إلى تطوير منظومة مؤسساتية متخصصة، فضلا عن إقرار جملة من الإجراءات القانونية الكفيلة بمواجهة هذه الظاهرة الحديثة والمتنامية.

ولأن مجابهة الجريمة الإلكترونية لا يمكن أن تقتصر على الآليات التقليدية وحدها، فقد أصبح من الضروري تكييف الأطر القانونية والمؤسساتية مع طبيعة هذه الجريمة المستحدثة، من خلال إنشاء هيئات مختصة، وتفعيل دور الضبط الإداري والقضائي، بالإضافة إلى استحداث إجراءات تقنية وتحقيقية تتماشى مع الطابع الرقمي للجريمة.

وانطلاقا من ذلك، يتناول هذا الفصل ثنائية الوقاية والمواجهة، من خلال استعراض المؤسسات الفاعلة في مكافحة الجريمة الإلكترونية، ثم تحليل أهم الإجراءات القانونية والتقنية المعتمدة في هذا المجال.

المبحث الأول: مؤسسات مجابهة الجريمة الالكترونية

أمام التطور السريع لتكنولوجيا المعلومات والاتصالات، ظهرت الجريمة الإلكترونية كأحد أبرز التهديدات التي تواجه أمن الأفراد والدول على حد سواء، نظرا لطبيعتها المستحدثة وصعوبة التنبؤ بها أو اكتشافها في الوقت المناسب. وقد دفعت هذه التحديات المتصاعدة بالسلطات العامة إلى تبني مقاربة وقائية متكاملة، تعنى بالتصدي المسبق لمخاطر الجريمة الإلكترونية قبل وقوعها.

وتعتمد هذه المقاربة الوقائية على جملة من الآليات، تتصدرها المؤسسات المتخصصة في المجال الرقمي، والتي يقع على عاتقها رصد التهديدات، وتحليلها، والتنسيق بين مختلف المتدخلين، إلى جانب تعزيز وعي المستخدمين بمخاطر الفضاء السيبراني. كما يلعب الضبط الإداري دورا مهما في حماية النظام العام الرقمي من خلال تدخلات احترازية وتنظيمية تهدف إلى تقليل فرص ارتكاب هذه الجرائم.

وفي هذا الإطار، يتناول هذا المبحث أبرز آليات الوقاية من الجريمة الإلكترونية، سواء من حيث البنية المؤسساتية أو من حيث الأدوار الوقائية التي تضطلع بها مختلف الجهات، وذلك عبر مطلبين رئيسيين: الأول مخصص للآليات المؤسساتية، والثاني للمؤسسات المتدخلة في مرحلة التحقيق والمتابعة.

المطلب الأول: الآليات المؤسساتية للوقاية من الجريمة الإلكترونية

في ظل تنامي الجريمة الإلكترونية وتعدد أساليبها، أصبح من الضروري إرساء آليات مؤسساتية فعالة تمكّن من رصد المخاطر والتدخل الوقائي قبل وقوع الجريمة. وقد تمثلت أبرز هذه الآليات في إنشاء هيئات متخصصة، إلى جانب تفعيل دور الضبط الإداري في حفظ النظام العام الرقمي. وسنتناول في هذا المطلب كلا الجانبين من خلال:

- الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام.

- الفرع الثاني: الضبط الإداري في مجال مكافحة الجريمة الإلكترونية.

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

استحدثها المشرع الجزائري بموجب قانون رقم 09-04 المؤرخ في 5أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، وتم تنظيم عملها بموجب المرسوم الرئاسي 15 -2061 المؤرخ في 8 أكتوبر 2015.

أولا: تعريف الهيئة.

تعدّ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال سلطة إدارية مستقلة تابعة لوزير العدل، وتتكوّن بشكل أساسي من أعضاء في الحكومة معنيين بالموضوع، إلى جانب مسؤولي مصالح الأمن، وقاضيين من المحكمة العليا يتم تعيينهما من قبل المجلس الأعلى للقضاء، تضم الهيئة كذلك قضاة، وضباط، وأعوان شرطة قضائية تابعين لمصالح الاستعلامات العسكرية والدرك والأمن الوطني، وذلك بهدف الكشف عن الجرائم المنصوص عليها في قانون العقوبات، بالإضافة إلى الجرائم الأخرى التي تدخل ضمن اختصاص القاضي المختص.[2]

ثانيا: مهام الهيئة.

أ- تتمثل الوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، بما في ذلك جرائم الذكاء الاصطناعي، في توعية مستخدمي هذه التقنيات بالمخاطر والتهديدات التي قد

[1] قانون رقم 09-04 المؤرخ في 5أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[2]. براهيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية للقانون و العلوم السياسية، الصادرة عن كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، المجلد 2، العدد2، ، نوفمبر 1997، ص153.

يتعرضون لها أثناء استخدامهم لها. فمن خلال تعزيز وعي المستخدمين بخطورة هذه الجرائم يمكن تقليل فرص وقوعهم كضحايا لها.[1]

ب –مكافحة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال وجرائم الذكاء الاصطناعي: وتنص المادة 14 من القانون 09-04 على وجود عدة أساليب تتبعها هذه الهيئة لمكافحة هذه الجرائم:

1–تقديم الدعم للسلطات القضائية ومصالح الشرطة القضائية في تحقيقاتها المتعلقة بالجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، بما يشمل جمع المعلومات وإجراء الخبرات القضائية، وفقا للمادة 14 الفقرة (ب) من القانون 09-04.

2–تنشيط وتنسيق الجهود على المستوى الوطني لمكافحة مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والمشتركين فيها، بما في ذلك الجرائم المتعلقة بالذكاء الاصطناعي.

3–بناء على إذن من السلطات القضائية، يتم القيام بجميع إجراءات التحري والأعمال التقنية المتعلقة بالتحقيقات، لدعم مصالح الشرطة القضائية المختصة في التعامل مع الجرائم التي تم ارتكابها أو تسهيل ارتكابها باستخدام تقنيات الذكاء الاصطناعي. ويتم ذلك دون المساس باختصاص الهيئات الوطنية الأخرى المكلفة بمكافحة أنواع معينة من الجرائم وفقا لما ينص عليه القانون.

4– تقديم الدعم لمصالح الأمن والدرك الوطنيين، وكذلك لجميع الإدارات والمصالح الحكومية المركزية (مثل المديريات العامة المختلفة)، فيما يتعلق بالجرائم التي تدخل ضمن اختصاص هذه الجهات، وذلك عند طلبهم المساعدة، على أن لا يؤدي هذا الدعم إلى تعطيل صلاحياتهم أو سحب أيادٍ لهم عن ممارسة مهامهم.

[1]. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2007، ص232.

5-يمكنها التدخل تلقائيا بعد الحصول على الموافقة المسبقة من السلطات القضائية، وذلك في كل مرة تستدعيها الظروف لإجراء بحث ميداني حول وقائع ذات صلة بالتحقيق الجاري، وفقا للمادة 4 الفقرة 2 من القانون 09-04.

6-6 لضمان تنفيذ مهامها بفعالية، تقوم بجمع وتحليل واستقراء كافة المعلومات المتعلقة بالأفعال والجرائم المرتبطة بتكنولوجيات الإعلام والاتصال وجرائم الذكاء الاصطناعي، وذلك بالتعاون مع مصالح الأمن والدرك الوطني، إدارات ومصالح الدولة (المديريات العامة)، بالإضافة إلى جميع الإدارات والمصالح العامة ذات الصلة.[1]

7-يتعيّن على مصالح الأمن والدرك الوطني، وكذا إدارات ومصالح الدولة (المديريات العامة)، إبلاغ الهيئة في أقرب الآجال الممكنة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك الجرائم المتعلقة بالذكاء الاصطناعي، وذلك في حدود ما تسمح به القوانين، لاسيما تلك المتعلقة بالسرية، وبناء على ما توصلت إليه أو بلغ إلى علمها من وقائع ذات صلة بهذه الجرائم.[2]

ج- تبادل المعلومات مع النظائر الخارجيين:

يهدف هذا التعاون إلى جمع كافة البيانات اللازمة لتحديد هوية المتورطين في جرائم الذكاء الاصطناعي ورصد أماكن تواجدهم. وتتولى الهيئة الوطنية مهمة تنشيط وتنسيق الأعمال التحضيرية قبل مشاركة هذه المعلومات مع المنظمات المماثلة على المستوى الدولي، مع الالتزام بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل.[3]

---

[1] عبد الفتاح بيومي حجازي، مرجع سابق ص233.

[2].المرجع نفسه، ص233.

[3]ـــ برباح يمينة، "تطبيقات الأمن المعلوماتي"، الملتقى الوطني الموسوم ب:الإطار القانوني لاستخدام المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان، يومي 7 و 8 فيفري 2017، ص9.

تعمل الهيئة على دراسة الروابط العملياتية مع الجهات المختصة في مختلف الدول، بهدف الحصول على معلومات متعلقة بجرائم الذكاء الاصطناعي والجرائم المعلوماتية، إضافة إلى تحديد الجهات المتورطة ومواقعها.

أما فيما يخص تطبيق إجراءات الوقاية وتنفيذ الأحكام القانونية الخاصة بسرية المراسلات، فلا يجوز اعتماد ترتيبات تقنية لرصد وجمع الاتصالات الإلكترونية إلا إذا كانت هذه الترتيبات متوافقة مع متطلبات حماية النظام العام ومتطلبات التحقيقات الجارية.

وقد ساهم إنشاء هذه الهيئة بشكل كبير في تعزيز قدرات القضاء، وذلك من خلال توفير كفاءات بشرية مؤهلة، إلى جانب تحديث التشريعات الجزائية بهدف حماية حقوق وحريات المواطنين وتشديد العقوبات على أي انتهاكات في هذا المجال. [1]

ثالثا: المعهد الوطني للأدلة الجنائية على الإجرام.

يتكون من إحدى عشرة دائرة متخصصة تغطي مجالات متعددة، حيث تساهم جميعها في توفير الخبرة وضمان التدريب والتعليم وتقديم الدعم التقني.

من بين هذه الدوائر، تبرز دائرة الإعلام الآلي والإلكتروني، المتخصصة في جرائم الذكاء الاصطناعي، والتي تتولى معالجة وتحليل وتقديم الأدلة الرقمية التي تسهل عمليات التحقيق، بالإضافة إلى تقديم الدعم التقني للمحققين أثناء إجراء المعاينات. [2]

[1].المادة رقم 14 من القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، دراسة منشور بكتاب أعمال الملتقى الدولي الرابع عشر الجرائم الإلكترونية، المنعقدة خلال 24 إلى 25 مارس 2017، طرابلس، ص133.

الفرع الثاني: الضبط الإداري

1- تعريف الضبط الاداري

يشير الضبط الإداري إلى مجموعة من القواعد التي تضعها السلطة العامة بهدف تحقيق الأمن والمحافظة على النظام العام، مع التأكيد على احترام سيادة القانون وعدم انتهاكه. وتسند مهمة تحقيق هذه الغاية إلى جهاز الضبط، الذي يضطلع بدور مزدوج يتمثل في الضبط الإداري والضبط القضائي.

ويعد الضبط الإداري، أو ما يعرف بالشرطة الإدارية، من أبرز وظائف الإدارة، حيث يهدف إلى الحفاظ على النظام العام في الأماكن العامة من خلال إصدار قرارات تنظيمية أو فردية، واستخدام الوسائل المادية عند الضرورة، وهو ما قد يفرض بعض القيود على الحريات الفردية لضمان سير الحياة العامة بشكل منتظم.

ويبرز دور الضبط الإداري في مجال مكافحة الجرائم الإلكترونية، حيث تتركز صلاحياته على الجانب الوقائي من الجريمة، عبر اتخاذ الإجراءات والتدابير الكفيلة بمنع وقوعها، وذلك بالحفاظ على عناصر النظام العام الثلاثة: الأمن العام، السكينة العامة، والصحة العامة.

2- انشاء سلطة الضبط .

بالنظر إلى إمكانية الجمع بين أعمال الضبط القضائي والإداري، كان من الطبيعي أن يكون للضبط الإداري دور في العالم الافتراضي، خاصة في ظل التطور التكنولوجي الفريد الذي نعيشه اليوم. وفي هذا السياق، تم تخصيص أجهزة شرطة لمراقبة غرف الدردشة والتحقق مما يحدث فيها، حيث تخول لها جميع الصلاحيات اللازمة للوقاية من مختلف صور الجريمة.

من بين هذه الصلاحيات، يتمثل دور مأمور الضبط القضائي في تفتيش أجهزة الحاسب الآلي الموجودة في مقاهي الإنترنت أو المؤسسات المختلفة، بهدف التحقق من مدى صلاحية البرمجيات المستخدمة. وقد يكشف هذا التفتيش عن وجود برمجيات غير صالحة أو مواد وصور إباحية، مما يستدعي التدخل القانوني.

من جهة أخرى، تم استحداث سلطة ضبط مكلفة بمهمة السهر على احترام متعاملي البريد والاتصالات الإلكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد، والاتصالات، والأمن السيبراني. وهذا ما نصت عليه المادة 13 من قانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 هـ (الموافق لـ 10 مايو 2018)، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، وفقا لما نشرته الجريدة الرسمية العدد 27[1].

3- العاملين في بيئة الانترنت مزودو الخدمات، ومزودو الدخول .

يتمتع بعض العاملين في بيئة الإنترنت، مثل مزودي الخدمات ومزودي الدخول، بصفة الضبطية الإدارية، حيث تمنح لهم صلاحيات الرقابة عبر المزود لمتابعة سير حركة العمل والتأكد من الالتزام بالنظام والقانون من قبل مستخدمي الإنترنت. وفي حال اكتشاف جريمة من خلال هذه الرقابة، يقتصر دور رجال الضبط الإداري على التحفظ على الأدلة إلى حين وصول رجال الضبط القضائي.

إلى جانب التدابير التي يتخذها رجال الضبط الإداري لمواجهة الجرائم الإلكترونية مبكرا ومنع وقوعها، هناك إجراءات تعتمد داخل المنشآت الحيوية تعرف بأمن المعلومات. وتشمل هذه الإجراءات الاحتياطات التي تتخذها الإدارات الحديثة للحيلولة دون وقوع الجرائم، وذلك عبر تحديد المعلومات الهامة، وتحليل المخاطر والتهديدات،

[1] قانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 هـ الموافق لـ 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية العدد 27.

وتقييم مدى تعرضها للانتهاكات، ثم تطبيق التدابير الوقائية المناسبة، وصولا إلى مرحلة التقييم النهائي.

يتم تحديد أدوار الموظفين مسبقا وفقا لنوع التهديدات التي قد تواجه المنشأة. في سياق مكافحة جرائم الإنترنت، يكلف بعض الموظفين بمراقبة الأنظمة والإبلاغ عن أي اعتداءات محتملة، بينما يتولى فريق آخر متخصص التعامل المباشر مع تلك الاعتداءات والتصدي لها بفعالية، [1] قد تظهر عليه علامات القلق أو الاضطراب في سلوكه اليومي، أو يتخذ مواقف عدائية مهددة، أو يسعى للحصول على أدوات تمكنه من تنفيذ أفعال إجرامية، [2] عند الرجوع إلى النصوص القانونية المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية، يلاحظ أنها لا تنص على ضرورة وجود حماية فنية كشرط لقيام الجريمة. واستنادا إلى المبادئ العامة المستقرة في تفسير القانون الجنائي، فإنه لا يجوز تقييد النصوص المطلقة أو تخصيص النصوص العامة إلا بنص خاص. وبما أن المشرع لم يشر صراحة إلى شرط الحماية الفنية، فإن ذلك يفهم منه أنه تعمّد استبعاد هذا الشرط. ومع ذلك، فإن معظم أنظمة المعالجة الآلية للمعطيات تكون مزوّدة فعليا بأنظمة حماية فنية، وهو ما يساهم في إثبات الجريمة، وخاصة فيما يتعلق بالركن المعنوي منها. [3]

المطلب الثاني: مؤسسات مرحلة التحقّيق والمتابعة

تعد مرحلة التحقيق والمتابعة من المراحل الحاسمة في التصدي للجريمة الإلكترونية، حيث تتدخل فيها جهات مختصة تعمل على كشف الجريمة وتقديم مرتكبيها للعدالة.

[1]– نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013، 86–88.

[2]–مزيود سليم، دور المؤسسات الاجتماعية في الوقاية من المجلة الجزائرية للاقتصاد والمالية، العدد 11 افريل 2019 ص78.

[3]– خالد داودي، الجريمة المعلوماتية، دار الاعصار العلم للنشر والتوزيع، الجزائر، ط 2، 2008، ص 112.

وتتوزع هذه المهام بين الضبط القضائي، الذي يتولى البحث والتحري، وبين المؤسسات القضائية والعقابية التي تتابع التحقيق وتصدر الأحكام. وسنتناول ذلك من خلال:

- الفرع الأول: الضبط القضائي.
- الفرع الثاني: المؤسسات القضائية والعقابية.

الفرع الأول: الضبط القضائي

تعتبر الضبطية القضائية صاحبة الاختصاص الاصيل في كل الجرائم بما فيها الجريمة الالكترونية، وقد منحها القانون اساليب تحري جديدة نبينها فيما يلي : [1]

1- على مستوى جهاز أقامت المديرية العامة للأمن الوطني وحدة مركزية في الجزائر العاصمة، وأخرى جهوية في قسنطينة ووهران، مجهزة بخلايا إعلام آلي وفرق متخصصة في التحقيق في الجرائم الإلكترونية والكشف عنها، تسعى المديرية العامة للأمن الوطني إلى تعزيز قدراتها من خلال إنشاء مخابر جديدة في بشار، ورقلة، وتمنراست، والتي هي حاليا في طور الإنجاز، بهدف تغطية كافة المناطق في البلاد وضمان التصدي الفعال للجرائم الإلكترونية، [2] تتضمن المخبرين الجهويين للشرطة العلمية في قسنطينة ووهران وحدة متخصصة في التحقيق في الجرائم الإلكترونية تعرف بـــدائرة الأدلة الرقمية والآثار التكنولوجية، وتنقسم هذه الدائرة إلى ثلاثة أقسام رئيسية مكلفة بتحليل الأدلة الرقمية والتعامل مع الجرائم التكنولوجية:

- قسم مختص في استغلال البيانات الرقمية الناتجة عن الحواسيب والشبكات.

[1]-أمحمدي بوزينة آمنة : اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، مداخلة مشارك بها في الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، 2007، ص 57.

[2]-ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في حقوق جامعة باتنة، سنة 2016، ص176.

- قسم متخصص في تحليل الأدلة المستخرجة من الهواتف النقالة.
- قسم لتحليل الأصوات، باستخدام أجهزة تقنية متقدمة لكشف الجرائم الإلكترونية.[1]

2-على مستوى جهاز الدرك الوطني، تضطلع مؤسسة الدرك الوطني بمهمة مكافحة الجريمة الإلكترونية من خلال المعهد الوطني للأدلة الجنائية وعلم الإجرام، الذي يقع مقره في بو شاوي ويتبع قيادة الدرك العامة. يختص قسم الإعلام والإلكترونيك داخل هذا المعهد في التحقيق والكشف عن الجرائم الإلكترونية[2]، تساهم مديرية الأمن العمومي والاستغلال والمصلحة المركزية للتحريات الجنائية في مكافحة الجريمة الإلكترونية، حيث تعنى هذه الهيئة ذات الاختصاص الوطني بالتحقيق والتصدي للجرائم الإلكترونية على مستوى البلاد.[3]

الفرع الثاني: المؤسسات القضائية والعقابية

أولا: المؤسسات القضائية :

1- محاكم عادية :

تختص في النظر في الملفات البسيطة للجريمة الالكترونية

2-محاكم متخصصة:

تعد المحاكم المتخصصة جهات قضائية خاصة تناط بها مهمة الفصل في نوع معيّن من النزاعات، وذلك نظرا للطابع الخاص الذي تتسم به بعض الجرائم من حيث نوعها، وخطورتها، وتأثيرها على النظام العام، بالإضافة إلى طبيعة شخصية مرتكبيها، وعددهم،

[1]-ربيعي حسين، المرجع نفسه، ص 177.

[2]- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، 2013، ص 116.

[3]-ربيعي حسين، مرجع سابق، ص 182.

ووسائل تنفيذها، وعندما تتضح معالم الجريمة من حيث التكييف القانوني للوقائع وطبيعتها الخاصة، يصبح من الضروري عرضها على جهة قضائية متخصصة، مع مراعاة عدم إحالة القضايا البسيطة أو العادية إلى هذه الجهات.

وبالنظر إلى خطورة الجريمة المعلوماتية وتفشيها في المجتمع، فقد أسند المشرع مهمة الفصل فيها إلى المحاكم المتخصصة، بهدف مكافحتها، والحد من انتشارها، والكشف عن مرتكبيها، وفي هذا الإطار، نصت المادة 329 من قانون الإجراءات الجزائية على أنه: يجوز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

كما نصت المادة 40 مكرر من نفس القانون : تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة امام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد37، 40، 329 من هذا القانون، مع مراعاة أحكام المواد 40 مكرر 1 الى 40 مكرر 5 .

استنادا إلى المرسوم التنفيذي رقم 06–348 المؤرخ في 12 رمضان عام 1427 هـــ، الموافق لـــ 05 أكتوبر سنة 2006،[1] والذي ينص على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ليشمل دوائر اختصاص محاكم أخرى، وفقا لأحكام المادة الأولى منه (كما نشر في الجريدة الرسمية رقم 63)، فإن هذا التمديد يشمل كل من محكمة سيدي امحمد، محكمة قسنطينة، محكمة ورقلة، ومحكمة وهران.

3 – القطب الجزائي المالي والاقتصادي : نصت على انشائه المواد 211 مكرر الى 211 مكرر 15 من قانون الاجراءات الجزائية .

4– القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

[1] المرسوم التنفيذي رقم 06–348 المؤرخ في 12 رمضان عام 1427 هـــ، الموافق لـــ 05 أكتوبر سنة 2006.

- تنص المادة 211 مكرر 22 من الأمر رقم 21-11 الصادر في 16 محرم 1443 الموافق لـــ 25 أغسطس 2021، الذي يعدل ويتمم الأمر رقم 66-155 الصادر في 18 صفر 1386 الموافق لـــ 8 يونيو 1966 والمتعلق بقانون الإجراءات الجزائية، على إنشاء قطب جزائي وطني بمقر مجلس قضاء الجزائر، يعنى بالنظر في الجرائم المحددة ضمن هذا الباب إذا كانت تصنف كجنح[1].
- ويكون اختصاص هذا القطب الجزائي الوطني لمكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال حصريا، وفقا لنص المادة 211 مكرر 24 من هذا الأمر، وذلك في الجرائم المذكورة على سبيل الحصر.

- الجرائم التي تهدد أمن الدولة أو تمس بالدفاع الوطني.
- جرائم نشر وترويج الأخبار الكاذبة بين المواطنين، والتي من شأنها الإخلال بالأمن أو السكينة العامة أو زعزعة استقرار المجتمع.
- جرائم نشر وترويج الأنباء المغرضة التي تمس بالنظام العام والأمن العام، سواء كانت ذات طابع منظم أو عابرة للحدود الوطنية.
- الجرائم المتعلقة بالاعتداء على أنظمة المعالجة الآلية للمعطيات الخاصة بالإدارات والمؤسسات العمومية.
- جرائم الاتجار بالأشخاص أو الأعضاء البشرية، وجرائم تهريب المهاجرين.
- جرائم التمييز العنصري وخطاب الكراهية.

[1] الأمر رقم 21-11 الصادر في 16 محرم 1443 الموافق لـــ 25 أغسطس 2021، الذي يعدل ويتمم الأمر رقم 66-155 الصادر في 18 صفر 1386 الموافق لـــ 8 يونيو 1966 والمتعلق بقانون الإجراءات الجزائية

ثانيا: المؤسسات العقابية:

تتعدد أنواع المؤسسات العقابية في الجزائر، حيث تصنف إلى ثلاثة فئات: المؤسسات المغلقة التي تتسم بالرقابة الصارمة، المؤسسات شبه المفتوحة التي توفر قدرا من الحرية، والمؤسسات المفتوحة التي تتيح مزيدا من الاندماج مع المجتمع.

1- المؤسسات المغلقة:

تسمى في التشريع الجزائري مؤسسات البيئة المغلقة بمقتضى المادة 26 من القانون2/72 (قانون تنظيم السجون)[1]، تتمثل الصورة التقليدية للسجون في إقامتها داخل المدن الكبرى ولكن على أطرافها، وتحيط بها أسوار عالية وتفرض عليها حراسة مشددة من الداخل والخارج، بما في ذلك أعلى الأسوار. وتتميّز هذه السجون بمعاملة قاسية للمساجين، حيث تسلب منهم حريتهم بشكل كامل، ويفرض نظام صارم يعاقب بشدة كل من يخالفه.

تنص المادة 211 مكرر 22 من الأمر رقم 21-11 الصادر في 16 محرم 1443 الموافق لـــ 25 أغسطس 2021، الذي يعدل ويتمم الأمر رقم 66-155 الصادر في 18 صفر 1386 الموافق لـــ 8 يونيو 1966 والمتعلق بقانون الإجراءات الجزائية[2]، على إنشاء قطب جزائي وطني بمقر مجلس قضاء الجزائر، يعنى بالنظر في الجرائم المحددة ضمن هذا الباب إذا كانت تصنف كجنح.

[1] المادة 65 مكرر 5 من قانون الاجراءات الجزائية.

[2] من الأمر رقم 21-11 الصادر في 16 محرم 1443 الموافق لـــ 25 أغسطس 2021، الذي يعدل ويتمم الأمر رقم 66-155 الصادر في 18 صفر 1386 الموافق لـــ 8 يونيو 1966 والمتعلق بقانون الإجراءات الجزائية.

يكون اختصاص هذا القطب الجزائي الوطني المختص في مكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال حصريا، وفقا لأحكام المادة 211 مكرر 24 من هذا الأمر، وذلك بالنسبة للجرائم المحددة على سبيل الحصر.[1]

2- المؤسسات شبه المفتوحة

وتسمى في التشريع الجزائري مؤسسات الحرية النصفية بمقتضى المادة 144 من قانون العقوبات[2]، تقع هذه المؤسسات خارج المدن، حيث يتم اختيار مواقعها في مناطق زراعية وصناعية تتيح إمكانية تشغيل النزلاء (المساجين) ضمن برامج تأهيلية. تتميز بأسوار متوسطة الارتفاع وبمستوى حراسة معتدل مقارنة بالمؤسسات المغلقة، كما توفر معاملة أفضل للمساجين، رغم أن نظامها يبقى صارما إلى حد ما لتحقيق الردع العام من خلال إجراءات الحراسة المعقولة.

إلى جانب ذلك، تعزز هذه المؤسسات الثقة لدى المحكوم عليهم وتشجعهم على التفاعل الإيجابي مع برامج الإصلاح والتأهيل. غير أن تخفيف الحراسة قد يزيد من احتمالات الهروب، وهو ما يستلزم تطبيق المادة 188 من قانون العقوبات، حيث يعاقب مرتكبو جريمة الهروب بالحبس، ويتم استكمال تنفيذ باقي العقوبة تحت نظام التأديب داخل المؤسسة.

[1] – -أحسن بوسقيعة، التحقيق القضائي، ط1، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014، ص 117.

[2] –serge Guichard jacques buisson, procédure période, éduction litec, N° 06 paris, 2010, P 233.

3- المؤسسات المفتوحة

تسمى في في التشريع الجزائري المؤسسات المفتوحة بمقتضى المادة 145 من قانون العقوبات [1] تفتقر المؤسسة المفتوحة إلى المظاهر المادية التي تبعث على الرهبة، مثل الأسوار العالية، القضبان الحديدية، وكثرة الحراس، حيث تتسم مبانيها بطابع عادي يشبه الأبنية الحكومية الأخرى، وغالبا ما تقام خارج المدن. يخصَّص هذا النوع من المؤسسات لفئات معينة من المحكوم عليهم، لاسيما المبتدئين الذين صدرت ضدهم أحكام بالحبس لمدد قصيرة، ويشرك فيها النزلاء في أعمال تأهيلية مخصصة لهم.

تتميز هذه المؤسسات بقدرتها على غرس حب التأهيل لدى النزلاء، وتشجيع الاعتماد على النفس، وتعزيز الثقة المتبادلة بينهم وبين الآخرين، فضلا عن انخفاض تكاليف تشغيلها، إلا أن من أبرز ما يؤخذ عليها هو ضعف قدرتها على تحقيق الردع العام، وسهولة فرار السجناء منها، نظرا لقلة عدد الحراس ولطبيعة المعاملة المخففة المعتمدة داخلها.

في هذا النوع من المؤسسات، يتلقى المحكوم عليهم برامج للتهذيب والتأهيل تهدف إلى دراسة الأسباب والعوامل التي ساهمت في انحرافهم، مع توجيههم نحو القيم الأخلاقية وتعزيز قناعاتهم بها. ويقوم فريق من المختصين في مجالات التربية، علم النفس، علم العقاب، ورجال الدين بإلقاء محاضرات وتنظيم دورات تدريبية حول الجريمة وإدانة السلوك الإجرامي، بالإضافة إلى إقامة دروس ومحاضرات دينية تدعو إلى الخلق الحسن وأهمية ممارسة الشعائر الدينية. كما يتم عقد جلسات فردية مع كل محكوم عليه لفهم العوامل والأسباب التي أدت به إلى هذا المصير.

[1]- إسحاق ابراهيم منصور، علم الاجرام والعقاب، ديوان المطبوعات الجامعية، ط2، الجزائر، 1991، ص 181-182.

بالإضافة إلى ذلك، تعمل المؤسسة على تأهيل المحكوم عليهم من خلال ورش عمل متنوعة تحدد بناء على رغباتهم، مثل النجارة أو محو أمية الكبار أو تعليم الصغار. كما تشجعهم على استكمال دراستهم داخل المؤسسة بالتعاون مع مجموعة من المدرسين المعينين لهذه الغاية، وتسعى المؤسسة أيضا إلى إنشاء مكتبة داخلية تهدف إلى تعزيز التعليم والتثقيف بين النزلاء[1].

تتعدد المؤسسات العقابية في الجزائر، وتشمل المؤسسات المغلقة وشبه المفتوحة والمفتوحة، حيث تهدف إلى مكافحة الجريمة وتحقيق الردع العام وإنذار الأفراد من العقاب، مما يساهم في تعزيز الثقافة الأمنية واستئصال النزعة الإجرامية لدى المحكوم عليهم.

تعتمد هذه المؤسسات على أساليب ردعية وإصلاحية تهدف إلى إعادة دمج السجناء في المجتمع من خلال برامج علاجية وصحية واجتماعية ونفسية تساعد في تعديل سمات شخصياتهم. ويشرف على هذه العملية فريق متخصص يضم أخصائيين اجتماعيين ونفسيين وأطباء ورجال دين ومدربين في التكوين المهني، حيث تتم دراسة المشكلات النفسية والاقتصادية والاجتماعية للنزلاء، والعمل على إيجاد الحلول المناسبة.

وتشمل هذه الجهود تحسين الحالة النفسية للمحكوم عليهم عبر الحد من مشاعر الخوف والقلق الناجمة عن العقاب وتأنيب الضمير، إلى جانب معالجة المشكلات الاقتصادية المرتبطة بخسارة فرص العمل، وتأثير السجن على مستقبلهم المهني والاجتماعي.

تسعى المؤسسات العقابية إلى شغل وقت فراغ المحكوم عليهم وتفريغ طاقاتهم في أنشطة مفيدة من خلال تنظيم برامج ترفيهية ورياضية. وتسهم هذه الأنشطة في الحد من

[1] إسحاق ابراهيم منصور، المرجع السابق، ص 182.

حالات التمرد والانحراف، وتقلل من فرص انتقال السلوك الإجرامي بين النزلاء. كما توفَّر التجهيزات اللازمة لهذه الأنشطة بما يتيح بيئة مناسبة للتعاون والعمل الجماعي، والتعبير عن القدرات والطاقات المختلفة لدى المحكوم عليهم.

ويعدّ النجاح الذي يحققه النزلاء في هذه الأنشطة مصدرا للإشباع والراحة النفسية، ما يساهم في تعزيز علاقاتهم الاجتماعية، ويمهّد الطريق لإعادة إدماجهم في المجتمع وتأهيلهم وتيسير تكيفهم الاجتماعي بعد انتهاء فترة العقوبة.

المبحث الثاني: إجراءات التحقيق كآلية لمجابهة الجريمة الإلكترونية

تعد إجراءات التحقيق من الركائز الأساسية في مكافحة الجريمة الإلكترونية، حيث تمكن الجهات المختصة من جمع الأدلة الرقمية وتحليلها للوصول إلى الجناة، خاصة في ظل الطابع المعقد والمتجدد لهذه الجرائم. ففي عالم الإنترنت، تتطلب عمليات التحقيق أدوات قانونية وتقنية متطورة للتعامل مع الجرائم التي تتسم بالخفاء والسرعة في تنفيذها، مما يقتضي تعديل وتحديث الإجراءات التقليدية لتتناسب مع الخصوصيات الرقمية. ويتناول هذا المبحث الإجراءات العامة المعتمدة لمكافحة الجريمة الإلكترونية، من خلال آليات التفتيش وضبط الأدلة والمعاينة والخبرة التقنية، بالإضافة إلى الإجراءات المستحدثة التي تشمل المراقبة الإلكترونية والتسرب الإلكتروني. هذه الإجراءات تعد أساسية لتأمين سير التحقيقات، وضمان جمع الأدلة بطريقة قانونية وفعالة تساهم في تقديم الجناة إلى العدالة.

المطلب الأول: الإجراءات العامة والمألوفة لمجابهة الجريمة المعلوماتية

يعتبر التحقيق في الجريمة الإلكترونية من أكثر العمليات تعقيدا نظرا للطابع الرقمي المتقلب للأدلة الإلكترونية، مما يستدعي استخدام إجراءات قانونية وتقنية دقيقة وفعّالة. وتشمل الإجراءات العامة المتبعة في هذا السياق تقنيات التفتيش وضبط الأدلة الرقمية، بالإضافة إلى المعاينة والخبرة التقنية التي تعتبر ضرورية للتحقق من صحة الأدلة وجمعها بطرق تتماشى مع القوانين المعمول بها. وفي هذا المطلب، سنتناول هذه الإجراءات بشكل مفصل، من خلال استعراض أهم الأساليب المتبعة في التحقيقات الجنائية لمكافحة الجريمة الإلكترونية.

الفرع الأول: التفتيش وضبط الأدلة

أولا: التفتيش

يعتبر التفتيش من أخطر الإجراءات التي تباشرها الضبطية القضائية بهدف البحث عن أدلة تثبت وقوع جريمة، وذلك وفقا للضوابط التي يحددها قانون الإجراءات الجزائية أو النصوص الخاصة. وتزداد أهمية هذا الإجراء في مجال الجرائم السيبرانية، حيث تشكل تهديدا مباشرا للحقوق والحريات الفردية من خلال استغلال الحاسب الآلي وما يحتويه من أدلة، سواء كانت مادية أو معنوية.

أ – **تعريف التفتيش تعددت التعريفات الفقهية للتفتيش،** لكنها تتفق جميعا على أنه إجراء من إجراءات التحقيق يباشره مختصون عند وقوع جناية أو جنحة، بهدف البحث عن أدلة تثبت الجريمة، متى اقتضت ضرورة التحقيق ذلك. ويتم هذا الإجراء في مكان يتمتع بالحرمة، سواء تم برضا من يجرى في مواجهته أم دون رضاه.

كما يعرَّف التفتيش أيضا بأنه إجراء تحقيق تباشره جهة مختصة حددها القانون، ويهدف إلى البحث عن الأدلة المادية لجناية أو جنحة تم التأكد من وقوعها داخل محل خاص ذي حرمة قانونية.[1]

يقصد بالتفتيش في الجريمة السيبرانية فحص النظم المعلوماتية، ولو عن بعد، بهدف جمع الأدلة المخزنة أو المسجلة إلكترونيا، مثل الملفات والبرامج المحفوظة على أجهزة الحاسوب، والمعطيات والاتصالات الإلكترونية، سواء كانت ذات طابع مادي أو معنوي، طالما تفيد كأدلة إلكترونية في كشف الحقيقة.

[1]-عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، دار الثقافة، ط1، 501–500 الأردن.

كما يعرف هذا التفتيش بأنه عملية بحث دقيقة أو اطلاع على محل يتمتع بحماية قانونية خاصة، لكونه يعد مستودعا لسر صاحبه، سواء تمثل هذا المحل في مسكن، أو شخص، أو جهاز حاسوب، أو نظم معلوماتية، أو شبكة الإنترنت[1].

ب – الشروط القانونية للتفتيش في الجرائم الإلكترونية:

يعتبر التفتيش إجراء قانونيا يمس الحرية الشخصية، ولذلك حرصت كافة التشريعات على تقييده بشروط وضمانات أساسية. ويهدف ذلك إلى تحقيق توازن بين مصلحة المجتمع في محاسبة المجرم وردعه، وبين ضمان حقوق الأفراد وحرياتهم. ومن بين هذه الشروط والضمانات ما هو موضوعي، ومنها ما يرتبط بالجوانب الشكلية.[2].

1-الشروط الشكلية : وتتمثل هذه الشروط في:

يتطلب إجراء التفتيش في البيئة الإلكترونية حضور بعض الأشخاص وفقا لما ينص عليه القانون، حيث يعد المتهم الشخص الرئيسي الذي يجب أن يكون حاضرا أثناء عملية التفتيش، باعتبار أن الإجراء المتخذ يمسّه مباشرة. ومع ذلك، إذا كان التفتيش يجرى في محل إقامته وتعذر عليه الحضور، يجوز له إنابة شخص آخر ليكون ممثلا عنه أثناء التفتيش، وإلا يشترط استدعاء شاهدين في بعض الحالات.

كما يحق للمتهم الاستعانة بمحامٍ خلال عملية التفتيش، مما يمنح المحامي الحق في الحضور أيضا. وفي حال كان التفتيش يجرى لدى شخص غير المتهم، يجب السماح

[1]–يوسف مناصرة الدليل الإلكتروني في القانون الجزائي دراسة مقارنة، ط1، الجزائر، دار الخلدونية، 2021، ص 348.

[2]-عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، مرجع سابق ص512-511

لحائز المكان بالحضور حفاظا على مصالحه. بالإضافة إلى ذلك، يخوّل القانون للنيابة العامة الحق في حضور إجراءات التفتيش التي يجريها قاضي التحقيق [1] .

وهو ما نص عليه المشرع الجزائري في المادة 01/45، نصت المادة على استثناءات، منها جرائم المساس بنظم المعالجة الآلية للبيانات، بسبب طبيعتها التقنية التي تتطلب التحرك السريع لاستخلاص الأدلة الرقمية قبل ضياعها[2] .

2-موعد إجراء التفتيش في الجرائم الإلكترونية: تباينت التشريعات الإجرائية في تحديد الميعاد الزمني لتفتيش نظم المعلوماتية. فقد أقر بعضها حظر تنفيذ هذا الإجراء خلال أوقات معينة من الليل، على سبيل الحرص على تقليل الاعتداء على الحرية الفردية وحرمة المسكن. بينما ربطت تشريعات أخرى التفتيش بتوقيت محدد لتحقيق ذات الغرض. وفي المقابل، تركت بعض التشريعات الأمر دون قيد زمني، بحيث يجوز إجراء التفتيش في أي ساعة من ساعات الليل أو النهار، مع منح السلطة التقديرية للجهة القائمة بالتفتيش لتحديد التوقيت المناسب، [3] والمشرع الجزائري قد تطرق للمسألة في المادة 47 من ق. إ. ج. ج .

ب – الشروط الموضوعية: الضوابط اللازمة لإجراء تفتيش صحيح تعد في الغالب من المتطلبات السابقة عليه، ويمكن تلخيصها في ثلاثة شروط أساسية: وجود سبب يبرره،

[1] -عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية أو الاستثنائية، المرجع السابق ص515-516

[2] –عبد اللطيف دحية وآخرون، المواجهة الإجرائية لجرائم المعلوماتية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، الجزائر، 2019م، ص 46

[3] –عائشة بوخبزة، الحماية الجزائية من الجريمة السيبيرائية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، وهران، الجزائر، 2013م، ص194.

وتحديد محل التفتيش بدقة، وتوفر الجهة المختصة قانونا بتنفيذه.[1]، وفيما يلي تفصيل كل شرط:

1-سبب التفتيش في البيئة الإلكترونية: السبب في التفتيش هو الدافع الذي يحرّك السلطة المختصة لاتخاذ قرارها بإجراء التفتيش والبدء في تنفيذه. وهو الأمر الذي ينشئ الأساس القانوني لهذا الإجراء، ويعطي المحقق الحق في إصدار أمر التفتيش. يتمثل السبب في وقوع الجريمة، سواء كانت جناية أو جنحة، مع توافر قرائن قوية وأدلة تشير إلى وجود ما يساعد في كشف ملابساتها لدى المتهم أو أي شخص آخر. ولا ينشأ هذا السبب إلا بعد وقوع الجريمة وظهور دلائل الاتهام ضد شخص معين، أو وجود أمارات واضحة على أن هناك من يحوز ما قد يساهم في الوصول إلى الحقيقة.

من ثم، لا يجوز قانونا إجراء التفتيش إلا إذا كان هناك احتمال معقول للعثور على دليل ذي صلة بالجريمة. وهذا القرار يخضع لتقدير السلطات القائمة على التحقيق، ويكون خاضعا لمراجعة المحكمة التي تراقب مدى سلامة الاستدلال والإجراءات المتخذة. فإذا ثبت أن سلطات التحقيق قامت بإجراء التفتيش دون وجود احتمال حقيقي لتحقيق فائدة منه، فإن ذلك يعد تعسفا في استخدام السلطة، ويعتبر غير مشروع .[2]

2-محل التفتيش: لضمان صحة ومشروعية التفتيش في الجرائم السيبرانية، يجب أن يكون التفتيش موجها نحو محل محدد أو قابل للتحديد، مع مراعاة أن يكون قانونيا

[1]-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، المرجع السابق، ص 99.

[2] -عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، مرجع سابق، ص 512-513.

ومشروعا. يشمل ذلك العناصر المادية والمعنوية للكمبيوتر، بالإضافة إلى ملحقاته وبرامجه، وكذلك الهاتف الذكي وشبكات الاتصال عن بعد[1].

في الجرائم الإلكترونية، لا يكون محل التفتيش قائما بذاته، بل يرتبط إما بمكان معين، مثل مسكن المتهم، أو بشخص محدد، كمالك الجهاز أو حائزه، كما هو الحال مع الحاسوب المحمول أو الهاتف الذكي. لذلك، قبل الشروع في عملية التفتيش، يجب مراعاة طبيعة المكان الذي توجد فيه الوسائل الإلكترونية المراد تفتيشها، إلى جانب الضمانات القانونية التي تحيط بها.

يشترط أن يكون محل التفتيش محددا تحديدا دقيقا لا يترك مجالا للالتباس، حفاظا على خصوصية الأفراد وحرياتهم. فلا يجوز، على سبيل المثال، تفتيش جميع الحواسيب داخل شركة معينة أو جميع الهواتف المحمولة الخاصة بأفراد أسرة واحدة دون مبرر قانوني واضح. كما توجد استثناءات قانونية لبعض الأشخاص والأماكن التي لا يجوز تفتيشها، مثل مساكن وسيارات أعضاء السلك الدبلوماسي، وأعضاء المجالس النيابية، ومكاتب المحامين نظرا لما يتمتعون به من حصانة قانونية، مما يجعل أي تفتيش يطالها مخالفا للقانون ويؤدي إلى بطلانه.[2]

في الجرائم الإلكترونية، لا يكون محل التفتيش قائما بذاته، بل يرتبط غالبا بمكان معين كمسكن المتهم، أو بشخص محدد كمالك أو حائز الجهاز، كما هو الحال بالنسبة للحاسوب المحمول أو الهاتف النقال. لذلك، قبل الشروع في التفتيش، لا بد من مراعاة طبيعة المكان الذي تتواجد فيه الوسائل الإلكترونية المستهدفة بالتفتيش، والضمانات القانونية المقررة له. ويشترط في محل التفتيش أن يكون محددا بشكل دقيق يمنع الجهالة،

[1]– لامية وعلي، كاهنة سعودي، إجراءات المكافحة الجريمة الإلكترونية، مرجع سابق، ص 82.

[2]– جمال براهيمي، مرجع سابق، ص 36.

حفاظا على حريات وخصوصيات الأفراد، فلا يصح، على سبيل المثال، تفتيش جميع الحواسيب الموجودة في شركة ما، أو جميع الهواتف النقالة الخاصة بأفراد عائلة واحدة.

كما تجدر الإشارة إلى أن هناك بعض الأشخاص والأماكن التي تستثنى من التفتيش بحكم تمتعها بالحصانة، مثل مساكن وسيارات وأشخاص أعضاء السلك الدبلوماسي، وأعضاء المجالس النيابية، وكذلك مكاتب المحامين. وأي تفتيش يطال هذه الفئات يعد مخالفا للقانون، ويترتب عليه البطلان.

أما فيما يخص السلطة المختصة بالتفتيش، فإن إذن التفتيش الصادر عن جهة غير مختصة يعتبر باطلا، مما يستلزم تحديد الجهة المخولة قانونا بالقيام به في قضايا الجرائم السيبرانية. وبالرجوع إلى التشريع الجزائري، نجد أن المشرّع قد حدّد هذه الجهة بنص المادة 5.

بناء على القانون 09-04، يحق للسلطات القضائية المختصة وضباط الشرطة القضائية، في نطاق قانون الإجراءات الجزائية والشروط المحددة في المادة 4، الدخول إلى المنظومات المعلوماتية والبيانات المخزنة فيها، سواء بشكل مباشر أو عن بعد، ويشمل ذلك: [1].

وبالتالي يمكن القول إن المشرع أسند الاختصاص الأصلي بالتفتيش في الجرائم السيبرانية إلى السلطة القضائية، غير أنه أجاز لها تفويض جهات أخرى للقيام بهذا الإجراء، نظرا لما تتسم به هذه الجرائم من خصوصية فنية تستلزم تدخل خبراء ذوي

[1]-القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

معرفة متخصصة في الأنظمة المعلوماتية، وذلك لضمان حماية البيانات محل التفتيش والحفاظ عليها من أي تصرف قد يؤدي إلى إتلافها أو ضياعها. [1]

ثانيا: ضبط دليل الإلكتروني

يعد ضبط الأشياء المتعلقة بالجريمة النتيجة المباشرة للتفتيش، ولذلك نلاحظ أن التشريعات الإجرائية غالبا ما تجمع بين أحكام الضبط والتفتيش في مكان واحد. ومع ذلك، لا يعني هذا أن الضبط يعادل التفتيش، حيث يمكن أن يكون الضبط نتيجة للمعاينة أو إجراءات أخرى، وهو ما سيتم تناوله فيما يلي:

ويعرف ضبط الأدلة الإلكترونية : بأنه وضع اليد على أي شيء يرتبط بالجريمة يسهم في كشف حقيقتها وتحديد مرتكبيها، لكنه ينحصر في الأشياء المادية فقط. وهذا يبرز صعوبة ضبط أدلة الجريمة المتعلقة بالمكونات المادية للكمبيوتر، مثل البصمات، بينما تكمن التحديات الأكبر في ضبط الوسائل التقنية المستخدمة في إتلاف البرامج، كالفيروسات، إلى جانب المكونات المعنوية للحاسوب.

وفي هذا السياق، ثار جدل واسع بين التشريعات الإجرائية والاتجاهات الفقهية حول مسألة ضبط الأشياء غير المادية والكيانات المنطقية التي لا تصلح بطبيعتها لأن تكون محلا لوضع اليد، مما أدى إلى انقسام الآراء إلى اتجاهين رئيسيين.

الاتجاه الأول : يعتقد أنصار هذا الاتجاه أنه يمكن تطبيق إجراءات الضبط على الأجهزة الحاسوبية بوصفها كيانات مادية منفصلة عن الكيانات الاعتبارية، مما يؤدي إلى عدم صلاحيتها. وقد اعتمد التشريع الألماني هذا النهج في تعامله مع هذه القضايا [1].

[1]- رضا هميسي، تفتيش المنظومات المعلوماتية في التشريع الجزائري مقال منشور بمجلة العلوم القانونية والسياسية، ع، 2012.

الاتجاه الثاني: يذهب أصحاب هذا الاتجاه إلى أن المعطيات المخزنة آليا يمكن أن تكون محلا للضبط وفقا للنصوص التقليدية.

غير أن المشرع الجزائري تدخل بموجب القانون رقم 09-04 الخاص بالقواعد المتعلقة بالوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، حيث وضع لذلك آليات خاصة، من بينها:

حجز المعطيات المعلوماتية عندما تكتشف السلطة التي تقوم بالتحقيق في نظام معلوماتي معطيات مفيدة في الكشف عن الجرائم أو تحديد مرتكبيها، وليس من الضروري حجز النظام بأكمله، بل يتم نسخ المعطيات محل البحث على وسيلة تخزين إلكترونية قابلة للحجز

- ❖ يتم حجز هذه المعطيات من خلال منع الوصول إليها، وذلك عبر وسائل متعددة، مثل الترميز أو تقييد الدخول إلى النظام، أو باستخدام أي وسيلة إلكترونية أخرى.
- ❖ كما يشمل الحجز المعطيات ذات المحتوى الإجرامي، التي يخضع صاحبها للعقوبات المنصوص عليها في التشريعات السارية، سواء في قانون العقوبات أو قانون الإجراءات الجزائية الجزائري. ويقتصر استخدام المعلومات المستخلصة من عمليات المراقبة المنصوص عليها في هذا القانون على حدود الضرورة القصوى المرتبطة بالتحريات والتحقيقات القضائية[2].
- ❖ **المودم (modem)** تمكّن هذه الوسيلة أجهزة الكمبيوتر من التواصل وتبادل البيانات مع بعضها البعض عبر شبكة الإنترنت.

[1] ابتسام بغو، اجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة ماستر، تخصص القانون الجنائي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهدي ام بواقي، الجزائر 2015-2016 ص 29.

[2] ابتسام بغو، المرجع سابق ص 30

❖ **ضبط البريد الالكتروني :** ينجز هذا الإجراء عبر تحديد صندوق البريد الإلكتروني العائد للمتهم المراد تفتيشه، وذلك بعد التوصل إلى اسم المستخدم وكلمة السر التي تتيح الدخول إليه. وبعدها يتم فتح البريد الإلكتروني وفحص محتوياته، سواء من خلال صندوق الوارد أو الصادر أو الرسائل المحفوظة أو المهملات. كما يمكن ضبط الرسائل الإلكترونية من خلال تشغيل برنامج البريد الإلكتروني المثبّت على جهاز المتهم، ومراجعة قائمة الرسائل الواردة لاستخراج الرسالة المطلوبة.[1]

الفرع الثاني: المعاينة والخبرة التقنية لمجابهة الجريمة المعلوماتية

أولا: المعاينة الالكترونية.

مسرح الجريمة هو المكان الذي ارتكبت فيه الجريمة، ويحتوي على أدلة جنائية قيمة يتركها الجاني أثناء تنفيذ جريمته. نظرا للاضطراب العصبي والذهني الشديد الذي يعاني منه الجاني في تلك اللحظة، فإنه يجد صعوبة في التحكم في أفعاله أو إزالة الآثار التي تدل عليه، ما يعني أنه حتى الجاني المحترف سيترك وراءه آثارا قد تكشف عن شخصيته، [2] يجب على ضباط الشرطة القضائية الانتقال إلى موقع الجريمة لتسجيل الآثار المادية وتوثيقها، مع الحفاظ على الأدلة، وتوثيق حالة المكان والأشخاص، وجمع كل ما يخدم التحقيق. ومن الضروري إخطار النيابة على الفور لتتحرك إلى مسرح الجريمة في القضايا التي تتطلب تدخلها المباشر، [3] المعاينة هي عملية مشاهدة مكان أو شخص أو شيء بالعين المجردة بهدف توثيق حالته وضبط أي عناصر قد تسهم في كشف الحقيقة. تستلزم هذه الخطوة سرعة الانتقال إلى موقع الواقعة، حيث يقوم ضابط الشرطة القضائية بجمع الأدلة والقرائن التي يمكن الاعتماد عليها في التحقيق، إضافة إلى التحقق المباشر

[1] خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 274.

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

[3] المادة 31 قانون إ.ج المصري"... الانتقال فور الى مكان الجريمة... "

من حالة الأشخاص والأشياء والأماكن ذات الصلة بالحادث، وتعتبر هذه المرحلة الأساس الأولي في عملية الاستدلال على ملابسات أي جريمة.

ونظرا للاختلاف الجوهري بين الجرائم المعلوماتية والجرائم التقليدية، خاصة وأن مسرح الجريمة الرقمية قد يتجاوز حدود الدولة، فإن المعاينة التقنية تجرى وفق إجراءات خاصة سيتم توضيحها لاحقا. [1]

تتجلى أهمية المعاينة في كونها تنقل إلى جهات التحقيق والمحاكمة صورة شاملة لموقع الجريمة، بما يحتويه هذا الموقع من تفاصيل دقيقة. وتتناول هذه التفاصيل موقع الجريمة ووصفها الداخلي، بالإضافة إلى الآثار الموجودة فيه التي ترتبط بالجريمة بشكل مباشر أو غير مباشر. كما تهدف المعاينة إلى تقديم كل ما يمكن أن يساعد جهات الشرطة والقضاء في تكوين تصور واضح حول كيفية وقوع الجريمة، واستخلاص بعض الأدلة من المعلومات والمعطيات التي تم جمعها أثناء عملية المعاينة. [2]

ولضمان فعالية المعاينة وتحقيق أهدافها المرجوة، أقرت بعض التشريعات عقوبات جنائية بحق أي شخص يقوم بتغيير حالة الأماكن المرتبطة بالجريمة، أو إزالة أي عنصر منها، أو تعديل موقع وقوعها، وذلك قبل أن تباشر سلطات التحقيق أو الاستدلال إجراء المعاينة الأولية، بغض النظر عن هوية الفاعل. [3]

في الجرائم التقليدية، تجرى المعاينة في مسرح الجريمة المادي، بينما تتطلب الجرائم المعلوماتية معاينة على مستويين متميزين لضمان جمع الأدلة الرقمية والمادية بشكل فعال:

---

[1] عبد العال الديري و محمد صادق اسماعيل، .الجرائم الالكترونية.ط .01، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 264.

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

[3] عبد العال الديري و محمد صادق اسماعيل، المرجع السابق، ص 265.

1: المسرح التقليدي:

المسرح التقليدي هو ذلك الذي يوجد غالبا خارج بيئة الحاسوب، ويتكوَّن من العناصر المادية للمكان الذي ارتكبت فيه الجريمة، وهو يشبه إلى حد كبير مسرح الجريمة التقليدية. ومن أمثلة الجرائم التي تقع ضمن هذا النطاق، تلك التي تستهدف شرائط الحاسوب(D.F) ، أو الكابلات الخاصة به، أو شاشة العرض الملحقة، أو مفاتيح التشغيل، أو الأقراص، وغيرها من المكونات المادية الملموسة للحاسوب.[1]

لا توجد صعوبة تقنية تحول دون تحديد مدى صلاحية مسرح الجريمة، الذي يحتوي على هذه المكونات، لإجراء المعاينة من قبل ضباط الشرطة العلمية. وتشمل هذه العملية التحفظ على الأشياء التي تعد أدلة مادية تثبت ارتكاب الجريمة وتنسبها إلى شخص معين، بالإضافة إلى وضع الأختام في الأماكن التي شملتها المعاينة. كما يتم ضبط جميع الأدوات والوسائل التي استخدمت في ارتكاب الجريمة، مع ضرورة إخطار النيابة العامة بكل هذه الإجراءات.

2: المسرح الافتراضي:

يقع المسرح الافتراضي عادة داخل البيئة الإلكترونية، ويتألف من البيانات الرقمية المخزنة في ذاكرة الأقراص الصلبة داخل الحاسوب. وتبرز في هذا المجال الجرائم التي تستهدف برامج الحاسوب أو بياناته، أو التي ترتكب باستخدامه، بالإضافة إلى الجرائم التي تنفَّذ عبر الإنترنت، مثل التزوير المعلوماتي والتخريب.[2]

-قلة الأدلة المادية التي تترك بعد الجرائم المرتكبة على أنظمة المعلومات.

---

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

– العدد الكبير من الأفراد الذين يمكنهم الوصول والتفاعل مع مسرح الجريمة الافتراضي في فترة زمنية قصيرة، مما يزيد من تعقيد جمع الأدلة وتحليلها، لإجراء المعاينة في العالم الافتراضي، يتعين على ضابط الشرطة القضائية أن ينتقل إلى هذا الفضاء الافتراضي، إما من مكتبه أو عبر اللجوء إلى مقاهي الإنترنت أو بالاستعانة بخبراء في المجال، وغيرها من الطرق التي تمكنه من جمع الأدلة والكشف عن الحقيقة.

تتخذ المعاينة في جرائم الإنترنت والحاسوب (الجرائم المعلوماتية) أشكالا متعددة تختلف باختلاف طبيعة الجريمة المرتكبة، إلا أن هناك وسائل عامة تستخدم بما يتوافق مع طبيعة الاتصال بالإنترنت أو الأداة المستخدمة في ارتكاب الجريمة. ومن بين هذه الوسائل، تقنية تصوير شاشة الحاسوب(Écran de captures d'impression) ، والتي يمكن إنجازها إما باستخدام آلة تصوير تقليدية، أو من خلال برامج حاسوبية متخصصة تتيح التقاط صورة لما يعرض على الشاشة، وهو ما يعرف بتجميد مخرجات الشاشة (Frozen)، إلى جانب وسائل أخرى مشابهة. [1]

ثانيا: الخبرة التقنية

شهد العالم تطورا تقنيا هائلا في مجال تكنولوجيا الإعلام والاتصال، مما أحدث تغييرا جذريا في المفاهيم المرتبطة بالدليل الجنائي. وقد أدى ذلك إلى تعزيز دور الإثبات العلمي للدليل وإلى إدراج الخبرة التقنية ضمن نطاق الخبرة القضائية، وأصبح من الضروري الاستعانة بخبراء متخصصين لفحص الأدلة التقنية وتقييم عملية الإثبات الرقمي وتحليل الجرائم الإلكترونية، وهو أمر لا يمكن الاستغناء عنه. فمن غير المعقول أن يفصل القاضي في قضايا تقنية المعلومات دون أن يستند إلى خبرة تقنية متخصصة،

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

تحقيقا لمبدأ التخصص الذي بات مبدأ معروفا وأساسيا، وفي حال إغفال هذا المبدأ، يكون حكمه عرضة للطعن والاعتراض بسبب العيب الواضح.

1- دور الخبرة التقنية

الخبرة الفنية هي إجراء تحقيقي يستعان فيه بخبير يمتلك مهارات فنية ومعرفة علمية متخصصة، غير متوفرة لدى جهات التحقيق والقضاء، وذلك للمساعدة في العثور على أدلة أو قرائن تسهم في كشف تفاصيل الجريمة وربطها بالمتهم[1]، الخبرة الفنية هي استشارة متخصصة يستند إليها القاضي أو المحقق في بناء قناعته بشأن القضايا التي تتطلب خبرة فنية ومعرفة علمية دقيقة لا يملكها بنفسه.

تعد الخبرة الفنية عنصرا أساسيا في إثبات الجرائم الإلكترونية، لأنها توفر الدعم الفني اللازم للسلطات التحقيقية والقضائية والجهات المختصة، مما يمكنها من الوصول إلى الحقيقة وتحقيق العدالة الجنائية بشكل فعال[2]، مع تفشي الجرائم الإلكترونية، أصبحت سلطات التحقيق والاستدلال والمحاكمة تعتمد بشكل متزايد على الخبراء الفنيين المتخصصين في مجال التقنية الإلكترونية. وقد ازدادت الحاجة إلى الخبرة الفنية في التحقيقات المتعلقة بهذه الجرائم، بهدف كشف غموضها، جمع الأدلة وتوثيقها، وضمان الحفاظ عليها. كما يسهم الخبراء في مساعدة المحققين على فهم التفاصيل التقنية المعقدة المرتبطة بالجريمة محل التحقيق، مما يسهل الوصول إلى الحقائق وإثباتها.

[1]- عبد الناصر محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية "دراسة تطبيقية مقارنة"، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007، ص 24.

[2]-بوكرر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن منشورات الحلبي الحقوقية، ب ط، بيروت، 2012.، ص 424.

نظرا للتطورات التكنولوجية التي أثرت على وسائل الإعلام والاتصال، تنوعت أنواع الحواسيب وشبكات الاتصال، وأصبحت العلوم والتقنيات المرتبطة بها تنتمي إلى مجالات علمية وفنية دقيقة ومتفرعة. ومع سرعة هذه التطورات وتعاقبها، يصبح من الصعب حتى على المتخصصين مواكبتها واستيعابها بالكامل، بل يمكن القول إنه لا يوجد حتى الآن خبير يمتلك معرفة شاملة بجميع أنواع الحواسيب وبرامجها وشبكاتها، أو قادر على التعامل مع كافة أشكال الجرائم التي ترتكب من خلالها أو تستهدف بها.

لذلك، منح المشرع للمحقق حرية كاملة، في أي مرحلة من مراحل التحقيق، لندب أي خبير يرى فيه الكفاءة الفنية اللازمة للاستفادة من خبرته في كشف ملابسات الجرائم الإلكترونية. [1]

كما أن القانون لا يلزم القاضي بالاستجابة لطلب المتهم أو أي من الخصوم بشأن ندب خبير، حيث تنص الفقرة الثانية من المادة (143) من قانون الإجراءات الجزائية الجزائري على أنه: وإذا رأى قاضي التحقيق أنه لا موجب لطلب الخبرة، فعليه أن يصدر في ذلك قرارا مسببا.... ومع ذلك، فإن الاستعانة بخبير فني في المسائل الفنية البحتة تعد ضرورية في الجرائم التقليدية، لكنها تصبح أكثر إلحاحا في مجال جمع الأدلة الرقمية لإثبات الجرائم الإلكترونية، نظرا لتعقيد هذه القضايا وارتباطها بتفاصيل تقنية دقيقة لا يمكن فهمها أو تحليلها إلا بواسطة خبير متخصص ومتمكن في مجاله، فالفن لا يكشفه ويفهمه إلا فن مكافئ، والذكاء لا يواجهه إلا ذكاء مماثل[2].

تظهر أهمية الاستعانة بالخبير الفني في إثبات الجرائم الإلكترونية بشكل أكثر وضوحا عند غياب هذا الخبير. ففي حال عدم وجوده، قد تفشل سلطات التحقيق

[1]– سليمان أحمد فضل، الجرائم الإلكترونية وسبل مواجهتها: دراسة مقارنة، دار المسيرة، عمّان، 2010، ص 134.

[2]– فهد عبد الله العبيد العازمي، الجريمة الإلكترونية: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص 640.

والاستدلال في كشف ملابسات الجريمة وجمع الأدلة المتعلقة بها، نتيجة نقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي تم استخدامها لارتكاب الجريمة، وهذا النقص قد يؤدي إلى تدمير الأدلة أو فقدانها، سواء بسبب الجهل بكيفية التعامل معها أو نتيجة الإهمال.

لم يغفل المشرع الجزائري هذا الجانب، حيث نص في المادة (05) الفقرة الأخيرة من القانون رقم 04-09، المتعلق بالقواعد الخاصة بالوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها، على أنه يجوز للسلطات المكلفة بتفتيش المنظومات المعلوماتية الاستعانة بأي شخص يمتلك خبرة في تشغيل هذه المنظومات أو في التدابير المتخذة لحماية البيانات التي تحتويها، وذلك بهدف مساعدتها وتزويدها بالمعلومات الضرورية لإنجاز مهمتها بفعالية.[1]

وأعتقد أن المشرع الجزائري قد صاغ هذا النص بصيغة عامة باستخدام عبارة كل شخص له دراية، وهو أمر مقصود بهدف توسيع نطاق المساعدة الفنية في مجال مكافحة الجرائم الإلكترونية، بحيث لا تقتصر فقط على الخبراء، بل تشمل أيضا جميع المتخصصين والعاملين في ميدان تكنولوجيات الإعلام والاتصال، كالمهندسين، وحملة الشهادات العليا في الإعلام الآلي، ومقدمي خدمات الاتصالات الإلكترونية، مثل مزودي خدمة الوصول إلى الإنترنت، ومزودي خدمات الإيواء والحوسبة، وكل من يمتلك خبرة أو دراية في هذا المجال.

لم يكتفِ المشرع الجزائري بهذا الحد، بل عمل على إنشاء هيئات وأجهزة متخصصة لمواجهة الجرائم الإلكترونية، مزوّدة بأحدث الوسائل والتقنيات المتطورة، وجعل من بين مهامها الأساسية تنفيذ الخبرات التي تحتاجها السلطات القضائية. ومن أبرز

[1]-عشر المادة 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة تكنولوجيات الإعلام و الاتصال و مكافحتها، المرجع سابق.

هذه الهيئات نذكر: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، الذي أنشأته قيادة الدرك الوطني سنة 2009، والمعهد الوطني للبحث في علم التحقيق الجنائي، المنشأ بموجب المرسوم الرئاسي رقم 04-432 المؤرخ في 20 ديسمبر 2004، والذي تم تنظيم مصالحه وأقسامه ومخابره بموجب قرار وزاري مشترك صادر بتاريخ 14 أفريل 2007، ويتضمن مصلحة مختصة بالخبرات المتعلقة بالأدلة التكنولوجية.

كما يذكر أيضا القسم الخاص بالخبرة الرقمية التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية، على مستوى المديرية العامة للأمن الوطني، والذي يمتد نشاطه إلى بعض الولايات، ويعنى بتقديم الخبرة الفنية المتخصصة في القضايا ذات الطابع الرقمي.

وقد تم مؤخرا إنشاء ثلاثة مخابر جنائية جهوية في شمال البلاد تابعة للأمن الوطني، تضم عدة أقسام متخصصة، من بينها قسم الأدلة الإلكترونية والرقمية. ومن المنتظر، بحسب تصريح الملازم أول هودة رشيدة، رئيسة فرقة مكافحة الجرائم المعلوماتية لأمن ولاية وهران وممثلة المديرية العامة للأمن الوطني، أن يتم تدعيم هذه الجهود بإنشاء ثلاث مخابر مماثلة في الجنوب مستقبلا. [1].

تم مؤخرا، بموجب المرسوم الرئاسي رقم 15-261 الصادر في 8 أكتوبر 2015، إنشاء هيئة وطنية مختصة في الوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها. وقد أسندت إليها مهمة دعم السلطات القضائية وأجهزة الشرطة القضائية في

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

عمليات البحث والتحري المتعلقة بهذه الجرائم، وذلك من خلال تقديم المساعدة، وجمع المعلومات، وإنجاز الخبرات القضائية اللازمة[1].

2- دور مقدمي الخدمات في التحري والتحقيق في الجرائم الماسة بأنظمة الإتصال والمعلوماتية .

تتنوع تكنولوجيات الإعلام والاتصال بشكل كبير، خاصة تلك المتعلقة بخدمات الاتصال السلكية واللاسلكية، مثل الهواتف النقالة والشبكات الرقمية التي تمثلها الإنترنت. وهذا التنوع يجعل عملية توفير هذه الخدمات لمستخدميها تعتمد على مجموعة من الفاعلين، وعلى رأسهم مقدمو الخدمات الذين حددهم القانون رقم 09-04، حيث يعرفهم على النحو التالي:

1-أي كيان، سواء كان عاما أو خاصا، يقدم لمستخدميه خدمات تتيح القدرة على التواصل من خلال منظومة معلوماتية و/أو نظام اتصالات.

2- وأي كيان آخر يقوم بمعالجة أو تخزين بيانات إلكترونية لصالح خدمة الاتصال المذكورة أو لصالح مستخدميها. [2]

المطلب الثاني: الاجراءات المستحدثة لمجابهة الجريمة الالكترونية

مع تطور أساليب الجريمة الإلكترونية وتنوعها، أصبحت الإجراءات التقليدية غير كافية لمواكبة هذه التحديات. لذلك، ظهرت مجموعة من الإجراءات المستحدثة التي تمكّن الجهات المختصة من التصدي بفعالية للجرائم الرقمية. وتشمل هذه الإجراءات المراقبة الإلكترونية واعتراض الاتصالات، بالإضافة إلى التصدي للتسرب الإلكتروني، وهي

[1]- الفقرة ب من المادة 13 من القانون رقم 09-04 المؤرخ في 05/08/2009.

[2]- القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

أساليب تواكب التقنيات الحديثة وتضمن جمع الأدلة بطرق أكثر دقة وأمانا. في هذا المطلب، سنتناول هذه الإجراءات المستحدثة بشكل تفصيلي، مع التركيز على أهم التقنيات القانونية والفنية المستخدمة لمكافحة الجريمة الإلكترونية.

الفرع الأول: الاعتراض و المراقبة الإلكترونية

أولا: مفهوم الاعتراض و المراقبة الإلكترونية

1- تعريف الاعتراض و المراقبة الإلكترونية

عرّفت لجنة خبراء البرلمان الأوروبي، خلال اجتماعها المنعقد في ستراسبورغ بتاريخ 06 أكتوبر 2006، والذي خصص لدراسة أساليب التحري التقنية وعلاقتها بالأعمال الإرهابية، عملية اعتراض المراسلات بأنها شكل من أشكال المراقبة السرية للمراسلات السلكية واللاسلكية. وتتم هذه العملية في سياق البحث والتحري عن الجرائم، بهدف جمع الأدلة والمعلومات المتعلقة بالأشخاص المشتبه في تورطهم أو مشاركتهم في ارتكاب الجريمة.[1]

استلهم المشرع الجزائري من المادة 100 من قانون الإجراءات الجزائية الفرنسي، حيث نص في المادة 65 مكرر (5) من قانون الإجراءات الجزائية الجزائري على تعريف دقيق لمراقبة المراسلات، باعتبارها أي عملية اعتراض أو تسجيل أو نسخ للمراسلات المنقولة عبر وسائل الاتصال السلكية واللاسلكية. وتشمل هذه المراسلات بيانات قابلة للتحليل والتوزيع والتخزين والاستقبال والعرض.

عند الرجوع إلى نص هذه المادة، نلاحظ أن المشرع الجزائري قد حدد المراسلات التي يمكن أن تكون محل اعتراض، وهي تلك التي تتم عبر وسائل الاتصال السلكية

[1]- بوكر رشيدة، مرجع سابق، ص 442.

واللاسلكية، دون أن يحدد طبيعة هذه المراسلات. هذا يفتح المجال أمام جميع أنواع الرسائل المكتوبة، بغض النظر عن شكلها (كتابة رموز، أشكال، صور) أو الوسيط الذي تكتب عليه (ورقي أو رقمي)، أو الوسيلة المستخدمة لإرسالها، سواء كانت سلكية مثل الفاكس أو التلغراف، أو لاسلكية مثل البريد الإلكتروني أو الهاتف النقال. باستثناء الكتب والمجلات والرسائل والحوليات، التي تعتبر مراسلات خاصة[1] .

وقد تأكد هذا الأمر في المادة (2) فقرة و) من القانون رقم (04/09) التي عرفت الاتصالات الالكترونية بأنها أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة الكترونية.[2]

وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون علم أو موافقة المعنيين، يتمثل الهدف من مراقبة المراسلات في الاستماع إلى المحادثات أو التقاط البيانات المرسلة وتسجيلها وبثها، سواء كانت خاصة أو سرية، في الأماكن العامة أو الخاصة، ومن ثم استخدامها كأدلة في مواجهة المتهم.

تعد المراسلات عبر البريد الإلكتروني من أبرز المراسلات الإلكترونية التي يحرص القائمون على التحقيق على إخضاعها لعمليات الاعتراض والمراقبة، نظرا لما تمثله من مصدر غني بالأدلة التي يمكن أن تسهم في إثبات الجرائم الإلكترونية. ويعزى ذلك إلى أن البريد الإلكتروني يعد من أكثر وسائل الاتصال الحديثة استخداما عبر الإنترنت، ووسيلة

[1] –BENNOUAR Abdelhakim, Les techniques spéciales d'enquête et d'investigation en Algérie, article publier sur; www.Mémoire Online 2000-2013, pp 2-3

[2] –وهو ما يستشف كذلك من خلال نص المادة (6/09) من القانون رقم (03/2000 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات التي اعتبرت المراسلات بانها كل اتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها الى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، ولا تعتبر الكتب والجرائد والمجلات واليوميات كمادة مرسلات.

فعّالة لربط الأشخاص حول العالم بسرعة عالية ودون عوائق. فهو يعمل كنظام لتبادل الرسائل والصور وغيرها من المحتويات الرقمية، سواء بإدراجها مباشرة في نص الرسالة أو بإرفاقها كملفات قابلة للتحميل. كما يستخدم البريد الإلكتروني كمخزن لحفظ المستندات والوثائق والمراسلات التي تعالج رقميا، وذلك داخل صندوق خاص وشخصي للمستخدم، يصعب اختراقه بفضل الحماية الفنية المخصصة له[1].

2- أساليب اعتراض مراقبة المراسلات

أ-اعتراض المراسلات:

يقصد بالمراسلات[2]: جميع الخطابات والرسائل والطرود والبرقيات والمشرع الجزائري[3] هي المادة 65 مكرر05 ق.إ.ج حصر مفهوم المراسلات في تلك التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية فقط.

ب- **تسجيل الأصوات:**

تتمثل مراقبة الاتصالات في تتبع وتسجيل جميع الاتصالات التي تتم عبر الوسائل السلكية واللاسلكية، وتشمل هذه المراقبة جميع أدوات الاتصال. ويتم ذلك عن طريق استخدام تقنيات خاصة دون الحصول على موافقة الأفراد المعنيين، بهدف التقاط وتسجيل وبث المحادثات الخاصة أو السرية التي يتبادلها الأفراد.[4]

ج-التقاط الصور.

---

[1] ربيحة زيدان، الجريمة الإلكترونية: دراسة تحليلية في ضوء التشريع الجزائري، دار هومة، الجزائر، 2011، ص 159.

[2] المادة 39 دستور ج ج د ش لسنة 2020، المؤرخ في 2020/12/30، الجريدة الرسمية رقم 82.

[3] ــ يقصد بالمراسلات الالكترونية هي الخدمة التي تسمح بانتقال الرسائل المرسلة عبر نظام الرسائل الالكترونية عن طريق شبكة الكترونية.

[4] ــ محمد فتحي عيد، "مقومات التعاون الدولي في مجال مكافحة المخدرات"، بحث مقدم في الندوة العلمية: التعاون الدولي في مجال مكافحة المخدرات، المنظمة من قبل أكاديمية نايف العربية للعلوم الأمنية، الرياض، خلال الفترة من 9 إلى 11 ديسمبر 2000، ص 69.

المراقبة الإلكترونية هي عملية تقنية تهدف إلى التقاط صور لأفراد أو مجموعات يتواجدون في أماكن خاصة. تتم هذه الإجراءات بسرية تامة، حيث تنطوي على انتهاك محتمل لحرمة الحياة الخاصة المكفولة دستوريا، إلا أن المشرّع قد أحاطها بضمانات وضوابط أساسية سيتم تناولها لاحقا.

وتشير هذه العملية إلى استخدام التقنيات الإلكترونية من قبل المراقب لجمع بيانات ومعلومات حول المشتبه فيه، سواء تعلق الأمر بشخص أو مكان أو شيء، وفقا لطبيعته. ومن خلال هذا التعريف، يتضح أن المراقبة الإلكترونية تعد وسيلة حديثة تقتصر على الجرائم المعلوماتية، كما تعتبر إحدى الأدوات الأساسية لجمع البيانات والمعلومات حول المشتبه بهم. [1]

لقد نص المشروع الجزائري من خلال المادة 4 من قانون 09 – 04[2] تستخدم المراقبة الإلكترونية في الحالات التي تتطلب الوقاية من الجرائم الخطيرة، مثل الإرهاب والتخريب والجرائم التي تهدد أمن الدولة. وتكون هذه المراقبة مبررة عندما تتوفر معلومات تفيد بأن هناك اتصالات تتعلق بتهديد محتمل للنظام العام أو الدفاع الوطني أو المؤسسات العامة أو الاقتصاد الوطني.

مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تخدم الأبحاث دون اللجوء الى مراقبة الاتصالات الالكترونية.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية.

3- القيود الواردة على عملية اعتراض ومراقبة المراسلات:

[1] ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة ماستر في القانون، تخصص: قانون جنائي للأعمال، كلية الحقوق و العلوم السياسية، جامعة العربي بن مهيدي أم البواقي، 2016/2015، ص 36.

[2] القانون /09 04، المؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

لتحقيق التوازن بين متطلبات التحقيق التي تقتضيها المصلحة العامة، وضمان احترام الحياة الخاصة التي تمثل مصلحة فردية، أحاط المشرع عملية الاعتراض بعدد من القيود القانونية. تهدف هذه القيود إلى الحيلولة دون تعسف السلطات العامة، وحماية الحريات الفردية، ويمكن تلخيصها على النحو التالي[1]:

أ- الحصول على إذن السلطة القضائية المختصة .

هذا يعني أنه قبل اللجوء إلى إجراءات الاعتراض والمراقبة، يجب الحصول على إذن مسبق يكون مكتوبا ومسببا من الجهات القضائية المختصة، وإلا اعتبر هذا الإجراء باطلا.

ولكي يكون الإذن صحيحا ومنتجا لآثاره القانونية، ينبغي أن يتضمن مجموعة من العناصر الأساسية، تتمثل في:

- طبيعة الجريمة التي تبرر الإجراء:

والتي ينبغي أن تكون من ضمن الجرائم المذكورة في المادة 56 مكرر 05 السابق الذكر.

- التعريف بالعملية

يشمل ذلك تحديد المراسلات والاتصالات المطلوب مراقبتها وتسجيلها، إلى جانب تحديد الأماكن المستهدفة بعملية الاعتراض. كما ينبغي تحديد مدة تنفيذ التدابير التقنية، بحيث لا تتجاوز أربعة أشهر، مع إمكانية تمديدها وفق الشروط ذاتها، وذلك وفقا لتقدير الجهة المختصة التي أصدرت الإذن، بما يتماشى مع مقتضيات التحري والتحقيق.

[1] جمال براهيمي، المرجع السابق، من 94.

ب- تسبيب اللجوء إلى الاعتراض أو مراقبة المراسلات .

يقصد به وجود مبرر قانوني وضرورة ملحة تبرر اللجوء إلى اعتراض أو مراقبة المراسلات، إذ يتعين على وكيل الجمهورية أو قاضي التحقيق المختص، قبل إصدار الإذن بتنفيذ هذه العملية، أن يقيّم مدى وجود هذه الضرورة، ويقدر جدية الأسباب التي تستند إليها، والفائدة المتوقعة منها في سبيل كشف الحقيقة وتوضيح ملابسات الجريمة والتعرف على مرتكبيها بشكل مسبق [1].

ج- تحديد الجرائم محل الاعتراض والمراقبة .

إن اللجوء إلى اعتراض أو مراقبة المراسلات الإلكترونية كإجراء تحقيق لا يسمح به في جميع الجرائم، بل يقتصر نطاق تطبيقه على نوع معين فقط. وتتمثل هذه الجرائم في تلك المحددة حصرا في نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية، بالإضافة إلى الجرائم المنصوص عليها في الفقرات أ، ب، ج من المادة 04 من القانون رقم 09-04[2].

د - سرية الإجراءات وكتمان السر المهني

يجب أن تتم عملية الاعتراض والمراقبة بسرية تامة، دون علم أو موافقة المشتبه فيه أو أصحاب الأماكن المعنية، مع الحرص على عدم المساس بالحماية المهنية المنصوص عليها في المادة 45، الفقرة الرابعة من قانون الإجراءات الجزائية.

[1] جمال براهيمي، المرجع السابق، من 94.

[2] القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

وعلى الرغم من التحديات والمخاوف المرتبطة بهذه الإجراءات المستحدثة، إلا أن الواقع يثبت مدى ضرورتها وأهميتها في التعامل مع الجرائم الحديثة، مما يجعل اللجوء إليها أمرا ملحا لضمان فعالية التحقيقات.

ثانيا: ضمانات الاعتراض والمراقبة الالكترونية

1- الضمانات الموضوعية

تتعلق الضمانات الموضوعية بموضوع المراقبة الإلكترونية وهي الجريمة محل المراقبة والشخص المراقب وتتمثل في:

أ-أن تتعلق بفئة معينة من الجرائم

ينبغي أن تستخدم المراقبة الإلكترونية حصرا في الجرائم التي نصت عليها المادة 65 مكرر 5 من قانون الإجراءات الجزائية، وهي: جرائم الاتجار بالمخدرات، الإرهاب، تبييض الأموال، جرائم الإعلام الآلي، جرائم الصرف، جرائم الفساد، الجريمة المنظمة عبر الوطنية، وجرائم التهريب. ويناط بالقاضي الذي يصدر الإذن مسؤولية تقدير مدى انطباق هذا الوصف الجنائي على الأفعال الجرمية محل التحري أو التحقيق، باعتباره شرطا موضوعيا وأساسيا لاتخاذ إجراء المراقبة الإلكترونية.[1].

يشترط لصحة إذن القاضي المختص أن يشير في مضمونه إلى الجريمة التي تبرر اتخاذ هذا الإجراء. فقد نصت المادة 65 مكرر 7/1 من قانون الإجراءات الجزائية على أنه: يجب أن يتضمن الإذن المشار إليه في المادة 65 مكرر 5 أعلاه الجريمة التي تبرر

[1]- فوزي عمارة ، اعتراض المراسلات وتسجيل الاصوات والتقاط الصور والتسرب كاجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الانسانية، ، كلية الحقوق والعلوم السياسية، جامعة منتوري قسنطينة العدد 33، 2010 جوان ، من 240 .

اللجوء إلى هذه التدابير. وبالتالي، فإن أي إذن لا يشمل الإشارة إلى نوع الجريمة يعتبر باطلا ولا يعتد به.

ب- مقتضيات التحري والتحقيق

لا يجوز اللجوء إلى عملية الاعتراض إلا إذا توفرت قرائن قوية تثبت أن هذا الإجراء سيسهم في كشف الحقيقة وإسنادها إلى المتهم، وإلا يكون الإجراء باطلا. وفي جميع الحالات، يبقى تقدير مدى ضرورة اللجوء إلى هذه العمليات من اختصاص قاضي التحقيق.

كما يرى البعض ضرورة إضافة شرط آخر، وهو أن يكون المتهم طرفا في المحادثات الخاضعة للمراقبة، حيث أجاز المشرّع الجزائري استثناء يسمح بمراقبة الأحاديث وتسجيلها، مع التركيز بشكل أساسي على تلك التي يكون المتهم مشاركا فيها، بهدف كشف حقيقة التهم الموجهة إليه.

ج- السلطة المختصة بإجراء هذه العمليات

يتم تنفيذ عمليات اعتراض المراسلات وتسجيل الأصوات تحت إشراف قاضي التحقيق، رغم أنه لا يجري هذه العمليات بنفسه. ونظرا لطبيعة هذه العمليات التي تتطلب خبرة تقنية متخصصة، يتم تكليف خبراء في هذا المجال بتنفيذها، بينما يركز قاضي التحقيق على الإشراف القضائي وضمان احترام الإجراءات القانونية، [1] ينبغي أن تتم المراقبة الإلكترونية في إطارها الشرعي ووفقا لمقتضيات القانون، [2] أما أثناء مرحلة التحري فوكيل الجمهورية هو المؤهل الوحيد المراقبة هذه العملية [3]من خلال اشتراط

[1]-فوزي عمارة، المرجع السابق، من 240.

[2]-المرجع نفسه، من 230.

[3]- المادة 65 مكرر 5 من قانون الإجراءات الجزائية.

الحصول على إذن من وكيل الجمهورية والخضوع للإشراف المباشر، يكون المشرع قد ضمن حماية حقوق الأفراد من خلال تقييد المراقبة الإلكترونية بإطار قانوني صارم.

د- الجهة المكلفة بالعملية

يتولى ضابط الشرطة القضائية تنفيذ العمليات، كما يجوز لقاضي التحقيق، أو لضابط الشرطة القضائية المكلّف من قبله، الاستعانة بأي عون مؤهل يتولى الجوانب التقنية المتعلقة بالعمليات المطلوب تنفيذها، سواء كان هذا العون يعمل لدى جهة عمومية أو خاصة، [1]و ذلك طبقا للمادة 65 مكرر 8 من قانون الإجراءات الجزائية.

2- الضمانات الشكلية

حدد المشرع الجزائري شروطا شكلية لتنفيذ المراقبة الإلكترونية، والتي تعتبر كضمانة قانونية تتيح الخروج عن القاعدة العامة المتعلقة بسرية الاتصالات والمحادثات الهاتفية. وهذه السرية محمية دستوريا بموجب أحكام المادة 47 من الدستور لعام 2020.

أ-صدور اذن مكتوب

وفقا لأحكام المادة 65 مكرر 5 من قانون الإجراءات الجزائية، لا يجوز لضابط الشرطة القضائية تنفيذ عملية الاعتراض إلا بعد الحصول على إذن مسبق من وكيل الجمهورية المختص أو قاضي التحقيق، وتتم العملية تحت إشرافهما المباشر.

أما في فرنسا، فتتم إجراءات الاعتراض بموجب إذن قضائي مستعجل خاص يصدر عن قاضي الحريات والحبس. [2]

[1]- أحسن بوسليمة، التحقيق القضائي، ط1، دار عومة للطباعة والنشر والتوزيع، الجزائر 2014، من 177.

[2] -serne Giochard jacques buisson, procédure période, éduction litec, N° 06 paris, 2010, P233.

يشترط المشرع أن يكون الإذن بالمراقبة الإلكترونية صادرا بشكل خطي ومفصل، حيث يجب أن يتضمن جميع التفاصيل الضرورية التي تمكن من تحديد نطاق المراقبة بدقة، بما في ذلك تحديد الاتصالات المستهدفة، الأماكن العامة أو الخاصة المشمولة بالمراقبة، ونوع الجريمة التي تستدعي هذه الإجراءات.

ب- تحرير محضر الاعتراض

وفقا للمادة 65 مكرر 9 من قانون الإجراءات الجزائية، يلزم ضابط الشرطة القضائية بتحرير محضر دقيق لكل عملية مراقبة إلكترونية، يتضمن توثيقا لتاريخ بدء الإجراء وتاريخ انتهائه، لضمان الشفافية والالتزام بالإجراءات القانونية[1]، يتعين على ضابط الشرطة القضائية تحرير محاضر مفصلة ودقيقة لكل إجراء تقني يتم خلال المراقبة الإلكترونية، بما في ذلك محاضر الدخول إلى المساكن، محاضر الالتقاط، محاضر التثبت، ومحاضر التسجيل الصوتي، لضمان توثيق دقيق لجميع الإجراءات.

ج-تسبب الأذن بالمراقبة

نصت العديد من التشريعات الوطنية، كالقانون الأمريكي والبلجيكي، على هذا الشرط الهام. أما المشرع الجزائري، فقد اشترط التعليل في حالة المراقبة الإلكترونية ضمن قانون الإجراءات الجزائية، بخلاف إجراء التسرب، الذي يستوجب أن يكون الإذن به مسببا تحت طائلة البطلان، وفقا لما تنص عليه المادة 65 مكرر 15 من ذات القانون. كما أن التعديل الدستوري لسنة 2020 أشار بدوره إلى ضرورة تسبيب الإذن بالمراقبة الإلكترونية، حيث نصت المادة 3/47 على أنه: لا يجوز المساس بالحقوق والحريات المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية[2].

[1]-فوزي عمارة، المرجع السابق، ص 240.

[2]-المرجع نفسه، ص 238.

د- تحديد مدة المراقبة

وفقا للمادة 65 مكرر 7 من قانون الإجراءات الجزائية، فإن مدة إجراء عملية الاعتراض محددة بأربعة أشهر، ويمكن تجديدها وفقا للشروط الشكلية والزمنية المحددة. ويجب أن يتم تحديد تاريخ بدء العملية وتاريخ انتهائها بدقة، لضمان تنفيذ الإجراءات في إطار زمني محدد وشفاف.

الفرع الثاني: التسرب الإلكتروني

يتطلب فهم مفهوم التسرب الإلكتروني دراسة متعمقة تشمل ثلاثة محاور رئيسية: التعريف الدقيق للمفهوم، استعراض الصور المختلفة للتسرب الإلكتروني، والضوابط القانونية التي تنظم عملياته وتضمن حماية الحقوق والخصوصية.

أولا: تعريف التسرب الإلكتروني:

التسرب لغة مشتق من فعل تسرب أي دخل وانتقل خفية، توغل [1]، التسرب الإلكتروني هو إجراء أمني وقضائي يتيح لضابط الشرطة القضائية التسلل إلى أنظمة المعلومات أو شبكات الاتصالات الإلكترونية للمشتبه فيهم في جرائم محددة قانونا، بهدف جمع الأدلة والمتابعة القضائية، ويتم ذلك في إطار من الضوابط القانونية الصارمة.

وهو ذات المعنى الذي أشار إليه المشرع الجزائري في المادة 26 من القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية، حيث تنص على أنه: مع مراعاة أحكام قانون الإجراءات الجزائية، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت إشرافه لضابط الشرطة القضائية بالتسرب الإلكتروني إلى منظومة معلوماتية أو إلى نظام واحد أو أكثر من أنظمة الاتصالات الإلكترونية،

[1]-المنجد الأبجدي، المطبعة الكاثوليكية، دار المشرق، بيروت، لبنان، 1967.

بهدف مراقبة الأشخاص المشتبه في ارتكابهم لأي من الجرائم المنصوص عليها في هذا القانون، وذلك من خلال إيهامهم بأنه فاعل معهم أو شريك لهم...[1]، النص المذكور مستمد مباشرة من المادة 16 من القانون رقم 20-15 الخاص بالوقاية من اختطاف الأشخاص ومكافحتها، حيث ورد بنفس الصياغة[2].

وبناء على ذلك، فإن التسرب الإلكتروني يشبه إلى حد كبير التسرب المادي، إذ ينطوي كلاهما على مفهوم التوغل، غير أن الفرق بينهما يكمن في طبيعة محل هذا التوغل؛ ففي التسرب المادي يتم التوغل بشكل مباشر بين مجموعة من المجرمين في العالم الواقعي الملموس، بينما يتم التوغل في التسرب الإلكتروني داخل منظومة معلوماتية أو أكثر[3].

أطلق على هذه العملية عدة تسميات، من بينها التسرب الإلكتروني الرقمي، الدوريات السيبرانية أو الافتراضية، إضافة إلى التحقيق والتحري تحت اسم مستعار عبر الإنترنت.

يختلف التسرب الإلكتروني عن المراقبة الإلكترونية، إذ يتجاوز المتسرب الإلكتروني حدود المراقبة التقليدية، حيث يتفاعل مباشرة مع المشتبه بهم، في حين تقتصر المراقبة الإلكترونية على متابعة الاتصالات الإلكترونية والتقاطها وتسجيلها بشكل فوري دون أي احتكاك مباشر.

---

[1] -قانون رقم 20-05 مؤرخ في 18 أبريل 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية، ج . ر . ج.ج، العدد 25، الصادر في 19 أفريل 2020.

[2]-قانون رقم 20-15 مؤرخ في 30 ديسمبر 2020، يتعلق بالوقاية من اختطاف الأشخاص ومكافحتها، ج. ر.ج. ج، العدد 81 في 30 ديسمبر2020.

[3]- المادة 2 القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

كما أن المراقبة الإلكترونية تعد إجراء وقائيا يهدف إلى متابعة الأنشطة المشبوهة، بينما يعتبر التسرب الإلكتروني إجراء وقائيا وردعيا، حيث يلجأ إليه ليس فقط لجمع الأدلة وإحباط المخططات الإجرامية قبل تنفيذها، ولكن أيضا لضبط المشتبه بهم، تحديد هوياتهم، ومعاقبتهم بعد ارتكاب الجريمة.

ثانيا: صور المتسرب الإلكتروني:

منح المشرع الجزائري للضابط المتسرب صلاحية إيهام الأشخاص المشتبه في ارتكابهم جرائم اختطاف الأشخاص، وجرائم التمييز وخطاب الكراهية، بأنه شريك أو فاعل معهم، وقد اقتصر على هاتين الصورتين دون الإشارة إلى حالة المتسرب كخاف. ومع ذلك، إذا تأملنا قانون الإجراءات الجزائية الفرنسي، خاصة المواد 1.35.706 و3.47.706، نجد أن المشرع الفرنسي لم يذكر هذه الصور بشكل صريح، بل اكتفى بالإشارة إلى الأفعال التي يسمح للعون أو الضابط القيام بها.

وهذا النهج يبدو منطقيا، لأن منح الضابط صلاحية إيهام المشتبه بهم بأنه شريك أو فاعل معهم، يتعارض تماما مع ما ورد في النصوص المنظمة للتسرب الإلكتروني في قانون الإجراءات الجزائية الجزائري. فهذه النصوص تحظر بشكل قاطع على الضابط القيام بأي فعل أو تصرف قد يؤدي إلى تحريض المشتبه بهم على ارتكاب جريمة بغرض الحصول على دليل ضدهم، ومن الجدير بالذكر أن قانون العقوبات يعتبر الشخص فاعلا أصليا إذا ساهم مباشرة في تنفيذ الجريمة أو حرض عليها من خلال القيام بأعمال معينة.

حتى في حالة التسرب المادي، ورغم أن القانون يجيز للضابط أو العون ارتكاب بعض الأفعال التي يعاقب عليها القانون في الأحوال العادية، إلا أن ما يحدث فعليا في الواقع العملي هو أن الضابط أو العون لا يقوم بأي من تلك الأفعال، بل يكتفي بمرافقة المشتبه فيهم خلال تنفيذهم للعمليات، ويكون بذلك مجرد شاهد عيان على ما يجري.

كما أن صورة المتسرب كناقل لأشياء الجريمة لم يرد ذكرها في التشريع الجزائري ضمن أشكال التسرب الإلكتروني، وذلك على عكس ما قد يحدث في العالم الواقعي، حيث يمكن فعلا إخفاء الأدلة أو الأشياء المتحصلة من الجريمة، وهو ما يصعب تخيله في البيئة الرقمية. وقد أحسن المشرع الفرنسي عندما لم يحدد صورا للمتسرب، بل اكتفى بذكر نوعية الأعمال التي يجوز للضابط أو العون القيام بها.

وبناء عليه، نرى أن المتسرب الإلكتروني لا يمكن تصنيفه ضمن صور محددة، بل يتمثل دوره في محاولة استدراج المشتبه فيهم عن طريق التفاعل معهم والدخول في مجموعاتهم، من خلال إيهامهم بتشاركه معهم نفس الأهداف والمخططات.

ثالثا: الضوابط القانونية لتنفيذ إجراء التسرب

تجرى إجراءات التسرب الإلكتروني تحت إشراف مباشر من السلطة القضائية، المتمثلة في وكيل الجمهورية وقاضي التحقيق، وذلك بالحصول على إذن مكتوب قبل الشروع في عملية التسرب (الفرع الأول) ، وعقب الانتهاء من المهمة ضمن الفترة المحددة قانونا، م[1]يتولى ضابط الشرطة القضائية تحرير محضر مفصل حول عملية التسرب (الفرع الثاني).

1- ضرورة الحصول على إذن التسرب بين النيابة أو قاضي التحقيق

تقتضي الشرعية الإجرائية أن يكون القانون هو المرجع الأساسي الذي يستمد منه ضابط الشرطة القضائية القواعد المنظمة لعمليات التحري، مع ضرورة تنفيذ هذه التحريات تحت إشراف ومراقبة السلطة القضائية. لذا، يتعين على ضابط الشرطة

[1]-وهو ما أقرته المادة 65 مكرر 15 على أنه : " ... ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر، يمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية"

القضائية الحصول مسبقا على إذن من وكيل الجمهورية قبل مباشرة أي إجراء، وفي حال فتح تحقيق رسمي في القضية، تصبح هذه المهمة من اختصاص قاضي التحقيق.

وقد منح المشرّع الجزائري لوكيل الجمهورية، إلى جانب إشرافه على أعمال الضبطية القضائية، سلطة إصدار الإذن لضابط الشرطة القضائية للقيام بإجراءات التسرب الإلكتروني، وفقا للصورة والتقنية المناسبة للجريمة محل المتابعة. إن الحصول على إذن مسبق من السلطة المختصة أو الجهة المشرفة على أعمال الضبطية القضائية يمنح صفة المشروعية لهذا الإجراء، رغم تعارضه مع حق الخصوصية الرقمية للمشتبه فيه.

أقرت الفقرة الأولى من المادة 65 مكرر 7 بأن الإذن المنصوص عليه في المادة 65 مكرر 5 يجب أن يتضمن كافة العناصر التي تتيح التعرف على طبيعة الاتصالات المطلوب اعتراضها، وتحديد الأماكن المستهدفة سواء كانت سكنية أو غير سكنية، إضافة إلى تحديد نوع الجريمة التي تبرر اتخاذ هذه الإجراءات، مع التنصيص على المدة الزمنية المقررة لتنفيذ الإجراء، والتي لا تتجاوز أربعة أشهر[1].

اشترطت هذه البيانات في الإذن لتسهيل عملية المراقبة واكتشاف أي تجاوزات قد تحدث نتيجة مخالفة الضابط للإذن الممنوح له. كما تهدف إلى تجنب الوقوع في أخطاء تنفيذية قد تؤدي إلى تعريض حرمة الأفراد وخصوصياتهم لخطر الانتهاك. لذلك، يجب تحديد العملية المراد تنفيذها، والموقع المخصص لتنفيذها، والأشخاص المستهدفين، وكذلك نوع العملية[2].

[1]–دراجي عبد القادر استحداث آليات جديدة للتحري والمتابعة في إطار مكافحة الفساد، مجلة الحقوق والحريات، كلية الحقوق جامعة باتنة 01 العدد 02 لشهر مارس 2016، ص 275.

[2]–ياسر الأمير فاروق مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، القاهرة، 2009ص570 .

2- تحرير محاضر التسرب توثيق العملية بدليل تقني

وفقا لنص المادة 18 من قانون الإجراءات الجزائية، توثّق جميع محاضر الضبطية القضائية في وثائق رسمية موقعة من قبل المكلف بالمهمة، حيث يلزم ضباط الشرطة القضائية بتحرير محاضر تفصيلية حول أعمالهم، وإبلاغ وكيل الجمهورية دون تأخير بالجنايات والجنح التي يطلعون عليها.

وتنص المادة 65 مكرر 09 من القانون ذاته على إلزام الضباط، أثناء تنفيذ مهام المراقبة الإلكترونية، بتوثيق جميع إجراءاتهم في محاضر رسمية، بحيث تشمل جميع مراحل المراقبة، وما تم تثبيته وتسجيله، بما في ذلك المواد المصورة والمرئية التي تم جمعها خلال العملية [1].

أوجب المشرع الجزائري على ضابط الشرطة القضائية أن يحرر محضرا عن كل مرحلة من مراحل العملية التي ينفذها، يوضح فيه الإجراءات المتخذة والنتائج التي أسفرت عنها من أدلة. فلا يجوز تأجيل تحرير المحاضر حتى المرحلة النهائية. يتضمن كل محضر تاريخ ووقت بداية العملية ونهايتها، كما يجب أن يرفق المحضر بنتائج العملية التي تشمل وصفا أو نسخة من المراسلات أو الصور أو المحادثات الهامة التي تساهم في إظهار الحقيقة. كما يحدد المحضر الجوانب التقنية المستخدمة في العملية، مثل الأجهزة المستعملة ومكان تثبيتها. وفي نهاية المهمة، ترفق هذه المحاضر ضمن أوراق ملف الدعوى أمام القاضي المختص، سواء كان وكيل الجمهورية أو قاضي التحقيق. [2]

[1]-تنص المادة 65 مكرر 09 من قانون الإجراءات الجزائية على أنه : "يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرق القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع ترتيبات تقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري."

[2]-سعدون فاطمة السياسة الجنائية الإجرائية لمكافحة جرائم الإرهاب، مذكرة ماجستير في الحقوق، كلية الحقوق جامعة الجزائر 1 الجزائر 2014، ص 69.

خلاصة

يتناول هذا الفصل الجهود المؤسسية والإجرائية المعتمدة في الجزائر لمواجهة الجريمة الإلكترونية، من خلال محورين أساسيين: الوقاية والتحقيق.

في الجانب الوقائي، تم تسليط الضوء على الآليات المؤسساتية كـــالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، إلى جانب دور الضبط الإداري في رصد ومتابعة الأنشطة المشبوهة. كما تم التطرق إلى دور الضبط القضائي والمؤسسات القضائية والعقابية خلال مرحلة التحقيق والمتابعة القضائية.

أما في الجانب الإجرائي، فقد تم استعراض الإجراءات التقليدية المتبعة في الجرائم المعلوماتية، مثل التفتيش، ضبط الأدلة، المعاينة والخبرة التقنية، إلى جانب الإجراءات المستحدثة التي فرضها تطور الجريمة الإلكترونية، كـــالاعتراض والمراقبة الإلكترونية والتسرب الإلكتروني، باعتبارها آليات متقدمة لتعقب المجرمين في الفضاء الرقمي.

تبرز هذه المعالجة أهمية تكامل الأدوار بين مختلف الفاعلين والوسائل القانونية والتقنية، لضمان نجاعة الردع والمواجهة في ظل التحديات المتسارعة التي تفرضها الجرائم الإلكترونية.

خاتمة

في الختام، يمكن تلخيص النتائج في النقاط التالية:

- الجريمة الإلكترونية ظاهرة مستحدثة تختلف في طبيعتها القانونية عن الجرائم التقليدية، ما يجعل القوانين والإجراءات القديمة غير كافية لمكافحتها.
- اتبع المشرع الجزائري نهجا مزدوجا بتعديل قانون العقوبات والإجراءات الجزائية، واستحداث قوانين خاصة مثل القانون رقم 09-04 لمواجهة هذه الجرائم.
- التشريعات الجديدة تهدف إلى حماية الحقوق الدستورية، خاصة حق المؤلف وحرمة الحياة الخاصة، وتقليل تأثير الجرائم الإلكترونية على المجتمع.
- رغم ذلك، لا تزال هناك نقائص في التشريعات الحالية وصعوبات في تطبيقها، مما يتيح أحيانا إفلات المجرمين من العقاب.
- من أبرز التحديات القانونية تنازع الاختصاص القضائي وتحديد القانون الواجب التطبيق في الجرائم العابرة للحدود.
- الإجراءات الجزائية للجرائم الإلكترونية تتميز بخصوصية تتطلب أساليب متخصصة في البحث، الضبط، والتثبت.
- تم توسيع قواعد الاختصاص القضائي لمواكبة طبيعة الجرائم الإلكترونية العابرة للحدود.
- التطور التشريعي، وخاصة إصدار القانون رقم 09-04، يعد خطوة مهمة لتعزيز منظومة مكافحة هذه الجرائم.

التوصيات:

لا تخفى خطورة الجريمة الإلكترونية التي تتزايد بسرعة، مما يستدعي تعزيز آليات المكافحة والتشريع. ومن أبرز الاقتراحات:

- تعزيز التعاون التشريعي والقضائي والأمني على المستويات الوطنية والدولية لمكافحة هذه الجرائم.
- دعم الدراسات الميدانية والأكاديمية لفهم دوافع الجريمة الإلكترونية والحد منها.
- توفير كوادر متخصصة في التحقيق الجنائي الإلكتروني.
- تنظيم الجانب القانوني لقيمة الأدلة الرقمية وإثباتها.
- تأسيس أجهزة وطنية للأمن السيبراني ضمن وزارة الدفاع الوطني.
- تدريب وحدات عسكرية وأمنية لحماية الأنظمة المعلوماتية من الهجمات السيبرانية.
- وضع نظام قانوني شامل وإنشاء محاكم متخصصة للجرائم المستحدثة.
- إبرام اتفاقيات دولية وإقليمية لمواجهة الجريمة الإلكترونية عبر الحدود.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: النصوص القانونية

❖ **الدساتير:**

- دستور ج ج د ش لسنة 2020، المؤرخ في 2020/12/30، الجريدة الرسمية رقم 82.

❖ **القوانين:**

- القانون رقم 86-05 المؤرخ في 04 مارس 1986، الجريدة الرسمية، العدد 10، المعدل والمتمم لقانون الإجراءات الجزائية.
- القانون رقم 06-22 المؤرخ في ديسمبر 2006، المعدل لقانون الإجراءات الجزائية.
- القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47.
- القانون رقم 20-05 المؤرخ في 18 أفريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية، الجريدة الرسمية، العدد 25.
- القانون رقم 20-15 المؤرخ في 30 ديسمبر 2020، المتعلق بالوقاية من اختطاف الأشخاص ومكافحتها، الجريدة الرسمية، العدد 81.
- قانون العقوبات رقم 04-15 المؤرخ في 10 نوفمبر 2004 هو قانون يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات الجزائري.

❖ **الأوامر:**

- الأمر رقم 66-155 المؤرخ في 08 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.
- الأمر رقم 21-11 المؤرخ في 25 أوت 2021، هو أمر يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 جوان 1966 المتضمن قانون الإجراءات الجزائية الجزائري.

❖ **المراسيم:**

- القرار الوزاري المؤرخ في 14 أفريل 2007، المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية، العدد 36، الصادرة في 03 جويلية 2009.

ثانيا: الكتب

- أحسن بوسقيعة، التحقيق القضائي، ط1، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014.
- إسحاق إبراهيم منصور، علم الإجرام والعقاب، ط2، ديوان المطبوعات الجامعية، الجزائر، 1991.
- بن سعيد صبرينة، الجريمة المستحدثة، دار الباحث، ط1، 2022.
- بوكرر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن منشورات الحلبي الحقوقية، ب ط، بيروت، 2012.

- خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي للنشر والتوزيع، الجزائر، ط2، 2008.
- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، ط1، 2008.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2008.

- ربيحة زيدان، الجريمة الإلكترونية: دراسة تحليلية في ضوء التشريع الجزائري، دار هومة، الجزائر، 2011.
- سليمان أحمد فضل، الجرائم الإلكترونية وسبل مواجهتها: دراسة مقارنة، دار المسيرة، عمّان، 2010.

- عبد العال الديري، محمد صادق إسماعيل، الجرائم الإلكترونية، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012.
- عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2007.
- عبد الله عبد الكريم، جرائم المعلوماتية والأنترنت، الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، 2011.
- عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، ط1، دار الثقافة، الأردن.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، 2004.
- المنجد الأبجدي، المطبعة الكاثوليكية، دار المشرق، بيروت، لبنان، 1967.
- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013.

- نبيه صالح، الوسيط في شرح مبادئ الإجراءات الجزائية، منشأة المعارف القانونية للنشر، عمان، دون طبعة.
- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، القاهرة، 2009.
- يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي – دراسة مقارنة، ط1، دار الخلدونية، الجزائر، 2021.

ثالثا: الرسائل الجامعية

❖ **الدكتوراه:**

❖ ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في الحقوق، جامعة باتنة، 2016.
❖ فهد عبد الله العبيد العازمي، الجريمة الإلكترونية: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.
❖ فوزي عمارة ، اعتراض المراسلات وتسجيل الاصوات والتقاط الصور والتسرب كاجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الانسانية، ، كلية الحقوق والعلوم السياسية، جامعة منتوري قسنطينة العدد 33، 2010 جوان.

❖ **الماجستير:**

- سعدون فاطمة، السياسة الجنائية الإجرائية لمكافحة جرائم الإرهاب، مذكرة ماجستير، جامعة الجزائر 1، 2014.
- سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، ماجستير، جامعة الحاج لخضر باتنة، 2012-2013.

- سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية وعلوم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد تلمسان، 2011.
- صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري – تيزي وزو، 2013.
- عائشة بوخبزة، الحماية الجزائية من الجريمة السيبرانية في التشريع الجزائري، مذكرة ماجستير، جامعة وهران، 2013.

ج. الماستر:

- عبد اللطيف دحية وآخرون، المواجهة الإجرائية لجرائم المعلوماتية، مذكرة ماستر، جامعة محمد بوضياف – المسيلة، 2019.
- ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة ماستر، جامعة العربي بن مهيدي – أم البواقي، 2015-2016.

د. أخرى:

- زيدان نبيل، دواقي يزيد، الجريمة المعلوماتية ودور الدرك الوطني، مذكرة تخرج لنيل شهادة القيادة والأركان، الدفعة 18، 2014-2015.

رابعا: المجلات والمقالات العلمية

- رضا هميسي، تفتيش المنظومات المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والسياسية، 2012.

- دراجي عبد القادر، استحداث آليات جديدة للتحري والمتابعة في إطار مكافحة الفساد، مجلة الحقوق والحريات، جامعة باتنة 1، العدد 2، مارس 2016.
- أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة.
- براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري، تيزي وزو، نوفمبر 1997.
- مزيود سليم، دور المؤسسات الاجتماعية في الوقاية من الجرائم المعلوماتية، المجلة الجزائرية للاقتصاد والمالية، العدد 11، أفريل 2019.
- برباح يمينة، تطبيقات الأمن المعلوماتي، مداخلة في ملتقى وطني، المركز الجامعي غليزان، 7-8 فيفري 2017.
- فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، الملتقى الدولي الرابع عشر حول الجرائم الإلكترونية، طرابلس، 24-25 مارس 2017.
- محفوظة الأمير عبد القادر، غرداين حسام، الجريمة الإلكترونية وآليات التصدي لها، ملتقى وطني، الجزائر، 29 مارس 2017.

1. سومية عكور، الجرائم المعلوماتية وطرق مواجهتها: قراءة في المشهد القانوني والأمني، ملتقى علمي، كلية العلوم الاستراتيجية، الأردن.
2. عبد الناصر محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية "دراسة تطبيقية مقارنة"، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007.
3. محمد فتحي عيد، "مقومات التعاون الدولي في مجال مكافحة المخدرات"، بحث مقدم في الندوة العلمية: التعاون الدولي في مجال مكافحة المخدرات، المنظمة من

قبل أكاديمية نايف العربية للعلوم الأمنية، الرياض، خلال الفترة من 9 إلى 11 ديسمبر 2000.

خامسا: المواقع الإلكترونية

- محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني،
- www.wata.cc
- إنتل سكيوريتي، خسائر قطاعات الأعمال من الهجمات الإلكترونية،
- www.aitnews.com
- عبد الإله مجيد، القراصنة يفضلون استهداف الدول الغنية،
- www.elaph.com
- منى شاكر فراج العسيلي، مقال منشور على
- http: //kenanaonline.com
- مركز هردو لدعم التعبير الرقمي، التنظيم القانوني والجرائم الإلكترونية، القاهرة، 2018.

سادسا: المراجع باللغة الأجنبية

- BENNOUAR Abdelhakim, Les techniques spéciales d'enquête et d'investigation en Algérie, article publié sur www.memoireonline.com

Serge Guichard, Jacques Buisson, Procédure Pénale, Édition Litec, N° 06, Paris, 2010.

فهرس المحتويات

فهرس المحتويات

Contenu

ملخص

ركز المشرع الجزائري اهتماما كبيرا على مواجهة جريمة الإنترنت، حيث وضع إجراءات وتدابير متعددة للتصدي لهذا النوع الجديد من الجرائم. ولتحقيق ذلك، اتبع المشرع سياسة مزدوجة في المكافحة، فقد أجرى تعديلات مهمة على قانون العقوبات بدءا من تعديل عام 2004 بالقانون رقم 04-15، ثم في تعديل آخر سنة 2006 بموجب القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، والتي تشكل القواعد العامة لمكافحة هذه الجرائم.

لكن المشرع لم يكتفِ بهذا فقط، بل قام أيضا بإصدار قوانين خاصة تركز على الوقاية والقمع، من أبرزها القانون رقم 09-04 الذي يحتوي على قواعد خاصة بالوقاية المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحة الجرائم الإلكترونية. والهدف الأساسي من هذه التشريعات هو القضاء على هذه الجرائم الخطيرة، أو على الأقل الحد من انتشارها وتأثيرها.

الكلمات المفتاحية:

الجريمة الإلكترونية، التجريم، التحقيق، المجابهة الجزائية، المؤسسات، الأدلة الرقمية.

Abstract :

The Algerian legislator has placed great emphasis on combating cybercrime by establishing various measures and procedures to address this emerging type of crime. To achieve this, the legislator adopted a dual approach in combating it, making significant amendments to the Penal Code, starting with the 2004 amendment under Law No. 04-15, followed by another amendment in 2006 under Law No. 06-22, which amended and supplemented the Code of Criminal Procedure. These amendments form the general framework for combating such crimes.

However, the legislator did not stop there; special laws were also enacted focusing on prevention and repression, most notably Law No. 09-04, which includes specific provisions related to the prevention of cybercrime through information and communication technology. The primary goal of these legislations is to eliminate these serious crimes or at least reduce their spread and impact.

Keywords: Cybercrime, Criminalization, Investigation, Criminal Enforcement, Institutions, Digital Evidence