



وزارة التعليم العالي والبحث العلمي

جامعة المجاهد عبد الحفيظ بوصوف – ميله –
كلية الحقوق



الرقم التسلسلي:.....

الرمز:.....

القسم: الحقوق

التخصص: القانون الجنائي

خصوصية إجراءات البحث والتحري عن الجريمة الإلكترونية

مذكرة ضمن متطلبات نيل شهادة

ماستر

إشراف الأستاذ:

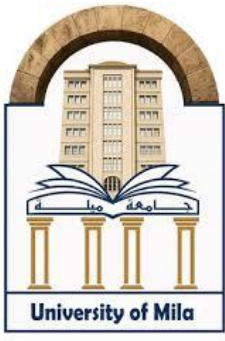
د / شطبي عبد السلام

إعداد الطالبتين:

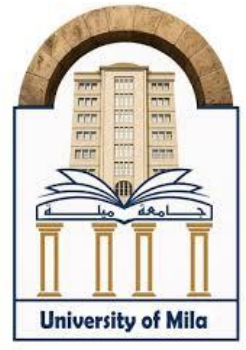
– لهشيلي شيماء

– لشيلي شيماء

السنة الجامعية: 2026/2025



وزارة التعليم العالي و البحث العلمي
جامعة المجاهد عبد الحفيظ بوصوف - ميله -
كلية الحقوق



الرقم التسلسلي: ...

القسم: الحقوق

الرمز:

التخصص: القانون الجنائي

خصوصية إجراءات البحث والتحري عن الجريمة الإلكترونية

مذكرة ضمن متطلبات نيل شهادة

ماستر

إشراف الأستاذ:

د / شطيبي عبد السلام

إعداد الطالبتين:

– لهشيلي شيما

– لشيلي شيما

أعضاء لجنة المناقشة

رئيسا	جامعة عبد الحفيظ بوصوف ميله	أستاذ محاضر 'ب'	د/ بوصبع فؤاد
مشرفا ومقررا	جامعة عبد الحفيظ بوصوف ميله	أستاذ محاضر 'أ'	د/ شطيبي عبد السلام
عضو مناقش	جامعة عبد الحفيظ بوصوف ميله	أستاذ محاضر 'ب'	د/ شباح بوزيد

السنة الجامعية: 2025/2026

ملخص:

تناولت هذه الدراسة أساليب التحقيق والتحري في مجال الجرائم الإلكترونية، من خلال مقارنة تجمع بين البعدين النظري والتطبيقي، فعلى الصعيد النظري عرفنا الجريمة الإلكترونية فقها وتشريعا في ضوء القانون الجزائي، وبيننا خصائصها كما استعرضنا أنماط الجناة ودوافعهم السياسية والاقتصادية والشخصية، مع تحليل الأركان الثلاثة للجريمة وتصنيفها بين جرائم ماسة بالأشخاص والأموال وجرائم التجارة الإلكترونية.

أما على الصعيد التطبيقي فقد درسنا الوسائل القانونية والتقنية المعتمدة في إجراءات البحث والتحري وحددنا الجهات المختصة بمكافحة هذه الجرائم، كما سلطنا الضوء على الدليل الإلكتروني من حيث مفهومه وخصائصه وأشكاله والصعوبات المتعلقة به، وقد أجرينا دراسة ميدانية تضمنت تحليل حكم قضائي في جنحة عرض إعلان مخل بالحياء.

وختمنا الدراسة بجملة من النتائج والتوصيات الرامية إلى تعزيز الإطار القانوني وتحديث آليات التحقيق بما يواكب التطور المتسارع للجريمة الإلكترونية.

الكلمات المفتاحية: إجراءات البحث والتحري، الجريمة الإلكترونية، الدليل الإلكتروني، الإثبات الإلكتروني الشرطة القضائية.

This study examines investigative and inquiry methodologies in the field of cybercrime through an approach that combines both theoretical and applied dimensions.

On the theoretical level, we define cybercrime from doctrinal and legislative perspectives in light of Algerian law, survey offender typologies and their political, economic, and personal motivations, and analyze the three constituent elements of the offense alongside its classification into crimes property, and electronic commerce offenses.

On the applied level, we examine the legal and technical instruments employed in search and investigation procedures, identify the competent authorities responsible for combating these offenses, and shed light on digital evidence with regard to its definition, distinguishing characteristics, forms, and the challenges associated with it. This is supported by a field study comprising the legal analysis of a judicial ruling in a misdemeanor case involving the display of an indecent advertisement.

The study concludes with a set of findings and recommendations aimed at strengthening the legal framework and modernizing investigative mechanisms in a manner commensurate with the rapid and accelerating evolution of cybercrime.

Keywords : Search and investigation procedures, Cybercrime, Electronic guide, Electronic proof, Judicial police.

الإهداء

"وقل إعملوا فسيرى الله عملكم ورسوله والمؤمنون وستردون إلى عالم الغيب والشهادة فينبئكم بما كنتم تعملون"
(التوبة 105)

صدق الله العلي العظيم

الحمد لله الذي بفضلته تتحقق الغايات من بعد الاستعانة به وإنهاء الدرب بتوقيقه وتحقيق الحلم بفضلته، لم تكن الرحلة قصيرة ولا الطريق محفوظا بالتسهيلات، لكنني فعلتها، فالحمد لله الذي يسر لنا البدايات وبلغنا النهايات بفضلته وكرمه. أهدي هذا النجاح لنفسي أولا ثم إلى كل من سعى معي لإتمام هذه المسيرة دمت لي سندا لا عمرا.

وبكل حب أهدي ثمرة نجاحي وتخرجي إلى النور الذي أثار دربي والسراج الذي لا ينطفئ نوره والذي بذل جهد السنين من أجل أن أعتلي سلالمة النجاح إلى من أحمل اسمه بكل فخر، من بدل الغالي والنفيس واستمدت منه قوتي واعتزازي بذاتي، من كان نعمة من الله وسندا لا يميل (والدي العزيز حفظه الله)

إلى روح أمي الطاهرة... التي رحلت عني جسدا وبقيت دعواتها ترافقني في كل دارك ومشواك، التي تسكن قلبي رغم غيابها، كل نجاح هو استمرار لحنانك الذي لا ينتهي، أهديك ثمرة جهدي وتعب سنواتي، راجية من الله أن يتقبلها صدقة جارية لروحك الطيبة. إليك أيتها الحبيبة، الغائبة الحاضرة في كل تفاصيل حياتي، كل نجاح أحق أن يهدى لك، فأنت من غرست في نفسي حب العلم والإصرار، رحمك الله وجعل قبرك روضة من رياض الجنة.

إلى إخواني الأعزاء، أتم السند والدعم، حفظكم الله ووفقكم.

إلى صديقاتي اللاتي جعلوا هذه الرحلة أكثر متعة وأقل صعوبة، شكرا لكل لحظة ودعم، لكل كلمة مشجعة، ولكل الذكريات الجميلة التي صنعناها معا (شيماء، إكرام، آسيا، خديجة، نهلة، جيهان، باية، سلطنة).

إلى كل من قام بدعمي وساندي في مسيرتي ودعمني من قريب أو من بعيد عائلتي الغالية من كبيرها لصغيرها، أهدي لكم تخرجي هذا.

" فإن مع العسر يسرا (5) فإن مع العسر يسرا (6) "

بعد كل تعب وسهر، جاء اليسر بفضل الله وبدعمكم، هذا النجاح ليس لي وحدي بل لكم جميعا، فقد كنتم سنداً لي شكرا من القلب، وأتمنى أن أكون مصدر فخركم كما كنتم مصدر قوتي.

شيماء لهشيلي

الإهداء

بسم الله الرحمن الرحيم

الحمد لله رب العالمين والصلاة والسلام على خاتم الأنبياء.

"من قال: أنا لها، نالها بإذن الله" لم تكن الرحلة قصيرة ولم يكن من المنتظر ولها أن تكون كذلك، كما لم يكن الطريق ممهدا أو محفوظا بالتسهيلات، غير أن الإصرار والعزيمة كانا أقوى من كل الصعوبات، فكان السعي المتواصل سبيلا لتحقيق هذا الحلم الذي بدا بعيد المنال، وها أنا اليوم أصل إلى مسك الختام بعد رحلة من الجهد والاجتهاد لأقطف ثمرة تعب طال انتظاره، في يوم كان بالأمس حلما وأصبح اليوم واقعا.

إلى رغم كل ما مررت به، إلى نفسي التي ظلت صامدة... هذا الإهداء لك، ليس فخرا بإنجاز يرى بل عرفانا بصبر طويل، وعهدا أنني مهما تكررت المحن سأواصل.

إلى من كلل العرق جبينه وعلمني أن النجاح لا يأتي إلا بالصبر والإصرار، إلى من لا ينفصل اسمي عن اسمه، إلى مصدر الدعم والعطاء، إلى داعمي الأول وسندي وقوتي بعد الله، إلى فخري واعتزائي، أهدي تخرجي إلى من حصد الأشواك عن دربي ليمهد لي طريق العلم... بابا الغالي رعاه الله وبارك في عمره.

إلى التي جعلت الجنة تحت أقدامها صاحبة اليد الخفية والقلب الحنون، إلى من كانت النور حين أظلمت دروبي، إلى من غرست في قلبي حب العلم وسقيت طموحي بدعوائك الصادقة، إلى سر قوتي ونجاحي... أمي الغالية حفظها الله وأطال في عمرها تخرجي اليوم هو ثمرة صبرك وفخرك هو إنجاز لي.

إلى ضلعي الثابت سندي الذي لا يميل، ورفاق عالمي الصغير، واليد التي تمتد لي قبل أن أطلب، إلى من كانوا دائما جزءا من قوتي وسببا في أن أقف بثبات في أصعب الأيام، إلى من كان وجودهم نعمة لا تقدر... لإخوتي وأخواتي الأعزاء إليكم يا من كنتم نور أيامي، دمت لي.

إلى من معهن كانت الأيام أسهل والضحكات أجمل، إلى رفاق الرحلة الذين ساهموا في صنع ذكريات لا تنسى، وجودكم كان فرحة لقلبي وسندا لتجاوز الصعوبات... صديقاتي الوفيات

ولكل من وقف إلى جانبي وترك أثرا طيبا في قلبي، أو دعم خطوة من خطواتي، أو قال كلمة صنعت فرقا... لكم جميعا أجمل معاني الامتنان والدعاء. وها أنا اليوم أرفع مشروعني هذا عربون شكر لله تعالى، الذي وفقني ومنحني القدرة على الوصول إلى هذه المرحلة التي لطالما حلمت بها.

شيماء لشيلي

الشكر والتقدير

الحمد لله أولا وآخرا الذي بنعمته تتم الصالحات، نحمده سبحانه وتعالى على توفيقه وإعائته لإتمام هذا العمل المتواضع، بداية يشرفنا أن نتقدم بأسمى عبارات الشكر إلى جامعتنا "الشهيد عبد الحفيظ بوالصوف ميله" التي تفضلت باحتضاننا وخلال مشوارنا الدراسي وأتاح لنا فرصة الاستفادة من خبراتها وإمكانياتها العلمية والعملية، ثم نتقدم بخالص عبارات الشكر والتقدير والاحترام إلى أستاذي المشرف على هذه المذكرة، على توجيهاته القيمة، ونصائحه العلمية السديدة، ومتابعته المستمرة التي كان لها الأثر البالغ في إنجاز هذا العمل في أحسن صورة ممكنة، منا جزيل الشكر وعظيم الإمتنان.

كما نتوجه بالشكر إلى أعضاء لجنة المناقشة الموقرة على تفضلهم بقبول قراءة هذه المذكرة وتقييمها، وعلى ما سيقدمونه من ملاحظات وإثراءات علمية قيمة تساهم في تطوير هذا البحث. ولا يفوتنا أن نعبر عن امتناننا لكل أساتذتنا الكرام الذين أشرفوا على تكويننا العلمي والأكاديمي خلال مشوارنا الدراسي، وكان لهم الفضل بعد الله في ما وصلنا إليه من مستوى علمي. كما نخص بعبارات الشكر والعرفان إلى من كانوا اليد التي تمتد لترفعنا حين تضعف العزائم، شكرا لعائلتنا على دعمهم المعنوي وتشجيعهم الدائم، وساندتهم لنا سواء من قريب أو من بعيد، من أجل إنجاز هذا العمل. وفي الأخير نسأل الله تعالى أن يجعل هذا العمل خالصا لوجهه الكريم وأن ينفع به، وأن يكون لبنة تضاف إلى صرح العلم، وأن يجعله شاهدا على جهد بذل في سبيل المعرفة ورمزا للإصرار والمثابرة، فإن أصبت فذلك بفضل الله وإن أخطأت فحسب الإنسان أنه اجتهد سعى.

والله ولي التوفيق، وهو نعم المولى ونعم النصير.

فهرس المحتويات

فهرس المحتويات

الصفحة	العنوان
أ-ب	ملخص
ج-د	الإهداء
هـ	الشكر
11	مقدمة
الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية	
18	تمهيد
19	المبحث الأول: مفهوم الجريمة الإلكترونية
19	المطلب الأول: تعريف الجريمة الإلكترونية
19	الفرع الأول: التعريف الفقهي للجريمة الإلكترونية
21	الفرع الثاني: التعريف التشريعي للجريمة الإلكترونية
23	الفرع الثالث: أنماط الجناة في الجريمة الإلكترونية
25	المطلب الثاني: خصائص الجريمة الإلكترونية
25	الفرع الأول: من حيث الركن المادي
26	الفرع الثاني: من حيث الإثبات
26	الفرع الثالث: من حيث التبليغ
27	المطلب الثالث: دوافع ارتكاب الجريمة الإلكترونية
27	الفرع الأول: الدوافع السياسية
28	الفرع الثاني: الدوافع المادية
28	الفرع الثالث: الدوافع الشخصية
29	المبحث الثاني: مظاهر الجريمة الإلكترونية وبنيتها القانونية.
29	المطلب الأول: أركان الجريمة الإلكترونية

فهرس المحتويات

29	الفرع الأول: الركن الشرعي
30	الفرع الثاني: الركن المادي
33	الفرع الثالث: الركن المعنوي
33	المطلب الثاني: الجرائم الإلكترونية الواقعة على الأشخاص والأموال
34	الفرع الأول: الجرائم الإلكترونية الماسة بالأشخاص
41	الفرع الثاني: الجرائم الإلكترونية الماسة بالأموال
45	المطلب الثالث: جرائم التجارة الإلكترونية
46	الفرع الأول: الجرائم المتعلقة بممارسة النشاط
53	الفرع الثاني: الجرائم المتعلقة بالإشهار التجاري الإلكتروني.
58	خلاصة الفصل
الفصل الثاني: أساليب البحث والتحري	
60	تمهيد:
61	المبحث الأول: الإجراءات الشرطية لضبط الجريمة الإلكترونية.
61	المطلب الأول: الاجراءات التقليدية للكشف عن الجريمة الالكترونية
61	الفرع الأول: تلقي الشكاوى والبلاغات والسماعات
64	الفرع الثاني: المراقبة المادية
65	الفرع الثالث: المعاينة والخبرة.
70	المطلب الثاني: الإجراءات المستحدثة للكشف عن الجريمة الإلكترونية
70	الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور
73	الفرع الثاني: التسرب الإلكتروني.
75	الفرع الثالث: التفتيش الإلكتروني
81	الفرع الرابع: المراقبة الإلكترونية والحجز داخل المنظومة المعلوماتية

فهرس المحتويات

86	المطلب الثالث: التنظيم القانوني للشرطة القضائية
86	الفرع الأول: الضبطية القضائية المختصة في البحث والتحري عن الجريمة الإلكترونية
90	الفرع الثاني: اختصاص الشرطة القضائية في مجال البحث والتحري عن الجريمة الإلكترونية.
95	المبحث الثاني: خصوصية الدليل الإلكتروني
95	الطلب الأول: مفهوم الدليل الإلكتروني
95	الفرع الأول: تعريف الدليل الإلكتروني
99	الفرع الثاني: خصائص الدليل الإلكتروني
101	المطلب الثاني: صعوبات وأشكال الدليل الإلكتروني
101	الفرع الأول: الصعوبات المتعلقة بالدليل الإلكتروني
102	الفرع الثاني: أشكال الدليل الإلكتروني
103	المطلب الثالث: دراسة حالة حول جنحة عرض إعلان مغل بالحياء عن طريق شبكة التواصل الاجتماعي (التعليق على حكم قضائي جزائي).
104	الفرع الأول: أركان جريمة عرض إعلان مغل بالحياء.
105	الفرع الثاني: إجراءات البحث والتحري.
107	خلاصة الفصل الثاني
108	الخاتمة
112	قائمة المصادر والمراجع
120	الملاحق

مقدمة

مقدمة:

الجريمة ظاهرة قديمة مرتبطة بالإنسان منذ الوجود، غير أن البشرية شهدت خلال فترة زمنية وجيزة مقارنة بمراحل التاريخ الإنساني السابقة تطورا متسارعا أحدث تحولا نوعيا عميقا في مختلف أنماط الحياة، فقد انتقلت المجتمعات من الاعتماد على الوسائل التقليدية والنادية إلى تبني أنماط حديثة قائمة على الرقمنة، وذلك نتيجة الانتشار الواسع لتقنية المعلومات منذ سبعينات القرن الماضي.

إذ لم يعد الزمان والمكان يشكل عائقا أمام انتقال البيانات وتبادلها، فقد أسهم هذا التحول في جعل استخدام الحواسيب وشبكات الاتصال جزءا لا يتجزأ من الحياة اليومية للأفراد والدول بغض النظر عن تحضرهم أو تطورهم الاقتصادي.

فقد استخدمت هذه التكنولوجيا الحديثة في كافة ميادين الحياة وسهلت الانفتاح على العالم بلا حدود، مما أسهم في تقليص المسافات الجغرافية، ومكنت من تعزيز التواصل بين الأفراد والمؤسسات بما يحقق اقتصاد في الوقت وتسريعا في عمليات التبادل وتداول المعلومات على نطاق واسع دون الحاجة إلى عناد التنقل، ونتيجة لذلك أصبح العالم أشبه بقرية صغيرة تتسم بسهولة التواصل والاستمرارية.

وفي ظل التنامي المتسارع للثورة المعلوماتية والاستخدام الإيجابي للتقنيات الحديثة، فقد يسر عدة نواحي في حياة الإنسان لاسيما توفر الوقت والجهد والمال، غير أن البعض قد أساء استخدامها في أنشطة غير مشروعة، مما قد يترتب عنه إلحاق أضرار مباشرة أو غير مباشرة بالمصالح المادية والمعنوية للأفراد، والتأثير سلبا على متطلبات حياتهم اليومية فضلا عن إمكانية تهديد سيادة الدول والمساس بسلامة كيانات المؤسسات الوطنية والدولية.

في هذا الصدد نتيجة الامتداد المتسارع للعصر الرقمي في مختلف المجالات لم تبقى الجرائم منحصرة في نمطها التقليدي القائم في وسط مادي ملموس بل أصبحت تستعمل تقنيات جديدة في وسط افتراضي غير ملموس، هذا ما يعرف بالجريمة الإلكترونية كإفراز سلبي للتطور الرقمي الذي شهده العالم.

تعد الجريمة الإلكترونية من أبرز الظواهر الإجرامية المستحدثة، تختلف في شكلها ومضمونها ووسائلها عن الجريمة بشكلها التقليدي، يستمد هذا النوع من الجرائم نشاطه من الإمكانيات الهائلة للحاسب الآلي والبرامج. يمكننا القول أن هذه التقنية تسمح بنقل المعلومة صوتا وصورة عبر الأنترنت في أي مكان في العالم، مما يسمح للبعض استغلال هذه الشبكة في ارتكاب جرائمهم، من هذا المنطق الجرائم الإلكترونية أصبحت

تشكل خطرا يهدد المجتمع والعالم ككل، حيث لا بنفك معدل انتشارها عن الارتفاع يوما بعد يوم، وهكذا أثارت الظاهرة تحديات للقانون الجنائي بشقيه، فعلى المستوى الموضوعي فإن هذه القواعد لم تتمكن من تجرمة كافة الأفعال الواقعة على البيئة الرقمية احتراما لمبدأ الشرعية، وعلى نطاق القواعد الإجرائية فقد عجزت القواعد التقليدية في التصدي لها باعتبارها وضعت لتواجه سلوكا ماديا.

وعليه نظرا للطبيعة الخاصة لهذا النمط الإجرامي المستحدث وجب على الأنظمة الجزائية أن تتدخل للوقاية السابقة واللاحقة لحدوث هذه الجرائم والبحث عن سبل الحد من تطورها مستقبلا، من خلال التوجه نحو استخدام الوسائل والأساليب المتطورة في مجال التحقيق ونجاعة الأساليب المتبعة بشأنه، ليقع على عاتق الهيئات المختصة مهمة الاستعداد لمواجهة تلك التطورات وتلافي أخطارها على الصعيد الأمني.

من هنا كرس المشرع الجزائري جملة من الإجراءات من شأنها مساعدة جهات التحقيق في الكشف عن الجريمة وإيجاد الدليل الرقمي الذي بموجبه يمكن متابعة مرتكب الجريمة.

إشكالية الدراسة:

في ظل التوسع المتواصل في استخدام التكنولوجيا في مختلف نواحي الحياة اليومية، أضحت البيئة الرقمية مهياة لظهور أنماط مستحدثة من الجرائم، حيث تحولت بعض الاستخدامات الإيجابية للتكنولوجيا إلى ممارسات سلبية مما أدى إلى بروز سلوكات إجرامية جديدة، هذا ما استدعى تدخل المشرع الجزائري للحد من هذه الظاهرة، من خلال تكريس نصوص قانونية خاصة وسن عقوبات ملائمة، إلى جانب إقرار إجراءات خاصة بالبحث والتحري تتولاها جهات مختصة بهدف كشف الجريمة وتحديد مرتكبها.

في هذا السياق، تبرز إشكالية أساسية على النحو التالي:

- ما مدى فعالية إجراءات البحث والتحري عن الجريمة الإلكترونية في التشريع الجزائري؟
- كما تتفرع من هذه الإشكالية عدة إشكاليات أو تساؤلات فرعية تتطلب معالجة دقيقة خلال الدراسة:
- ما المقصود بالجريمة الإلكترونية؟
- ماهي أركان الجريمة الإلكترونية؟
- فيما تتمثل أنواع وتصنيفات هذه الجريمة؟
- كيف نظم المشرع الجزائري الإجراءات الخاصة بالبحث والتحري في مجال الجرائم الإلكترونية؟
- ما مدى حجية الدليل الإلكتروني في الإثبات الجزائي؟

أهمية الموضوع:

- من الناحية العلمية تكتسي دراسة إجراءات البحث والتحري عن الجرائم الإلكترونية أهمية بالغة في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصال، وما صاحبه من تنامي ملحوظ في هذا النوع من الجرائم من حيث الكم والكيف باعتبارها ظاهرة إجرامية معاصرة.
- كما أن موضوع الحال يصنف من بين أهم المواضيع المطروحة للنقاش على النطاق الدولي والوطني، فهو يظل محل اهتمام متواصل من قبل الباحثين وكذا الفقه والتشريع من أجل وضع استراتيجيات قانونية.
- التزايد المستمر للنشاط الإجرامي عبر النظم المعلوماتية، وتزايد درجة خطورة هذا النشاط وارتفاع مستوى التهديدات التي يشكلها على الأمن العام، في المقابل يبرز قصور لدى سلطات البحث و التحقيق في وضع تكييف النموذج النظري لهذه الجرائم أو الاستقرار على منظومة إجرامية واضحة لمتابعتها نظرا لطبيعتها المتجددة و سرعة تطورها، وهذا نتيجة لغياب النصوص القانونية في بعض الحالات، مما يؤدي إلى محدودية فعاليتها و عجزها عن مواكبة خصوصيات الجريمة محل البحث و التحقيق.
- علاوة على ذلك يستمد الموضوع أهميته العملية من خلال حاجة الأشخاص الملحة اليوم إلى استعمال تكنولوجيا الاتصال ووسائل التواصل المستحدثة، وإبراز نقاط القوة والضعف ولثغرات التي من شأنها أن تشكل انطلاقة لتعديل القوانين أو تحديثها أو تغييرها بشكل ينسجم مع التطورات المستحدثة، وهذا للحد منها داخل المجتمع والتقليل من آثارها وكذا زيادة الوعي لدى مستخدمي الأجهزة الحديثة بمخاطر هذه الجريمة.

أهداف الموضوع:

- تهدف هذه الدراسة إلى تحقيق مجموعة من الغايات المهمة منها:
- تسليط الضوء على خصوصية إجراءات التحقيق في مواجهة الجرائم الإلكترونية.
- إثراء الرصيد العلمي والمعرفي ببحث جديد في مجال الجرائم الإلكترونية، قد يساعد باحثين آخرين في المستقبل.
- الإحاطة بمختلف جوانب الموضوع النظرية والتطبيقية، وتحليل الإشكالات التي يثيرها مع محاولة المساهمة العلمية في تقديم إضافة ولو بسيطة تحتوي على تفسيرات وحلول مناسبة.
- محاولة إسقاط الموضوع على الواقع العملي ومعرفة مدى فعاليته، والتعرف على موقف المشرع الجزائري حيال هذه الظاهرة.

أسباب اختيار الموضوع:

وقع اختيارنا لهذا الموضوع لعدة أسباب، نقسم هذه الأخيرة إلى أسباب ذاتية وأخرى موضوعية.

أسباب ذاتية:

- الرغبة والميلول للبحث في هذا الموضوع ودراسته ولتسارع انتشاره تطوره مع تطور البيئة المعلوماتية ووسائلها التقنية الحديثة.
- يرتبط هذا الموضوع ارتباط وثيقا بتخصصنا الدراسي، إذ يندرج ضمن نفس المجال بل ويعتبر جوهره، ويتميز بطابع إجرائي يتيح لنا فهم الجوانب التطبيقية وتعزيز معارفنا النظرية من خلال الممارسة العملية.
- لدينا مكتسبات قبلية حول موضوع الحال وأردنا التعمق أكثر لمعرفة صلاحيات الضبطية القضائية في مكافحة هذا النوع من الجرائم.

أسباب موضوعية:

- حادثة موضوع بحثنا، كونه ينصب حول ما انتجته التكنولوجيا الحديثة من تطور وتغير في المنظومة القانونية، والحاجة إلى الإلمام بمجال التحقيق في الجرائم الإلكترونية عبر تسليط الضوء على أبرز خصائصه التي تمكن من التصدي لهذا النوع من الإجرام، وذلك من خلال تناول أهم عناصر وأساليب التحقيق المعتمدة في الجرائم الإلكترونية، إضافة إلى إبراز دور الأجهزة المختصة في ضمان حسن سير هذه العمليات.
- الحاجة إلى فهم أساليب البحث والتحقيق في الجرائم الإلكترونية، وإبراز التحديات التي تواجه الجهات المختصة أثناء التحقيق.
- المساهمة في تقديم حلول واقتراحات لتفعيل إجراءات البحث والتحري لاسيما المستحدثة منها ومن ثم المساهمة في الحد من هذا النوع من الجرائم.

المنهج المتبع:

اقتضت طبيعة البحث الاستعانة بعدة مناهج تتكامل فيما بينها وهي:

- المنهج الوصفي: عند التطرق إلى المفاهيم العامة حول الجرائم الإلكترونية وبيان خصائصها ودوافع ارتكابها، وكذا تصنيفات هذا النوع من الجرائم.

- المنهج التحليلي: عند تحليل النصوص القانونية المتمثلة في قانون العقوبات، قانون الإجراءات الجزائية ونخص بالذكر القانون 14-25، والقانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، أضيف إلى هذا القانون 05-18 المتعلق بالتجارة الإلكترونية، دون أن ننسى التعليق على حكم الذي كان بمناسبة دراسة حالة لجنة إعلان عرض مخل بالحياة.

حدود الدراسة:

تضم هذه الحدود مايلي، الحدود الزمانية التي تكون من 2004 إلى يومنا هذا أي منذ ظهور القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أما الحدود المكانية فموضوع الحال ينصب على التشريع الجزائري.

الدراسات السابقة:

- دراسة الباحث ربيعي حسين تحت عنوان " آليات البحث والتحقيق الجرائم المعلوماتية " بجامعة باتنة 1، كلية الحقوق والعلوم السياسية قسم الحقوق سنة 2015-2016، تناولت هذه الدراسة مختلف الجوانب المتصلة بالجريمة الإلكترونية سواء من ناحية المفاهيم القانونية والإجراءات الخاصة بالبحث والتحقيق، أيضا الجوانب الفنية والقانونية التي تحكم عمل المحققين في مجال الجرائم الإلكترونية، بالنسبة للنتائج المتحصل عليها نذكر منها يستحيل القضاء على الظاهرة الإجرامية المعلوماتية بشكل نهائي وذلك لاتصالها المباشر بتقنية المعلوماتية، ظهور فئات جديدة من المجرمين والضحايا تحت وصفي مجرمي المعلوماتية وضحايا الإجرام المعلوماتي، بالإضافة إلى أن إجراءات البحث والتحقيق المعلوماتي هي إجراءات من نوع خاص يشترط لمباشرتها التقيد بمجموعة من الشروط...
- دراسة الباحث حمد محمد الدوسري تحت عنوان " أنواع الجرائم الإلكترونية وتحديات مكافحتها " بجامعة يحي فارس المدية، كلية الحقوق والعلوم السياسية قسم الحقوق في 14/05/2025، هدفت هذه الدراسة إلى دراسة الجريمة الإلكترونية التي ظهرت في ظل التطور التكنولوجي المتسارع ومعرفة الإطار المفاهيمي والقانوني لها، اتبعت هذه الدراسة المنهج التحليلي الوصفي، وتوصل الباحث في هذه الدراسة إلى مجموعة من النتائج منها الجرائم الإلكترونية من أخطر أنواع الجرائم المستحدثة إذ تنشأ عن الاستخدام غير المشروع للتقنيات الرقمية والمعلوماتية، وتتم من خلال أجهزة الحاسوب أو الهواتف الذكية وبوسائل يصعب تتبعها أو التنبؤ بها، كما أنها تشمل جميع الأنشطة التي تستهدف البيانات الرقمية...

صعوبات الدراسة:

واجهنا في موضوع الدراسة عدة صعوبات أبرزها:

- تشعب إجراءات البحث والتحري وشساعة مجال تطبيقها.
- قلة المراجع والمصادر الحديثة، وندرة الدراسات السابقة التي تناولت الجانب الإجرائي إذ اتجهت أغلب الأبحاث إلى معالجة الظاهرة الإجرامية الإلكترونية من زاوية السلوك الإجرامي والعقوبات المقررة لها، دون إيلاء الاهتمام الكافي للإجراءات المتبعة في هذا المجال.
- صعوبة التواصل مع الجهات الأمنية والقضائية التي تختص بمتابعة أعمال البحث والتحقيق في الجرائم الإلكترونية، وكذا الصعوبة في الحصول على معلومات ميدانية أو بيانات تطبيقية.
- التخوف من تكرار مواضيع سابقة وعدم تقديم إضافة علمية جديدة.
- العزوف عن تقديم الإحصائيات الخاصة بالجرائم الإلكترونية.

خطة البحث:

وحتى نتمكن من معالجة هذه الإشكالات المطروحة ارتأينا تقسيم الخطة للدراسة إلى فصلين معتمدين على التقسيم الثنائي للخطة، بحيث تناولنا في الفصل الأول المعنون بالإطار المفاهيمي للجريمة الإلكترونية والمنقسم إلى مبحثين الأول متعلق بمفهوم الجريمة الإلكترونية، أما المبحث الثاني يتحدث عن الأركان المكونة للجريمة الإلكترونية وتصنيفات هذه الجريمة الماسة بالأشخاص والأموال وأيضا جرائم التجارة الإلكترونية، أما الفصل الثاني المعنون بالميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية فهو يتحدث عن إجراءات جمع الاستدلالات المتعلقة بالجريمة الإلكترونية في المبحث الأول، وخصوصية الدليل الإلكتروني كونه أداة إثبات في مثل هذا النوع من الجرائم في المبحث الثاني.

الفصل الأول

الإطار المفاهيمي للجريمة الإلكترونية

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

تمهيد:

يشهد العالم في العصر الرقمي تطورا متسارعا في وسائل التكنولوجيا والاتصال، الأمر الذي أفرز أنماطا جديدة من السلوك الإجرامي، وأبرزها الجريمة الإلكترونية التي أصبحت تمثل تحديا حقيقيا للأنظمة القانونية والأمنية على حد سواء، فمع الانتشار الواسع لاستخدام الأنترنت والأجهزة الذكية لم تعد الجريمة محصورة في نطاقها التقليدي، بل امتدت إلى الفضاء الافتراضي.

وانطلاقا من أهمية موضوع الحال، يهدف هذا الفصل إلى وضع إطار مفاهيمي واضح للجريمة الإلكترونية من خلال التطرق في المبحث الأول إلى مفهومها عبر استعراض التعريفات الفقهية والقانونية وكذا معرفة أنماط الجناة في الجريمة الإلكترونية، أضف إلى هذا بيان الخصائص التي تميزها عن غيرها من الجرائم التقليدية، أما في المبحث الثاني فسيتم تسليط الضوء على مظاهر الجريمة الإلكترونية وبينيتها القانونية، من خلال دراسة أركانها وتنظيمها القانوني.

المبحث الأول: مفهوم الجريمة الإلكترونية.

تعتبر الجرائم الإلكترونية من الظواهر الحديثة وهذا لارتباطها بالأنظمة المعلوماتية، نقول أنها من أخطر التحديات القانونية والأمنية في العصر الحديث نظرا لخصوصيتها وتعقيد وسائل ارتكابها فضلا عن صعوبة اكتشافها وإثباتها، وقد تم ظهور هذه الجريمة لأول مرة في الدول المتقدمة التي اكتسبت التكنولوجيا العالية لمعالجة المعطيات ثم انتشرت في باقي الدول الأخرى، بناء على هذا خصصنا المبحث لدراسة الجريمة الإلكترونية بتحديد مفهومها وإبراز خصائصها والدوافع التي تجعل من الشخص مجرم، أضف إلى هذا الأركان التي تقوم عليها الجريمة وتصنيفات أو أنواع الجريمة الإلكترونية .

المطلب الأول: تعريف الجريمة الإلكترونية.

الجريمة الإلكترونية موضوع واسع من الصعب تحديد تعريف خاص بها، غير أن الفقهاء والباحثين بعد الاجتهادات التي قاموا بها توصلوا إلى عدة تعريفات، سنتطرق في هذا المطلب إلى ثلاثة فروع: الفرع الأول بعنوان التعريف الفقهي للجريمة الإلكترونية، الفرع الثاني التعريف القانوني للجريمة الإلكترونية والفرع الثالث خاص بتسميات مختلفة للجريمة الإلكترونية.

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية.

لم يتوصل الفقه إلى تعريف جامع مانع للجريمة الإلكترونية، وبالتالي تعددت التعريفات بشأنها وفق المنظور الذي تبناه الفقه، في هذا الإطار يشير الفقيه " فان ديرهلست ووينف " إلى أن هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة... وفي أغلب الأحيان تستخدم المصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف.¹

¹ محمد رحموني، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أحمد دراية، أدرار، ع 41، 10 جانفي 2018، ص ص 434، 435.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

انقسم الأنصار وتباينت التعريفات باختلاف الأسس التي اعتمدت عليها، إذ يستند بعضها إلى موضوع الجريمة، في حين يركز بعضها الآخر على الوسيلة المستخدمة في ارتكابها بينما تعتمد تعريفات أخرى على السمات والخصائص الشخصية لمرتكب الفعل الإجرامي.

1. التعريف الذي يستند على موضوع الجريمة:

يختلف واضعو التعريف من هذا المنظور في أن الجريمة الإلكترونية ليست هي الجريمة التي يكون الحاسب هو أداة ارتكابها، بل هي كافة الجرائم التي تقع على الحاسب نفسه أو داخل نظامه مستغلا المعالجة الآلية للبيانات. فهي: "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال المادية أو المعنوية".¹

2. التعريف الذي اعتمد على وسيلة ارتكاب الجريمة:

الجريمة عبر الأنترنت لا يتم ارتكابها من دون مساعدة من الحاسب الآلي الذي هو الطريق الثاني في الاشتراك في الجرائم بل هو الطريق الأساسي لارتكاب الجريمة من حيث الدور المساعد والمساهم لتنفيذ الاعتداء، وقد عرفت هي كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية ولا يختلف الأمر سواء كان الحاسب الآلي لإتمام النشاط الإجرامي أو كان محلا له.²

3. التعريف على أساس صفات شخصية لمرتكب الفعل:

منها التعريف الذي وضعته وزارة العدل الأمريكية في دراسة أعدها معهد ستانفورت واعتمدتها هذه الوزارة في دليلها لعام 1979، والذي يعرفها بأنها: "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها". ومنها أيضا مما جاء به الفقيه DAVID THOMSON بأنها: "أية جريمة يكون متطلبا لاقترانها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب".³

¹ طاهر محمود أبو القاسم، الجرائم الإلكترونية صعوبات وسائل التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية، مصر، 2019، ص 25.

² حسن طاهري، الجرائم الإلكترونية، الطبعة 1، دار الخلدونية، الجزائر، 2022، ص ص 8، 9.

³ محمد رحموني، المرجع السابق، ص ص 436، 437.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

ويرجع تبني هذا التعريف إلى طابعه الشمولي الذي يغطي كافة الإحتمالات الجرمية في الفضاء الإلكتروني مع مراعاة الخصوصية الفنية للظاهرة، فالجريمة الإلكترونية ليست على مستوى واحد وإنما تحتوي على عددا مختلفا ومتنوعا من التقنيات لتقوم عدة تصنيفات من الجرائم الحاسب الآلي.

الفرع الثاني: التعريف التشريعي للجريمة الإلكترونية.

لم يعرف المشرع الجزائري الجريمة الإلكترونية، وإنما تبنى للدلالة على الجريمة مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات" معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة، ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لا بد من تحقيقه حتى يمكن توفر أركان الجريمة استنادا إلى القانون 04-15 المعدل والمتمم لقانون العقوبات.¹

فقد خصص المشرع ضمن أحكامه في القسم السابع مكرر نصوصا تجرم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، ثم عزز هذا التوجه بصدور القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

ولغرض توضيح هذا المفهوم، سيتم التطرق إلى تعريف المصطلح في ضوء أحكام كل من القانونين 04-51 و 09-04 على النحو التالي:

أولا: في القانون 04-15 المؤرخ في 10 نوفمبر 2004 المتعلق بقانون العقوبات.

بالرجوع إلى قواعد القانون 04-15 من المادة 394 مكرر إلى المادة 394 مكرر 2 نجد أنه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات، حيث حددها في المادة 394 مكرر كالاتي:

- الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.
- حذف أو تغيير لمعطيات المنظومة إذ ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

¹ أغنية عباس، الجريمة الإلكترونية في البيئة الرقمية ومدى تأثيرها على الجريمة المنظمة العابرة للحدود الوطنية، المجلة الجزائرية للسياسات العامة، جامعة الجزائر 3، المجلد 12، ع 3، 30 ديسمبر 2024، ص 88.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

أما المادة 394 مكرر 1 فقد أشارت إلى: إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.¹

كما أن المادة 394 مكرر 2 من هذا القانون نصت على: "يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 1000000 إلى 5000000 دج كل من يقوم عمدا وعن طريق الغش بما يلي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."²

ثانيا: في القانون 04-09 المؤرخ في 5 غشت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

لم يذكر هذا القانون الجريمة الإلكترونية وإنما حدد مصطلحاتها، حيث نصت المادة 2 منه على: "يقصد في مفهوم هذا القانون بما يلي:

- الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات اللاسلكية.
- منظومة معلوماتية: أن نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.
- معطيات معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية تؤدي وظيفتها."³

ثالثا: القانون 14-25 المؤرخ في 16 يوليو 2025 المتضمن قانون الإجراءات الجزائية.

¹ محمد رحموني، المرجع السابق، ص 439.

² الأمر رقم 66-156، المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم بالقانون رقم 04-15 في 10 نوفمبر 2004، ج.ر، ع 71، 2004.

³ القانون رقم 04-09، المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، ع 47، 2009.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

إضافة إلى القانونين السابقين هناك القانون 14-25 المتضمن قانون الإجراءات الجزائية في الفصل الثالث تحت عنوان "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال" في مادته 335 جاءت بـ: "يوجد في دائرة اختصاص مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها.

كما يخص بالحكم في الجرائم المنصوص عليها في هذا الفصل إذا كانت تشكل جناحاً، يقصد في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيا الإعلام والاتصال".¹

ومنه فقانون الإجراءات الجزائية لم يعرف الجريمة الإلكترونية واكتفى بذكر مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

من خلال ما سبق يمكن أن نعرف الجريمة الإلكترونية بأنها أي فعل غير قانوني أو غير مشروع يرتكب باستخدام الحاسوب أو الأنترنت عن طريق أي منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة رقمية، وهذا بهدف الاعتداء على الأفراد أو المؤسسات أو الأنظمة المعلوماتية.

الفرع الثالث: أنماط الجناة في الجريمة الإلكترونية.

تتعدد الأطراف المتورطة في الجريمة الإلكترونية حيث قد يشترك في ارتكابها أفراد ينتمون إلى بيئات مهنية مختلفة، بالنسبة للجناة قد يكونو موظفين داخل المؤسسات أو تقنيين ذوي الخبرة في المجال المعلوماتي، وما يتعلق بالمجني عليهم فإن ردود أفعالهم تده هذه الجرائم تختلف عن تلك التي تصدر عن ضحايا الجرائم التقليدية.

أولاً: القراصنة الإلكترونيون.

هناك صنفان من القراصنة وهم:

1 الهواة **hackers**: هم شباب فضوليون يسعون للتسلية وكشف الأخبار، وكلمة (hacker) مشتقة من كلمة (hack) التي تعني بها يقطع إرباً، وكذلك من الفعل (to hack) ويعني الدخول اقتحاماً في

¹ القانون رقم 14-25، المؤرخ في 9 صفر عام 1447 الموافق ل 3 غشت سنة 2025، يتضمن قانون الإجراءات الجزائية، ج.ر، ع 54، 2025.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

شبكة نظام الحاسب الآلي، ليحصل الفاعل على ما يريده من معلومات، ويرتكبون جرائمهم تحدياً لإجراءات أمن نظم الشبكات، لكن لا تتوفر لديهم - في الغالب - دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات الذات، من أجل العدالة والحرية ضد نظام الشر ولا يشكلون خطورة على الصناعات وأنظمة المعلومات.¹ يمكننا القول أن هذه الفئة تتسم بعدم توافر نية إتلاف البيانات أو تخريب أنظمة الحاسوب وشبكات الاتصال، حيث ينحصر دافعها الأساسي في الاستكشاف والبحث عن كل ما هو جديد ضمن الفضاء الافتراضي.

2 **المحترفون أو المخترقون crackers:** هي كلمة مستمدة من الإنجليزية من الفعل (crack) ويعنى التحطيم أو الكسر أو السطو أو السحق²، عادة ما يستخدم مجرمو هذا النمط قدراتهم الفنية في اختراق الأنظمة والأجهزة تحقيقاً لأهداف غير شرعية كالحصول على معلومات سرية أو للقيام بأعمال تخريبية، وهم القراصنة المحترفون ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم الإلكترونية خطورة، ويكون القراصنة من هذه الطائفة ذوي مكانة اجتماعية عادية أو متخصصين في العلوم الإلكترونية.³

ثانياً: المخادعون الإلكترونيون fraudulent.

يتمتعون بقدرات فنية عالية وذكاء باعتبارهم - عادة - أصحاب كفاءات و إخصائيين في المعلوماتية، وتتصب معظم جرائمهم على شبكات تحويل الأموال، ويمكنهم التحايل والتلاعب بحسابات المصارف أو فواتير الكهرباء والهاتف أو تزوير بطاقات الإئتمان وما شابه، وتهدف اعتداءاتهم بالأساس إلى الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب الجرائم.⁴

وانطلاقاً مما تقدم فالمخادعون أشخاص يرتكبون جرائم معلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم.⁵

ثالثاً: الجواسيس الإلكترونيون spies.

¹ طاهر محمود أبو القاسم، المرجع السابق، ص 50.

² طاهر محمود أبو القاسم، المرجع السابق، ص 51.

³ جاسم محمد جندل، الجرائم الإلكترونية، دار المعتز للنشر والتوزيع، 2022، ص 45.

⁴ طاهر محمود أبو القاسم، المرجع نفسه، ص 52.

⁵ فتية بوهرين، الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد 14، ع 4، 2021، ص

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

يهدفون إلى جمع معلومات لمصلحة دولهم لأسباب سياسية، أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها، ويطلق عليهم أيضا لصوص نظم المعلومات، ويعتبر مجرمو هذه الفئة مكتشفين غير شرعيين لتلك النظم، وفي كثير من الأحيان يستغرق لصوص نظم المعلومات ساعات طويلة في العمل، ويمتنعون عن النوم والطعام، خصوصا في حالة توصيلهم لمعلومات مهمة تتعلق بهدفعهم. ونظرا لحدثة تلك الجرائم ولتنوعها والطابع التقني الذي يستخدم في ارتكابها، يواجه الجهاز الأمني صعوبات عديدة في اكتشاف وملاحقة مرتكبيها.¹

المطلب الثاني: خصائص الجريمة الإلكترونية.

تختلف الجريمة الإلكترونية عن غيرها من الجرائم التقليدية في عدة جوانب، حيث تتسم بجملة من الصفات أو الخصائص نبينها في مايلي:

الفرع الأول: من حيث الركن المادي.

ما يميز الجريمة الإلكترونية أنها جريمة مستترة، وعالمية أي عابرة للحدود، وكذا جريمة ناعمة هذا ما سنوضحه في الفرع.

أولا: الجريمة الإلكترونية جريمة مستترة.

أي ترتكب في الخفاء لا يشعر بها المجني عليه ويرتكبها الفاعل بواسطة كمبيوتر متصل بشبكة الاتصال وعن بعد، ويكفي الفاعل التمتع و الدراية بمعرفة استخدام الكمبيوتر لإرتكاب الجريمة، بعد التعرف على مرتكبي الجريمة من أهم وأصعب المعطيات الناجمة عن الجرائم المعلوماتية البحتة، وذلك لسرعة وسهولة ضياع المعطيات الإلكترونية التي يمكن إتلافها ومحوها وحذفها وتغيرها وهذا ما يصعب مهام رجال الأمن وعناصر الضبطية القضائية.²

ثانيا: جريمة عابرة للحدود الجغرافية.

¹ طاهر محمود أبو القاسم، المرجع السابق، ص 52.

² حسين طاهري، المرجع السابق، ص ص 15، 16.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

أي تنفذ عن بعد بمعنى أنها تتعدى الحدود الجغرافية للدول فتعتبر الجرائم العابرة للقارات، لأنه مع انتشار شبكة الاتصالات العالمية والأنترنيت أمكننا ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر.¹

إن القدرة التقنية للمعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الاجرامية التي يعتمد فيها المجرمين على استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعنى أن المسرح الجريمة الالكترونية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي لحصول الجريمة الالكترونية، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء.²

ثالثا: الجريمة الالكترونية جريمة ناعمة.

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي لارتكابها كالقتل، السرقة وغيرها فالجرائم الالكترونية لا تتطلب أدنى مجهود عضلي ممكن، بل تعتمد على المجهود الذهني المحكم والتفكير العلمي المدروس القائم على معرفة تقنية ممتازة بالحاسب الآلي والتعامل السليم بالشبكة على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع ولكنه يقترب هذا النوع من الجرائم بدافع اللهو، أو لمجرد إظهار تفوقه على آلة الكمبيوتر، أو على البرامج التي يشتغل بها وأكد لمصلحة ما.³

الفرع الثاني: من حيث الإثبات.

تواجه عملية تتبع الجرائم الالكترونية واكتشافها تحديات كبيرة، نظرا لطبيعتها غير المادية واعتمادها على بيانات رقمية قابلة للتعديل والإخفاء بسهولة ضمن السجلات الالكترونية، كما أن هذا النوع من الجرائم لا يكتشف إلا بعد مرور فترة زمنية طويلة على ارتكابها، وغالبا ما يتم ذلك بالصدفة.

وانطلاقا مما تقدم توصف الجرائم الالكترونية بأنها خفية ومستترة في أغليبتها، حيث لا تترك أثر لها بعد ارتكابها، كما يصعب الاحتفاظ الفني لآثارها إن وجدت، وهذا كله يصعب من مهمة المحقق العادي في

¹ غنية عباس، المرجع السابق، ص 88.

² محمد رحموني، المرجع السابق، ص 441.

³ غنية عباس، المرجع السابق، ص 89.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

التعامل في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها، وفي كل الأحوال تحتاج مواجهة هذه الجريمة إلى خبرة فنية عالية متخصصة لإثباتها.¹

الفرع الثالث: من حيث التبليغ.

أظهرت الدراسات و التقارير أن نسبة كبيرة من ضحايا الجرائم الإلكترونية لا يقومون بالتبليغ عنها، إما لأنهم لا يكتشفون تعرضهم للجريمة أصلاً، وإما لأنهم يخشون من التشهير أو المساس بسمعتهم خصوصاً إذا كانت الجريمة تتعلق بمعلومات حساسة أو بمؤسسة مالية أو تجارية كبرى، وفي أحيان كثيرة تكتشف الجريمة بالمصادفة وبعد مرور وقت طويل على حدوثها ما يؤدي إلى صعوبة استرجاع البيانات أو محاسبة الجاني.²

المطلب الثالث: دوافع ارتكاب الجريمة الإلكترونية.

تعد دوافع ارتكاب الجريمة الإلكترونية عنصراً أساسياً لفهم هذا النمط الإجرامي المستحدث، إذ لا يصدر السلوك الإجرامي في البيئة الرقمية بمعزل عن محفزات متعددة، وهذه الدوافع تتنوع وتختلف بتعدد الفاعلين واختلافهم، سنوضح أكثر دوافع ارتكاب الجريمة الإلكترونية في هذا الجزء على النحو التالي.

الفرع الأول: الدوافع السياسية.

يستخدم بعض المجرمين الفضاء الإلكتروني كمنصة للتعبير عن مواقفهم السياسية أو تنفيذ أجنداث إيديولوجية معينة، ويعد هذا النوع من الجرائم من أخطر الأنواع خاصة ما يتعلق بالإرهاب الإلكتروني، الذي انتشر بشكل خاص في منطقة الشرق الأوسط حيث يستخدم الإرهابيون الشبكات الرقمية لأغراض مثل نشر الدعاية أو التبرعات أو التحريض عن العنف، أو تنفيذ عمليات الحرب، كما تستهدف المواقع الحكومية والمؤسسات الأمنية كجزء من هذه الهجمات.³

فخطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة التي تضار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية مما يجعلها هدف سهل المنال، فبدلاً من استخدام المتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية وإغلاق المواقع الحيوية، ومثال ذلك أنظمة القيادة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو

¹ محمد رحموني، المرجع السابق، ص 441.

² أحمد محمد الدوسري، أنواع الجرائم الإلكترونية وتحديات مكافحتها، مجلة المنار للدراسات والبحوث القانونية والسياسية، جامعة يحي فارس، المدية، المجلد 9، ع 1، جوان، 2025، ص 95.

³ أحمد محمد الدوسري، المرجع السابق، ص ص 98، 99.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، أو اختراق النظام المصرفي مما يضر بأعمال البنوك والأوراق المالية العالمية.¹

الفرع الثاني: الدوافع المادية.

حيث يسعى العديد من مرتكبي الجرائم الرقمية إلى تحقيق مكاسب مادية سريعة وغير مشروعة، من خلال استغلال الثغرات الأمنية في المواقع الإلكترونية، خاصة في ظل تزايد معدلات البطالة وانعدام الاستقرار المعيشي في بعض المجتمعات، إما يدفع البعض نحو سرقة البيانات البنكية، أو اختراق الحسابات الإلكترونية، أو استهداف المواقع التجارية بهدف الإبتزاز أو البيع غير المشروع، كما أن بعضهم يتجه إلى انتهاك حقوق الملكية الفكرية من خلال نسخ وبيع البرمجيات بطريقة غير قانونية، وهو ما يشكل خطرا كبيرا على الشركات المنتجة والمستهلكين على حد سواء.²

الفرع الثالث: الدوافع الشخصية.

ترتكب جرائم الحاسب الآلي بدوافع شخصية خاصة بمرتكبها، قد تكون بهدف الانتقام من صاحب العمل، كقيام أحد المحاسبين بالتلاعب بالبرامج المحاسبية بالشركة - بعد أن يتم إبلاغه برغبة رب العمل بفصله - بحيث تخنق هذه البرامج وتتآكل رغبة في الانتقام، كما قد ترتكب لهدف الاحتفاظ بالوظيفة، أضف إلى هذا ارتكاب هذه الأفعال خدمة لمصالح الغير، فقد تقوم بعض الشركات والمصانع والمنشآت باستئجار محترفي التقنية بهدف التجسس على منشآت أخرى بقصد الإطلاع على أسرار المهنة أو آخر ما تم التوصل إليه من علوم لاختصار الوقت في البحث، أو لأجل المنافسة التجارية.³

¹ اسمهان بن مالك، خصائص الجريمة المعلوماتية وأسباب ارتكابها، مجلة البيان للدراسات القانونية والسياسية، جامعة البشير الإبراهيمي، برج بوعريريج، المجلد 4، ع 1، 15 جوان 2019، ص 118.

² أحمد محمد الدوسري، المرجع السابق، ص 98.

³ عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لإستكمال شهادة الماستر، كلية الاقتصاد والعلوم التجارية وعلوم التسيير، قسم علوم التسيير، جامعة قاصدي مرباح ورقلة، 2018/2019، ص ص 22، 23.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

في نفس السياق هناك دافع الفضول أو الرغبة في التعلم والتجربة، حيث يقوم بعض الأفراد باختراق الأنظمة فقط لإثبات قدرتهم على تجاوز الحماية الأمنية، وقد تتحول هذه المحاولات إلى أعمال إجرامية متعمدة، خصوصا إذا صاحبها ألحق أضرار بالبيانات أو استغلال للمعلومات.¹

المبحث الثاني: مظاهر الجريمة الإلكترونية وبنيتها القانونية.

أدى التطور التكنولوجي إلى بروز أنماط متعددة من الجرائم الإلكترونية، اختلفت أشكالها طبقا للوسائل المستعملة وطبيعة الأفعال المرتكبة، ولقد انعكس هذا على البيئة القانونية لهذه الجرائم لاسيما من حيث أركانها المكونة لها، وعليه درسنا في هذا المبحث الأركان المكونة للجريمة الإلكترونية ممثلة في الركن الشرعي، والمادي، والمعنوي، أضف إلى ذلك أصناف أو أنواع الجرائم التي اعتبرت من الجريمة الإلكترونية.

المطلب الأول: أركان الجريمة الإلكترونية.

تعد أركان الجريمة الإلكترونية الأساس القانوني الذي تقوم عليه المسؤولية الجزائية في هذا النوع المستحدث من الجرائم، إذ لا يكفي مجرد وقوع الفعل عبر الوسائط الرقمية لقيام الجريمة، بل يجب توفر مجموعة من العناصر التي يحددها القانون، ومن ثم يقتضي فهم طبيعة القانون للجريمة الإلكترونية والوقوف على أركانها المختلفة، فقد خصصنا هذا المطلب لدراسة الأركان الممثلة في الركن الشرعي، الركن المادي، والركن المعنوي.

الفرع الأول: الركن الشرعي.

يمثل هذا الركن الأساس القانوني الذي يجعل من الفعل المرتكب جريمة تستوجب العقاب، بعبارة أوضح لا يمكن اعتبار أي سلوك جريمة إلا إذا وجد نص قانوني يجرمه ويحدد له العقوبة

¹ عبد الرؤوف زبوش، مصطفى زغيشي، الجرائم الإلكترونية الاقتصادية - المفهوم والدوافع - مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس، بركة، المجلد 7، ع 1، جوان 2024، ص 407.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

بالنسبة للجريمة الإلكترونية فهي كغيرها من جرائم القانون تقوم على مبدأ الشرعية الجزائية التي يستمد أساسه من المادة 34 من الدستور: " لا إدانة إلا بمقتضى قانون صادر قبل ارتكاب الفعل المجرم." ¹

وانطلاقاً من القاعدة العامة الموجودة في قانون العقوبات بالأخص في المادة الأولى منه التي نصت على: " لا جريمة ولا عقوبة أو تدبير أمن بغير قانون" ²، وضع المشرع نصوص قانونية عامة وخاصة تجرم الأفعال المرتكبة عبر تكنولوجيا الإعلام والاتصال، بداية مع القانون السالف الذكر في الفصل الثالث المعنون بـ " الجنايات والجنح ضد الأموال "، بالضبط في القسم السابع " المساس بأنظمة المعالجة الآلية للمعطيات " المواد من 394 مكرر إلى 394 مكرر 7 التي جاءت بالعقوبات المقررة على كل من ارتكب أفعال مجرمة صنفت كصور من الجريمة الإلكترونية .

في حين جاء القانون 09-04 المؤرخ في 21 شعبان 1430 الموافق 5 غشت 2009 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها كجانب وقائي يحد من وقوع الجرائم المعلوماتية، من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتسجيل وتجميع محتواها في حينها، والقيام بإجراءات التفتيش داخل المنظومة المعلوماتية. ³

الفرع الثاني: الركن المادي

يعرف هذا الركن بأنه العنصر الخارجي الملموس الذي يجسد الفعل الإجرامي في الواقع الرقمي، بمعنى آخر هو ذلك السلوك الذي يقوم به الجاني باستخدام وسائل تقنية ويؤدي إلى نتيجة غير مشروعة يعاقب عليها القانون، يحتوي الركن المادي على ثلاثة عناصر أساسية بمجرد توفرها تتحقق الجريمة، والمتمثلة في السلوك الإجرامي، النتيجة الإجرامية، العلاقة السببية.

أولاً: السلوك الإجرامي.

هو النشاط الذي يقوم به الجاني عبر الوسائل الإلكترونية، وقد يكون فعل إيجابي أي القيام بالفعل، وإما سلبي أي الامتناع عن القيام بالفعل.

1. الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك:

¹ المادة 34 من الدستور الجزائري، الصادر بموجب المرسوم الرئاسي 20-422 في 30 ديسمبر 2020، ج.ر، ع 180، سنة 2020.

² الأمر رقم 66-156 المتضمن قانون العقوبات المعدل والمتمم بالقانون 04-15، سبق ذكره.

³ حمز خضري، حمزة عشاش، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة عمار ثلجي، الأغواط، المجلد 6، ع 2، جوان 2020، ص 173.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

نصت المادة 394 مكرر في قانون العقوبات¹ على أن الدخول أو الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك يشكل فعلا إجراميا، ولهذا الفعل حسب المادة المذكورة صورتين كالتالي:

- الصورة البسيطة: يتمثل النشاط الإجرامي في هذه الصورة فعل الدخول الذي يتحقق بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبه، لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن مقابل نفقات.
 - الصورة المشددة: نصت المادة 394 مكرر في الفقرتين الثانية والثالثة من قانون العقوبات على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين إما محو أو تحويل المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه من خلال تخريب نظام اشتعال المنظومة.²
2. إدخال المعطيات بطريق الغش.

يقصد بفعل الإدخال حسب المادة 394 مكرر 1 من قانون العقوبات إضافة معطيات جديدة إلى نظام المعالجة الآلية أو التعديل من معلومات داخله كان يتضمنه مسبقا فغير فيها، ومثال ذلك حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو من غيره كحالة السرقة و التزوير.³

ثانيا: النتيجة الإجرامية.

يمكننا القول أن النتيجة هنا هي الأثر الذي يترتب على السلوكات السابقة الذكر، المشرع الجزائي عاقب على تحقيق النتيجة في الجريمة الإلكترونية، كما عاقب على بعض الأفعال المشكلة لخطورة محتملة ودون انتظار وقوع أضرار فعلية، على سبيل المثال تشديد العقوبة إذا نتج عن الولوج الغير مشروع إلى نظام المعلومات

¹ انظر المادة 394 مكرر من قانون العقوبات.

² حمز خضري، حمزة عشاش، المرجع السابق، ص 174.

³ المرجع نفسه، ص 174.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

وإلغاء البيانات أو البرامج أو نسخها أو المساس بعمل النظام المعلوماتي وتعطيل كل الشبكة المعلوماتية أو الحاسب الآلي.¹

أما ما يتعلق بمحل الجريمة الإلكترونية فهو الشيء أو المصلحة التي يقع عليها الاعتداء في الجريمة، بعبارة أخرى الهدف الذي يناله الفعل الإجرامي في البيئة الرقمية، كما أن محل الجريمة هنا ذو طابع غير مادي كونه يتعلق بعناصر رقمية وليس أشياء مادية تقليدية.

وقد يكون في مثابة المحل كل ما له قيمة في الفضاء الرقمي البيانات والمعلومات الرقمية، الأنظمة المعلوماتية والشبكات، الحسابات الإلكترونية، الحقوق المالية أو الاقتصادية، الملكية الفكرية الرقمية...
ثالثا: العلاقة السببية.

تتجلى نظريات العلاقة السببية في المجال الإلكتروني بصفة واضحة، لاسيما في الحالات التي تتداخل فيها عدة عوامل وأسباب تؤدي مجتمعة إلى حدوث النتيجة الإجرامية، الأمر الذي إشكالية تحديد السبب القانوني المنتج للضرر وإسناد المسؤولية الجنائية إلى الفاعل، وعليه تتمثل النظريات في:

1. **نظرية تعادل الأسباب:** ومؤداه أن جميع العوامل المؤدية إلى تحقيق النتيجة الإجرامية متعادلة من حيث قيمتها السببية طالما أن كل منها لازم لتحقيق النتيجة ولو تداخلت عوامل أخرى دون النظريات الأهم أو الأقل²، فالجريمة الإلكترونية قائمة في حق الفاعل متى ساهم سلوكه في إحداث النتيجة الإجرامية، حتى وإن اشتركت معه عوامل أخرى في وقوعها.

2. **نظرية السببية الملائمة:** بمقتضى هذه النظرية يعد نشاط الجاني سببا لتحقيق النتيجة الإجرامية الإلكترونية إذا تبين أن له صالحا لإحداثها وفقا للمجرى العادي للأمر حتى ولو ساهمت معه عوامل أخرى في إحداث النتيجة، سواء كانت سابقة أو معاصرة مادامت العوامل مؤلوفة أو متوقعة، فالنتائج الشادة وغير المؤلوفة التي تنتج عن السلوك لا تعتبر في وجهة نظر القانون رغم قيام تلك الرابطة من وجهة النظر الطبيعية البحتة.

¹ نادية بوراس، محاضرات مقدمة في مقياس الجريمة الإلكترونية، أقيمت على طلبة الحقوق السنة الثانية ماستر، السنة الجامعية 2023/2022، ص 19.

² عبد السلام شطيبي، محاضرات مقدمة في مقياس القانون الجنائي للبيئة، أقيمت على طلبة الحقوق السنة الثانية ماستر، السنة الجامعية 2026/2025، ص 16.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

3. نظرية السبب المباشر: يعنى النتيجة الإجرامية الإلكترونية إلى الجاني إذا كان نشاطه هو السبب أو العامل الأقوى والفاعل في إحداثها، بينما لا يؤخذ بباقي العوامل التي تضافرت مع هذا النشاط وساعدت في إحداث النتيجة سواء كانت سابقة أو لاحقة عليه، وذلك لكفاية فعل الجاني بذاته لإحداث النتيجة.¹ في هذا السياق تعني السببية في إطار الركن المادي للجريمة الإلكترونية إسناد النتيجة المعاقب عليها لسلوك الفاعل عن طريق الربط بينهما، ولا يختلف المفهوم العادي لصلة السببية عما هو الحال في الجريمة الإلكترونية.²

فالعلاقة هي التي تكون بين السلوك الإجرامي والنتيجة الحاصلة، أي أن الضرر لم يكن ليحدث لولا هذا الفعل الإلكتروني.

واستخلصنا لما سبق أن ليس كل الجرائم الإلكترونية تتحقق بتوفر كل العناصر، فهناك البعض بمجرد ارتكاب الفعل الإجرامي تعتبر جريمة تامة حتى لو لم تتحقق النتيجة، على سبيل المثال مجرد الدخول غير المشروع إلى نظام معلوماتي يعتبر جريمة معاقب عليها قانوناً.

الفرع الثالث: الركن المعنوي

إن تحقق الركن المادي للجريمة لا يكفي وحده لقيام المسؤولية الجزائية عنها، وإنما ينبغي توافر الركن المعنوي للجريمة الذي جوهره الإرادة الإجرامية، ويتخذ إحدى الصورتين القصد الجنائي والخطأ غير العمدى، فيعرف القصد الجنائي على أنه علم الجاني بالعناصر المكونة للجريمة واتجاه إرادته إلى إحداث هذه العناصر أو إلى قبولها، وعليه القصد الجنائي المتطلب لقيام الجرائم الإلكترونية هو القصد الجنائي العام، الذي يفترض علم الجاني بعناصر الجريمة واتجاه إرادته إلى ارتكابها، إلى جانب هذا يتطلب وجود قصد جنائي خاص يتمثل في اتجاه الإرادة إلى غاية معينة وهي نية التملك وغيرها من النوايا.³

المطلب الثاني: الجرائم الإلكترونية الواقعة على الأشخاص والأموال.

¹ المرجع نفسه، ص 16.

² نادية بوراس، المرجع السابق، ص 19.

³ خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة المنصورة، 2021/2020، ص

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

مع التطور الملحوظ في مجال تكنولوجيا المعلومات ظهرت أنماط جديدة من الجرائم تعرف بالجريمة الإلكترونية، وهذه الأخيرة تنقسم بدورها إلى جرائم أخرى متنوعة تستهدف الأشخاص وأموالهم بوسائل تتجاوز الإطار التقليدي للجريمة.

وعليه الجرائم الماسة بالأشخاص تتخذ صور جمة من بينها التجسس الإلكتروني، الابتزاز عبر الأنترنت، التشهير والقذف، وهي أفعال تنال من الكرامة الإنسانية والإعتبار الشخصي والأمن المعنوي للفرد، أما الجرائم الماسة بالأموال فتشمل مختلف صور الاحتيال والنصب والاستيلاء غير المشروع على الأموال.

الفرع الأول: الجرائم الإلكترونية الماسة بالأشخاص.

تشمل هذه الجرائم كل اعتداء يتم عبر الوسائل الرقمية ويستهدف الفرد في حياته الخاصة أو كرامته أو سلامته النفسية، في دراستنا لها سلطنا الضوء على جريمة التجسس الإلكتروني، جريمة الابتزاز الإلكتروني، جريمة القذف والتشهير.

أولاً: جريمة التجسس الإلكتروني.

يعرف التجسس الإلكتروني على أنه الجريمة التي تستخدم فيها التكنولوجيا كأداة للجوسسة، تتسم بميزة خاصة هي السهولة والحرية في تحقيق النتيجة، بعيدا عن رقابة من جهة معينة، وهو مفهوم عام يشمل الأفراد والجماعات والدول، قد يكون هذا التجسس فردي أي قيام أحد الأشخاص غير المصرح بهم بالدخول إلى نظام التشغيل في مختلف أجهزة الاتصالات بطريقة غير مشروعة لأغراض غير سوية، حيث يتيح للشخص المتجسس أن ينتقل أو يمسح أو يضيف ملفات أو برامج، كما أن التجسس الإلكتروني قد يكون دولي باستخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح به أو غير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة بالدول والحكومات والتنصت عليها بقصد الحصول على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها مثل التحسيس على العمليات العسكرية والأمنية والسياسية والاقتصادية والاجتماعية

تتلخص أركان جريمة التجسس الإلكتروني في ثلاثة أركان كما هو الشأن بالنسبة للجرائم التقليدية، سنوضح ذلك كما يلي:

1. الركن الشرعي:

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

طبقا لنص المادة الأولى من قانون العقوبات التي نصت على: "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون"¹، جرم المشرع الجزائري أفعال التجسس الإلكتروني من خلال مجموعة من النصوص القانونية، خاصة في قانون العقوبات الجزائري والقوانين المكملة له.

تم إدراج نصوص خاصة لمكافحة الجرائم الإلكترونية بموجب تعديلات التي أدخلت على قانون العقوبات، من أبرز هذه المواد المادة 394 مكرر التي جرمت الدخول أو البقاء عن طريق الغش في نظام معلوماتي دون إذن، وهو الأساس القانوني لأفعال التجسس الإلكتروني، المادة 394 مكرر 1 عاقبت على حذف أو تغيير أو إتلاف المعطيات المعلوماتية، أو إدخال بيانات بطريقة غير مشروعة.

أضف إلى هذا المادة 394 مكرر 2 التي جرمت عرقلت سير النظام المعلوماتي أو إحداث خلل فيه، المادة 394 مكرر 3 المتعلقة باستعمال المعطيات المتحصل عليها بطرق غير مشروعة.²

2. الركن المادي:

هي الصورة التي يتم من خلالها ارتكاب جريمة التجسس الإلكتروني سواء عن طريق الشروع في ارتكابها أو تنفيذها فعلا، وكون لها أثر مادي ملموس غير أنه في مثل هذا النوع من الجرائم غالبا ما يكون الفعل المعنوي أي لا يترتب عنه ضرر خارجي، وإنما يتأثر المجني عليه تأثرا معنويا قد يؤدي إلى ضرر مادي ونظرا لقيام الجاني بفعل التجسس، فهذا يعني أن كل عناصر الركن المادي من فعل ونتيجة وعلاقة سببية قد تم تحققها بمجرد الاطلاع غير المشروع.³

على هذا الأساس يتمثل الفعل المادي في الحصول على معلومات أو بيانات دون إذن، منها الولوج غير المشروع إلى نظام معلوماتي كاختراق الحسابات أو الأجهزة، اعتراض الاتصالات الإلكترونية، استعمال برامج أو أدوات التجسس لمراقبة نشاط الغير، وكذا عند النقاط أو تسجيل أو نقل البيانات بطرق سرية. بالنسبة للنتيجة الإجرامية تتمثل في المساس بسرية المعلومات أو انتهاك الحياة الخاصة أو الحصول على معطيات ذات طابع شخصي أو مهني، أما العلاقة السببية تكمن في وجوب وجود علاقة مباشرة بين الفعل المادي والنتيجة بمعنى أن يكون الحصول على المعلومات أو انتهاك الخصوصية ناتج عن فعل الجاني الذي قد يكون اختراق أو تنصت أو غير ذلك.

¹ الأمر 66-156، المتضمن قانون العقوبات المعدل والمتمم بالقانون 04-15، سبق ذكره.

² أنظر المواد 394 مكرر، 394 مكرر 1، 394 مكرر 2، 394 مكرر 3 من قانون العقوبات الجزائري.

³ سلمى مشري، محاضرات في مقياس الجريمة الإلكترونية، ألقيت على طلبة السنة الثانية ماستر، علوم جنائية، ص 7.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

غير أن جريمة التجسس الإلكتروني قد تعتبر جريمة تامة بمجرد القيام بالفعل دون تحقق نتيجة.

3. الركن المعنوي:

يحتوي على القصد الجنائي العام الذي يتكون بدوره من عنصرين هما العلم أي علم الجاني أن الفعل الذي يقوم به غير مشروع، واتجاه إرادته إلى ارتكاب هذا الفعل، أما القصد الجنائي الخاص يتمثل في سوء نية الجاني وقد تكون الغاية من ذلك إلحاق الضرر بالغير أو تحقيق منفعة غير مشروعة.

في هذا السياق يعتبر الركن المعنوي في جريمة التجسس الإلكتروني مفتاح الأساس في إثبات وقوع الجريمة من عدمها، فهو الدليل على علم الفاعل بالطبيعة القانونية لفعله الإجرامي، أي اتجاه إرادته للقيام بالفعل، وهو سيبقى في ذلك ظهور الركن المادي للجريمة لأن النية الإجرامية تكون هي الأسبق وهي تأكيد فعلي لإرتكاب الجريمة، وهنا الأمر يختلف عن الجرائم المادية التي يصعب في الغالب كشف النية الإجرامية من خلالها لأنها لا ترتكب بفعل الوسائط الإلكترونية.¹

ثانيا: جريمة الابتزاز الإلكتروني.

تعد هذه الجريمة من أخطر صور الجريمة الإلكترونية لما تنطوي عليه من إعتداء مزدوج على حرية الأفراد وخصوصيتهم. حيث يعرف الابتزاز بشكل عام أنه سلوك يتضمن مساومة الشخص للحصول على مكاسب مادية أو معنوية أو جنسية أو لمجرد الانتقام عن طريق وسائل الإكراه والقسر بتهديده بإفشاء أسرار ممكن أن تسيء له أو تلحق به ضرر، وهو أنواع منه الابتزاز الإلكتروني الذي يعني التهديد والمساومة التي تقع بواسطة آلية إلكترونية.²

كما يمكننا القول أن جريمة الابتزاز الإلكتروني هي محاولة إكراه وسلب الإرادة والحرية لإيقاع الأذى الجسدي أو المعنوي على الضحايا عن طريق وسائل يتقن الجاني في استخدامها لتحقيق جرائمه الأخلاقية أو المادية أو كلاهما معا.³

¹ سلمى مشري، المرجع السابق، ص 7.

² فاطمة العرفي، حجية الدليل الرقمي في إثبات جريمة الابتزاز الإلكتروني في القانون الجزائري، مجلة صوت القانون، جامعة خميس مليانة، المجلد 8، ع 2، أكتوبر 2022، ص 495.

³ سامية حمريش، صليحة رحالي، الجريمة الإلكترونية وإنعكاساتها على المنظومة الأخلاقية: الابتزاز الإلكتروني -أمودجا-، مجلة الباحث للدراسات الأكاديمية، جامعة لخضر، بانتة 1، المجلد 12، ع 2، جوان 2022، ص 363.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

قد يكون الابتزاز الإلكتروني مادي بمعنى أن يقوم الجاني بتهديد المجني عليه المرتقب بوسائل مادية ملموسة كالصور والمقاطع المرئية والمستندات، ويكون هذا النوع من الابتزاز عن طريق الاتصالات الإلكترونية وهي كل المراسلات والإرسالات التي تقع سواء في شكل علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات، يتم تبادلها أو إرسالها بطريق إلكتروني عبر الأسلاك أو الألياف البصرية أو بطريقة كهرو ميغناطسية.

أما الابتزاز المعنوي يقصد به التهديد بوسائل غير ملموسة وذلك باستخدام عبارات شديدة للتهديد والوعد بفضح أمر الضحية حتى يغلب على ظن الأخير أن المبتز منفذ لتهديده ولا محالة في ذلك¹، وقد تتنوع أسباب ودوافع ارتكاب هذه الجريمة كابتزاز الضحية لتحويل أموال عبر الحسابات البنكية أو وسائل الدفع الإلكتروني أو تحقيق مكاسب سريعة دون جهد مشروع وغيرها من الأفعال التي اعتبرها المشرع فعل إجرامي.

استخلصنا مما سبق أن جريمة الابتزاز الإلكتروني من الجرائم المستحدثة التي عالجها المشرع الجزائري ضمن أحكام قانون العقوبات تحت ما يسمى بجنحة الابتزاز الإلكتروني والتهديد خاصة عبر الأنترنت، في المواد من 303 إلى 371 من القانون السالف الذكر. وتتمثل أركان جريمة الابتزاز الإلكتروني في ما يلي.

1. الركن الشرعي:

تطبيقاً لمبدأ " لا جريمة ولا عقوبة أو تدبير أمن بغير قانون "²، سن المشرع الجزائري مجموعة من المواد التي تكيف سلوك الابتزاز، فالأساس القانوني المباشر لجريمة الابتزاز حتى لو تمت عبر الأنترنت يتمثل في المادة 303 مكرر التي تجرم المساس بحرمة.

الحياة الخاصة كالقيام بالنقاط أو تسجيل أو نقل صور أو أقوال دون إذن، و المادة 303 مكرر 1 التي عاقبت على نشر أو استعمال تلك الصور أو المعلومات دون موافقة صاحبها.³

¹ مريم عراب، جريمة التهديد والابتزاز الإلكتروني، مجلة الدراسات القانونية المقارنة، جامعة أحمد بن أحمد، وهران، 2، المجلد 7، ع 1، 2021، ص 1210.

² الأمر 156-66 المتضمن قانون العقوبات المعدل والمتمم بالقانون 15-04، سبق ذكره.

³ أنظر المادتين 303 مكرر، 303 مكرر 1 من قانون العقوبات.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

في نفس القانون عاقبت المادة 371 على التهديد بأنواعه لارتكاب جناية أو جنحة ضد الأشخاص أو الأموال، خاصة إذا كان هذا التهديد مصحوب بأمر أو شرط، أو كان الغرض منه إجبار الضحية على القيام بفعل أو الامتناع عنه.

2. الركن المادي:

السلوك الإجرامي في هذه الجريمة يظهر في الحصول على منتج رقمي خاص بالضحية ثم تهديده بنشره في البيئة الرقمية، مما يعني أن مسرح الجريمة هو منصات رقمية واسعة الاستخدام، سواء ظهرت في شكل صور أو فيديوهات أو رسائل صوتية أو رسائل دردشة مكتوبة، مما يخيف الضحية ويدفعها للرضوخ لطلبات المبتز.

والنتيجة الإجرامية تتمثل في التهديد بنشر المنتج الرقمي الذي يشكل ضغط على إرادة الضحية ويدفعه للرضوخ لمطالب المبتز دون رضاه، منعا لحدوث التشهير والفضيحة في الفضاء الرقمي وبالتالي خسارته لرأس المال الاعتباري أو الرمزي.¹

قد يكون محل الابتزاز الإلكتروني المصلحة التي يسعى للاعتداء عليها أو استغلالها للضغط على الضحية، ممثلة في الأموال مثلا، أو السمعة والشرف، الحرية الشخصية أي عند إجبار الشخص عن القيام بفعل أو الامتناع عنه، أو قد تمس الخصوصية للحياة الخاصة كالصور، الفيديوهات، المحادثات الشخصية وغيرها.

أما فيما يخص العلاقة السببية فيجب أن يكون هناك ارتباط مباشر بين الفعل الإجرامي والنتيجة، في جريمة الحال من الصعب تحديد العلاقة السببية بسبب التعقيدات المتعلقة بها كونها تقع في بيئة افتراضية، وما يرافق ذلك من تداخل و المراحل التي تمر بها الجريمة من الدخول عبر الكمبيوتر والأوامر المدخلة والنتيجة المراد الحصول عليها، وهل تحققت بالفعل أم لا، من هذا المنطق فالعلاقة السببية في جريمة الابتزاز تكمن في خوف ورضوخ الضحية وتلبية لطلبات الجاني نتيجة تهديد هذا الأخير للضحية بالنشر والعلانية في الفضاء الرقمي لأسرار ومعلومات وبيانات تتعلق بخصوصيته.²

3. الركن المعنوي:

¹ فاطمة العرفي، المرجع السابق، ص 498.

² المرجع نفسه، ص 498.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

يقصد به توفر القصد الجنائي العام المتمثل في علم الجاني بأن الأفعال التي يقوم بها غير مشروعة، وأن الوسائل الإلكترونية المستعملة تستخدم للضغط والتهديد وكل هذا من شأنه المساس بحرية وإرادة الضحية، وكذا اتجاه إرادة الجاني إلى القيام بالأفعال المجرمة رغم علمه بذلك، أما القصد الجنائي الخاص يكون سوء نية الشخص مرتكب الفعل.

ثالثا: جريمة القذف والتشهير الإلكتروني.

جرائم القذف والتشهير من الجرائم التقليدية نصت عليها معظم التشريعات العقابية سواء كانت عربية أو أوروبية، وهي الجرائم التي تطل الأفراد وكذا المؤسسات والأنظمة السياسية والاجتماعية والدينية وهذه الجرائم لا تتم علانية بالكتابة أو القول أو الفعل أمام الجمهور، ومع تطور استعمال الأنترنت أصبحت هذه الجريمة حديثة الأسلوب في ارتكابها.¹

ذكر المشرع الجزائري جريمة القذف والتشهير في قانون العقوبات، حيث أدرج في مضمون هذا القانون مواد تنص على القذف والتشهير، بداية مع جريمة القذف ذكرت في نص المادة 296 التي نصت على: "يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعة عليها به أو إسنادها إليهم أو إلى تلك الهيئة..."²، وعليه يمكن تعريف القذف على أنه كل إسناد غير صحيح لواقعة من شأنها المساس بشرف الشخص أو اعتباره.

بالنسبة للتشهير جاء في نص المادة 297 التي نصت على: "يعد سب كل تعبير مشين أو عبارة تتضمن تحقيرا أو قذحا لا ينطوي إلى إسناد أية واقعة"³، ومنه استخلصنا أن التشهير هو كل نشر علني لوقائع أو معلومات من شأنها المساس بسمعة أو اعتبار الشخص.

يهدف هذا النوع من الجرائم إلى تشويه سمعة الأفراد عن طريق المواقع الإلكترونية ومنصات التواصل الاجتماعي، التي باتت تستغل في كشف الأسرار الشخصية للأفراد دون رضاهم أو نشر صور التقطت في المناسبات أو أي مكان دون إذن، وبفعل سهولة التداول عبر شبكة الأنترنت أصبحت في متناول جمهور واسع.

¹ حسين طاهري، المرجع السابق، ص 26.

² الأمر 156-66 المتضمن قانون العقوبات المعدل والمتمم بالقانون 15-04، سبق ذكره.

³ الأمر 156-66 المتضمن قانون العقوبات المعدل والمتمم بالقانون 15-04، سبق ذكره.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

من خلال ما سبق سنذكر أركان هذه الجريمة كمايلي.

1. الركن الشرعي:

يعد مبدأ الشرعية في التجريم والعقاب الركيزة الأساسية التي تقوم عليها ثنائية التجريم والعقاب، وقد كرس المشرع الجزائري هذا المبدأ من خلال نص المادة الأولى من قانون العقوبات التي نصت على: " لا جريمة ولا عقوبة أو تدبير أمن بغير قانون"، بناء على هذا لا يمكن اعتبار الفعل المرتكب جريمة إلا جاء نص قانوني صريح يجرم ذلك.

وجريمة الحال جرمها المشرع الجزائري في قانون العقوبات بالضبط في القسم الخامس الموسوم ب " الاعتداءات على شرف واعتبار الأشخاص، وعلى حياتهم الخاصة وإفشاء الأسرار" وتحديدا في المواد 296، 298، 299 لإضافة إلى المادة 303 مكرر.

2. الركن المادي:

يتمثل في سلوك غير مشروع يأتيه الجاني من خلال إسناد واقعة إلى الغير تمس شرفه أو اعتباره بأي طريقة من طرق العلانية، ويتحقق الركن المادي لهذه الجريمة بتوافر النشاط الإجرامي المتمثل في فعل الإسناد، وموضوع ينصب عليه النشاط يتمثل في الواقعة المحددة المنسوبة إلى المجني عليه، وصفة النشاط الإجرامي المتمثلة في علانية الإسناد، وفي نفس السياق لا تتحقق جريمة القذف إلا إذا كان الإسناد للواقعة المحددة إسنادا علنيا، فإذا انعدمت العلانية بكل صورها انعدمت بالتالي جريمة القذف وأصبحت الجريمة مجرد مخالفة يعاقب عليها القانون بالسب غير العلني.¹

أما النتيجة الإجرامية لهذه الجريمة المساس بشرف واعتبار الضحية، كما قد تؤدي إلى الإضرار بسمعته أما الغير، والعلاقة السببية عندها تكون النتيجة المتحصل عليها ناتجة مباشرة عن الفعل الإلكتروني المرتكب. بالإضافة إلى أن هذه الجريمة تعتبر جريمة تامة بمجرد ارتكاب السلوك الإجرامي حتى لو لم تتحقق النتيجة الإجرامية.

3. الركن المعنوي:

¹ عبد السلام علي، جريمة القذف عبر مواقع التواصل الاجتماعي دراسة تحليلية مقارنة بين التشريع الجزائري والتشريعات الأجنبية والعربية، مجلة الدراسات القانونية والاقتصادية، جامعة سي الحواس، بريكة، المجلد 5، ع 2، ديسمبر 2022، ص 578، 579.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

بما أن جريمة القذف من الجرائم العمدية، فإن القانون لا يتطلب لتحقيقها قصدا خاصا بل يكفي بتوافر القصد العام الذي يتحقق من خلال نشر القاذف الأمور المتضمنة عبارات القذف، قاصدا علانيته وهو عالم بذلك، ووفقا للقواعد العامة فإن القصد العام يتكون من عنصرين هما علم الجاني بعناصر الجريمة وأن يعلم أن الواقعة التي يسندها إلى المجني عليه توجب عقابه أو احتقاره عند أهل وطنه، وانصراف إرادة الجاني إلى تبليان الفعل وتحقيق النتيجة، أي أن تتوافر لديه إرادة الإسناد وإرادة العلانية وأن تكون الإرادة سليمة خالية من عيب من عيوب الإكراه أو التهديد.¹

الفرع الثاني: الجرائم الإلكترونية الماسة بالأموال.

بعد دراستنا في الفرع الأول للجرائم الإلكترونية الماسة بالأشخاص ها نحن نقف في هذا الفرع عند الجرائم الماسة بالأموال، ومن بين هذه الجرائم سنتطرق إلى جريمة الاحتيال عبر الأنترنت، جريمة غسيل الأموال إلكترونيا، جريمة السرقة الإلكترونية.

أولا: جريمة الاحتيال عبر الأنترنت.

عرفت جريمة الاحتيال على أنها استيلاء على مال منقول للغير بخداع المجني عليه وحمله على تسليمه، وجريمة النصب هي من جرائم الأموال التقليدية أساسها الغش والاحتيال.² مع التطور الذي شهده العصر الحديث تحولت من جريمة ذات طابع تقليدي إلى وسيلة أكثر ذكاء وتصرفا بواسطة شبكة الأنترنت، سمية بجريمة الاحتيال عبر الأنترنت أو الاحتيال الإلكتروني. وعرفت هذه الأخيرة بأنها جريمة تعتمد على خداع الأفراد أو الشركات للحصول على معلومات حساسة مثل أرقام بطاقات الائتمان أو تفاصيل الحسابات البنكية عادة ما يتم هذا الاحتيال عبر رسائل البريد الإلكتروني أو مواقع الأنترنت المزيفة التي تشبه المواقع الرسمية للبنوك أو الشركات الكبرى.³ كان الغرض من هذه الجريمة جمع المعلومات الشخصية والمالية واستخدامها لاحقا في أنشطة مالية غير مشروعة، وتحتوي جريمة الاحتيال عبر الأنترنت على الركن الشرعي، الركن المادي، الركن المعنوي سنقوم بتوضيحهم.

1. الركن الشرعي:

¹ عبد السلام علي، المرجع السابق، ص 580.

² حسين طاهري، المرجع السابق، ص 43.

³ حمد محمد الدوسري، المرجع السابق، ص 98.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

طبقاً لنص المادة 1 من قانون العقوبات التي تنص: "لجريمة ولا عقوبة أو تدبير أمن بغير قانون"¹ بما أن جريمة الإحتيال الإلكتروني جريمة مركبة تتداخل فيها عناصر الإحتيال التقليدي مع تقنيات الجريمة الإلكترونية، مما يمنحها طابعاً خاصاً يميزها عن غيرها من الجرائم.

فإن الأساس الرئيسي المادة 372 من قانون العقوبات² تجرم الإحتيال بصفة عامة، والذي يتحقق باستعمال طرق احتيالية لخداع المجني عليه والاستيلاء على ماله، وينطبق هذا النص على الإحتيال عبر الإنترنت متى توافرت أركانه، حتى وإن تم بوسائل رقمية.

2. الركن المادي:

تقوم هذه الجريمة على ثلاثة عناصر، بداية مع السلوك الإجرامي الممثل في قيام الجاني باستخدام وسائل إلكترونية أو رقمية بهدف خداع المجني عليه واستغلال جهله أو ثقته، ومن أبرز هذه الوسائل الرسائل الإحتيالية عبر البريد الإلكتروني، المواقع الإلكترونية الوهمية، الحسابات المزورة على شبكات التواصل الاجتماعي، أو التطبيقات المزيفة، وغالباً ما تتضمن هذه الوسائل إدعاءات كاذبة مثل الفوز بجائزة، أو ضرورة تحديث معلومات بنكية، أو طلب مساعدة مالية مستعجلة³

3. الركن المعنوي:

أي توافر القصد الجنائي بنوعيه، فالقصد الجنائي العام يتحقق بتوافر عنصره العلم يكون بعلم الجاني بأن الوسائل التي يستعملها هي احتيالية أو تدليسية وإدراكه أنه بذلك يخدع الضحية، والإرادة أي اتجاه إرادته إلى القيام بهذا السلوك الإحتيالي، وأنه لم يقع فيه عن طريق الخطأ أو الإهمال.

إلى جانب هذا يوجد القصد الجنائي الخاص الذي ينصب في سوء نية الجاني، حيث تكون الغاية من ذلك الاستيلاء على مال الغير أو منفعة غير مستحقة، ومن أجل تحقيق فائدة مادية.

ثانياً: جريمة غسيل الأموال الإلكترونية.

تتميز جريمة غسيل الأموال عن غيرها من الجرائم بكونها لا تنشأ بصورة مستقلة بل تأتي كمرحلة لاحقة لجرائم أصلية سابقة تولد عائدات غير مشروعة، قد عرفت هذه العملية على أنها تحويل أو نقل الأموال التي

¹ الأمر 156-66 المتضمن قانون العقوبات المعدل والمتمم بالقانون 15-04، سبق ذكره.

² انظر المادة 372 من القانون العقوبات.

³ أبو بكر تيتاوي، إلياس مالك قرادي، جرائم النصب والإحتيال الإلكتروني، شهادة ماستر، معهد الحقوق المركز الجامعي المقاوم آمود بن مختار إيليزي، 2025/2024، ص 13.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

يتم الحصول عليها بطرق غير مشروعة أو المتهربة من الالتزامات القانونية إلى أشكال أخرى من أشكال الاحتفاظ بالثروة للتغطية على مصادرها والتجهيل بها.¹

مع التطور التكنولوجي الحاصل ظهرت صورة جديدة من هذه الجريمة سميت بجريمة غسيل الأموال إلكترونيا، اعتمدت هذه الأخيرة على الوسائل الرقمية والتكنولوجيا لإخفاء أو تمويه مصدر الأموال غير المشروعة وجعلها تبدو كأنها تبدو كأنها أموال قانونية.

في هذا الصدد برز ما يسمى الغسيل الرقمي، الذي هو عبارة عن تحويلات نقدية عبر شبكة الأنترنت ومن مزايا هذه الطريقة تسهيل عمليات الدفع للمتعاملين في الأموال والتجارة الإلكترونية، ولكن في المقابل زادت احتمالات القرصنة وصعوبة الرقابة على المتعاملين في ظل الالتزام بسرية المعلومات المصرفية.² تحتوي على ثلاثة أركان سنوضحهم كما يلي.

1. الركن الشرعي:

تطبيقا لمبدأ الشرعية الجنائية القائم على قاعدة "لا جريمة ولا عقوبة إلا بنص" الجريمة لا تقوم إلا إذا كان الفعل المرتكب مجرم قانونا ومحدد العقوبة، الأمر 156/66 المتعلق بقانون العقوبات لم يسن مواد صريحة تجرم غسيل الأموال إلكترونيا كون هذه الأخيرة مستحدثة، غير أنه خصص القسم السادس مكرر لتبييض الأموال من خلال المواد 389 مكرر إلى 389 مكرر 7.

أضف إلى هذا تم إصدار قانون خاص يجرم هذه الظاهرة وهو القانون 05-01 المتعلق بقانون الوقاية من تبييض الأموال وتمويل الإرهاب ومكافهتهما في المواد 2 وما يليها من هذا القانون.

2. الركن المادي:

يتشكل الركن المادي لهذه الجريمة من ثلاث عناصر تتجلى في وجود جريمة أولية أو أصلية سابقة تعتبر مصدرا للمال غير المشروع، و أن تنتج عن تلك الجريمة مال غير نظيف، وأن يقوم الجاني أو الجناة بحسب الأحوال بارتكاب نشاط إجرامي يتحقق به غسل هذا المال غير المشروع، ويتوضح هذا النشاط في إجراء عملية

¹فريد علوش، جريمة غسيل الأموال دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2009/2008، ص 13.

²حسين طاهري، المرجع السابق، ص 40.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

أو سلسلة من العمليات الاقتصادية والمالية البسيطة أو المركبة، بغية تطهير هذا المال غير المشروع وإدخاله في الحركة المالية ليظهر كأنه مشروع.¹

بعبارة أوضح خالصنا أن السلوك المادي هنا هو أفعال إيجابية تتمثل في تحويل الأموال عبر الأنترنت، إجراء عمليات دفع إلكترونية وهمية، وغيرها من الأفعال التي ترتكب عبر الوسائط الإلكترونية. والنتيجة الإجرامية تتمثل في تحقق غاية الجاني وهي إخفاء أو تمويه المصدر غير المشروع للأموال، أما العلاقة السببية فهي الرابطة التي تربط السلوك المادي والنتيجة المتحققة، بحيث يكون النشاط الإلكتروني الذي قام به الجاني هو السبب المباشر في تمويه مصدر الأموال أو صعوبة تتبعها.

3. الركن المعنوي:

يتشكل الركن المعنوي لهذه الجريمة من عنصرين، عنصر العلم لدى الجاني بعناصر الركن المادي للجريمة، وعنصر الإرادة أي إرادة تحقيق النتيجة الإجرامية وإضفاء صفة الشرعية على الأموال القذرة.²

ثالثاً: جريمة السرقة الإلكترونية

السرقة وفقاً للقواعد العامة لقانون العقوبات هي اختلاس شيء غير مملوك له، وعليه جريمة سرقة المعلومات والبرامج هي كل فعل من شأنه الاستيلاء على برامج المعلوماتية المملوكة للغير في داخل جهاز الكمبيوتر المرتبطة بشبكة الأنترنت، وذلك عبر إرسال برامج فيروس من شأنه نسخ هذه البرامج والمعلومات والحصول عليها كالتعديل في البيانات أو الوظائف الخاصة بوسيلة الدفع الإلكتروني الذي يمكن أن يتم من خلال استغلال وجود ضعف أمني في النظام التشغيلي يسهل عملية السرقة أو من خلال اعتداءات مادية على الرقابة ذاتها.³

إلى جانب ذلك السرقة الإلكترونية تعد من الجرائم الحديثة التي ظهرت مع تطور تكنولوجيا الإعلام والاتصال، يمكننا القول أنها الاستيلاء الغير مشروع على أموال أو بيانات أو خدمات مملوكة للغير وذلك بواسطة وسائل إلكترونية.

حتى تقوم الجريمة لا بد من توافر جملة من الأركان، سنوضحها على النحو التالي.

¹ سفيان بن نقي، جريمة غسيل الأموال بين الوسائط الإلكترونية والنصوص التجريبية، مجلة الأبحاث القانونية والسياسية، جامعة محمد لمين دباغين، سطيف2، المجلد 3، ع 2، 2021، ص 158.

² سفيان بن نقي، المرجع السابق، ص 158.

³ حسين طاهري، المرجع السابق، ص ص 41، 42.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

1. الركن الشرعي:

المشرع الجزائري لم يخصص نصوص قانونية متعلقة بالسرقة الإلكترونية وإنما أدرجها مع السرقة، فطبقا بقاعدة " لا جريمة ولا عقوبة إلا بنص " وقانون العقوبات في الفصل الثالث منه المسمى ب " الجنايات والجناح ضد الأموال " في القسم الأول الخاص بالسرقات و الإبتزاز جاءت مواد تكيف بعض صور السرقة الإلكترونية خاصة إذا تعلق بالأموال منها المادة 350¹، أيضا القانون 04-09 في مواد من 3 إلى 10².

2. الركن المادي:

السلوك المادي في جريمة الحال هو فعل الاختلاس أي الاختراق والاستيلاء على أشياء مملوكة للغير عبر الوسائل الإلكترونية أبرزها الدخول غير المشروع لمنظومة معلوماتية، الاستيلاء على بيانات أو أموال إلكترونية مثل سرقة رصيد بنكي، أو باستعمال وسائل احتيالية إلكترونية.

بالنسبة للنتيجة الإجرامية فهي تتمثل في نقل حيازة المال أو البيانات من المجني عليه إلى الجاني دون علمه ورضاه وحرمانه من الانتفاع به وهذه تكون الغاية الأساسية التي تمت من أجلها السرقة الإلكترونية، والعلاقة السببية الموجودة بين السلوك والنتيجة أنه لو لم يتم الفعل الإجرامي لما حدث الضرر، وقد تعتبر الجريمة تامة حتى لو لم تكن هناك نتيجة.

محل جريمة السرقة الإلكترونية هو المال ولا يكون دائما ماديا، بل قد يكون رصيد بنكي، أو بيانات ذات قيمة، أو أصول رقمية وغيرها من أشياء ذات قيمة.

3. الركن المعنوي:

تعد السرقة من الجرائم العمدية التي تستلزم توافر قصد جنائي عام المتمثل في معرفة الجاني وقت ارتكابه الفعل واتجاه إرادته الحرة و إدراكه السليم بجميع أركان الجريمة، إلى جانب القصد الجنائي العام يجب توافر القصد الجنائي الخاص أي نية محددة هي نية تملك الشيء المسروق وحرمان مالكه منه نهائيا.³

المطلب الثالث: جرائم التجارة الإلكترونية.

¹ انظر المادة 350 من قانون العقوبات.

² انظر المواد من 3 إلى 10 من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

³ بومدين رحال، نورة سعداني، الحماية الجنائية الواقعة على أموال التجارة الإلكترونية (جريمة السرقة والنصب)، مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 9، ع 2، 2016، ص 99.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

في ظل التحول الرقمي المتسارع وانتشار استخدام الأنترنت ووسائل الدفع الإلكتروني، برزت التجارة الإلكترونية كنوع من أشكال ممارسة النشاط التجاري الحديث، غير أن هذا التطور لم يخل من تحديات قانونية حيث أفرزت أنماط جديدة من الجرائم مرتبطة بالتجارة الإلكترونية، حيث عالجها المشرع الجزائري في القانون 05-18 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية، الذي جرم عدة أفعال واعتبرها جريمة معاقب عليها بنص قانوني.

في موضوع الحال درسنا جرائم متعلقة بممارسة النشاط نذكر منها جريمة المتاجرة الإلكترونية بمنتجات غير مشروعة، الجرائم المتعلقة بمتطلبات المعاملات التجارية الإلكترونية كفرع أول، أما الفرع الثاني فخصصناه لدراسة الجرائم المتعلقة بالإشهار الإلكتروني، منها مخالفة ضوابط الإشهار الإلكتروني، والمتعلقة بموانع الإشهار الإلكتروني.

الفرع الأول: الجرائم المتعلقة بممارسة النشاط.

تعرف الجرائم المتعلقة بممارسة النشاط في مجال التجارة الإلكترونية بأنها كل الأفعال الغير مشروعة التي ترتكب عبر الوسائط الرقمية أو استخدام الشبكات المعلوماتية. لمعرفة أكثر ما يخص هذا النوع من الجرائم، خصصنا الفرع لدراسة جرائم المتاجرة الإلكترونية غير مشروعة، وكذا المتعلقة بمتطلبات المعاملات التجارية الإلكترونية. أولاً: جرائم المتاجرة الإلكترونية بمنتجات غير مشروعة.

قد تكون المتاجرة الإلكترونية بمنتجات ممنوعة، أو منتجات حساسة أو من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمن العمومي.

1. جريمة المتاجرة الإلكترونية بمنتجات ممنوعة.

يقصد بالمنتجات الممنوعة مختلف السلع أو المواد التي حظرها القانون ومنع إنتاجها أو تصديرها أو إستيرادها أو عرضها للبيع أو تداولها، نظرا للخطر الذي تشكله سواء النظام العام أو الأمن أو الصحة أو الآداب العامة.

هذه الجريمة كغيرها من الجرائم لقيامها لابد من توفر أركانها الممثلة في الركن الشرعي، الركن المادي، الركن المعنوي.

أ. الركن الشرعي:

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

يقوم هذا الركن على وجود نص قانوني صريح يجرم السلوك محل التجريم ويحدد العقوبة المقرر له، بما يجسد مبدأ الشرعية الجنائية القائم على قاعدة " لا جريمة ولا عقوبة إلا بنص "، وعليه يتمثل الزمن الشرعي لجريمة المتاجرة الإلكترونية لمنتجات ممنوعة في المادة 37 من القانون 05-18 المتعلق بالتجارة الإلكترونية التي نصت على: " دون المساس بتطبيق العقوبات الأشد المنصوص عليها في التشريع المعمول به، يعاقب بغرامة من 200000 دج إلى 1000000 دج كل من يعرض للبيع، أو يبيع عن طريق الاتصال الإلكتروني، المنتجات أو الخدمات المذكورة في المادة 3 من هذا القانون.

يمكن القاضي أن يأمر بغلق الموقع الإلكتروني لمدة تتراوح بين شهر (1) إلى ستة (6).¹ أضف إلى هذا المادة 3 من نفس القانون، نصت على ما يلي: " تمارس التجارة الإلكترونية في إطار التشريع والتنظيم المعمول بهما.

غير أنه. تمنع كل معاملة عن طريق الاتصالات الإلكترونية تتعلق بما يلي:

- لعب القمار والرهان واليانصيب.
- المشروبات الكحولية والتبغ.
- المنتجات الصيدلانية.
- المنتجات اتلتي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية.
- كل سلعة أو خدمة محظورة بموجب التشريع المعمول به.
- كل سلعة أو خدمة تستوجب إعداد عقد رسمي.²

ب. الركن المادي:

يكون هذا الركن من ثلاثة عناصر أساسية تتحقق من خلالها جريمة المتاجرة الإلكترونية بمنتجات ممنوعة، بداية مع السلوك الإجرامي هو ذلك السلوك الخارجي الملموس الذي يقوم به الجاني عبر الأنترنت، يتخذ صور متعددة هي :

- عرض أو لعب القمار أو الرهان واليانصيب عن طريق الاتصالات الإلكترونية: القمار الإلكتروني هنا يتشابه مع القمار العادي كما تتشابه مسمياته في الأنترنت مثل ابوكر، الروليت، و إدارة محرك البحث

¹ القانون رقم 05-18 المؤرخ في 24 شعبان 1439 الموافق ل 10 مايو 2018 المتعلق بالتجارة الإلكترونية .

² القانون رقم 05-18، المتعلق بالتجارة الإلكترونية، سبق ذكره.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

قول ستدفق عشرات المواقع الإلكترونية المتعلقة بالقمار وتعرض خدماتها في أشكال ورسومات جذابة، وتوجد مواقع باللغة العربية واللغات الأخرى، أما الرهان فهو مجموعة أموال يدفعها مجموعة من الأشخاص متشاركين على شيء ما، وتمنح في النهاية جميعها إلى الفائز بينهم. وتعرف لعبة اليانصيب بأنها اللعبة التي يساهم فيها عدد كبير من الناس، كل يدفع مبلغ صغير ابتغاء كسب النصيب.

- عرض أو بيع المشروبات الكحولية والتبغ عن طريق الاتصالات الإلكترونية: يعتبر هذا السلوك محرماً شرعاً، أما من الناحية القانونية فيجوز بيع المشروبات والتبغ تبعاً للقانون الجزائري، إلا أنه يمنع الترويج والرعاية والإشهار للمشروبات الكحولية.
- عرض أو بيع المنتجات الصيدلانية عن طريق الاتصالات الإلكترونية: هذه الصورة جاءت في المادة 169 من القانون 85-05 المتعلق بحماية الصحة وترقيتها، والمتمثلة في الأدوية، الكواشف البيولوجية، المواد الكيميائية الخاصة بالصيدليات، المنتجات الغلينية، مواد التضميض، النوكليد الإشعاعي، الإضمامة، السلف، وكل المواد الأخرى الضرورية للطب البشري.¹
- عرض أو بيع المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية عن طريق الاتصالات الإلكترونية: يقصد بها تلك التي ترتبط بتقليد هذه الحقوق، أي يتعلق الأمر بكل فعل في مواجهة السلع أو الخدمات الأصلية التي منحت لها الحماية القانونية بإسم حقوق الملكية الفكرية بصفة عامة، وتبعاً لذلك كل سلعة أو خدمة تدخل في نطاق التجريم والتي تتخذ مظهر محدد وفقاً لأحكام قوانين الملكية الفكرية بشتى ميادينها. أما الوارد على حقوق الملكية الصناعية والتجارية فإما أن يمس بفئة الابتكارات الجيدة وأما بفئة البيانات المميزة.
- عرض أو بيع كل سلعة أو خدمة محظورة بموجب التشريع المعمول به عن طريق الاتصالات الإلكترونية: بمعنى حظر أو بيع أي منتج مجرم التعامل فيه طبقاً للقوانين الجزائرية.
- عرض أو بيع كل سلعة أو خدمة تستوجب عقد رسمي عن طريق الاتصالات الإلكترونية.² من خلال ما سبق ينصب محل الجريمة على منتجات يحظر القانون تداولها.

¹ منيرة بن جدو، مبروك بن زيوش، الحماية الجزائية لمحل العقد الإلكتروني في ظل القانون 18-05 المتعلق بالتجارة الإلكترونية، مجلة الفكر القانوني والسياسي، جامعة عمار ثلجي، الأغواط، المجلد 5، ع 2، 2021، ص ص 106، 107-108.

² منيرة بن جدو، مبروك بن زيوش، المرجع السابق، ص 108.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

بالنسبة للنتيجة الإجرامية لا يشترط دائما تحققها، إذ قد تعتبر الجريمة قائمة بمجرد عرض المنتجات الممنوعة أو الترويج لها، كما يجب أن تكون هناك صلة مباشرة بين السلوك المرتكب والنتيجة المتحققة هذا مايعرف بالعلاقة السببية أي يكون النشاط الإلكتروني هو السبب في تداول أو انتشار المنتجات الممنوعة.

ج. الركن المعنوي:

باعتبار جريمة المتاجرة الإلكترونية للمنتجات الممنوعة من الجرائم العمدية، وجب توفر القصد الجنائي العام المتمثل في عنصر العلم والإرادة، حيث يكون المورد الإلكتروني على دراية بأن هذه المنتجات ممنوعة من التداول الإلكتروني ومع ذلك تتجه إرادته إلى ارتكاب الفعل المجرم رغم علمه أنه جريمة معاقب عليها.

2. جريمة المتاجرة الإلكترونية بمنتجات حساسة أو من شأنها المساس بمصالح الدفاع الوطني والنظام

العام والأمن العمومي:

يمكننا تعريف هذه الجريمة بأنها كل سلوك غير مشروع يتم عبر وسائل التجارة الإلكترونية، يقوم من خلاله شخص طبيعي أو معنوي بعرض أو بيع أو توزيع أو الترويج لمنتجات مصنفة قانونا على أنها حساسة أو محظورة، من شأن تداولها الإضرار بأمن الدولة أو إستقرار المجتمع أو سلامة الأفراد. في هذا الصدد تقوم الجريمة على أركان مكونة لها.

أ. الركن الشرعي:

طبقا لنص المادة: " لا جريمة ولا عقوبة أو تدبير أمن بغير قانون"¹، الأساس القانوني الذي تقوم عليه هذه الجريمة قانون التجارة الإلكترونية من خلال المادة 38 التي نصت على: "دون المساس بتطبيق العقوبات الأشد المنصوص عليها في التشريع المعمول به، يعاقب بغرامة من 500000 دج إلى 2000000 دج كل من يخالف أحكام المادة 5 من هذا القانون.

يمكن القاضي أن يأمر بغلق الموقع الإلكتروني والشطب من السجل التجاري."²

ب. الركن المادي:

¹الأمر 156-66 المتضمن قانون العقوبات المعدل والمتمم بالقانون 15-04، سبق ذكره.

² قانون رقم 05-18، المتعلق بالتجارة الإلكترونية، سبق ذكره.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

يتمثل الركن المادي لهذه الجريمة في مخالفة أحكام المادة 5 من هذا القانون التي حددت محل الجريمة بدقة وجُرمت كل معاملة عن طريق الاتصالات الإلكترونية في العتاد والتجهيزات والمنتجات الحساسة المحددة عن طريق التنظيم المعمول به، وكذا كل المنتجات أو الخدمات الأخرى التي من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمن العمومي.¹

تعد هذه الجريمة من الجرائم الشكلية، حيث يكفي مجرد عرض أو ترويج للمنتجات الحساسة لقيم الركن المادي، حتى لو لم تتم عملية البيع فعلا، أما العلاقة السببية تكمن في كون استخدام الوسائط الرقمية هو السبب في إتاحة أو تسهيل أو تسهيل تداول هذه المنتجات المحظورة.

ج. الركن المعنوي:

يقوم هذا الركن على القصد الجنائي العام بعنصريه العلم والإرادة، إذ يجب أن يكون الفاعل عالما بطبيعة المنتجات محل التداول وخطورتها، فضلا عن إدراكه عن ما يترتب عن تداولها من تهديد لمصالح الدولة أو الإخلال بالنظام العام والأمن العمومي، كما يتعين أن تتجه إرادته الحرة إلى ارتكاب فعل المتاجرة الإلكترونية لهذه المنتجات.

وغالبا ما يتوافر القصد الجنائي الخاص المتمثل في سوء نية الجاني والإضرار بمصالح الدولة.

ثانيا: جرائم مخالفة المتطلبات المتعلقة بالمعاملات التجارية الإلكترونية.

يشمل هذا الجزء مخالفة أحكام العرض الإلكتروني، ومخالفة الأحكام المتعلقة بطلبية المنتج.

1. مخالفة أحكام العرض الإلكتروني.

هي كل سلوك غير مشروع يتمثل في القيام بعرض سلع أو خدمات عبر الوسائط الإلكترونية. تتمثل الأركان المكونة لهذه الجريمة في مايلي.

¹ عبد السلام شطيبي، خصوصية المتابعة الجزائية لجرائم التجارة الإلكترونية بين حداثة النص التشريعي عوائق التطبيق، الملتقى الدولي الموسوم بالتجارة الإلكترونية بين حتمية تكنولوجيا الاتصال وسبل حماية المستهلك الإلكتروني، كلية الحقوق والعلوم السياسية، جامعة المدية، 19 جوان 2021، ص 6.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

أ. الركن الشرعي:

حيث يتمثل الركن الشرعي لهذه الجريمة في نص المادة 39 من القانون 18-05¹، الذي جرم مخالفة الأحكام المتعلقة بالعرض الإلكتروني، من خلال تقرير عقوبات على كل مورد إلكتروني لا يحترم الشروط القانونية المفروضة عند عرض السلع أو الخدمات عبر الوسائل الإلكترونية. أضف إلى ما سبق المادة 11 من القانون السابق الذكر التي ذكرت المعلومات الواجب توافرها في العرض التجاري الإلكتروني أن مخالفتها تعتبرت جريمة.

ب. الركن المادي:

يكمن الركن المادي لهذه الجريمة في مخالفة أحكام المادة 11 والذي ينطوي على إحدى السلوكات التالية:

- رقم التعريف الجبائي، والعناوين المادية والإلكترونية، ورقم هاتف المورد الإلكتروني.
- رقم السجل التجاري، أو رقم البطاقة المهنية للحرفي.
- طبيعة وخصائص وأسعار السلع أو الخدمات المقترحة باحتساب كل الرسوم.
- حالة توفر السلعة أو الخدمة.
- كفاءات ومصاريف وآجال التسليم.
- الشروط العامة للبيع، لاسيما البنود المتعلقة بحماية المعطيات ذات الطابع الشخصي.
- شروط الضمان التجاري وخدمة ما بعد البيع.
- طريقة حساب السعر، عندما لا يمكن تحديده مسبقا.
- كفاءات وإجراءات الدفع.
- شروط فسخ العقد عند الإقتضاء.
- وصف كامل لمختلف مراحل تنفيذ المعاملة الإلكترونية.
- مدة صلاحية العرض عند الإقتضاء.
- شروط وآجال العدول عند الإقتضاء.
- طريقة تأكيد الطلبية.
- موعد التسليم وسعر المنتج موضوع الطلبية المسبقة وكفاءات إلغاء الطلبية المسبقة، عند الإقتضاء.

¹ أنظر المادة 38 من القانون 18-05 المتعلق بالتجارة الإلكترونية.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

- طريقة إرجاع المنتج أو استبداله أو تعويضه.
- تكلفة استخدام وسائل الاتصالات الإلكترونية عندما تحتسب على أساس آخر عبر التعريفات المعمول بها.¹

والنتيجة المتحققة إلحاق الضرر بالمجني عليه، سواء كان الضرر فعلي كتعرض المستخدم للخداع أو الغش نتيجة معلومات مضللة، غير أن الفعل قد يكون من شأنه إلحاق الضرر دون تحقيق نتيجة. والعلاقة التي تجمع بين السلوك الإجرامي والنتيجة الإجرامية تكون عند مخالفة أحكام العرض الإلكتروني.

ج. الركن المعنوي:

يتمثل في عنصر العلم أي علم الجاني بكافة العناصر المكونة للجريمة سواء علمه بأن النشاط الذي يقوم به يعد عرض إلكتروني خاضع لتنظيم قانوني، وعلمه بالالتزامات القانونية ورغم ذلك خالف هذه الأحكام، أما عنصر الإرادة يقصد به اتجاه إرادة الجاني إلى ارتكاب الفعل المخالف.

2. مخالفة الأحكام المتعلقة بطلبية المنتج:

سنتحدث في هذه الجزئية عن مخالفة الأحكام المتعلقة بطلبية المنتج، تعرف الطلبية بأنها تعهد بالبيع يمكن أن يقترحه المورد الإلكتروني في حالة عدم توفر المنتج في المخزون، وهي تمر بثلاث مراحل إلزامية بالنسبة للمورد الإلكتروني ويترتب على عدم إحترام إحداها قيام الجريمة.² وسنوضح أركانها:

أ. الركن الشرعي:

طبقا للمادة 1 من قانون العقوبات والمادة 39 من القانون 18-05 جرم المشرع الجزائري مخالفة الأحكام والضوابط الخاصة بالطلبية الإلكترونية وسن عقوبة لذلك، فبمجرد إرتكاب الأفعال التي وضعها القانون يقوم الجرم.

أيضا المادة 12 من القانون السابق الذكر التي جاءت بالمراحل اللازمة للطلبية.

ب. الركن المادي:

¹ عبد السلام شطيبي، خصوصية المتابعة الجزائية لجرائم التجارة الإلكترونية بين حادثة النص التشريعي وعوائق التطبيق، المرجع السابق، ص 6، 7.

² المرجع نفسه، ص 7.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

السلوك الإجرامي هنا يكون عند مخالفة أحكام المادة 12 من القانون 05-18¹، بمعنى أوضح يتجسد السلوك في كل فعل أو إمتناع يؤدي إلى الإخلال بالضوابط القانونية للطلبية الإلكترونية، من أبرز صورته عدم تمكين المستهلك من الإطلاع على الشروط التعاقدية قبل إبرام الطلب، حرمانه من مراجعة تفاصيل الطلبية أو تعديلها أو تصحيح الأخطاء، إبرام الطلبية دون تأكيد صريح من المستهلك.

كما إستخلصنا أن النتيجة الإجرامية تتمثل في المساس برضا المستهلك الإلكتروني وتعرض حقوقه للخطر إضافة إلى إنهزاز الثقة في المعاملات الإلكترونية، أما العلاقة السببية تتحقق عند إثبات أن السلوك المخالف هو السبب المباشر في النتيجة.

ج. الركن المعنوي:

يتكون من القصد الجنائي العام المتمثل في العلم والإرادة أي علم الجاني المتعامل بوجود قواعد قانونية تنظم الطلبية، ورغم علمه بذلك إلا أن إرادته اتجهت إلى ارتكاب الفعل المخالف. بالنسبة للقصد الجنائي الخاص لا يشترط توفره لدى الجاني في هذا النوع من الجرائم، فبمجرد مخالفة الأحكام القانونية المنظمة للطلبية تقوم الجريمة.

الفرع الثاني: الجرائم المتعلقة بالإشهار التجاري الإلكتروني.

إذا كان الإشهار الإلكتروني هو كل إعلان يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع سلع أو خدمات عن طريق الاتصالات الإلكترونية²، فهو يمثل وسيلة تأثير نفسي على الجمهور تحقيقا لغايات تجارية، حيث يعرف المورد الإلكتروني لمنتجاته كما يعد مرآة عاكسة للمستهلك الإلكتروني لتحديد ما إذا كان هذا المنتج يتطابق مع رغباته أم لا.³

¹ أنظر المادة 12 من القانون 05-18 المتعلق بالتجارة الإلكترونية.

² أنظر المادة 6 من القانون 05-18 المتعلق بالتجارة الإلكترونية.

³ عبد السلام شطيبي، خصوصية المتابعة الجزائية لجرائم التجارة الإلكترونية بين حداثة النص التشريعي وعوائق التطبيق، المرجع السابق،

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

يتميز هذا النوع من الإشهار في كونه يتم بوسيلة إلكترونية موجه إلى جمهور المستهلكين، ينصب على بيان مزايا السلع والخدمات المعلن عنها فيتضمن مدحا لهذه المنتجات وإظهار محاسنها، كما أنه يحفز المستهلكين على التعاقد.¹

سن المشرع الجزائري مجموعة من الضوابط، فبمجرد مخالفة أحكام المواد 30، 31، 32، 34 من القانون 05-18 تقوم مجموعة من الجرائم، هذا ما نصت عليه المادة 40 من القانون السالف الذكر التي جاءت بـ: "دون المساس بحقوق الضحايا في التعويض، يعاقب بغرامة من 50000 دج إلى 500000 دج كل من خالف أحكام المواد 30 و 31 و 32 و 34 من هذا القانون."²

وعليه نستخلص مما سبق أن المادة 30 تخص جريمة مخالفة القواعد التنظيمية التي تنظم الإشهار، والمادة 31 تخص جريمة المساس بحماية الحياة الخاصة والمعطيات الشخصية، أما المادة 32 ذكرت فيها جريمة الإخلال بحقوق المستهلك في المجال الإلكتروني، والمادة 34 لجريمة إشهار أو تسويق إلكتروني لمنتجات أو خدمات محظورة.

ونحن في دراستنا سنسلط الضوء على جريمتين، بداية مع عدم احترام ضوابط الإشهار الإلكتروني، ثم جريمة إشهار أو تسويق لمنتجات أو خدمات محظورة، سنوضحكم كما يلي.

أولاً: جريمة عدم احترام ضوابط الإشهار الإلكتروني.

تعرف جريمة عدم احترام ضوابط الإشهار الإلكتروني في التشريع الجزائري بأنها كل فعل أو امتناع يصدر عن متعامل اقتصادي عبر الوسائط الإلكترونية، يتمثل في نشر أو بث إشهار لا يحترم الشروط والضوابط القانونية المفروضة، أضف إلى هذا تكون هذه الجريمة من شأنها خداع المستهلك أو التأثير غير المشروع على إرادته.

تقوم هذه الجريمة كغيرها من الجرائم على مجموعة من الأركان ممثلة في الركن الشرعي، الركن المادي، الركن المعنوي.

¹ حسين جفالي، الحماية الجنائية للمستهلك من الإشهار التجاري الإلكتروني غير المرغوب فيه في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثلجي، الأغواط، المجلد 2، ع 4، 2018، ص 525.

² انظر المادة 40 من القانون 05-18 المتعلق بالتجارة الإلكترونية.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

أ. الركن الشرعي:

باعتبار قانون العقوبات الشريعة العامة للتجريم نصت المادة 1 منه على: "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون".¹ أي لا يكون الفعل مجرم إلا إذا جاء نص قانوني يجرم ذلك، حيث جاء في هذا القانون أيضا الحالات المشددة لهذه الجريمة على سبيل المثال عند الغش و الاحتيال.

أضف إلى هذا الأساس القانوني الذي تقوم عليه هذه الجريمة يكمن في القانون 05-18 المتعلق بالتجارة الإلكترونية الذي جاء فيه الإطار الأساسي للإشهار الإلكتروني، خصص له الفصل السابع تحت عنوان "الإشهار الإلكتروني" في المواد من 30 إلى 34 من القانون سالف الذكر، أيضا المواد من 38 إلى 42 منه التي حددت العقوبات المطبقة على مخالفة ضوابط الإشهار الإلكتروني، قد تكون غرامات مالية أو عقوبات أخرى.

ب. الركن المادي:

يتكون من ثلاثة عناصر بداية مع السلوك الإجرامي قد يكون هذا الأخير فعلا إيجابيا أو سلبيا، وهو كل تصرف يخالف الضوابط القانونية للإشهار الإلكتروني، بعبارة أوضح مخالفة الأحكام الموجودة في نص المادة 30 من القانون السالف الذكر²، ومن أبرزها نشر إعلان كاذب أو مضلل، عدم ذكر البيانات الإلزامية ودون تحديد الشخص الذي صممت الرسالة لصالحه، إرسال إعلانات إلكترونية دون موافقة سابقة من المستهلك، إخفاء الطابع الإشهاري للمحتوى وكذا الترويج لمنتجات أو خدمات محظورة أو غير مرخصة.

أما النتيجة الإجرامية فتتمثل في الإضرار بمصالح المستهلك والنظام العام، تضليل المستهلك وخداعه.

والعلاقة السببية يقصد بها العلاقة الموجودة بين السلوك المرتكب والنتيجة المتحصل عليها أي أن الإعلان المخالف هو السبب في تضليل المستهلك أو وقوع الضرر.

¹ الأمر 156-66 المتضمن قانون العقوبات المعدل والمتمم بالقانون 04-15، سبق ذكره.

² جاء في نص المادة 30 من القانون 05-18: "... أن تكون محددة بوضوح كرسالة تجارية أو إشهارية، أن تسمح بتحديد الشخص الذي تم تصميم الرسالة لحسابه، ألا تمس بالأداب العامة والنظام العام، أن تحدد بوضوح ما إذا كان هذا العرض التجاري يشمل تخفيضا أو مكافآت أو هدايا في حالة ما إذا كان هذا العرض تجاريا أو تنافسيا أو ترويجيا، التأكد من أن جميع الشروط الواجب استيفائها للاستفادة من العرض التجاري، ليست مضللة وغامضة."

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

ج. الركن المعنوي:

يحتوي هذا الركن على القصد الجنائي العام المتمثل في علم الفاعل أن الإعلان أو الإشهار الإلكتروني مخالف للقانون فقد يكون إشهار كاذب، مضلل، أو يفتر للبيانات الإلزامية، وكذا اتجاه إرادته إلى نشر الإعلان رغم علمه بذلك.

كما أن هذه الجريمة قد تكون عن طريق الخطأ سواء بإهمال منه وتقصير، فمثلا إهمال المستهلك عند مراقبة محتوى الإعلان، نشر معلومات غير صحيحة بسبب قلة الحيلة، أو عدم الدقة في المعلومات الإشهارية. **ثانيا: جريمة إشهار أو تسويق إلكتروني لمنتجات أو خدمات محظورة.**

تعد هذه الجريمة من الجرائم المرتبطة بمخالفة قواعد التجارة الإلكترونية، يمكن تعريفها على أنها كل قيام لشخص طبيعي أو معنوي عبر الوسائط الإلكترونية بالترويج أو الإعلان عن منتجات أو خدمات يمنع القانون تداولها أو تسويقها.

تقوم هذه الجريمة على ثلاثة أركان تتمثل في الركن الشرعي، الركن المادي، الركن المعنوي.

أ. الركن الشرعي:

طبقا لنص المادة 1 من قانون العقوبات التي نصت على: "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون"¹ والمادة 34 من القانون 18-05² جرم المشرع الجزائري جريمة إشهار أو تسويق إلكتروني لمنتجات أو خدمات محظورة، وذلك بتجريمة كل عرض أو بيع لمنتجات محظورة قانونا سواء كان هذا عبر المواقع الإلكترونية أو المنصات الرقمية.

ب. الركن المادي:

يتمثل السلوك الإجرامي في قيام المورد الإلكتروني بالإعلان الإلكتروني لكل السلع الممنوعة من بيع عن طريق الاتصالات الإلكترونية، والمتمثلة في المشروبات الكحولية والتبغ، المنتجات الصيدلانية، المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية، أيضا كل سلعة أو خدمة تستوجب إعداد عقد رسمي،

¹الأمر 66-156 المتضمن قانون العقوبات المعدل والمتمم بالقانون 04-15، سبق ذكره.

²انظر المادة 34 من القانون 18-05 المتعلق بالتجارة الإلكترونية.

الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية

على سبيل المثال بيع العقار وبيع المنتجات أو الخدمات التي من شأنها المساسا بمصالح الدفاع الوطني والنظام العام والأمن العمومي.¹

النتيجة الإجرامية تتمثل في خلق حالة خطر قانوني نتيجة نشر هذا النوع من الإشهار، حتى ولو لم يتحقق شراء فعلي أو استعمال للمنتج، ومنه ينتج عن ذلك المساس بالنظام العام أو الصحة العامة، تعريض المستهلك للخطر، والإخلال بالقواعد الاقتصادية.

أما العلاقة السببية تكمن في كون النشاط الإشهاري هو السبب في تحقيق النتيجة أو من شأنه تحقيقها. استخلصنا محل هذه الجريمة المتمثل في أدوية غير مرخصة، خدمات غير مشروعة، مشروبات كحولية وتبغ، مخدرات، أسلحة، ومنتجات مقلدة.

ج. الركن المعنوي:

يحتوي على القصد الجنائي العام الممثل في علم الجاني أن المنتج ممنوع تداوله والخدمة غير مرخصة أي كلاهما محظوران ومخالفان للقانون، واتجاه إرادة الفاعل إلى نشر أو تسويق هذا المنتج رغم علمه بأنه غير مشروع، وذلك لتحقيق منفعة لصالحه.

كما أن هذه الجريمة تعد بالخطأ إن وجد كإهمال أو عدم التحقق من مشروعية المنتج، أيضا التسرع في نشر الإعلان دون رقابة وغيرها من الأفعال غير العمدية.

¹ منيرة بن جدو، مبروك بن زيوش، الإشهار الإلكتروني وحمايته جنائيا في القانون الجزائري، مجلة الرسالة للدراسات والبحوث الإنسانية، جامعة العربي التبسي، تبسة، المجلد 6، ع 4، 30 ديسمبر 2021، ص 81.

خلاصة الفصل

وفي ختام هذا الفصل، يظهر لنا جلياً أن الجريمة الإلكترونية تشكل أبرز التحديات المعاصرة التي تواجه المنظمات القانونية في مختلف الدول والجزائر ليست بمنأى عن هذه التحديات، فقد رأينا أن المشرع الجزائري قد واجهها بالنظر إلى طبيعتها المستحدثة وكذا تطور وسائل ارتكابها بشكل متسارع بفضل الطفرة التكنولوجية، وقد تم في هذا الفصل الإحاطة بالجانب النظري للجريمة الإلكترونية، من خلال تعريفها وبيان خصائصها ودوافع ارتكابها، إضافة إلى الأركان المكونة لها، فضلاً عن استعراض أبرز صورها المختلفة.

وقد أظهر هذا الإطار اتساع نطاق الجرائم الإلكترونية لتشمل طيفاً واسعاً من الأفعال الإجرامية، من أبرزها التجسس الإلكتروني، الابتزاز الإلكتروني، الاحتيال عبر الأنترنت، غسيل الأموال إلكترونياً، المتاجرة الإلكترونية بمنتجات حساسة أو من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمن العمومي، كما تتفرع عن هذه الجرائم أنماط أخرى أكثر تطوراً وتعقيداً.

الفصل الثاني

المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة
الإلكترونية

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

تمهيد:

الجريمة الإلكترونية تتميز بطابع الحداثة والسرعة في تنفيذها فضلا عن الدقة العالية في إخفاء آثارها، هذا ما يجعل اكتشافها أمرا بالغ الصعوبة، يقوم بارتكابها مجرمين ذو ذكاء ومستوى علمي عالي مع حرصهم على إخفاء الأدلة المادية أو السلوك المكون للجريمة باستخدام وسائل تقنية متطورة.

ومن ثم فإن كشف هذه الجرائم وتتبع مرتكبيها يعد من أبرز التحديات التي تواجه أجهزة العدالة والجهات المختصة لإدارة مكافحة جرائم الحاسب وشبكات المعلومات، وعليه سندرس في هذا الفصل الأساليب أو الطرق المتبعة من طرف الضبطية القضائية للكشف عن الجرائم الإلكترونية تسمى بإجراءات البحث والتحري، حيث سلطنا الضوء على الإجراءات التقليدية للكشف عن الجريمة الإلكترونية وكذا الإجراءات المستحدثة للكشف عن الجريمة الإلكترونية، ومن جهة أخرى درسنا التنظيم القانوني للشرطة القضائية، أما بالنسبة للجزء الثاني من الدراسة خصصناه لمعرفة الدليل الإلكتروني باعتباره أداة لإثبات هذه الجريمة.

المبحث الأول: إجراءات جمع الاستدلالات المتعلقة بالجريمة الإلكترونية.

نظرا لخصوصية الجريمة الإلكترونية وتزايدها الملحوظ نتيجة التطور السريع في تكنولوجيا المعلومات والاتصال، برزت أنماط جديدة من الجرائم يتم ارتكابها في البيئة الرقمية.

فرضت هذه الخصوصية على المشرع الجزائري التدخل من أجل وضع إطار قانوني يواكب هذا التطور ويمكن السلطات المختصة من مكافحتها بفعالية سن مجموعة من القانونين، خاصة القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إضافة إلى أحكام قانون الإجراءات الجزائية الجزائري.

تأسيسا على ما سبق اعتمدت الضبطية القضائية على إجراءات شرطية خاصة تتلاءم مع طبيعة البيئة الرقمية، جاءت بهدف الكشف عن هذه الجرائم وجمع الأدلة والاستدلالات لمواجهتها وضبط مرتكبيها، وقد تكون هذه الإجراءات تقليدية ومستحدثة، علاوة على ذلك تطرقنا إلى معرفة الضبطية القضائية المختصة في البحث والتحري عن الجريمة الإلكترونية.

المطلب الأول: الإجراءات التقليدية للكشف عن الجريمة الإلكترونية.

في عنوان هذا المطلب سلطنا الضوء على الإجراءات التقليدية الخاصة بالجريمة الإلكترونية، حيث قسمنا هذه الدراسة إلى ثلاثة فروع.

الفرع الأول يتضمن تلقي الشكاوى والبلاغات والسماعات، الفرع الثاني يتضمن المراقبة المادية أو التقليدية، أما الفرع الثالث خصصناه للمعاينة والخبرة.

الفرع الأول: تلقي الشكاوى والبلاغات والسماعات.

غالبا ما تكون الجريمة غير مكشوفة ما لم يتم الإبلاغ عنها لدى الجهات المختصة غير أن الإشكال الذي تقع فيه الأجهزة الأمنية يتمثل في أن الجرائم المعلوماتية لا يتم التبليغ عنها في الوقت المناسب نظرا لصعوبة اكتشافها وإدراك وقوعها.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

هنا تظهر أهمية الأجهزة الأمنية في رصد حركة مرتكبي الجرائم الإلكترونية والكشف عنها، فتلقي الشكاوى والبلاغات الواجب الأول على أعضاء الشرطة القضائية، سواء ما ورد منها من الأفراد أو الناس أم من الموظفين العموميين المكلفين بخدمة عامة عن جرائم وقعت أثناء تأدية عملهم أو بسببها، والتبليغ هو مجرد إيصال خبر الجريمة للسلطات العامة، وقد يكون من مجهول أو معلوم، وقد يكون شفهيًا أم كتابيًا وهو حق مقرر لكل إنسان مجني عليه ذا مصلحة.¹

منح المشرع الجزائري لاسيما في قانون الإجراءات الجزائية سلطة تلقي الشكاوى والبلاغات لضباط الشرطة القضائية، هذا ما جاءت به المادة 26 منه التي نصت على: "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 20 و 21 أعلاه، ويتلقون الشكاوى والبلاغات بأي وسيلة، بما فيها الطريق الإلكتروني، ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية..."²

من خلال ما سبق رجال الشرطة وجب عليهم قبول البلاغات والشكاوى التي تقدم إليهم سواء كانت كتابية أو شفوية، وعند وردها للقسم أو نقطة الشرطة، تقيد في دفتر خاص بتلقي البلاغات كما يجب على المتحري أو المتحقق إخطار رئاسته في حالة الجرائم الإلكترونية.³

حيث جاءت المادة 27 من قانون الإجراءات الجزائية بما يلي: "يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم وأن يبادروا بغير تمهل إلى إخطار وكيل الجمهورية المختص إقليميا بالجنايات والجناح التي تصل إليهم..."⁴

وقد جاء في تعريف الشكاوى أنها تطلق على البلاغ المقدم من المجني عليه، أي تلك التصريحات والبيانات التي يبتدع بها أصحابها لضباط الشرطة القضائية بخصوص الجرائم والاعتداءات التي تقع عليهم حيث يعتبرون بهذه الصفة ضحايا مشتركين،⁵ جرائم لا يمكن تحريك الدعوى فيها إلا بناء على شكاوى من الطرف المتضرر، بحيث لا يجوز للنيابة العامة مباشرة أي من إجراءات التحقيق أو رفع الدعوى في غياب هذه

¹ محمد شنه، إجراءات البحث والتحري عن الجرائم في التشريع الطبعة 1، ألفا للوثائق للنشر والتوزيع، الجزائر، 2024، ص ص 72، 73.

² القانون رقم 14-25 المؤرخ في 9 صفر 1447 الموافق 3 غشت 2025، يتضمن قانون الإجراءات الجزائية، ج.ر، ع 54، 2025.

³ فيروز عوض الكريم صالح مبرغني، إجراءات التحري والضبط في الجريمة الإلكترونية، أطروحة دكتوراه، كلية الدراسات العليا والبحث العلمي، جامعة شنددي، 1437/ 2017، ص 68.

⁴ الأمر 155-66، الموافق ل 8 يوليو 1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 14-25.

⁵ محمد شنه، المرجع نفسه، ص 73.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

الشكوى، غير أن القيد لا يمتد إلى الأعمال الأولية التي تباشرها جهات الضبط القضائي باعتبارها مشروعة لا تمس حقوق وحرّيات الأفراد.

بالنسبة للبلاغ فهو إجراء يقوم بواسطته شخص لم يتضرر من الجريمة بإبلاغ نبئها إلى الشرطة القضائية، وتتمثل هذه المعلومات التي تقدم إلى ضباط الشرطة القضائية من قبل أشخاص قصد التبليغ عن جريمة وقعت يكونوا قد علموا بها أو عاينوها وهم بهذه الصفة يعتبرون مبلغين.¹

كما قد يقع على عاتق ضباط الشرطة القضائية إلزام إجرائي يقضي بإحاطة الأطراف علماً بإمكانية استدعائهم أو تبليغهم عبر الوسائط الإلكترونية (العناوين البريدية أو أرقام الهواتف)، مع شرط الموافقة الصريحة منهم بهذا الشأن، وإلزامية إخطار الجهة القضائية المختصة بأي تعديل يطرأ على هذه البيانات وتدوين كافة الإجراءات في محاضر السماع، وهذا ما استتجنه من الفقرة 3 من المادة 27 من قانون الإجراءات الجزائية. بعد تلقي الضبطية القضائية الشكاوى والبلاغات، يتم في نطاق هذه الاستدلالات سماع أقوال من لديهم معلومات عن الجريمة ومرتكبيها ويخص الإجراء المشتبه فيه المعلوماتي، وفي هذا السياق عملية سماع الأقوال ركيزة أساسية في مرحلة الاستدلال من أجل جمع معلومات وبيانات أكثر حول الجريمة، وقد تشمل إجراءات الاستماع الأشخاص الذين حامت حولهم الشبهات، إلا أن سلطة الضبط القضائي في هذا الإجراء ليست مطلقة بل تتقيد بمجموعة من الضوابط القانونية والضمانات الإجرائية التي تكفل التوازن بين فاعلية البحث الجنائي وحماية الحقوق والحرّيات.

حيث يشترط القانون أن تكون الأسئلة الموجهة إلى المشتبه به في نطاق جمع المعلومات مع تجنب الأسئلة التفصيلية التي تدخل في نطاق الإنتداب، فإذا اعترف المشتبه به بارتكاب الجريمة اقتصر اقتصر على إثبات هذا الاعتراف²، هذا كما جاء به المشرع الجزائري في المادة 26 الفقرة 2 من قانون الإجراءات الجزائية التي نصت على: "عند مباشرة التحقيقات وتنفيذ الإنابات القضائية، لا يجوز لضابط الشرطة القضائية طلب أو تلقي أوامر أو تعليمات أو تسخيرات إلا من الجهة القضائية التي يتبعونها، وذلك مع مراعاة أحكام المادة 38 أدناه..."³، كما أنه ليس لضابط الشرطة القضائية إكراه أحد على الحضور أمامه، فإذا رفض المشتبه به الحضور أمامه فلا يملك وسيلة لإكراهه على ذلك، إذ لا يستطيع إصدار أمر بضبطه وإحضاره ولا يرتكب هذا

¹ محمد شنه، المرجع السابق، ص 74.

² رابح لهوي، البحث والتحري عن الجريمة الإلكترونية والشرعية، دار الأيام للنشر والتوزيع، عمان، 2021، ص 159.

³ الأمر 155-66 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 14-25.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

الشخص جريمة بامتناعه، ويعمل ذلك بالطبيعة العامة لأعمال البحث والتحري وتجربتها من وسائل القهر والإجبار.¹

يمكننا القول أن هذه القواعد التقليدية موجودة في كل أنواع الجرائم لاسيما الجريمة الإلكترونية لذا سمي بالمشتبه به المعلوماتي وفي غالبية الأحيان يكون شخص مجهول، من جهة أخرى هناك أقوال الشاهد المعلوماتي، ينصرف هذا المصطلح إلى أولئك المتخصصين في المعلوماتية من فئة الفنيين أصحاب الخبرة والتخصص في مجال نظم المعلوماتية، وهم يملكون في الغالب معلومات قيمة ومهمة حول الجريمة المعلوماتية الواقعة، وأبرز هؤلاء الشهود مثلاً متعهد الوصول ومتعهد الإيواء وناقل المعلومات ومتعهد الخدمات ومورد المعلومات ومنتجو الخدمات المعلوماتية.²

تقتصر إفادة الشاهد المعلوماتي على تقديم البيانات الجوهرية المتعلقة بآليات النفاذ للأنظمة محل الإشتباه وتقنيات فك التشفير، فالطبيعة التقنية " الخبرة " لهذه الإفادة تخرجها من عباءة الشهادة التقليدية لتدخلها في حيز الخبرة الفنية. والمشرع الجزائري لم يفرض الإلتزام بالشهادة في الجرائم المعلوماتية، ما عدا إلزام مزودي الخدمات بالتعاون لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات، فالقواعد التقليدية تبقى عاجزة عن فرض مثل هذا الإلتزام على الشاهد المعلوماتي بالرغم من ضرورته وأهميته في مجال التحري والتنقيب عن جرائم المعلوماتية.³

الفرع الثاني: المراقبة المادية.

سميت بالمراقبة المادية أو التقليدية، يمكن تعريفها بأنها: "وضع شخص أو وسائل نقل أو أماكن أو مواد تحت رقابة سرية ودورية، بهدف الحصول على معلومات لها علاقة بالشخص محل الاشتباه، أو أمواله، أو بالنشاط الذي يقوم به".⁴

¹ رايح لهوي، المرجع السابق، ص 159.

² المرجع نفسه، ص 164.

³ المرجع نفسه، ص 167.

⁴ محمد شنه، المرجع السابق، ص 104.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

والمراقبة هي الأسلوب الواقعي والأمثل للرؤية الفعلية والملاحظة البصرية لدى رجل هيئة الشرطة نحو الاستمرار في جمع المعلومات للوصول بها إلى الاستدلالات المؤدية لكشف الجريمة، فهي رصد لكافة المظاهر الخارجية للأشخاص والأماكن بحيث تفيد إلى حد كبير في كشف الحدث الجرمي وتهدف إلى منع تحققه.¹ وعموما فإن هذه المراقبة تهدف إلى تتبع حركات وتقلات الأشخاص والأشياء، كما تمارس هذه العملية دون أي تدخل مباشر في النشاط الإجرامي القائم بل تقتصر على الرصد والمتابعة بهدف جمع المعلومات، هذا ما جاءت به المادة 25 من قانون الإجراءات الجزائية التي نصت على: "يمكن ضباط الشرطة القضائية، وتحت سلطتهم أعوان الشرطة القضائية، ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره، أن يمددوا عبر كامل الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه فيهم بارتكاب الجرائم المبينة في المادة 24 أعلاه، أو مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات من ارتكاب هذه الجرائم أو قد تستعمل في ارتكابها".²

نستنتج من المادة السابقة أن المراقبة يباشرها ضباط وأعوان الشرطة القضائية عبر كامل الإقليم الوطني، وهي تركز على البحث والتحري المباشر حول الأشخاص المشتبه بهم في ارتكابهم جنحة أو جنائية تتعلق بالجرائم الموصوفة بالخطيرة، حيث تأخذ هذه المراقبة صور وطرق مختلفة إما ملاحظة وراجلة، وفردية، أو تكون ثنائية عن طريق مراقبين اثنين، وإما باستعمال المركبات وهي ما يطلق عليها المراقبة الراكبة، أضف إلى ذلك المراقبة الثابتة التي تتم من خلال ملاحظة ثابتة قد تكون بناية أو محل مغلق أو سطح منزل.³ النوع الآخر من المراقبة سمي بمراقبة حركة الأموال والأشياء وعائدات الإجرام، والمراقبة لا بد من استعمالها بطريقة مشروعة وتكون مبنية على أسباب جدية دون الإساءة لاستعمال السلطة أو التعسف بها أو الانحراف حتى لا يكون رجال الشرطة القضائية أمام المساءلة التأديبية والجنائية.

الفرع الثالث: المعاينة والخبرة.

تشكل المعاينة والخبرة الإلكترونية اليتين أساسيتين تدعمان فعالية البحث والتحقيق في الجرائم الإلكترونية، باعتبارهما من أهم الإجراءات التي تساعد في كشف الأدلة الرقمية، سنوضح كلاهما في هذا الفرع.

أولاً: المعاينة.

¹ رايح لهوي، المرجع السابق، ص 122.

² الأمر 155-66 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 14-25.

³ محمد شنه، المرجع السابق، ص 106.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

بمجرد إخطار جهات الضبط القضائي بموجب شكوى أو بلاغ، يتوجب عليهم الانتقال الفوري إلى مسرح الجريمة لمباشرة المعاينات اللازمة للآثار المادية مع توثيق حالة الأماكن والأشخاص، واستيفاء كافة الاستدلالات التي من شأنها كشف الملابس وتحديد هوية الجاني.

في هذا السياق تعرف المعاينة أنها: "الإجراء الذي يتضمن وصف مكان الحادث بما فيه من أشياء وأشخاص والفحص الدقيق لكافة المحتويات بهدف مخلفات الجاني بالمكان، والتي تشير إلى شخصيته وشركائه وما قد يفيد في إثبات ارتكاب الجريمة وتوضيح قدر من الاستنتاجات المنطقية، تشكل في حد ذاتها الأساس الذي تقام عليه عملية التحقيق والبحث".¹

مسرح الجريمة قد يكون مسرح تقليدي يقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية قد يترك الجاني آثار عدة كال بصمات وغيرها، وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه.²

من ناحية أخرى هناك مسرح سيبراني يقع داخل بيئة الحاسوب ويتكون من البيانات الرقمية التي تتواجد وتنتقل داخل بيئة الحاسوب وشبكاته، في ذاكرته وفي الأقراص الصلبة الموجودة بداخله، والتعامل مع الأدلة الموجودة في هذا المسرح يجب أن لا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع.³

استنادا إلى ما سبق تنصب المعاينة في الجرائم المعلوماتية على المكونات المادية وذلك بالانتقال إلى مسرح الجريمة والتحفظ على أجهزة الحاسب الآلي ومستلزماته وملحقاته من وسائل اتصال بالشبكة العنكبوتية كالطابعة، جهاز الماسح الضوئي، وجميع الأشياء التي من الممكن أن تكون أدلة إلكترونية كشرائط الفيديو الرقمية Dvd، Cd، Flash Disque، ويتطلب ذلك سرعة الانتقال إلى محل الجريمة للمحافظة على آثار الجريمة قبل العبث بمضمونها أو إتلافها أو التخلص منها، كما تنصب المعاينة على المكونات المعنوية والتي

¹ كاهنة آيت حمودة، البحث والتحري الجنائي في مسرح الجريمة الإلكترونية، مجلة الفكر القانوني والسياسي، جامعة عمار ثلجي، الأغواط، المجلد 7، ع 1، 15 ماي 2023، ص 186.

² رابح لهوي، المرجع السابق، ص 169.

³ المرجع نفسه، ص 170.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

تتمثل في البرامج والبيانات الموجودة في جهاز الحاسب الآلي،¹ وعليه تكون المعاينة حسب طبيعة الجريمة الإلكترونية المرتكبة، إذا كانت واقعة على المكونات المادية يكون الانتقال مادي إلى مسرح الجريمة، وإذا كانت الجريمة واقعة على مكونات غير مادية يكون الانتقال افتراضي أو إلكتروني.

بناء على ما تم عرضه، المشرع الجزائري لم يضع تعريفا دقيقا لمفهوم المعاينة، غير أن قانون الإجراءات الجزائية قد اشار إليها بوصفها إجراء من الإجراءات التي تباشرها مختلف السلطات التحقيقية على اختلاف فئاتها واختصاصاتها، حيث تعتبر المعاينة إجراء جوهري لإثبات الجرائم وجمع الأدلة لاسيما في مواد التلبس والتفتيش، هناك المادة 78 من قانون الإجراءات الجزائية التي نصت على: "لا يجوز البدء في تفتيش المساكن معاينتها قبل الساعة الخامسة (5) صباحا ولا بعد الساعة الثامنة (8) مساء..."²

إضافة إلى المادة 81 منه التي منحت لضباط الشرطة القضائية الحق في الإستعانة بأهل الخبرة أو المعانين المختصين لضمان دقة المعاينات، وتنسيقا بين المادتين وتحليلهما استنتجنا أن المشرع الجزائري لم يفصل المعاينة العادية عن المعاينة الإلكترونية، بمعنى بالرغم أن المواد تعالج الجريمة التقليدية فإنه يمكن تطبيقها على الجريمة الإلكترونية. ويتعين على ضباط الشرطة القضائية الالتزام بجملة من القواعد والإرشادات الفنية عند معاينة مسرح الجريمة الإلكترونية، إذ تشكل هذه الإجراءات إطارا منهجيا يهدف إلى سلامة الأدلة الرقمية والحفاظ على حجيتها القانونية، وعليه يجب مراعاة الضوابط التالية:

- عند العثور على حاسبات آلية وأجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها، وتدوين الحالة التي هي عليها إذا كانت غير شغالة أو في حالة تشغيل أو موصولة بالكهرباء أو بجهاز لاحق آخر، كما ينبغي ترقيم لواحقها بشكل متسلسل.³
- ينبغي عدم وقف تشغيل الحاسوب حرصا على عدم فقدان الاتصال وفي ذلك الوقت ينبغي التنبيه إلى احتمال تعرض الحاسوب أو البرامج المشغلة له لأية عمليات تخريبية بواسطة فيروسات أو برمجيات خبيثة

¹ رجاء أومدور، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريش، 2021/2020، ص ص 154، 155.

² الأمر 155-66 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 14-25.

³ زينب جيهان بوعجاجة، دنيا زاد درابلي، الإجراءات المستحدثة للتحقيق في الجرائم الإلكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريش، 2023/2022، ص 29.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

عندها ينبغي فصله عن شبكة الأنترنت وفي بعض الحالات يفضل فصل الطاقة الكهربائية عنه على الفور حفاظا على ما تبقى على الجهاز من معطيات ومعلومات.¹

- جمع المعدات والتجهيزات المكتبية وخاصة الإلكترونية منها والتي يمكن أن تكون قد استعملت في عمليات الحفظ أو التخزين أو النسخ أو المسح الضوئي والكاميرات وأجهزة الفاكس.²
- إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية والعلمية.
- إعداد خطة المعاينة، موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.
- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يتمكن إجراء عمليات التحليل.³

ثانيا: الخبرة.

الخبرة هي عبارة عن إجراء من إجراءات التحقيق أو وسيلة تحدد التفسير الفني للأدلة الإلكترونية بالاستعانة بالمعلومات العلمية، وهي في الواقع ليست دليلا مستقلا عن الدليل المادي، وإنما هي تقييم فني لهذا الدليل حيث أن الأدلة قد تكون غير مرتبة ويلزم تحويلها إلى أدلة مقروءة، وقد يكون تلاعب في حسابات معينة أو نظم إلكترونية معينة، يحث الكشف عنها إلى مختصين لإثبات هذا التلاعب وقد يحتاج الأمر إلى عمليات فنية دقيقة للتمكن من الدخول إلى الأنظمة المعلوماتية والإلكترونية نتيجة استخدام تقنيات التشفير والتأمين المتطور التي يصعب فكها.⁴

في هذا السياق كون الجرائم الإلكترونية مرتبطة بمسائل فنية وعلمية بحثية، لا بد على القائم بالتحقيق الاستعانة بالخبراء والمختصين لأن تصدي المحقق لفحص شيء وإبداء الرأي فيه دون أن تتوفر لديه المعرفة اللازمة يجعل قراره معيبا يضر بمصلحة التحقيق ويعيق الوصول إلى الحقيقة، وكل هذا يصب في أهمية التقارير التي ينجزها خبراء تقنية المعلومات في مجال الجرائم الإلكترونية ويعطيها مكانة متميزة من حيث الإلزام.⁵

¹ حسين طاهري، المرجع السابق، ص 398.

² المرجع نفسه، ص 399.

³ كاهنة آيت حمودة، المرجع السابق، ص 187.

⁴ حسين طاهري، المرجع السابق، ص ص 381، 382..

⁵ جاسم محمد جندل، الجرائم الإلكترونية، الطبعة الأولى، دار المعتر للنشر والتوزيع، الأردن، 2022/1443، ص 200.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

وقد اهتم المشرع الجزائري بالاستعانة بالخبراء لجهات التحقيق، وأجاز للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم، هذا ما جاءت به المادة 239 من قانون الإجراءات الجزائية التي نصت على: "لجهات التحقيق أو الحكم، عندما تعرض عليها مسألة ذات طابع فني، أن تأمر بئدب خبير تلقائيا أو بناء على طلب النيابة العامة أو من الخصوم أو محامهم..."¹

نظرا لخصوصية هذا النوع من الجرائم يتم الاستعانة بخبير مختص يتمتع بكفاءة علمية ومهنية عالية، إضافة إلى امتلاكه مهارات متقدمة وقدرة تقنية على التحكم في مجال الإعلام الآلي.

تبعاً لذلك الاستعانة بخبير لها أهمية في مجال الجرائم الإلكترونية تظهر عند غيابه، فقد تعجز الشرطة عن كشف غموض الجريمة وقد تعجز هي أو جهة التحقيق عن جمع الأدلة حول الجريمة، وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه.²

كما أن اختيار الخبير في الجرائم الإلكترونية يتوقف على نوع الجريمة المرتكبة ومجال الخبرة المطلوبة وطبيعتها الفنية، فلا يكفي حصول الخبير على درجة علمية معينة وإنما ينبغي أن تكون لديه خبرة علمية تخصصية وكفاءة فنية عالية في حقل أو أكثر من حقول تقنية المعلومات ونظمها ووسائلها.³

ينقسم الخبراء إلى نوعين، في الطائفة الأولى ضباط الشرطة القضائية الذين يعملون في مجال المعمل الجنائي والأدلة الجنائية، يقتضي تخصصهم تلقيهم وتدريبهم تدريباً خاصاً ودراسة بعض العلوم كالكيمياء والطبيعة والهندسة والتصوير، وذلك لمعاونتهم في التحليل العلمي في مجال التخصص فحص الأسلحة النارية وللكشف عن التزوير والتزييف، أما الطائفة الثانية هم الخبراء من خريجي الكليات العلمية كالطب والهندسة والعلوم ويتم تدريب هؤلاء وتلقيتهم بعض المواد القانونية والشرطية بما يتفق واحتياجاتهم في مجال الفحص.⁴

بالرجوع للقانون فقد ذكر المشرع كيفية اختيار الخبراء في نص المادة 240 من قانون الإجراءات الجزائية والمادة 241 منه، والشروط المتعلقة بالخبرة الإلكترونية كالآتي:

¹ الأمر 155-66 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 14-25.

² علي عبد الفتاح، مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل، الطبعة الثانية، مكتبة الوفاء القانونية، الإسكندرية، 2024، ص 302.

³ جاسم محمد جندل، المرجع السابق، ص 200.

⁴ مختار تابري، الخبرة في الجريمة المعلوماتية، مجلة الحوار المتوسمي، جامعة الجليلي اليابس، سيدي بلعباس، المجلد 11، ع 3، 17 جانفي 2021، ص 384.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

- الإحاطة بتركيب الحاسب وصناعته وطراره ونظم تشغيله الرقمية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور أو السر أو كود التشفير.
- طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز وتوزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.
- قدرة الخبير على اتقان مهمته دون أن يترتب على ذلك تدمير للأدلة المتحصلة من الوسائل الإلكترونية.
- التمكن من نقل أدلة الإثبات غير المرتبة وتحويلها إلى أدلة مقروءة أو المحافظة على دعائها لحين القيام بأعمال الخبرة بغير أن تلحقها تدمير أو إتلاف مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائها.¹

المطلب الثاني: الإجراءات المستحدثة للكشف عن الجريمة الإلكترونية.

نظرا لخصوصية الجريمة الإلكترونية وتعقدها التقني لم تعد الوسائل التقليدية كافية للتصدي لهذا النوع من الجرائم، الأمر الذي نتج بروز مجموعة من الإجراءات المستحدثة التي تعتمد أساسا على التكنولوجيا المتقدمة، وعليه قمنا بتقسيم هذا المطلب إلى أربعة فروع حيث خصصنا كل فرع لدراسة إجراء معين، فقد تضمن الفرع الأول اعتراض المراسلات وتسجيل الأصوات والنقاط الصور، الفرع الثاني فيه التسرب الإلكتروني، الفرع الثالث خصصناه للتفتيش الإلكتروني، أما المراقبة الإلكترونية والحجز داخل المنظومة المعلوماتية درسناه في الفرع الرابع.

الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والنقاط الصور.

في إطار البحث والتحري تعتمد السلطات المختصة على بعض الوسائل التقنية الحديثة من بينها اعتراض المراسلات والنقاط الصور وتسجيل الأصوات، والتي لم يقدم المشرع الجزائري تعريفا لها وإنما اكتفى بوضع تنظيم لهته العملية، وذلك من خلال تخصيص الفصل الرابع في قانون الإجراءات الجزائية تحت عنوان " في اعتراض المراسلات وتسجيل الأصوات والنقاط الصور " لاسيما المواد من 114 إلى 119 منه، أضيف إلى هذا القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

أولاً: تعريف اعتراض المراسلات.

¹حسين طاهري، المرجع السابق، ص ص 382، 383.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

هي عملية مراقبة سرية للمراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في الجريمة، وتتم المراقبة عن طريق اعتراض أو تسجيل أو نسخ للمراسلات والتي هي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الانتقال أو العرض.¹

وبالرجوع إلى القانون 04-09 فقد ذكر مصطلحات تخص الجريمة الإلكترونية، وهذا في المادة 2 منه التي نصت على: "...الاتصالات الإلكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية."²

ثانيا: شروط اعتراض المراسلات.

أحاط المشرع عملية اعتراض المراسلات بشروط وضوابط قانونية سنوضحها كالآتي:

1. الشروط المطلوبة في المراسلات محل الاعتراض: يشترط في المراسلات التي يمكن أن تكون محلا لإجراء الاعتراض أو المراقبة أن تتسم بالسرية والخصوصية، ولا شك أن ذلك لا يتحقق إلا في ظل توافر عنصرين هما:

- فحوى الرسالة والتي تنصب على معلومات أو أفكار سرية أو شخصية.

- تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون المراسلة.

مع الإشارة أن المشرع الجزائري لم يبنى إجراء مراقبة الاتصالات الإلكترونية كإجراء للتحقيق القضائي وكذلك التحري بموجب القانون 04-09، بل أعطى تصريح للجهات القضائية باستعمال الاعتراض بهدف الوقاية من بعض الجرائم التي تشكل خطرا على الدولة.

وإتماما لهذا الهدف تم استحداث الهيئة الوطنية الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والتي أوكل لها القانون مهمة تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مع السلطات القضائية، وذلك من خلال المادة 13 من القانون 04-09.³

¹ محمد شنه، المرجع السابق، ص 108.

² القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر، ع 47، 2009.

³ نوال مجدوب، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والسياسية، المركز الجامعي الشريف بو شوشة أفلو، الأغواط، المجلد 6، ع 1، 28 جانفي 2023، ص 203.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

2. الشروط القانونية لاعتراض المراسلات:

تتمثل هذه الشروط في:

- الأمر بالاعتراض لا بد أن يكون إذن مكتوب صادر من سلطة قضائية مختصة ، أي من طرف وكيل الجمهورية بمرحلة التحقيق الابتدائي، أو من طرف قاضي التحقيق بمرحلة التحقيق القضائي تحت طائلة بطلان الإجراء القضائي، ولا شك أن اشتراط الإذن هو إجراء حتمي من منطلق أسلوب اعتراض المراسلات السلكية واللاسلكية يتم دون علم المعنيين¹، وهذا ما جاءت به المادة 117 من قانون الإجراءات الجزائية التي حددت الأشخاص المكلفين بالجوانب التقنية للعمليات المذكورة في المادة 114 منه.
- تحديد نوع الجرائم محل الاعتراض حيث لا تتم هذه العملية إلا على الجنايات والجناح الخطيرة، ذكرتها المادة 114 الفقرة 1 من قانون الإجراءات الجزائية على سبيل الحصر من بينها الجرائم المتصلة بتكنولوجيا الإعلام والاتصال...
- التسبب أي تبيان دواعي اللجوء إلى الاعتراض ومراقبة المراسلات، وتبيان مدى تلك الدواعي ودورها في إظهار الجريمة والجناة²، بمعنى يجب أن يكون الاعتراض مسببا ويحدد فيه الشخص المستهدف ونوع المراسلات وكذا المدة الزمنية.
- تحديد المدة الزمنية للأمر بالاعتراض، حسب المادة 116 الفقرة 2 من قانون الإجراءات الجزائية التي نصت على: "يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد ضمن نفس الشروط الشكلية والزمنية إلى غاية انتهاء مقتضيات التحري أو التحقيق القضائي".³

الفرع الثاني: التسرب الإلكتروني.

لم يقتصر تدخل المشرع الجزائي في مواجهة صعوبة الكشف المبكر عن الجريمة الإلكترونية على إقرار مشروعية مراقبة الاتصالات الإلكترونية، بل تجاوز ذلك إلى تمكين ضباط الشرطة القضائية من استعمال أساليب أكثر تطورا، من بينها جواز التسلل إلى داخل الجماعات الإجرامية وانتحال صفات إعضائها، وهو الأسلوب الذي يعرف قانونا بالتسرب، سنقوم بدراسته في هذا الفرع.

أولا: تعريف التسرب الإلكتروني.

¹ المرجع نفسه، ص 203.

² المرجع نفسه، ص 204.

³ الأمر 155-66 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 14-25.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

تعد الجريمة الإلكترونية أو ما سميت بالجريمة الماسة بأنظمة المعالجة الآلية للمعطيات من الجرائم التي إجاز فيها المشرع الاعتماد على إجراء التسرب من أجل التحري فيها، إذ عرف هذا الإجراء في نص المادة 121 من قانون الإجراءات الجزائية على أنه: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جنائية أو جنحة بإيهامهم انه فاعل معهم أو شريك لهم أو خاف".¹

إذن التسرب هو تلك العملية المحضر لها مسبقا، تهدف إلى التوغل داخل شبكة إجرامية لمعرفة نشاطاتها والكشف عن الأشخاص المتورطين فيها، سواء كان هؤلاء الأشخاص فاعلين أصليين أو شركاء، وذلك عبر تعبئة مختلف الإمكانيات البشرية والتقنية اللازمة.²

ثانيا: شروط القيام بعملية التسرب الإلكتروني.

للقيام بعملية التسرب وجب توافر جملة من الشروط نذكرها كمايلي:

- الإذن: يجب أن يصدر الإذن من وكيل الجمهورية قبل بداية التحقيق ومن قاضي التحقيق بعد افتتاحه، وهذا ما أكدته المادة 120 من قانون الإجراءات الجزائية.³
 - تضمين الإذن القضائي جملة من البيانات: بمعنى يجب أن يرد الإذن مكتوبا تحت طائلة البطلان، ومتضمنا لبيانات تحدد صحته، كتيبان نوع الجريمة ومحلها، هوية الضابط المتسرب.⁴
- وهذا طبقا للمادة 124 من قانون الإجراءات الجزائية التي نصت على: "يجب أن يكون الإذن المسلم تطبيقا للمادة 120 أعلاه، مكتوبا ومسببا، البطلان.

تذكر في الإذن، الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته.⁵

¹ الأمر 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 25-14.

² عبد المطلب طاهري، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2014/2015، ص 22.

³ انظر المادة 120 من قانون الإجراءات الجزائية.

⁴ نسيم قادري، عن أساليب التحقيق الخاصة المتعلقة بالجريمة الإلكترونية ذات البعد الاقتصادي: أية فعالية؟، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية، المجلد 12، ع 3، جانفي 2022، ص 647.

⁵ الأمر 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 25-14.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

- تسبب الإذن القضائي المرخص لعملية التسرب: لا يصح الإذن بالتسرب الإلكتروني إلا بتضمينه مبررات وتفسيرات توضح دوافع اللجوء لهذه العملية.
- تقييد عملية التسرب بفترة زمنية: المدة المحددة لهذا الإجراء هي 4 أشهر قابلة للتجديد، يجوز للقاضي الذي رخص بها أن يأمر بوقفها في أي وقت قبل انقضاء المدة، وللمتسرب مواصلة النشاط هنا للوقت الضروري الكافي لتوقيف العملية في ظروف تضمن أمنه دون مسؤوليته جزائياً، بشرط ألا تتجاوز 4 أشهر، كما يمكن تمديد المدة لمدة 4 أشهر أخرى إذا لم يتمكن العون المتسرب من إنهاء نشاطه في ظروف تضمن أمنه¹، وقد ذكرت هذه المدة في المادة 124 من قانون الإجراءات الجزائية.²

ثالثاً: إجراءات التسرب الإلكتروني

إن عملية التسرب في نطاق الجريمة الإلكترونية تتمثل في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي، وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو اشتراكه في محادثات غرف الدردشة والظهور بمظهر كما لو كان فاعلاً مثلهم، مستخدماً أسماء أو صفات وهمية بهدف الحصول على معلومات هامة تفيد التحقيق.³

في هذا الإطار وبتوافر الشروط سالفة الذكر يباشر عضو الضبط القضائي مهامه وتنفيذ مهامه في إطار إرائي محكم، حيث أن مباشرتها تكون باسم مستعار ولا يجوز إظهار الهوية الحقيقية للضابط أو المتسرب في أي مرحلة من مراحل الإجراءات، ويعاقب كل من يكشف عن هويته⁴، وقد أكدت على ذلك المادة 125 من قانون الإجراءات الجزائية⁵ التي جاء في مضمونها عدم الكشف عن الهوية الحقيقية ومعاقبة كل من قام بذلك. وقد خول المشرع لضباط أو أعوان الشرطة القضائية إمكانية الاستعانة بجملة من الوسائل والقيام ببعض الأفعال المنصوص عليها في المادة 123 من القانون 14-25، وذلك دون أن تترتب عليهم أية مسؤولية جزائية، وتتمثل هذه الأفعال أو الوسائل في:

¹ رجاء أومدور، المرجع السابق، ص 178، 179.

² انظر المادة 124 من قانون الإجراءات الجزائية.

³ عبد المطلب طاهري، المرجع السابق، ص 23.

⁴ رجاء أومدور، المرجع السابق، ص 179.

⁵ انظر المادة 125 من قانون الإجراءات الجزائية.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

- اقتناء أو إجازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائقي أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

الفرع الثالث: التفتيش الإلكتروني.

في إطار مواكبة التطور التكنولوجي وما أفرزه من أنماط إجرامية مستحدثة، اتخذ المشرع مجموعة من الإجراءات في مجال البحث والتحري من بينها التفتيش، حيث لم يعد هذا الأخير مقتصرًا على الأماكن المادية بل امتد ليشمل الأجهزة والأنظمة المعلوماتية، وهذا لجمع الأدلة الرقمية والكشف عن الجرائم المرتكبة عبر الفضاء الإلكتروني، سنعرفه أكثر في هذا الفرع.

أولاً: تعريف التفتيش الإلكتروني.

التفتيش بوجه عام هو إجراء قضائي يهدف إلى الحصول على أدلة تساعد في كشف الحقيقة، ويتميز بخاصتي الجبر والإكراه، أي أن الإنسان يخضع له مجبراً إذا لم يوافق على إجرائه برضاه، ويتضمن هذا الإجراء مساساً بمستودع سر الإنسان سواء كان مسكناً أو في جسمه، وهو إجراء يهدف إلى جمع الأدلة التي تساهم في كشف الحقيقة.¹

أما ما يتعلق بالتفتيش في الجريمة الإلكترونية فيقصد به تفتيش النظم المعلوماتية ولو عن بعد من خلال جمع الأدلة المخزنة أو المسجلة بشكل إلكتروني كالملفات والبرامج المخزنة في الحواسيب والمعدات والاتصالات الإلكترونية سواء كانت معطيات ذات طابع مادي أو معنوي تفيد كدليل إلكتروني في الكشف عن الحقيقة²، إضافة إلى ما سبق أقر المشرع الجزائري في إطار أحكام قانون الإجراءات الجزائية صلاحيات للسلطات الضبطية وضباط الشرطة القضائية تخول لهم لأغراض التفتيش، اللوج إلى المنظومات المعلوماتية أو إلى أي جزء منها، فضلاً عن المعطيات المعلوماتية المخزنة بداخلها وكذلك إلى منظومات تخزين المعلومات، وهذا ما قد جاءت به المادة 5 من القانون 04-09³ في الجزء الخاص بتفتيش المنظومة المعلوماتية.

¹ رجاء أومور، المرجع السابق، ص 137.

² ليندة بومحراث، إجراءات التحقيق الخاصة بالجرائم السيبرانية، مداخلة ضمن فعاليات اليوم الدراسي: حول الجريمة السيبرانية، كلية الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، المنعقد في 20 أبريل 2022، ص 14.

³ انظر المادة 5 من القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

ثانيا: مدى إمكانية إجراء التفتيش في الجرائم الإلكترونية.

إن التفتيش لا يعد غاية في حد ذاته وإنما يمثل وسيلة تهدف إلى تحقيق غاية محددة، تكمن في البحث عن دليل يتصل بجريمة سبق وقوعها، وتضطلع أجهزة الشرطة بدور محوري وأساسي في هذا الإطار، لاسيما عند تكليفها بتنفيذ إجراءات التفتيش من قبل سلطات التحري، سواء في الحالات الإستثنائية أو في حالة التلبس بالجريمة، في سياق مباشرة هذا الإجراء، ويتعين التمييز بين حالتين أساسيتين:

الغرض الأول: تفتيش العناصر المادية للحاسوب.

يحتوي الحاسب الآلي على مجموعة من المكونات المادية المتمثلة في الوحدات المختلفة (وحدات الإدخال كلوحة المفاتيح والماسح الضوئي والميكروفون، وحدات الإخراج كالشاشة والطابعة والسماعات)، حيث يدخل في نطاق التفتيش التقليدي وفقا لقانون الإجراءات الجزائية، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات والمتمثلة أساسا في:

- إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات¹، وقد ورد التفتيش في قانون الإجراءات الجزائية بالضبط في القسم الثالث تحت عنوان " في الانتقال والتفتيش والضبط " لا سيما في المادة 155 وما يليها من هذا القانون.

- إذا كانت مكونات الكمبيوتر منعزلة عن غيرها من أجهزته أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في نظام آخر فإن عملية الكشف تصبح صعبة جدا وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى يتعين مراعاة القيود والضمانات التي أوجبها المشرع الجزائري على التفتيش داخل النظم المعلوماتية والتي تضمنها قانون الإجراءات الجزائية.²

بناء على ما تم عرضه، خلصنا أن هناك أماكن ذات صبغة خاصة تكون خاضعة لحماية مشددة فلا يجوز مباشرتها إلا باستيفاء كافة الضمانات الإجرائية والموضوعية المقررة قانونا في قواعد التفتيش التقليدي،

¹ محمد رزيق، إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة ألكلي محمد أولحاج، لبويرة، 2018/2019، ص 16.

² محمد رزيق، المرجع السابق، ص 16.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

أما بالنسبة للأماكن العامة يتقيد التفتيش فيها بذات الضوابط والقيود النازمة لتفتيش الأشخاص، مع مراعاة التوازن بين مقتضيات التحقيق والحريات الشخصية.

الغرض الثاني: التفتيش الماس بالمكونات المعنوية.

في هذه الحالة قد أثار جدل فقهي كبير حول صلاحية المكونات المعنوية لأن تكون محلا للتفتيش باعتبار البيانات الإلكترونية أو البرامج في ذاتها تقتدر إلى مظهر ملموس، وقد انقسم الفقه إلى فريقين: وفي هذا الصدد ذهب اتجاه بالقول بصلاحية هذه المكونات لأن تكون محلا للتفتيش كونها تتناسب مع الهدف من التفتيش وهو ضبط الأدلة للكشف عن الجريمة، وحجتهم في ذلك أنه وإن كانت برامج الحاسوب عبارة عن بصمات أو ذبذبات إلكترونية متواجدة أو موجات كهرومغناطيسية إلا أنها قابلة للتسجيل والتخزين والتحميل وبالتالي يجوز تفتيشها.¹

هناك من يرى أن المكونات المعنوية تخضع للتفتيش مثلها مثل المكونات المادية، وعلة ذلك أن القوانين الإجرائية عندما تمنح سلطات التحقيق إمكانية ضبط أي شيء يكون ضروريا لجمع الأدلة فإن ذلك يجب تفسيره ليشمل ضبط البيانات المخزنة أو المعالجة إلكترونيا، كما يشمل بيانات الحاسب الآلي غير المحسوسة.² أما عن موقف المشرع الجزائري فقد اتضح من خلال القانون 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إذ نص صراحة على تفتيش أنظمة الحاسب الآلي من خلال نص المادة 5 منه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول بغرض التفتيش ولو عن بعد إلى: - منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها. - منظومة تخزين معلوماتية."³ أضف إلى هذا الفقرة 3 من نفس المادة في حالة تخزين المعلومات خارج الإقليم الوطني حيث نصت على: "إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية."⁴

¹ كاهنة آيت حمودة، المرجع السابق، ص 188.

² رجاء أومرود، المرجع السابق، ص 139.

³ القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، سبق ذكره.

⁴ القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، سبق ذكره.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

وعليه يمكننا القول أنه بغض النظر عن نطاق التفتيش، سواء تعلق بالمكونات المادية أو المعنوية في هذا المجال، فإنه يظل خاضعا لجملة من الضوابط والإجراءات القانونية التي تنظم ممارساته، سنوضح أكثر هذه الأخيرة في العنصر القادم.

ثالثا: ضوابط التفتيش الإلكتروني.

للقيام بعملية التفتيش داخل المنظومة المعلوماتية وجب توفر جملة من الضوابط أو الشروط حتى يكون التفتيش صحيح من الناحية القانونية، تنقسم هذه الأخيرة إلى نوعين ضوابط موضوعية وأخرى شكلية.

1. الضوابط الموضوعية:

تتخصر في مايلي:

- وقوع جريمة إلكترونية: علمنا أن التفتيش الإلكتروني هو أحد إجراءات الاستدلال لهذا فإنه يشترط لقيام جهات التحقيق بهذا الإجراء وقوع جريمة إلكترونية بالفعل، سواء كانت تلك الجريمة جنائية أو جنحة، ذلك لأن التفتيش يكون بعد وقوع الجريمة وليس قبلها، لهذا لا يحق لجهات التحقيق القيام بهذا الإجراء قبل وقوع الجريمة لأن القيام بهذا الإجراء مرتبط بوقوع الجريمة الإلكترونية¹، ومنه رأينا أنه لقيام التفتيش لا بد من وجود جريمة باعتباره لا يجرى بدون سبب قانوني.
- محل التفتيش: يقصد به بشكل عام مستودع سر الإنسان، وهذا المستودع إما أن يكون في محل له حرمة خاصة كالمسكن أو قد يكون الشخص أو رسائله هذا بالنسبة للجرائم التقليدية، أما بالنسبة للجرائم الماسة بأنظمة الاتصال والمعلوماتية فمحل التفتيش هو الحاسب الآلي²، بمكوناته المادية والمعنوية وكذا شبكات الاتصال الخاصة به.
- هدف التفتيش: بمعنى أن يكون الغرض منه ضبط شيء تتعلق بالجريمة الإلكترونية التي وقعت، أي جمع الأدلة وكشف الحقيقة عن مرتكب الجريمة، لهذا لا بد أن يكون السبب في التفتيش هو تحقيق

¹ سعاد راضي حسين، الإجراءات الجزائية في تفتيش محل الجرائم الإلكترونية، مجلة الشرق الأوسط للدراسات القانونية والفقهية، جامعة الأردن المجلد 4، ع 4، 2024، ص 134.

² عز الدين عثمان، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية، مجلة دائرة البحوث ودراسات القانونية والسياسية، المركز الجامعي مرسل عبد الله، تيبازة، المجلد 2، ع 4، 29 جانفي 2018، ص 58.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

ذلك الغرض وإلا يقع باطلا إذا كان التفتيش لأي غرض آخر بخلاف ضبط الأدلة التي تتعلق بالجريمة.¹

- السلطة المختصة بالتفتيش: باعتبار التفتيش إجراء من إجراءات التحقيق الابتدائي التي تمس حقوق وحريات الافراد، حرص المشرع على إسنادها لجهة قضائية تكفل تلك الحقوق والحريات، وتتمثل هذه الجهة القضائية في قاضي التحقيق أو النيابة العامة باختلاف التشريعات كسلطة أصلية، أو استثناء في رجال الضبط القضائي²، وبالرجوع للمادة 155 من قانون الإجراءات الجزائية³ الجهة المختصة بالتفتيش قاضي التحقيق ويمكنه الاستعانة بأمين الضبط، سواء في التفتيش التقليدي أو الإلكتروني.
- الإذن بالتفتيش: لم ينص المشرع في المادة 5 من قانون 04/09 صراحة على وجوب استصدار إذن بتفتيش نظم معلوماتية من طرف ضباط الشرطة القضائية في حالة التحريات المتعلقة بالجرائم المتلبس بها أو في حالة التحريات الأولية، بالرجوع إلى الفقرة 5 من المادة سابقة الذكر نصت على: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية..." فقد نصت أن قيام ضباط الشرطة القضائية لتفتيش نظم المعلوماتية يكون بناء على قواعد قانون الإجراءات الجزائية⁴، إذ يتعين عليهم الانتقال إلى مساكن الأشخاص المشتبه في ممارستهم الجريمة أو حيازتهم لأشياء ذات صلة بالفعل الإجرامي، ألا يباشر التفتيش إلا بناء على إذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق، كما يجب على الضابط إظهار الإذن قبل الدخول إلى المسكن والشروع في التفتيش ضمانا لاحترام حرمة المساكن وحماية للحقوق الفردية.

2. الضوابط الشكلية:

تخص الإجراءات الواجب احترامها عند القيام بتفتيش الأجهزة أو الأنظمة الرقمية حتى يكون التفتيش قانونيا وصحيا.

¹سعاد راضي حسين، المرجع نفسه، ص 135.

² عز الدين عثمانى، المرجع نفسه، ص 59.

³انظر المادة 155 من قانون الإجراءات الجزائية.

⁴ مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04/09، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2013/2012، ص 90.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

- وقت إجراء التفتيش: حدد المشرع في قانون الإجراءات الجزائية الإطار الزمني لهذا الإجراء، حيث حصره في الفترة الممتدة من الخامسة صباحا إلى الثامنة مساء، هذا ما جاءت به المادة 78 منه " لا يجوز البدء في تفتيش المساكن أو معابنتها قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساء...¹"، غير أنه في حالات استثنائية يجوز الخروج عن تلك القاعدة فعندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والبعض من أنواع الجرائم الأخرى، فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص، وعليه يتبين أن المشرع الجزائري أجاز إجراء التفتيش في أي وقت من أوقات النهار والليل في جرائم معينة حددها المشرع ومن بينها الجرائم المتعلقة بالمعالجة الآلية للمعطيات.²
- حضور الأشخاص المعنيين أثناء التفتيش: عند تفتيش الأشخاص لم تشترط التشريعات الجزائية حضور شهود عند تفتيشهم، أما فيما يتعلق بتفتيش المساكن ينص القانون على وجوب حصول إجراء التفتيش المتعلق بالمساكن وملحقاتها بحضور المشتبه فيه أو المتهم عندما يتم تفتيش مسكنه سواء من طرف قاضي التحقيق أو ضابط الشرطة القضائية³، وحال تعذر تنفيذ ذلك بسبب امتناع المعني بالأمر عن حضور عملية التفتيش أو لكونه في حالة فرار، يباشر هذا الإجراء بحضور شاهدين لا يخضعان لسلطة القائم بعملية التفتيش.
- غير أن المشرع الجزائري استثنى هذه القواعد في نص المادة 76 الفقرة الأخيرة من قانون الإجراءات الجزائية⁴، حيث استغنى عن ضمانات الأشخاص في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الإلكتروني خاصة وأن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه.⁵

¹ الأمر 155-66 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 14-25.

² عز الدين عثمانى، المرجع السابق، ص 57.

³ ليندة بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمه لخضر، الوادي، المجلد 8، ع 2،

1 جوان 2017، ص 493.

⁴ انظر المادة 76 من قانون الإجراءات الجزائية.

⁵ ليندة بن طالب، المرجع نفسه، ص 493.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

- محضر التفتيش: باعتبار أن التفتيش من أعمال التحقيق، لا بد من تحرير محضر يثبت فيه ما أسفر التفتيش عنه من أدلة، والقانون لم يتطلب شكلا خاصا، وبالتالي لصحة محضر تفتيش نظم الحاسوب لا يشترط سوى ما تستوجبه القواعد العامة في المحاضر عموما، بأن يكون مكتوبا باللغة الرسمية وأن يكون مؤرخا وموقعا عليه، كما يجب أن يتضمن كافة الإجراءات المتبعة من طرف الشخص المتخصص في الحاسوب والأنترنت الذي تم الاستعانة به في مجال الخبرة الفنية الضرورية.¹

الفرع الرابع: المراقبة الإلكترونية والحجز داخل المنظومة المعلوماتية.

سنفصل المراقبة الإلكترونية عن الحجز داخل المنظومة المعلوماتية، وندرس كل واحدة على حدى.

أولا: المراقبة الإلكترونية.

استحدث هذا الإجراء بموجب القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

1. تعريفها:

عند البحث والدراسة نجد أن المشرع الجزائري لم يتصد لضبط تعريف المراقبة الإلكترونية لا في مواد قانون الإجراءات الجزائية ولا في مواد القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وإنما ترك ذلك للفقهاء حيث عرفها البعض على أنها: "إجراء يعتمد فيه الإنصات والتسجيل ومحلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة أي سواء كانت مما يتبادلها الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية واللاسلكية."²

تبعا لذلك يمكن القول أن المراقبة الإلكترونية عملية رصد منهجي لشبكات الاتصالات أو نشاط تقني يقوم به مختصون باستخدام وسائل إلكترونية متقدمة بهدف جمع بيانات متعلقة بمشتبه فيه في إطار زمني محدد، كما أن هذه المراقبة غالبا ما تنصب على المراسلات الإلكترونية بمختلف أنواعها أو البرنامج الذي تمت بواسطته، على سبيل المثال برنامج الفيسبوك، الماسنجر، الفاير وغيرهم...

¹ المرجع نفسه، ص 494.

² عبد الحليم بن بادة، المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني بين الحق في الخصوصية ومشروعية الدليل الإلكتروني، مجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية المجلد 10، ع 3، 31 ديسمبر 2019، ص 390.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

2. حالات اللجوء إلى إجراء المراقبة الإلكترونية:

جاء في الفصل الثاني الموسوم ب مراقبة الاتصالات الإلكترونية في نص المادة 4 من القانون 04-09¹

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية لأغراض وقائية وهي:

- في حال جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، ويمنح إذن المراقبة في هذا المجال النائب العام لدى مجلس قضاء الجزائر لمدة ستة (6) أشهر قابلة للتجديد.
- في حال الإعتداءات على المنظومات المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو المصالح الإستراتيجية للإقتصاد الوطني، وهنا يمنح إذن المراقبة من طرف السلطة القضائية المختصة

كما أورد المشرع حالات أخرى يلجأ فيها إلى المراقبة الإلكترونية وهي:

- في حال صعوبة الوصول إلى نتيجة من دون المراقبة الإلكترونية عند إجراء التحريات والتحقيقات القضائية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

3. شروط المراقبة الإلكترونية:

المراقبة الإلكترونية وباعتبارها وسيلة إجرائية في مجال الجريمة السيبرانية، قيدها المشرع الجزائري بمجموعة من الشروط تم استنتاجها مما ورد من أحكام في المادة 4 من القانون 04-09 وتتمثل في:

- أن يتم تنفيذ هذا الإجراء تحت سلطة القضاء.
- الحصول على الإذن من الهيئات المختصة بذلك.
- أن تكون هناك ضرورة تتطلب هذا الإجراء.
- توفر عناصر نجاح العملية، وذلك عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري أو التحقيق دون اللجوء إلى المراقبة الإلكترونية.²

ثانيا: الحجز داخل المنظومة المعلوماتية.

¹ انظر المادة 4 من القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

² ليندة بومحراث، المرجع السابق، ص 20.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

المشرع الجزائري تناول القواعد الخاصة بضبط البيانات المعلوماتية وفقا للقانون 09-04 تحت تسمية " حجز المعطيات المعلوماتية "، سنوضح إجراء الحجز في هذا الجزء من الدراسة.

1. التعريف:

ذكر الحجز في نص المادة 6 من القانون 09-04 التي تنص على أنه: " عندما تكتشف السلطة التي تبشر التفتيش في المنظومة المعلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبها، وأنه ليس من الضروري حجز كل منظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية.¹" يعرف الحجز بأنه العثور على الأدلة الخاصة بالجريمة التي تبشر التحقيق بشأنها وحفظ هاته الأدلة، والضبط هو الغاية من التفتيش والنتيجة المباشرة المستهدفة، ولذلك عند إجرائه أن تتوفر فيه القواعد نفسها التي تنطبق بشأن التفتيش ويؤدي بطلان التفتيش إلى بطلان الضبط.²

2. وظيفة الحجز في الجريمة الإلكترونية:

للحجز وظيفتين سنتناولهم على النحو التالي:

- الوظيفة الأولى: جمع أدلة الإثبات وفحص البيانات الرقمية، وتعد أول خطوة في عملية التحقيق الجنائي، وهي تحديد مصدر الدليل الرقمي المتوقع حتى يتم الحصول عليه بصورة رقمية توطئة لفحصه وتحليله، فمصادرة البيانات تختلف قد تكون أقراص صلبة، ذاكرات عشوائية، أقراص خارجية...
- الوظيفة الثانية: مصادرة المعطيات ومثال ذلك نسخ المعطيات النسخة الأصلية غير قابلة للدخول إليها، أو عن طريق استرجاعها كلية، كما أن الحجز لا يؤدي بالضرورة إلى مسح أو حذف المعطيات بصفة نهائية.³

3. الشروط القانونية لإجراء الحجز الإلكتروني.

¹ القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، سبق ذكره.

² عبد القادر فلاح، **حجز وحفظ المعطيات في الجريمة الإلكترونية**، مجلة صوت القانون، جامعة الجبالي بونعامة، خميس مليانة، المجلد 8، ع 1، 20 نوفمبر 2021، ص 180.

³ عبد القادر فلاح، المرجع السابق، ص 181.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

على نهج المشرع الفرنسي تبنى المشرع الجزائري في القانون 09-04 السالف ذكره إجراءات مستحدثة بضبط وحجز المعطيات والبيانات المعلوماتية وغيرها من الأدلة الرقمية بما يناسب وطبيعتها اللامادية، حيث خصص مجموعة من المواد شكلت الشروط القانونية لهذا الإجراء، تتمثل في:

- حجز المعطيات والبيانات الآلية: حيث يشمل على الأشياء المادية وعلى البيانات المعالجة إلكترونياً، أما بالنسبة لتحديد محل الحجز فقد تحجز كل معطيات المخزنة المفيدة في الكشف عن الجرائم أو مرتكبيها، واستثناء يتم الحجز الجزئي أي اكتفاء بالمحتوى الذي يتعلق بالمجرم.
- الحجز عن طريق منع وصول المعطيات: وهذا خوفاً من ضياع أو إتلاف الأدلة الرقمية حيث أعط القانون للسلطات المعنية قيام بهذا الإجراء، هذا ما نصت عليه المادة 7 من القانون 09-04، كما نلاحظ من خلال المادة 9 أن المشرع الجزائري حصر حالات اللجوء إلى الحجز عن طريق منع الوصول في الحالة الواحدة، كما نصت المادة 8 من نفس القانون على التحفظ على البيانات محل الجريمة أو أدواتها.
- وضع حدود لاستعمال المعطيات بمقتضى ما جاءت به المادة 9 من القانون السالف الذكر، كما أنه إثر أي عملية تفتيش أو معاينة إيجابية يتم استخراج نسخ من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق، وتبقى المحجوزات تحت تصرفها إلى أن تنتهي المحاكمة.¹
- أضف إلى هذا يمكن أن يحجز جزء من المنظومة فقط، وذلك باعتماد مجموعة من الإجراءات حسب ما يفهم من نص المادة 6 من القانون 09-04 سالف الذكر وتتمثل في:
- نسخ المعطيات على دعامة تخزين إلكترونية تكون قابلة للحجز (سواء المعطيات محل البحث أو المعطيات اللازمة لفهم المعطيات محل البحث.)
- الوضع في احرار وفقاً لما هو مقرر في قانون الإجراءات الجزائية.
- السهر على سلامة المعطيات في المنظومة المعلوماتية.
- امكانية استعمال وسائل تقنية لتشكيل أو إعادة تشكيل المعطيات لتكون قابلة للاستغلال لأغراض التحقيق بشرط عدم المساس بمحتوى المعطيات.²

¹ عبد القادر فلاح، المرجع السابق، ص 181.

² رجاء أومرود، المرجع السابق، ص 150، 151.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

4. العوائق والعراقيل التي تواجه حيز الأدلة الإلكترونية.

- توجد العديد من الصعوبات التي تواجه تعطيل عملية ضبط الأدلة التقنية الإلكترونية، والتي من أهمها:
- الطبيعة الغير مرئية والمختلطة للدليل الرقمي وذلك أنه يكون على شكل مجالات أو نبضات مغناطيسية أو كهربائية، لا يستطيع الرجل العادي إدراكها فهي موجودة في العالم الافتراضي، وعليه فإنه يوجد فرق بينه وبين الجليل التقليدي الذي يعتمد على آثار مثل الشعر، البصمات، الدماء...
- صعوبة تحديد مكان تواجد الحاسب الآلي مصدر النشاط الإجرامي لذلك تستعين سلطات التحقيق بنظام الفحص الإلكتروني يسمى بعلم البصمات المعاص، الذي يتم من خلال تتبع الحركة العكسية لمسار الأنترنت إلى غاية الوصول إلى العنوان الرقمي للجهاز.
- سهولة محو الدليل أو تدميره في وقت وجيز جدا من طرف الجاني، بحيث لا تتمكن السلطات من التحقيق عن الجريمة، ومثال ذلك نجد ما قام به أحد مهربي الأسلحة بالنمسا بإدخال التعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه في تخزين عناوين عملائه والمتعاملين معه، وعليه بمجرد الدخول أو نسخ هذه البيانات يتم إلتفافها في نفس اللحظة تماما.

المطلب الثالث: التنظيم القانوني للشرطة القضائية.

تعد الشرطة القضائية أحد أهم الأجهزة المكلفة بالبحث والتحري عن الجرائم وجمع الأدلة، حيث تلعب دورا محوريا في الكشف عن الجرائم التقليدية والحديثة على حد سواء، غير أن خصوصية الجريمة الإلكترونية تستدعي توافر كفاءات متخصصة وإجراءات ملائمة لفعاليات البحث والتحري.

سنحاول من خلال هذا المطلب دراسة التنظيم القانوني للشرطة القضائية من خلال التطرق إلى الضبطية القضائية التي تتولى البحث والتحري في مجال مكافحة الجرائم الإلكترونية، ثم بيان اختصاصات الشرطة القضائية في هذا المجال.

الفرع الأول: الضبطية القضائية المختصة في البحث والتحري عن الجريمة الإلكترونية.

نظرا للطابع الخاص الذي تتميز به الجريمة الإلكترونية، أصبح من الضروري توفير كادر بشرية مؤهلة وتجهيزات تقنية متخصصة تعنى بعمليات البحث والتحري في هذا النوع من الجرائم، سنحاول في هذا الفرع دراسة الأجهزة الأمنية المكلفة بالبحث والتحري عن الجرائم الإلكترونية وكذا الهيئات القضائية.

¹ عبد القادر فلاح، المرجع السابق، ص 182.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

أولا: الأجهزة المكلفة بالبحث والتحري عن الجرائم الإلكترونية.

1. الضبطية القضائية:

تعد الضبطية القضائية الجهة المختصة اختصاصا أصيلا بالنظر في مختلف الجرائم، بما في ذلك الجريمة الإلكترونية وقد أقر لها المشرع جملة من أساليب التحري المستحدثة، والتي سيتم عرضها وبيانها فيما يلي:

أ- على مستوى جهاز الأمن الوطني (الشرطة): تتولى المديرية العامة للأمن الوطني مهمة التحقيق في الجرائم الإلكترونية من خلال قسمين متخصصين، حيث يشمل القسم الأول المخابر والقسم الثاني الفرق، سنوضحهم على النحو التالي:

المخابر: يوجد مخبر مركزي للشرطة القضائية بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة ووهران تحتوي على فروع تقنية من بينها خلية الإعلام الآلي وفرق متخصصة مهمتها التحقيق والكشف عن جرائم الأنترنت، بالإضافة إلى ثلاث مخابر على مستوى بشار، ورقلة، وتمنراست قيد الإنجاز لأجل تعميم هذا النشاط على كافة ربوع الوطن.

كما يضم المخبر الجهوي للشرطة العلمية على مستوى قسنطينة ووهران مخبرا خاصا يتولى مهمة التحقيق في الجريمة الإلكترونية تحت اسم " دائرة الأدلة الرقمية والآثار التكنولوجية " تضم ثلاث أقسام:

- قسم استغلال الرقمية الناجمة عن الحواسيب والشيكات.

- قسم استغلال الأدلة الناجمة عن الهواتف النقالة.

- قسم تحليل الأصوات، وذلك بالاستعانة بأجهزة مادية للكشف عن الجرائم الإلكترونية.¹

وجود فرقة على مستوى كل ولاية: في سبيل ضمان فعالية التحقيق في مواجهة الجرائم المعلوماتية تم إنشاء ما يعرف بالمصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وهي مصلحة تابعة لمديرية الشرطة القضائية مقرها على مستوى الجزائر العاصمة، ثم أشأت خلايا تابعة للفرق الاقتصادية والمالية على مستوى كل أمن الولايات، تشمل خلية مكافحة الجرائم المعلوماتية، ثم مع تطور الجرائم واعتماد Modem

¹ عبد فلاح، نادية آيت عبد المالك، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجبالي بونعامة، خميس مليانة، المجلد 4، العدد 2، 2019، ص 1695.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

و3G تم ترقية الخلية لتصبح فرقة في حد ذاتها، حيث أصبحت مستقلة وتابعة للفرق الولائية للشرطة القضائية، وتوجد فرق على مستوى كل ولاية.¹

ب- على مستوى جهاز الدرك الوطني: تعمل مؤسسة الدرك الوطني على مكافحة الجريمة الإلكترونية بواسطة المعهد الوطني للأدلة الجنائية وعلم الإجرام، الكائن مقره في بوشاوي التابع لقيادة الدرك العامة قسم الإعلام والإلكترونيك الذي يختص بالتحقيق والكشف عن الجرائم الإلكترونية، وأيضا بواسطة مديرية الأمن العمومي والاستغلال والمصلحة المركزية للتحريات الجنائية، وهي هيئة ذات اختصاص وطني مهمتها التصدي للجريمة الإلكترونية.²

كما توجد أجهزة أخرى على مستوى الدرك الوطني نذكر منها: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني، مديرية الأمن العمومي والاستغلال، المصلحة المركزية للتحريات الجنائية، إضافة إلى كل فصائل الأبحاث التابعة للدرك الوطني والمكلفة بالتحقيق في الجرائم المعلوماتية.³

2. مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية:

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية عن طريق المرسوم الرئاسي رقم 15-261 ومقره بئر مراد رايس، وهو تابع لمديرية الأمن للدرك الوطني.⁴

ثانيا: الهيئات المكلفة بالبحث والتحري عن الجرائم الإلكترونية.

هناك هيئات تقنية تدعم العمل الأمني، سنقوم بدراستها في هذا الجزء على النحو التالي.

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

في نصوص المرسوم الرئاسي حسب أحكام المواد من 1 إلى 4 منه تعرف الهيئة بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر

¹ رجاء أومرود، المرجع السابق، ص 104.

² عبد القادر فلاح، نادية آيت عبد المالك، المرجع نفسه، ص 1696.

³ سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوة منتوري، قسنطينة 1، المجلد 30، ع 3، ديسمبر 2019، ص 54.

⁴ عبد القادر فلاح، نادية آيت عبد المالك، المرجع السابق، ص 96.16

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

العاصمة، تتولى الهيئة المهام المنصوص عليها في المادة 14 من القانون 09-04 وذلك تحت رقابة السلطة القضائية وطبقا لأحكام قانون الإجراءات الجزائية.¹

وردت مهام هذه الهيئة على سبيل الحصر في الفقرة 2 من المادة 4 من المرسوم الرئاسي 15-261، من أبرزها اقتراح العناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصالو مكافحته، تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المعلوماتية، تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مسارها من أجل استعمالها في الإجراءات القضائية، مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية...²

بخصوص تنظيم الهيئة أشارت المادة 4 من المرسوم الرئاسي 19/172 أنها تتشكل من مجلسين، مجلس توجيه ومديرية عامة، مجلس التوجيه يرأسه وزير الدفاع أو ممثله، كما تشير المادة المذكورة إلى أن الهيئة تتشكل من الوزارات التالية: وزارة الدفاع الوطني، الوزارة المكلفة بالداخلية، وزارة العدل، الوزارة المكلفة بالمراسلات السلوكية واللاسلكية.³

2. المعهد الوطني للأدلة الجنائية وعلم الإجرام:

يتكون هذا المعهد من إحدى عشر دائرة متخصصة في مجالات مختلفة، جميعها تتضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، ومن بين هذه الدوائر توجد دائرة الإعلام الإلكتروني، التي تتولى معالجة وتحليل وتقديم كل دليل رقمي يسعد العدالة، كما تقدم المساعدة التقنية للمحققين في المعايينات.⁴

3. الهيئات القضائية الجزائية المتخصصة:

أسفر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000، والذي ركز على ثلاثة محاور أساسية تتمثل في تعزيز حقوق الإنسان وتيسير حق اللجوء إلى القضاء، وإعادة الاعتبار لمنظومة التكوين والتأهيل، عن إحداث تحولات جوهرية في قطاع العدالة وقد جسدت هذه الإصلاحات من خلال مراجعة

¹ حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، 2015/2016، ص 172.

² المرجع نفسه، ص 172، 173.

³ حنان مهداوي، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، جامعة عمار ثلجي، الأغواط، المجلد 6، ع 2، 2 نوفمبر 2022، ص 1073.

⁴ المرجع نفسه، ص 1073.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

واستحداث جملة من النصوص القانونية بما ينسجم مع الالتزامات الدولية للجزائر، إلى جانب تحسين نوعية خدمات المرفق القضائي.

وفي هذا الإطار، أكدت توصيات لجنة إصلاح العدالة على ضرورة تعديل القانون الجزائي بشقيه الموضوعي والإجرائي، بما يمكن من مواجهة المظاهر الإجرامية الخطيرة وعلى رأسها تنامي الجريمة المنظمة وتزايد مخاطر استخدام تكنولوجيا المعلومات على أمن الأفراد وخصوصيتهم.¹

من أجل كل هذا عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص اقليمي موسع بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل الحصر وتوصف أنها خطيرة وعلى درجة عالية من التعقيد والتنظيم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.²

و لقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية المرسوم 348-06 المؤرخ في 5-10-2006 المعدل والمتمم بالمسوم 16-267، حيث جاء التقسيم كمايلي:

- محكمة سيدي أحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية: الجزائر، الشلف، الأغواط، البليدة، تيزي وزو، الجلفة، المدية، المسيلة بومرداس.
- محكمة قسنطينة يمتد اختصاصها للمجالس القضائية: قسنطينة، أم البواقي، باتنة، بجاية، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعرييج، طارف، خنشلة، سوق أهراس، ميلة.
- محكمة ورقلة: مجلس ورقلة، أدرار، تامنرست، إيليزي، بسكرة، الوادي، غرداية.
- محكمة وهران: مجلس وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تموشنت، غليزان.³

الفرع الثاني: اختصاص الشرطة القضائية في مجال البحث الجريمة الإلكترونية.

تعد الضبطية القضائية الركيزة الأساسية في منظومة العدالة، إذ خول لها القانون ممارسة مهام محددة وفقا لما تقتضيه النصوص القانونية، من خلال تعيين الأشخاص المخول لهم صلاحية البحث والتحري عن الجرائم،

¹ سعيدة بوزنون، المرجع السابق، ص 54.

² سعيدة بوزنون، المرجع السابق، ص 54.

³ المرجع نفسه، ص ص 54، 55.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

وجمع الأدلة اللازمة لكشف مرتكبيها وتقديمهم للعدالة، وتمارس هذه الهيئة مهامها وصلاحياتها في حدود دوائر الاختصاص، وعليه من خلال هذا الفرع سنتطرق الى

أولاً: الاختصاص الإقليمي.

يقصدُ بالاختصاص الإقليمي محيط الدائرة الإقليمية التي يباشر فيها ضباط وأعوان الشرطة القضائية اختصاصهم وصلاحياتهم المخول لهم قانوناً.

ويحدد مدى هذا الاختصاص ونطاقه بحسب صفة عضو الشرطة القضائية. وكذلك حسب الهيئة التي ينتمون إليها وبحسب نوع الجريمة موضوع البحث والتحري، فقد يكون اختصاص محلي أو وطني.¹

1. الاختصاص المحلي للشرطة القضائية في الجريمة الإلكترونية.

أ- تعريف الاختصاص المحلي:

يعرف الاختصاص المحلي بأنه ذلك النطاق الإقليمي أو الدائرة الجغرافية التي تباشر ضمنها الشرطة القضائية مهامها في مجال البحث والتحري عن الجرائم، وقد كرس المشرع هذا المبدأ بموجب المادة 24 من قانون الإجراءات الجزائية²، "يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة إلا أنه يجوز لهم، في حالة الاستعجال، أن يباشرون مهمتهم في كافة دائرة اختصاص المجلس القضائي الملحقون به"³

ب- تمديد الاختصاص المحلي العادي لضباط الشرطة القضائية:

يوجد العديد من الاختصاصات التي تمارسها الشرطة القضائية في إطارها العادي تختلف عن مهامها الاستثنائية التي تُمارس في إطار التلبس أو استعمال أساليب التحري الخاصة، وسيوضح ذلك فيما يلي:

- تلقي الشكاوى والبلاغات الإلكترونية: تُعد الشكاوى تصرفاً قانونياً يصدر عن الشخص المتضرر أو من يمثله قانوناً، وتُقدم إما شفاهةً أو كتابةً إلى الجهات المختصة. أما البلاغ فيقصد به كل إخطار يُوجه إلى ضباط الشرطة القضائية من أي شخص، سواء كان المتضرر أو غيره، بقصد إعلامه بوقوع جريمة أو الاشتباه في حدوثها.

¹ عبد السلام شطيبي، محاضرات في مقياس قانون الإجراءات الجزائية، أقيمت على طلبة السنة الثانية ليسانس، كلية الحقوق والعلوم السياسية، جامعة عبد الحفيظ بوضوفة، ميلة، 2025/2026، ص 46

² عبد السلام شطيبي، محاضرات في مقياس قانون الإجراءات الجزائية، المرجع السابق، ص 46.

³ الأمر 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 25-14، سبق ذكره.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

• جمع الاستدلالات الإلكترونية: تنص المادة 26 من قانون الإجراءات الجزائية على أن: "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 20 و21 أعلا، ويلتقون الشكاوي والبلاغات بأي وسيلة، بما في ذلك الطريق الإلكتروني، ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية".¹ يمكن تعريف جمع الاستدلالات بأنها مجموعة الإجراءات التي تهدف إلى البحث والتحري عن الجرائم وجمع المعلومات والقرائن المتعلقة بها، بغية تمكين النيابة العامة من تكوين تصور واضح حول الوقائع. ولا ترمي هذه الإجراءات إلى الفصل في موضوع الدعوى أو تمكين اقتناع قضائي نهائي، إذ يظل ذلك من اختصاص قاضي التحقيق أو جهة الحكم.

كما أنه تشمل أعمال الاستدلال مختلف الوسائل التي تستخدم في الكشف عن الجرائم وجمع الأدلة، على اختلاف صورها، بقصد نسبتها إلى مرتكبيها، إلى جانب تلقي الشكاوي والبلاغات وتحرير المحاضر التي توثق كافة الإجراءات التي يباشرها ضباط الشرطة القضائية.

كما أن هاته الإجراءات تتم في إطار احترام مبدأ الشرعية الإجرائية. ومن بين أهم الإجراءات التي تندرج ضمن جمع الاستدلال نذكر، سماع أقوال الضحايا والمشتبه فيهم والشهود، ضبط الأشياء المتعلقة بالجريمة ووضعها تحت الحراسة...

• توقيف المشبه فيهم للنظر في الجريمة الإلكترونية: إذا قدر ضابط الشرطة القضائية ضرورة توقيف المشتبه فيه لمقتضيات التحقيق، تعين عليه إخطار وكيل الجمهورية، مع النقيذ بدة التوقيف التي لا تتجاوز 48 ساعة. كما يجب تمكين المشتبه فيه كم الاتصال بعائلته، مع مراعات ذات الضوابط القانونية المقررة في حالة التلبس.

• توجيه نداء للجمهور واستعمال وسائل الإعلام: وفقاً لأحكام المادة 24 من قانون الإجراءات الجزائية، يجوز لضباط الشرطة القضائية توجيه نداء للجمهور قصد الحصول على معلومات أو شهادات من شأنها المساهمة في سير التحريات. كما أنه يمكنهم وبناءً على إذن من وكيل الجمهورية المختص إقليمياً، اللجوء إلى وسائل الإعلام لنشر أوصاف أو صور لأشخاص محل بحث، بهدف تسهيل تعقبهم.

¹ الأمر 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 25-14، سبق ذكره.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

- تحرير المحاضر الإلكترونية: تُلزم المادة 27 من قانون الإجراءات الجزائية ضبط الشرطة القضائية بتحرير محاضر تثبت مختلف الأعمال والإجراءات التي يباشرها أثناء أداء مهامهم.¹
- ج- **تمديد الاختصاص المحلي الموسع:** يجوز توسيع الاختصاص الإقليمي لضباط الشرطة القضائية ليشمل دوائر قضائية خارج نطاق اختصاصهم الأصلي، بما في ذلك محاكم أخرى غير المحكمة التي يباشرون فيها ضمنها مهامهم، وذلك في الحالات التالية:
- يمكن تمديد الاختصاص المحلي ليشمل كامل دائرة اختصاص المجلس القضائي الذي يتبع له الضباط، لاسيما في الحالات الاستعجال، شريطة إخطار وكيل الجمهورية المختص، وذلك وفقاً لأحكام المادة 24 فقرة 3 من قانون الإجراءات الجزائية.
- كما يمكن، في حالات الاستعجال، توسيع الاختصاص ليشمل كامل التراب الوطني، بناءً على طلب من الجهات القضائية المختصة وبمساعدة ضباط الشرطة القضائية المختصين إقليمياً، مع وجوب إخطار وكلاء الجمهورية المختصين، طبقاً لإحكام نفس المادة سالفة الذكر.
- يجوز أيضاً تمديد الاختصاص إلى دائرة اختصاص محكمة أخرى موسعة إقليمياً، وذلك وفقاً لما نص عليه المرسوم التنفيذي رقم 348.06 المتعلق بالأقطاب الجزائية المتخصصة، وذلك استناداً إلى المواد 24 مكرر في جميع فقراتها.²

2. الاختصاص الوطني لضباط الشرطة القضائية في مجال مكافحة الجريمة الإلكترونية.

وسع قانون الإجراءات الجزائية اختصاص الشرطة القضائية بحسب الصفة الأصلية للمنتمي لجهاز الشرطة القضائية أو بحسب طبيعة الجريمة موضوع البحث.

وعليه إن اختصاص الضباط التابعين لمصالح الأمن العسكري يمتد على المستوى الوطني حيث تنص المادة 24 مكرر 6 من قانون الإجراءات الجزائية: "لا تطبق أحكام الفقرات الثانية والثالثة والرابعة والخامسة من هذه المادة على ضباط الشرطة القضائية للمصالح العسكرية للأمن أو للمصالح المركزية للشرطة القضائية، الذين لهم الاختصاص في كافة الإقليم الوطني".³

¹ عبد السلام شطبي، محاضرات في مقياس قانون الإجراءات الجزائية، المرجع السابق، ص 49، 50.

² المرسوم الرئاسي رقم 348-06، المؤرخ في 5 أكتوبر 2006، المتضمن تمديد الاختصاص القضائي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، ع 63، الصادر بتاريخ 8 أكتوبر 2006، ص 18.

³ الأمر 156-66 المتضمن قانون الإجراءات الجزائية المعدل بالقانون 14-25، سبق ذكره.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

عمل المشرع، بموجب أحكام المادة 24 مكرر 7 من نفس القانون، على توسيع الاختصاص الإقليمي لضباط الشرطة القضائية، بحيث يشمل فئات معينة من الجرائم دون التقيد بجهة انتمائهم الأصلية، سواء تعلق الأمر بالدرك الوطني أو الأمن الوطني أو مصالح الأمن العسكري، إذ يمتد هذا الاختصاص إلى كامل التراب الوطني،¹ حيث تنص المادة على: "غير أنه فيما يتعلق بجرائم القل العمدي، والمخدرات والمؤثرات العقلية، والجريمة المنظمة عبر الحدود الوطنية، والجرائم المتصلة بتكنو لوجيا الإعلام والاتصال وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، وجرائم الفساد و جرائم التهريب، وجرائم الاتجار بالبشر، و جرائم الاتجار بالأعضاء، وجرائم تهريب المهاجرين، وجرائم اختطاف الأشخاص، يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني".²

وفي هذا الإطار يتميز نشاط ضباط الأمن العسكري بخصوصية قانونية، بالنظر إلى اتصاله المباشر بالمصالح العليا للدولة وأمنها، وهو ما يضيف على الجرائم التي يباشرونها طابعاً وطنياً شاملاً من حيث الامتداد. وعليه، فإن اختصاصهم لا يخضع كأصل عام لقيود زمانية أو مكانية، بما يتلاءم وطبيعة المهام المسندة إليهم. كما تضيف المادة السابقة الذكر، أنه يجوز لضباط الشرطة القضائية وتحت إشراف أعوانهم مباشرة عمليات المراقبة عبر كامل التراب الوطني، متى لم يعترض وكيل الجمهورية المختص على ذلك بعد إخطاره، ويشترط لمباشرة هذه العمليات وجود مبرر جدي، يتمثل في قيام أسباب معقولة تدعو للإشتباه في تورط الأشخاص المعنيين في ارتكاب إحدى الجرائم المنصوص عليها في المادة 24 من ذات القانون. ويستفاد من هذا التنظيم أن المشرع الجزائري قد أقر جملة من الإجراءات الخاصة لمواجهة هذا النوع من الجرائم، لا سيما تلك التي تنسم بالخطورة والتعقيد، وذلك بهدف تعزيز فعالية التحري والتحكم فيها، بما يضمن تحقيق التوازن بين مقتضيات البحث عن الحقيقة و حماية الحقوق والحريات.³

¹ كمال بلارو، الشرطة القضائية في التشريع الجزائري، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق، قسم القانون الخاص، جامعة الإخوة منتوري قسنطينة 2، 2021/2020، ص 13.

² الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون 25-14، سبق ذكره.

³ كمال بلارو، الشرطة القضائية في التشريع الجزائري، المرجع السابق، ص 13.

المبحث الثاني: خصوصية الدليل الإلكتروني

يكتسي الدليل الرقمي أهمية متزايدة في المنظومة الجنائية المعاصرة، وذلك من خلال التطور التكنولوجي السريع وما أظهره من أنماط جديدة للإجرام تقتضي وسائل إثبات تتلاءم مع طبيعتها التقنية. حيث أن الدليل التقليدي أصبح غير كافٍ وحده للإحاطة بمختلف صور هاته الجرائم المستحدثة، الأمر الذي أذا إلى ظهور الدليل الإلكتروني باعتباره وسيلة حديثة للكشف عن الحقيقة وإثبات الوقائع الإجرامية. إلا أن هذا الدليل يمتاز بخصوصيات تميزه عن غيره من الأدلة، سواءً من حيث طبيعته الغير المادية، أو سهولة نسخه وتعديله ومحو آثاره، أو من حيث الوسائل الفنية والقانونية اللازمة لاستخراجه وحفظه وتحليله. وعليه سنقوم من خلال هذا المبحث بدراسة مفهوم الدليل الإلكتروني كمطلب أول وذلك بالتطرق إلى تعريفه وخصائصه، وايضا صعوبات وأشكال الدليل الإلكتروني كمطلب ثاني وذلك عن طريق ذكر صعوبات الدليل الإلكتروني وأيضاً أشكاله.

المطلب الأول: مفهوم الدليل الإلكتروني

تُعد عملية الإثبات الجنائي في العصر الحديث قائمةً بدرجة كبيرة على الدليل الإلكتروني، بوصفه الوسيلة الأكثر فاعلية في إثبات الجرائم المستحدثة، بل وبعض الجرائم التقليدية المعقدة. ويُشكل هذا النوع من الأدلة بوابةً أساسيةً تُمكن من الوصول إلى مختلف التفاصيل المرتبطة بالواقعة محل التحقيق. وعليه سنتناول تعريف الدليل الإلكتروني كفرع أول وخصائصه كفرع ثاني.

الفرع الأول: تعريف الدليل الإلكتروني

تتدرج عملية تحديد المفاهيم من الركائز الأساسية في بناء الإطار النظري لأي دراسة علمية، لما لها من دور محوري في ضبط موضوع البحث وتحديد حدوده. وفي هذا الإطار، ومن أجل الوصول إلى تعريف واضح ومتكامل للدليل الإلكتروني، يتعين تناول هذا المصطلح بالتحليل من خلال تفكيك عناصره الأساسية، وذلك عبر تعريف الدليل أولاً، ثم توضيح مفهوم إلكتروني ثانياً، تمهيداً لاستخلاص تعريف شامل للدليل الإلكتروني.

أولاً: تعريف الدليل

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

لتبيان معنى الدليل يجب توضيح اهم التعاريف اللغوية والاصطلاحية

يعرف الدليل لغة، بأنه: دَل، يَدُل، دلالة، والجمع أدلة وأدلاء. وهو المرشد¹، والدليل ما يستدل به وقد دله على الطريق أي أرشده، يدلّه بالضم، دلالة بفتح الدال وكسرها، ودلالة بالضم والفتح أعلى، ويقال أدل بالضم، والاسم الدال بالتشديد الدال، ويقال فلان يدل فلانا أي يثق به.

والدليل يطلق في اللغة على الرشد للمطلوب على معنى أنه فاعل الدلالة ومظهرها، فيكون معنى الدليل الدال "فعيل" بمعنى الفاعل كعليم وقدير، مأخوذ من دليل القوم، ولأنه يرشدهم إلى مقصدهم².

أما اصطلاحاً فيعرف، بأنه: لم تعرف التشريعات الجزائية الدليل لأنه ليس من وظائفها التعريف، غير أن قانون أسس الإجراء الجزائية السوفيتية قد عرف الأدلة بأنها: "المعلومات الحقيقية التي على ضوئها يحدد المحقق أو المحكمة طبقاً للطرق المقررة قانوناً توافر أو تخلف فعل الخطر اجتماعياً وتأثير ذلك الشخص الذي ارتكب الفعل".

وقد عرف قضاة المحكمة العليا في الدولة الجزائرية الدليل على أنه: "البينة أو الحجة التي يتخذ منها القاضي البرهان على اقتناعه بالحكم الذي يصدره، وقد يكون الدليل أما مباشراً كالاقرار، وشهادة الشهود، وتقدير الخبرة، أو غير مباشرة كالقرائن".

كما تطرق الفقه إلى تعريف مصطلح الدليل فعرفه الفقيه سوانسون (SWANSON) بأنه: "أي شيء يفيد في إثبات أو نفي مسألة عينة في القضية، أو كل ما يتصل اتصالاً مباشراً بإدانة متهم أو تبرئته استناداً إلى المنطق، ويجب التركيز على كلمة (أي شيء لأنه أي شيء بالمفهوم الواسع يمكن أن يكون دليل"³.

ثانياً: تعريف مصطلح إلكتروني

1. المعنى اللغوي للمصطلح:

بالرجع إلى المعاجم نجد العديد من التعريفات المتعلقة بمصطلح محل الدراسة.

¹ خليل الجر، المعجم العربي الحديث، مكتبة لاوس باريس، فرنسا، 1983، ص 450.

² أبي الفضل جمال الدين بن منظور الإفريقي، لسان العرب، المجلد 11، دار بيروت للطباعة والنشر، لبنان، 1955، ص 426.

³ صهيب سهيل غازي زامل، البحث والتحري عن الدليل الإلكتروني في المسائل الجزائية دراسة مقارنة، أطروحة دكتوراه في القانون الجنائي، جامعة وهران 2، وهران، 2021-2022، ص 14.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

تعريف الإلكترون: جسم دقيق جدا يحمل شحنة كهربائية سالبة، ويُعد جزءاً أساسياً من مكونات الدرة. كما يمثل وحدة من وحدات الطاقة المستخدمة في الفيزياء النووية، إذ تعبر طاقته عن الطاقة الحركية التي يكسبها عند حركته داخل المجال الكهربائي.

تعريف الإلكترون: كيان متناهي الصغر، يفوق في دقته كل ما قد تدركه العين المجردة، بل يتعذر رؤيته حتى باستخدام أقوى المجاهر. ويقدر صغره بدرجة هائلة، إذ أن تجمع مليارات منه لا يبلغ وزن ريشة خفيفة، حجمه لا يتجاوز في أقصاه حجم رأس الدبوس. وهو عبارة عن شحنات كهربائية دقيقة في حالة حركة مستمرة حول النواة، التي تعد بدورها جزءاً مركزياً من الدرة¹.

2. التعريف القانوني لمصطلح إلكتروني:

يُعد تحديد المفاهيم من القضايا التي لا يستهدف منها التعمق في التعريفات داخل النصوص التشريعية ومع ذلك فقد اتجهت غالبية التشريعات الجنائية العربية إلى وضع تعريف لمصطلح "الإلكتروني"، وذلك لما يحيط به من حادثة وغموض متجددين.

وفي هذا السياق، عرفه قانون سلطنة عمان رقم 69-2008 بشأن المعاملات الإلكترونية، في مادته الأولى، بأنه: أية وسيلة تتصل بالتقنية الحديثة وذات قدرات كهربائية، أو رقميو، أو مغناطسية، أو لاسلكية، أو كهرومغناطسية، أو ضوئية، أو أية قدرات مماثلة لذلك .

وفي سياق مغاير عرف القانون الاتحادي للدول العربية الموسوم بعنوان المعاملات والتجارة الإلكترونية مصطلح الإلكترون على أنه: ما يتصل بالتكنولوجيا الحديثة ويكون ذا قدرات كهربائية، أو رقمية، أو مغناطسية، أو لاسلكية أو بصرية، أو كهرومغناطسية أو مؤتمنة، أو ضوئية أو ما شابه ذلك².

ثالثاً: تعريف الدليل الإلكتروني

تنوعت التعاريف المتعلقة بالدليل الإلكتروني، وقد انقسمت هذه التعاريف بين التفسير الموسع وآخر مضيق له، ويرجع ذلك إلى موضوع العلم الذي ينتمي إليه الدليل.

1. تعريف الفقه الجنائي للدليل الإلكتروني

¹ نعمه أنطوان وآخرون، المنجد في اللغة العربية المعاصرة، الطبعة الثانية، دار النشر، بيروت، 2001، ص 37.

² صهيبي سهيل غازي زامل، المرجع السابق، ص 16.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

يعرف ممدوح عبد الحميد عبد المطلب ومحمد طارق عبد الرؤوف الخن الدليل الإلكتروني بأنه: بيانات أو ملفات في شكل رقمي تتعلق بدعوى مدنية أو جنائية، كما يعرف يعرفه فئة أخرى من الفقه بأنه: الدليل المأخوذ من أجهزة الحاسوب الآلي فيكون في شكل مجالات، أو نبضات مغناطيسية، أو كهربائية يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده امام القضاء. ذهب جانب آخر من الفقه ومن بينهم محمد الأمين البُشيري وعمر محمد بن يونس، إلى تعريف الدليل الإلكتروني على أنه: "مجموعة من المعلومات التي يقبلها العقل والمنطق ويُعتد بها علمياً، ويتم الحصول عليها وفق إجراءات علمية وقانونية، من خلال معالجة وترجمة البيانات الحاسوبية المخزنة في أنظمة الحاسوب وملحقاتها وشبكات الاتصال".

من جهة أخرى، يعرف مصطفى محمد موسى الدليل الإلكتروني بأنه: المعلومات المخزنة أو المنقولة بصيغة رقمية، والتي يُعتمد عليها في إجراءات التحقيق وأمام الجهات القضائية، سواء لإثبات الإدانة أو تقرير البراءة¹.

2. تعريف المنظمات الدولية للدليل الإلكتروني:

تعرف فرقة العمل المعنية بالدليل الرقمي SWGDE، بأنه: المعلومات أو البيانات ذات القيمة الثبوتية التي تخزن أو ترسل في شكل رقمي. وقد عرفت كذلك المنظمة الدولية لأدلة الحاسوب E.O.C. I في أكتوبر 2001 بأنه: المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية².

مما سبق يتبين لنا أن كل التعاريف بخصوص الدليل الإلكتروني متقاربة مع بعضها البعض، وأنها سعت لفهم هذا النوع الجديد من الأدلة المستحدثة.

مما سبق نخلص إلى أن الدليل الإلكتروني هو الدليل المتحصل عليه من معلومات مخزنة في نظام المعالجة الآلية وجميع ملحقاتها أو من خلال أي وسيلة إلكترونية أخرى. وذلك عن طريق اتخاذ إجراءات قانونية وفنية من قبل السلطات المختصة قانوناً لتقديمه للقضاء وذلك بعد تحليل معطياته وتفسيرها في أشكال وصور أخرى لإثبات وقوع الجريمة أو نفيها.

¹ صهيب سهيل غازي زامل المرجع السابق، ص ص 17، 18.

² محمد بن فردية، الدليل الجنائي الرقمي وحججه أمام القضاء الجزائي، دراسة مقارنة، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمن ميرة، بجاية، المجلد 9، ع 1، أكتوبر 2016، ص 73.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

الفرع الثاني: خصائص الدليل الإلكتروني

تتسم بيئة الدليل الإلكتروني بكونها قائمة على الرقمية، نتيجة ارتباطها بالمجال الافتراضي الذي تنشأ فيه، وبما أن مسرح الجريمة في هذا السياق ذو طبيعة إلكترونية، فإن ذلك يضيف على الدليل الإلكتروني جملة من الخصائص المميزة من أبرزها ما يأتي:

أولاً: دليل ذو طابع علمي.

يُقصد بالدليل هنا أنه يمثل معطيات ذات قيمة في الإثبات الجنائي، تكون مخزنة أو منقولة أو معالجة في صورة رقمية. وهذه المعطيات قادرة على الإسهام في كشف الجريمة، غير أن طبيعتها التقنية تحول دون إدراكها أو تحليلها إلا من خلال توظيف أساليب علمية وتقنية متخصصة.

ثانياً: دليل ذو طابع تقني.

نظراً للطبيعة التقنية للدليل الإلكتروني، فإنه يتميز بقابليته للاستتساخ، بحيث يمكن استخراج نسخ مطابقة للأصل دون أن تفقد قيمتها الإثباتية. وتعد هذه الخاصية ميزة لا تتوافر في الدليل المادي التقليدي كما تتيح إمكانية حفظه من التلف أو التغير أو الحذف بفعالية أكبر

ثالثاً: دليل سهل الإخفاء.

قد يقابل سهولة الحصول على الدليل الإلكتروني صعوبة في الاحتفاظ به، نظراً للتطور المستمر في تكنولوجيا المعلومات. فمرونة هذا النوع من الأدلة تجعله عرضة للفقْدان أو الإتلاف أو الإخفاء بسهولة.

كما يتميز الدليل الإلكتروني بطبيعته الديناميكية، إذ يمكن نقله بسرعة فائقة من مكان إلى آخر عبر شبكات الاتصال، دون التقيد بحدود الزمان والمكان¹

رابعاً: الدليل الرقمي متنوع ومتطور.

يُشير مفهوم الدليل الإلكتروني، بوصفه مفهوماً متطوراً ومتعدد الأبعاد، إلى مجموع البيانات والمعلومات التي يمكن تداولها وحفظها بصيغ وأشكال متنوعة. ويشمل ذلك الأدلة المرتبطة بالحاسوب الآلي أو غيره من الأجهزة الرقمية، فضلاً عن تلك المتولدة عبر شبكات الاتصال السلكية واللاسلكية، بما في ذلك شبكة الأنترنت.

¹ كاهنة آيت محمود، المرجع السابق، ص 184.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

وتتميز الآثار الرقمية المستخرجة من هذه الوسائط بثرائها وتنوعها، إذ قد تتضمن معطيات تكشف عن وقائع تشكل جريمة، ويمكن ان ترتقي إلى مستوى الدليل القاطع عن البراءة أو الإدانة. ومن بين هذه البيانات محتويات صفحات المواقع الإلكترونية، والبريد الإلكتروني، والنصوص، والصور، ومقاطع الفيديو الرقمية، إضافة إلى الملفات المخزنة على الحاسوب الشخصي، وغيرها من المعلومات المرتبطة باستخدام شبكة الإنترنت.

خامسا: الدليل الإلكتروني صعب التخلص منه.

تعد خاصية صعوبة التخلص من الدليل الإلكتروني من أبرز السمات التي تميزه، إذ لم يكن اعتباره قابلاً للإزالة بالسهولة التي تعرف بها الأدلة التقليدية. فبينما يمكن التخلص من الأدلة المادية، كالوثائق الورقية أو الأشرطة المسجلة، من خلال إتلافها أو حرقها، بل وحتى محو بصمات الأصابع، أو التأثير على الشهود بطرق مختلفة، فإن الأمر يختلف بالنسبة للدليل الإلكتروني.

ذلك أن عملية حذف الملفات الرقمية، سواء عبر الحاسوب أو شبكة الأنترنت، باستخدام أوامر مثل (ERASE, REMOVE, DELETE)، لا تعني زوالها بشكل نهائي. إذ تبقى هذه البيانات قابلة للاسترجاع من خلال برامج وتقنيات متخصصة، قادرة على إستعادة الملفات التي تم حذفها أو إلغاؤها من النظام.

ويترتب على هذه الخاصية آثار قانونية مهمة، حيث تثير مسألة التخلص من الدليل الإلكتروني إشكاليات خاصة. فإذا أثبت الخبير التقني أن قد استخدم وسائل أو برامج لإزالة الأدلة، فإن ذلك يُعد قرينة ضده، ويُسمهم في إدانته وفقاً للنصوص القانونية التي تُجرّم مثل هذه الأفعال، ومن ثم تبرز ضرورة تدعيم القواعد القانونية بنصوص أثر صرامة، تأخذ بعين الاعتبار الطبيعة الخاصة للأدلة الرقمية، والعلاقة القائمة بين محاولة إخفائها و القرائن المستمدة منها في البيئة الرقمية¹.

سادسا: الدليل الجنائي ذو طبيعة ثنائية.

يقصد بالطبيعة الثنائية للدليل الإلكتروني كونه لا يتجسد في شكل مادي موحد، وإنما يقوم على بنية تقنية مستمدة من نظم تكنولوجيا المعلومات، أساسها نظام الترميز الثنائي الذي يعتمد على تتابع غير محدود من الوحدات الرقمية المتمثلة الرقمين (0 و 1)، ورغم تماثل هذه الوحدات من حيث طبيعتها، فإن اختلاف أنماط ترتيبها وتكوينها هو الذي يُمكن من توليد مختلف أشكال البيانات والمعلومات.

¹ محمد الطيب حفيش، أمينة عابد، آليات البحث والتحري في الجريمة الإلكترونية، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسي، جامعة إليزي، 2024.2025، ص 74.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

وعليه فإن الدليل الإلكتروني لا يتخذ وجوداً مادياً محسوساً بالمعنى التقليدي، بل يتمثل في معطيات رقمية غير ملموسة، قوامها سلاسل من الإشارات الثنائية التي ترجع في أصلها إلى بنية رقمية واحدة. ويُفهم من ذلك أن كافة المخرجات داخل البيئة الرقمية إنما تنشأ عن معالجة هذه الوحدات الثنائية، التي تُعبر في حقيقتها عن إلكترونية متتابعة تستمد وظيفتها من تدفق الطاقة داخل الأنظمة المعلوماتية.

سابعاً: الدليل الرقمي عابر للحدود.

يتميز الدليل الرقمي بكونه عابر للحدود، إذ لا يشترط وجوده في نطاق جغرافي محدد على غرار الأدلة التقليدية، بل قد يتوزع في أكثر من موقع، سواء داخل إقليم الدولة الواحدة أو خارجه. ويُعزى ذلك لارتباطه بالبيئة الافتراضية التي تتجاوز بطبيعتها الحدود الإقليمية للدولة.

كما أن اعتماده على الشبكة المعلوماتية العالمية، باعتبارها وسيلة اتصال دولية لا تعترف بالقيود الجغرافية في تبادل البيانات والمعلومات، يجعل من انتقال الدليل الرقمي بين الدول أمراً يسيراً وسريعاً. الأمر الذي يطرح إشكالات قانونية تتعلق بالاختصاص القضائي، وتنازع القوانين وآليات التعاون الدولي في مجال جمع الأدلة الرقمية وحجبتها.¹

المطلب الثاني: صعوبات وأشكال الدليل الإلكتروني.

الدليل الإلكتروني وسيلة أساسية في الإثبات الجنائي، غير أن خصوصيته تثير عدة صعوبات قانونية وعملية تتعلق بجمعه وحفظه وتقديمه أما القضاء، كما تتنوع أشكال هذا الدليل بتنوع الوسائط الإلكترونية وهذا ما سنوضحه من خلال هذا المطلب.

الفرع الأول: الصعوبات المتعلقة بالدليل الإلكتروني

أولاً: الطبيعة غير المادية للدليل الإلكتروني.

يتميز الدليل الجنائي في الجرائم التقليدية بطابع مادي ملموس، يتيح للسلطات المختصة معاينة مسرح الجريمة وضبط الآثار التي تسهم في كشف ملابساتها. غير أن الأمر يختلف في الجرائم الإلكترونية، إذ تنشأ في بيئة رقمية مغايرة تماماً، حيث تتجسد الأدلة في شكل نبضات أو إشارات مغناطيسية وكهربائية، أو بيانات ومعلومات رقمية داخل الفضاء الافتراضي.

¹ صهيب سهيل غازي زامل، المرجع السابق، ص ص 21، 22.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

وبناءً على ذلك، فإن غياب الطابع المادي للدليل الرقمي يطرح تحديات كبيرة أمام المحققين، سواء من حيث اكتشافه أو جمعه أو تحليله، مما يستلزم توافر خبرات تقنية متخصصة وكفاءة عالية للتعامل مع هذا النوع المستحدث من الأدلة.

ثانياً: سهولة تدمير ومحو الدليل الإلكتروني.

يُعد تدمير ومحو الأدلة الإلكترونية من أبرز التحديات التي تعترض عملية استخلاص الدليل الرقمي، نظراً لما تتسم به هذه العملية من سهولة وسرعة في التنفيذ. فمرتكبو الجرائم الإلكترونية غالباً ما يتمتعون بقدر عالٍ من الذكاء والمهارة التقنية، مما يمكنهم من إتلاف أو تعديل الأدلة في وقت وجيز. وعليه، فإن الدليل الإلكتروني يكون عرضة للمحو أو التلاعب بطرق غير مرئية داخل أنظمة الحاسوب ومكوناتها، الأمر الذي يزيد من صعوبة اكتشافه والمحافظة عليه، ويُعقد من مهمة الجهات المختصة في تتبعه وإثباته¹.

ثالثاً: ضخامة البيانات المتعين فحصها.

فلعلهُ من أكبر التحديات والعراقيل التي تواجه سلطات التحقيق ورجال الضبط لاستخلاص الدليل الإلكتروني، وهو ذلك الكم الكبير والوفير للمعلومات والبيانات المراد فحصها وتحليلها، لذلك يتوجب على المحقق أن تتوفر لديه في مجال الحاسب الآلي وملحقاته القدرة على هذا الكم الهائل من المعلومات والبيانات المخزنة في جهاز الحاسب الآلي أو في دوائر التخزين الرقمي².

الفرع الثاني: أشكال الدليل الإلكتروني

يتخذ الدليل الإلكتروني أو ما يعرف بالدليل الرقمي أشكالاً يجب عليها معرفتها من أجل تسهيل مهمة فرق البحث وتمكينها من الوصول إلى معلومات ذات كفاءة أثناء عملية التفتيش، سنوضحهم كالتالي:

- الأقراص المرنة والأقراص الصلبة، هي من أهم الأدلة لأنها تحتوي على البيانات وعلى المعلومات، كلمات المرور، الصور، التقارير، وعلى خطط ارتكاب الجريمة مثلاً وغير ذلك

¹ مسعود خطوي، خصوصية الدليل الإلكتروني، مجلة الفكر القانوني والسياسي، جامعة عمار ثلجي، الأغواط، المجلد 7، ع 1، 2022، ص 6.

² خلود فراحتية، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، تخصص قانون الإعلام آلي وأنترنيت، جامعة محمد البشير الإبراهيمي، برج بوعرييج، 2021/2022، ص 34.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

- أشرطة تخزين المعلومات التي تستخدم عادة لحفظ النسخ الاحتياطية، إضافة إلى أدلة ورقية على سبيل المثال مخرجات الطباعة والتقارير والرسوم البيانية.
- أجهزة الحاسبات الآلية وتتضمن معها ملحقات الحاسب من شاشات وغير ذلك.
- أجهزة المودم والتي تستخدم في نقل المعلومات، ويمتاز بعضها بإمكانية العمل كجهاز الرد على رسائل الهاتف answer machine ما يجعله دليل محتمل بالغ الأهمية، وعند العثور على مودم يجب الاهتمام بتسجيل الكابلات المتصلة به عند ضبطه، وكيف كانت متصلة بالحاسب أو الهاتف مع النقاط وتسجيل رقم الهاتف¹.
- القطع الإلكترونية التي يمكن أن تكون أدلة

المطلب الثالث: دراسة حالة حول جنحة عرض إعلان مغل بالحياة عن طريق شبكة التواصل الاجتماعي (التعليق على حكم قضائي جزائي).

أفرز التطور التكنولوجي الحديث أنماط جديدة من الجرائم، من بينها الجرائم المرتكبة عبر مواقع التواصل الاجتماعي، والتي تطرح إشكالات قانونية خاصة تتعلق بإثبات الجريمة وتحديد هوية مرتكبها بالاعتماد على الدليل الإلكتروني.

ويعد الحكم محل الدراسة نموذجا قضائيا يبرز كيفية تعامل القضاء الجزائري مع جريمة عرض إعلان مغل بالحياة عبر الفضاء الرقمي باعتبارها من الجرائم الماسة بالآداب العامة، وكذا مدى كفاية الأدلة التقنية لإسناد الفعل الإجرامي إلى المتهم في إطار احترام قواعد الإثبات ومبدأ قرينة البراءة.

في هذا الصدد قضية الحال تم الفصل فيها على مستوى المحكمة الابتدائية -قسم الجنج- بتاريخ 2026/4/18، التي كانت النيابة العامة طرفا فيها ممثلة للحق العام ضد المتهم، حيث تخلص الوقائع في قيام المتهم بالترويج لأفكار الشذوذ الجنسي والتحريض على فساد الأخلاق وممارسة الرذيلة بنشر صور وعبارات مخلة بالحياة، وهذا عبر مواقع التواصل الاجتماعي (فيسبوك) حيث تم الرصد لهذا الحساب الإلكتروني من طرف فرقة مكافحة الجرائم السيبرانية، وانطلاقا مما سبق يطرح القاضي من خلال الوقائع تساؤلا قانونيا يتمثل

¹ خلود فرحاتية، المرجع السابق، ص 35.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

في كيف فعل القضاء الجزائي نتائج إجراءات البحث والتحري عن الجريمة الإلكترونية الممثلة في جنة عرض إعلان مغل بالحياء.¹

كما أن أهمية الموضوع تبرز في التوازن بين حرية التعبير وطريقة نشر الإعلان من جهة، وحماية الآداب العامة وفق أحكام قانون العقوبات من جهة أخرى ومدى أهمية الدليل الإلكتروني في الوصول إلى الحقيقة.

الفرع الأول: أركان جريمة عرض إعلان مغل بالحياء.

لقيام هذه الجريمة لا بد من توفر الأركان المكونة لها كغيرها من الجرائم، تتمثل هذه الأركان في الركن الشرعي، الركن المادي، الركن المعنوي سنوضحهم كمايلي.

أولاً: الركن الشرعي.

تعد جريمة عرض إعلان مغل بالحياء من الجرائم الماسة بالآداب العامة والأخلاق، ويقصد بها كل نشر أو عرض أو تعليق أو بث إعلان أو صورة أو عبارة أو وسيلة إشهارية تتضمن ما يخل بالحياء العام أو يمس بالأخلاق والآداب العامة، سواء في الأماكن العمومية أو عبر وسائل الإعلام والاتصال، كما يستند تجريم هذا الفعل أساساً إلى أحكام قانون العقوبات.

وعليه طبقاً للمادة 1 من قانون العقوبات التي نصت على: "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون"²، والمادة 333 مكرر³ في القسم السادس المعنون بـ "انتهاك الآداب" في قانون العقوبات، جرم المشرع الجزائي كل من عرض أو وزع أو نشر صور أو رسومات أو مواد من شأنها الإخلال بالحياء العام بطريقة علنية.

ثانياً: الركن المادي.

ينقسم بدوره إلى ثلاثة عناصر، بداية مع السلوك الإجرامي، في قضية الحال يتمثل الفعل المادي في عرض محتوى إعلاني غير أخلاقي يتعارض مع الآداب العامة ونشره أمام الجمهور، حيث يروج لأفكار الشذوذ الجنسي والتحريض على فساد الأخلاق وممارسة الرذيلة.

¹ حكم قضائي صادر عن المحكمة الابتدائية، الغرفة الجزائية، ملف رقم 26/00200، المؤرخ في 2026/4/16، قضية (غ س) ضد النيابة العامة، قسم الجناح محكمة جيجل، 2026، ص ص 1، 2.

² الأمر 156-66 المتضمن قانون العقوبات المعدل والمتمم.

³ انظر المادة 333 من قانون العقوبات.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

بالنسبة للنتيجة الإجرامية في الأصل إلحاق الضرر بالغير، غير أن قضية الحال تحتوي على الطرف المشتبه فيه دون الضحية، وعليه هذا النوع من الجرائم يقوم بمجرد ارتكاب الفعل المجرم علينا وتوجيهه للجمهور.

ثالثا: الركن المعنوي.

يتمثل في علم الجاني أن الفعل الذي يقوم به مجرم ومخالف للقانون، أي أن ذلك الإعلان الذي تم عرضه أو نشره يتضمن محتوى مغل بالحياء، واتجاه إرادته إلى القيام بذلك الفعل رغم علمه وبمحض اختياره وليس تحت الإكراه، بالنسبة للقصد الجنائي الخاص لا يشترط قيامه في مثل هذه الجرائم بل يكفي القصد الجنائي العام لتكون الجريمة تامة.

وبناء عليه رأيت المحكمة أن أركان الجريمة لم تكتمل خاصة في جانب إسناد الفعل إلى المتهم، مما حال دون قيام المسؤولية الجزائية.

الفرع الثاني: إجراءات البحث والتحري.

من خلال الحكم محل التعليق، هناك إجراءات متابعة خاصة بقضية الحال.

أولاً: جمع الاستدلالات من قبل فرقة متخصصة تسمى فرقة مكافحة الجريمة السيبرانية، وذلك بعد رصد حساب إلكتروني على مواقع التواصل الاجتماعي (فيسبوك)، وبالتالي النصوص الإجرائية مفعلة من الناحية التطبيقية.

ثانياً: تبيان الحكم لكيفية وإجراءات استنباط الدليل الإلكتروني، حيث نلاحظ مراحل متبعة ومتسلسلة تمثلت في تتبع الحساب محل الشبهة والتحري حول صاحبه بالاعتماد على الوسائل التقنية الحديثة، ومعاينة المنشورات والصور المنشورة عبر منصة (فيسبوك) التي تروج لأفكار الشذوذ الجنسي والتحريض على فساد الأخلاق وممارسة الرذيلة، ثم استخدام المعطيات التقنية المتعلقة بالحساب لاسيما بروتوكول الأنترنت الذي تبين أنه مرتبط برقم هاتفي معين.

كما قامت الضبطية القضائية بتحرير محاضر رسمية تثبت إجراءات المعاينة والفحص التقني للأدلة الرقمية، مع مواجهة المتهم بالمنشورات محل المتابعة أثناء جلسة المحاكمة، غير أن المحكمة اعتبرت أن الدليل الإلكتروني المقدم غير كافٍ لإثبات نسبة الحساب إلى المتهم بصورة يقينية، خاصة وأن رقم الهاتف المرتبط بالحساب موضوع المتابعة مجهول المالك، أضف إلى هذا إنكار المتهم امتلاكه للحساب موضوع المتابعة.¹

¹ حكم قضائي، صادر عن المحكمة الابتدائية، الغرفة الجزائية، سابق الذكر.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

ثالثاً: أهمية إجراءات البحث والتحري التي قامت بها الضبطية القضائية الممثلة في فرقة مكافحة الجرائم السيبرانية، وأثرها البالغ على قناعة القاضي الجزائي حيث هيأت الملف للنياحة العامة من جهة لتكييف وتحليل قضية الحال جنحة علرض إعلان مغل بالحياء، ومن جهة اخرى للقاضي الجزائي تقرير العقوبة وتطبيق النصوص القانونية.

الفصل الثاني: المميزات الخاصة لإجراءات التحقيق التمهيدي في الجريمة الإلكترونية

خلاصة الفصل الثاني:

خلاصة القول، يتضح أن آليات البحث والتحري في الجرائم الإلكترونية تتميز جوهريا عن نظيرتها في الجرائم التقليدية، وهذا التمايز يمتد ليشمل الوسائل الإجرائية المعتمدة والضوابط القانونية النازمة لها. وذلك بالنظر إلى الخصوصية التقنية المعقدة التي تتسم بها الجريمة الإلكترونية، فضلا عن ديناميكيته المتسارعة وطابعها العابر للحدود الوطنية مما يفرض تحديات سيادية وإجرائية جسيمة، بناء على ذلك تبرز ضرورة تحقيق توازن دقيق بين فعالية الأجهزة الأمنية في تعقب الجناة وكشف الجريمة، وبين الالتزام الصارم بصون الحقوق والحريات الأساسية وحماية المعطيات الشخصية.

وقد تطرقنا في الفصل إلى أهم الضوابط القانونية والأساليب التي تحكم عمليات التحري الرقمي، بداية مع الإجراءات الشرطية لضبط الجريمة الإلكترونية حيث توجد إجراءات تقليدية وأخرى مستحدثة، وهذا من خلال النصوص القانونية خصوصا القانون 04-09 الخاص بتنظيم تلك الإجراءات بشكل يكفل الفعالية القانونية، مروراً إلى الضبطية القضائية المختصة بعمليات البحث والتحري واختصاصاتها في هذا المجال، وصولاً إلى الدليل الإلكتروني كأداة يعتز بها المشرع الجزائري للكشف عن هذا النوع من الجرائم، وتجسيدا للجانب التطبيقي تطرقنا إلى حكم قضائي صادر عن المحكمة الابتدائية يتعلق بجنحة عرض إعلان مخل بالحياء عبر مواقع التواصل الاجتماعي (فيسبوك)، حيث اعتبرنا قضية الحال أبرزت أهمية عملية للدليل الإلكتروني في مجال الإثبات.

الخاتمة

الخاتمة:

إن الجرائم الإلكترونية تعتبر من أخطر الجرائم التي نتجت عن الثورة المعلوماتية وهذا راجع إلى التطور المستمر ومساسها بمختلف المجالات مما جعلها عقبة أمام جميع جوانب الحياة اليومية، ولكونها تتميز بخصائص مختلفة كثيرًا عن الجريمة التقليدية في كونها جريمة عابرة للحدود الدولية وكذا الصعوبة في إثباتها وقلة الإبلاغ عليها.

يتضح أن خصوصية إجراءات البحث والتحري في الجريمة الإلكترونية في ظل التشريع الجزائري تعكس سعي المشرع إلى مواكبة التحولات الرقمية، والتشريعات الرائدة في المجال المعلوماتي، وذلك عن طريق إقرار قواعد إجرائية تتلاءم مع طبيعة الدليل الإلكتروني وخصائصه التقنية، فقد عمل المشرع على إدراج آليات قانونية مستحدثة ضمن قانون الإجراءات الجزائية، مدعمة بنصوص خاصة، لاسيما القانون 04.09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بما يسمح بتوسيع صلاحيات الضبطية القضائية وتمكينها من وسائل حديثة للتحري.

بالإضافة إلى القانون 05.18 المتعلق بالتجارة الإلكترونية، الذي كرس تجريم الأفعال الماسة بالأنظمة المعلوماتية والمعطيات، كما أقر آليات إجرائية خاصة تتلاءم مع طبيعة الدليل الإلكتروني مع توسيع صلاحيات البحث والتحري وتعزيز التعاون.

كما أن المشرع الجزائري عمل على إتباع طرق حديثة تعمل على تسهيل عملية التحري عن الجرائم الإلكترونية نظرًا للخصوصية التي تتميز بها، حيث عمد المشرع الجزائري وعلى سبيل الحصر بتحديد من يتمتع أو من هم الأشخاص المكلفون بالتحري، كما منحو جملة من الصلاحيات الموسعة تحت رقابة وإشراف وكيل الجمهورية وهذا من أجل تسهيل مهامهم نسبيًا، ويعكس المشهد القانوني المعاصر تزايدًا ملحوظًا في استعمال مفردات ومصطلحات حديثة ومتباينة من حيث الدلالة والمضمون، وهو ما يُعزى أساسًا إلى الانتشار الواسع للإنترنت وما أفرزه من تحولات عميقة في سلوك الأفراد و أنماط الإجرام.

فقد لجأ المشرع إلى توظيف مصطلح "الاختراق" ضمن قانون الوقاية من الفساد، في حين اعتمد مصطلح "التسرب" في سياق جرائم أخرى، لاسيما المرتبطة بالجريمة الإلكترونية، الأمر الذي يعكس نوعًا من عدم الاتساق الاصطلاحي. وهو وضع يقتضي تدخلًا تشريعيًا يرمي إلى توحيد المصطلحات الجزائية من خلال مقارنة عملية دقيقة، مع إعادة ضبطها بما يضمن الانسجام والتكامل بين القوانين الخاصة وقانون الإجراءات

الخاتمة

الجزائية، غير أن التطبيق العملي لهذه النصوص يكشف عن وجود تحديات حقيقية، تتعلق أساسًا بمدى فعالية هذه الإجراءات في مواجهة التطور السريع للجريمة الإلكترونية، وبقدرتها على تحقيق التوازن بين مقتضيات البحث والتحري وضمانات حماية الحقوق والحريات الأساسية.

النتائج:

وقد توصلنا من خلال دراستنا إلى مجموعة من النتائج، يمكن استخلاصها كالآتي:

- بالرغم من انتشار الجريمة الإلكترونية في العالم إلا أنها لم تحض بتعريف مانعًا جامعا لها.
- الجريمة الإلكترونية تتميز عن باقي الجرائم الأخرى بأنها ذات طابع دولي عابر للحدود الوطنية فهي عالمية الوجود.
- قصور بعض النصوص الإجرائية عن الإحاطة الكاملة بخصوصيات الدليل الإلكتروني، خاصة من حيث جمعه وحفظه وتقديمه أمام القضاء.
- التباين بين سرعة تطور الوسائل التكنولوجية وبطء التحديث التشريعي، مما يخلق فجوة قانونية في بعض الصور الإجرائية المستحدثة.
- وجود صعوبات تعيق عمل إجراءات مكافحة الجريمة الإلكترونية، تتازع القوانين والاختصاص القضائي بين الدول.
- نقص الخبرة لدى رجال الضبط القضائي والأجهزة الأمنية بصفة عامة فيما يتعلق بثقافة الحاسب الآلي وأنظمة الاتصال.
- ظهور الأقطاب الجزائية المتخصصة بالفصل في الجرائم الخطرة من بينها الجرائم الإلكترونية إلا أنه يمكن القول أن تفعيلها ضعيف بسبب قلة القضايا و ذلك يرجع إلى عزوف المجني عليه عن الشكوى ومباشرة الدعوى العمومية.

التوصيات:

- ضرورة مراجعة وتحيين النصوص القانونية ذات الصلة، بما يضمن مواكبة التطورات التقنية المتسارعة في مجال الجرائم الإلكترونية.
- العمل على إصدار قوانين صارمة تهدف إلى الحد من هذه الجرائم مع ضرورة تشديد الرقابة على الأجهزة والبرامج المستخدمة.

الخاتمة

- التركيز على تأهيل وتدريب متخصصين من الأجهزة القضائية وجهات الضبط القضائي لمواجهة الجرائم الإلكترونية بفعالية وكفاءة.
- تعزيز التعاون الدولي بين الدول لمكافحة هذه الظاهرة الإجرامية، عبر توقيع اتفاقيات جماعية وثنائية، خاصة في مجال التعاون القضائي والأمني.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولاً: المصادر.

1. النصوص القانونية.

أ. النصوص التشريعية.

الدستور:

- دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر بموجب المرسوم الرئاسي 20-422، المؤرخ في 30 ديسمبر 2020، ج.ر، ع 82، سنة 2020.

القوانين:

- القانون رقم 09-04، المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، عدد 47، الصادرة بتاريخ 16 أوت 2009
- القانون رقم 18-05، المؤرخ في 24 شعبان 1439 الموافق ل 10 مايو 2018، المتعلق بالتجارة الإلكترونية، ج.ر، عدد 28، الصادرة في 16 مايو 2018.

الأوامر:

- الأمر 66-156، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.
- الأمر 66-155، الموافق ل 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية.

ب. النصوص التنظيمية.

المراسيم.

- المرسوم الرئاسي رقم 06-348، المؤرخ في 5 أكتوبر 2006، المتضمن تمديد الاختصاص القضائي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 63، الصادر بتاريخ 8 أكتوبر 2006.

الأحكام والقرارات القضائية.

- حكم قضائي صادر عن المحكمة الابتدائية، الغرفة الجزائية، ملف رقم 26/00200، المؤرخ في 2026/4/16، قضية (غ س) ضد النيابة العامة، قسم الجناح محكمة جيجل، 2026.

ثانيا: المراجع.

1. الكتب.

- طاهر محمود أبو القاسم، الجرائم الإلكترونية صعوبات التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية، مصر، 2019.
- حسين طاهري، الجرائم الإلكترونية، الطبعة 1، دار الخلدونية، الجزائر، 2022.
- جاسم محمد جندل، الجرائم الإلكترونية، دار المعتز للنشر والتوزيع، عمان، 2022.
- محمد شنه، إجراءات البحث والتحري عن الجرائم في التشريع الجزائري، الطبعة 1، ألفا للوثائق للنشر والتوزيع، الجزائر، 2024.
- لهوى رابح، البحث والتحري عن الجريمة الإلكترونية والشرعية، دارالأيام للنشر والتوزيع، عمان، 2021.
- عبد الفتاح علي، مكافحة الجرائم الإلكترونية بين نظم المعلومات والإعلام البديل، الطبعة 2، مكتبة الوفاء القانونية، الإسكندرية، 2024.
- أنطوان نعمه وآخرون، المنجد في اللغة العربية المعاصرة، الطبعة 2، دار النشر، بيروت، 2001.

ثالثا: الأطروحات والمذكرات.

1. أطروحات الدكتوراه.

- خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة المنصورة، 2021/2020.
- علواش فريد، جريمة غسيل الأموال دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2009/2008.
- فيروز عوض الكريم صالح مبرغني، إجراءات التحري والضبط في الجريمة الإلكترونية، أطروحة دكتوراه، كلية الدراسات العليا والبحث العلمي، جامعة شندي، 2017/1437.
- أومرود رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريج، 2021/2020.
- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2016/2015.

قائمة المصادر والمراجع

- بلارو كمال، الشرطة القضائية في التشريع الجزائري، أطروحة دكتوراه، كلية الحقوق، قسم القانون الخاص، جامعة الإخوة منتوري، قسنطينة2، 2021/2020.
- صهيب سهيل غازي زامل، البحث والتحري عن الدليل الإلكتروني في المسائل الجزائية-دراسة مقارنة-، أطروحة دكتوراه، قانون جنائي، جامعة وهران2، وهران، 2022/2021.
- 2. مذكرات ماجستير.
- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04-09، شهادة ماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013/2012.
- 3. مذكرات ماستر.
- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال شهادة الماستر، كلية الاقتصاد والعلوم التجارية وعلوم التسيير، قسم علوم التسيير، جامعة قاصدي مرباح، ورقلة، 2019/2018.
- أبو بكر تيتاوي، إلياس مالك قرادي، جرائم النصب والاحتيال الإلكتروني، شهادة ماستر، معهد الحقوق المركز الجامعي المقاوم آمود بن مختار إيليزي، 2025/2024.
- بوعجاجة زينب جيهان، درابلي دنيا زاد، الإجراءات المستحدثة للتحقيق في الجرائم الإلكترونية، مذكرة ماستر كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعرييج، 2023/2022.
- طاهري عبد المطلب، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2015/2014.
- رزيق محمد، إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة أكلي محمد أولحاج، البويرة، 2019/2018.
- فراحتية خلود، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعرييج، 2022/2021.
- حفيش محمد الطيب، عابد أمينة، آليات البحث والتحري في الجريمة الإلكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة إيليزي، 2025/2024.

رابعاً: المقالات

قائمة المصادر والمراجع

- بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد 14، ع 4، نوفمبر 2021.
- غنية عباس، الجريمة الإلكترونية في البيئة الرقمية ومدى تأثيرها على الجريمة المنظمة العابرة للحدود الوطنية، المجلة الجزائرية للسياسات العامة، جامعة الجزائر 3، المجلد 12، ع 3، ديسمبر 2024.
- حمد محمد الدوسري، أنواع الجرائم الإلكترونية وتحديات مكافحتها، مجلة المنار للدراسات والبحوث القانونية والسياسية، جامعة يحي فارس، المدينة، المجلد 9، ع 1، جوان 2025.
- اسمهان بن مالك، خصائص الجريمة المعلوماتية وأسباب ارتكابها، مجلة البيان للدراسات القانونية والسياسية، جامعة البشير الإبراهيمي، برج بوعريرج، المجلد 4، ع 1، 15 جوان 2019.
- زبوش عبد الرؤوف، زغيشي مصطفى، الجرائم الإلكترونية الإقتصادية - المفهوم والدوافع -، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس، بريكة، المجلد 7، ع 1، جوان 2024.
- حمز خضري، حمزة عشاش، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي، الأغواط، المجلد 6، ع 2، جوان 2020.
- العرفي فاطمة، حجية الدليل الرقمي في إثبات جريمة الإبتزاز الإلكتروني في القانون الجزائري، مجلة صوت القانون، جامعة خميس مليانة، المجلد 8، ع 2، أكتوبر 2022.
- سامية حمريش، صليحة رحالي، الجريمة الإلكترونية وانعكاساتها على المنظومة الأخلاقية: الإبتزاز الإلكتروني -أمودجا-، مجلة الباحث للدراسات الأكاديمية، جامعة الحاج لخضر، باتنة 1، المجلد 12، ع 2، جوان 2025.
- عراب مريم، جريمة التهديد والإبتزاز الإلكتروني، مجلة الدراسات القانونية المقارنة، جامعة أحمد بن أحمد، وهران 2، المجلد 7، ع 1، 2021.
- علي عبد السلام، جريمة القذف عبر مواقع التواصل الإجتماعي دراسة تحليلية مقارنة بين التشريع الجزائري والتشريعات الأجنبية والعربية، مجلة الدراسات القانونية والاقتصادية، جامعة سي الحواس، بريكة، المجلد 5، ع 2، ديسمبر 2022.
- بن نقي سفيان، جريمة غسيل الأموال بين الوسائط الإلكترونية والنصوص التجريبية، مجلة الابحاث القانونية والسياسية، جامعة محمد لمين دباغين، سطيف 2، المجلد 3، ع 2، 2021.
- رجال بومدين، سعداني نورة، الحماية الجنائية الواقعة على أموال التجارة الإلكترونية (جريمة السرقة والنصب)، مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 9، ع 2، 2016.

قائمة المصادر والمراجع

- منيرة بن جدو، مبروك بن زيوش، الحماية الجزائية لمحل العقد الإلكتروني في ظل القانون 05-18 المتعلق بالتجارة الإلكترونية، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الأغواط، المجلد 5، ع 2، 2021.
- جفالي حسين، الحماية الجنائية للمستهلك من الإشهار التجاري الإلكتروني غير المرغوب فيه في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي، الأغواط، المجلد 2، ع 4، 2018.
- بن جدو منيرة، مبروك بن زيوش، الإشهار الإلكتروني وحمايته جنائيا في القانون الجزائري، مجلة الرسالة للدراسات القانونية والبحوث الإنسانية، جامعة العربي التبسي، المجلد 6، ع 4، 30 ديسمبر 2021.
- آيت حمودة كاهنة، البحث والتحري الجنائي في مسرح الجريمة الإلكترونية، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الأغواط، المجلد 7، ع 1، 15 ماي 2023.
- مختار تابري، الخبرة في الجريمة الإلكترونية، مجلة الحوار المتوسطي، جامعة الجيلالي الياابس، سيدي بلعباس، المجلد 11، ع 3، 17 جانفي 2021.
- مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، المركز الجامعي شريف بو شوشة أفلو، الأغواط، المجلد 6، ع 28، 1 جانفي 2023.
- قادري نسيم، عن أساليب التحقيق الخاصة المتعلقة بالجريمة الإلكترونية ذات البعد الاقتصادي: أية فعالية؟، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية، المجلد 12، ع 3، 1 جانفي 2022.
- سعاد راضي حسين، الإجراءات الجزائية في تفتيش محل الجرائم الإلكترونية، مجلة الشرق الأوسط للدراسات القانونية والفقهية، جامعة الأردن، المجلد 4، ع 4، 2024.
- عز الدين عثمان، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، المركز الجامعي مرسلني عبد الله، تيبازة، المجلد 2، ع 4، 29 جانفي 2018.
- ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمه لخضر، الوادي، المجلد 8، ع 2، 1 جوان 2017.

قائمة المصادر والمراجع

- بن بادة عبد الحليم، المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني بين الحق في الخصوصية ومشروعية الدليل الإلكتروني، مجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية، المجلد 10، ع 3، 31 ديسمبر 2019.
- فلاح عبد القادر، حجز وحفظ المعطيات في الجريمة الإلكترونية، مجلة صوت القانون، جامعة جيلالي بونعامة، خميس مليانة، المجلد 8، ع 1، 30 نوفمبر 2021.
- فلاح عبد القادر، آيت عبد المالك نادية، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة، خميس مليانة، المجلد 4، ع 2، 2019.
- سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوة منتوري، قسنطينة 1، المجلد 30، ع 3، ديسمبر 2019.
- مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الأغواط، المجلد 6، ع 2، 2 نوفمبر 2022.
- بن فردية محمد، الدليل الجنائي الرقمي وحجبه أمام القضاء الجزائري -دراسة مقارنة-، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، بجاية، المجلد 9، ع 1، أكتوبر 2016.
- خطوي مسعود، خصوصية الدليل الإلكتروني، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الأغواط، المجلد 7، ع 1، 2022.
- خامسا: المداخلات العلمية.**
- شطبي عبد السلام، خصوصية المتابعة الجزائية لجرائم التجارة الإلكترونية بين حادثة النص التشريعي وعوائق التطبيق، الملتقى الدولي الموسوم بالتجارة الإلكترونية بين حتمية تكنولوجيا الاتصال وسبل حماية المستهلك الإلكتروني، كلية الحقوق العلوم السياسية، جامعة المدية، 19 جوان 2021.
- بومحراث ليندة، إجراءات التحقيق الخاصة بالجرائم السيبرانية، مداخلة ضمن فعاليات اليوم الدراسي: حول الجريمة السيبرانية، كلية الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، المنعقد في 20 أبريل 2022.
- سادسا: محاضرات.**

قائمة المصادر والمراجع

- بوراس نادية، محاضرات في مقياس الجريمة الإلكترونية، أُلقيت على طلبة الحقوق السنة الثانية ماستر، 2023/2022.
- شطبي عبد السلام، محاضرات مقدمة في مقياس القانون الجنائي للبيئة، أُلقيت على طلبة السنة أولى ماستر، 2026/2025.
- مشري سلمى، محاضرات في مقياس الجريمة الإلكترونية، أُلقيت على طلبة السنة الثانية ماستر، علوم جنائية،
- شطبي عبد السلام، محاضرات في مقياس قانون الإجراءات الجزائية، أُلقيت على طلبة السنة أولى ماستر، 2026.

الملاحق

نسخة عادية

الجمهورية الجزائرية الديمقراطية الشعبية

باسم الشعب الجزائري

حكم

بالجلسة العلنية المنعقدة بمقر

بتاريخ:

النظر في قاضي الجناح

برئاسة السيد (ة): رئيس

وبمساعدة السيد (ة): أمين ضبط

وبحضور السيد (ة): وكيل الجمهورية

صدر الحكم الجزائي الآتي بيانه بين الأطراف التالية
السيد وكيل الجمهورية مدعيا باسم الحق العام.

من جهة

ضد /

1 (: متهم حاضرا

من مواليد: متزوج (ة)

ابن: ساكن

بمساعدة الأستاذ (ة):

من جهة أخرى

بيان وقائع الدعوى

- حيث أن المتهم متابع من طرف النيابة لوجود قرائن قوية بارتكابه ومنذ زمن لم يدركه أمد التقادم القانوني بعد بدائرة اختصاص بجنحة عرض اعلان مغل بالحياة الفعل المنصوص والمعاقب عليه بالمادة 333 مكرر من قانون العقوبات

- حيث أن المتهم أحيل امام قسم الجناح وفقا لإجراء الاستدعاء المباشر حسب نص المادة 472 من قانون الإجراءات الجزائية.

- حيث تتلخص وقائع القضية أنه بتاريخ 17/01/2023 تم رصد حساب الكتروني على موقع التواصل الاجتماعي فايسبوك من طرف فرقة مكافحة الجرائم السيبرانية بأمن دائرة يدعو و يروج لأفكار الشذوذ الجنسي و التحريض على فساد الاخلاق و ممارسة الرذيلة تحت اسم ، بناء على ذلك تم التحري عن صاحب الحساب اين تم التوصل ان رقم بروتوكول الانترنت الحساب هو 105.109.225.248 و الذي كان مربوط برقم الهاتف في المسجل باسم المدعو المقيم فيما بقي صاحب رقم

الهاتف للحساب مجهول

لم يتم سماع المشتبه فيه

عن جلسة المحاكمة /

- حيث أن المتهم حضر جلسة المحاكمة و بعد التأكد من هويته و مواجهته بالجرم المنسوب اليه

صفحة 1 من 3

مجلس قضاء

محكمة:

قسم الجناح

26/ رقم الجدول:

26/ رقم الفهرس:

26/ تاريخ الحكم:

استدعاء مباشر

النيابة ضد /

طبيعة الجرم /

جنحة عرض اعلان مغل

بالحياة



26/ رقم الجدول:

26/ رقم الفهرس:

اجاب منكرا واقعة امتلاك الحساب الذي بموجبه تم عرض المنشورات المخلة بالحياء و اكد ان الهاتف الثابت المفعّل بواسطته الحساب فعلا مسجل به و لكن الرقم الهاتفي للحساب ليس ملك له لم يسبق له و ان انشأ حساب بهذا الاسم .
- حيث ان ممثل النيابة التمس إدانة المتهم وعقابه بعام 01 حبس نافذ و 50000 دينار غرامة مالية نافذة.
حيث ان دفاع المتهم التمس تبرئة ساحة موكله .
حيث ان الكلمة الاخيرة كانت للمتهم و دفاعه طبقا لنص المادة 503/3 من قانون الاجراءات الجزائية.
حيث ان القضية وضعت قيد النظر لجلسة 13/04/2026 للفصل فيها طبقا للقانون و نبهنا المتهم بذلك .

****وعليه فإن المحكمة****

بعد الاطلاع على أوراق الملف والمناقشات التي دارت بالجلسة.
بعد الإطلاع على أحكام قانون الإجراءات الجزائية.
بعد الاطلاع على أحكام المادة 333 مكرر من قانون العقوبات .
بعد النظر قانونا .
في الدعوى العمومية:
حيث انه من المقرر قانونا حسب نص المادة 349 من قانون الاجراءات الجزائية انه يجوز اثبات الجرائم بأي طريق من طرق الاثبات ما عدا الاحوال التي ينص القانون على غير ذلك و للقاضي ان يصدر حكمه تبعا لاقتناعه الشخصي ، و لا يسوغ للقاضي ان يبني قراره الا على الادلة المقدمة له في معرض المرافعات و التي حصلت فيها المناقشة فيها حضورا امامه .
حيث انه من المقرر قانونا طبقا لنص المادة 514 من قانون الاجراءات الجزائية ، انه اذا رأت المحكمة ان الواقعة موضوع المتابعة لا تكون آية جريمة في قانون العقوبات او انها غير ثابتة او غير مسندة للمتهم قضت ببرأته من المتابعة بغير عقوبة و لا مصاريف .
- حيث تبين للمحكمة بعد اطلاعها على ملف القضية ان عرض اعلان مخل بالحياء الفعل المنصوص والمعاقب عليه بالمادة 333 مكرر من قانون العقوبات ، غير قائمة الاركان في مواجهة المتهم .
لانعدام الدليل الجزائي الذي يثبت للمحكمة ان الحساب في موقع التواصل الاجتماعي المسمى () الذي بواسطته تم نشر و عرض اعلان مخل بالحياء انه فعلا مملوك للمتهم الذي تم متابعته في قضية الحال بناء على ضبط ان بروتوكول الحساب السالف الذكر تم تفعيله بواسطة الرقم الثابت المملوك للمتهم و هو الامر الذي لا يرقى لمقام الدليل الكافي من اجل اسناد الجرم للمتهم ، الذي اصر على انكار الوقائع و اكد انه لم يسبق و ان امتلك حساب على الفايس بوك ، كما ان صاحب الرقم الهاتفي الذي بموجبه تم انشاء الحساب بقي مجهولا و غير معروف و هو ما يعزز انكار المتهم .
حيث ان محكمة الجنج محكمة دليل لا يسعها القضاء في غياب دليل كاف أو قرينة قوية خاصة و ان المتهم غير مطالب بتقديم أي دليل لبرأته باعتبارها الأصل فيه و إنما يقع ذلك على عاتق سلطة الإتهام و المدعى المدني ، و عليه و تبعا لذلك يتعين على المحكمة التصريح ببراءة المتهم من الجرم المنسوب اليه طبقا لنص المادة 514 من قانون الاجراءات الجزائية .
- حيث ان المصاريف القضائية تبقى على عاتق الخزينة العمومية تطبيقا لنص المادة 518 من قانون الإجراءات .

****ولهذه الأسباب****

حكمت المحكمة حال فصلها في قضايا الجنج علنيا ابتدائيا حضورا للمتهم /
في الدعوى العمومية /التصريح ببراءة المتهم / من الجرم المنسوب اليه طبقا لنص المادة 514 من قانون الاجراءات الجزائية و المصاريف القضائية على الخزينة العمومية .
بذا صدر الحكم، ونطق به علنا بالجلسة العلنية المنعقدة بالتاريخ المذكور أعلاه، وأمضي أصله من طرف الرئيس وأمين الضبط.

قوانين

المصطلحات

المادة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ - الجرائم المتصلة بتكنولوجيات الإعلام والاتصال :

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

ب - منظومة معلوماتية :

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

ج - معطيات معلوماتية :

أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

د - مقدم الخدمات :

1 - أي كيان عام أو خاص يقدم لمستهلمي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات.

2 - وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستهلميها.

هـ - المعطيات المتعلقة بحركة السير :

معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءًا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة.

و - الاتصالات الإلكترونية :

أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

قانون رقم 09 - 04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

- بناء على الدستور، لا سيما المواد 119 و 120 و 122 - 7 و 126 منه،

- وبمقتضى الأمر رقم 66 - 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدل والمتمم،

- وبمقتضى الأمر رقم 66 - 156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

- وبمقتضى الأمر رقم 75 - 58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدل والمتمم،

- وبمقتضى القانون رقم 2000 - 03 المؤرخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدل والمتمم،

- وبمقتضى الأمر رقم 03 - 05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

- وبمقتضى القانون رقم 08 - 09 المؤرخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

- وبعد رأي مجلس الدولة،

- وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول

أحكام عامة

الهدف

المادة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة 1^أ من هذه المادة موجبة حصريا لجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياء الخاصة للغير.

الفصل الثالث

القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادة 5 : يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ - منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب - منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة 1^أ من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لحدا المعاملة بالمثل.

يسكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

مجال التطبيق

المادة 3 : مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتوياتها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني

مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ - للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب - في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج - لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د - في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة 1^أ من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

المكلفة بالتحريرات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينتجونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادة 11 : مع مراعاة طبيعة وتنوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ - المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب - المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج - الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د - المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدمها،

هـ - المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة 1^ة من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالسجن من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوع تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادة 8 : يمكن السلطة التي تبشر بالتفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات

الفصل السادس التعاون والمساعدة القضائية الدولية الاختصاص القضائي

المادة 15 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام. يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادة 19 : ينشر هذا القانون في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

حرر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

تحدد كليات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ - التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

ب - وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم.

مهام الهيئة

المادة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ - تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

ب - مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

ج - تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.