وزارة التعليم العالي والبحث العلمي
المركز الجامعي الشيخ المقاوم آمود بن مختار –ايليزي–
معهد الحقوق

مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص: قانون جنائي وعلوم جنائية

بعنوان

آليات البحث والتحري في الجرائم الالكترونية

اعداد الطلبين:

- حفش محمد الطيب
- عابـد أمينـــة

تحت اشراف الدكتور

شروف مراد

وتتكون لجنة المناقشة من الأساتذة:

الأستاذ: زروقة هشام	المركز الجامعي ايليزي	رئيسا
الدكتور: شروف مراد	**أستاذ محاضر–ب–المركز الجامعي ايليزي**	**مشرفا ومقررا**
الأستاذ: عبدوعلي الطاهر	المركز الجامعي ايليزي	مناقشا

السنة الجامعية: 2025/2024


بسم الله الرحمن الرحيم

إهـــداء وشكر

إلهي، لا يطيب الليل إلا بشكرك، ولا يصفو نهار إلا بطاعتك، ولا تأنس اللحظات إلا بجلال ذكرك، ولا تهنأ الآخرة إلا بعفوك ورحمتك، ولا تكتمل نعيم الجنة إلا برؤية وجهك الكريم.

أهدي ثمرة جهدي هذه:

إلى من وكله الله بالهيبة والوقار، وعلمني العطاء بدون انتظار، وأحمل إسمه بكل افتخار، إلى سندي ودعمي في الحياة وفي مسيرتي العلمية "**أبي**".

إلى ملاكي في هذه الحياة، إلى من تجسدت فيها أسمى معاني الحب والتفاني والحنان، إلى قدوتي التي أستلهم منها القوة والصبر، إلى نبع السعادة الذي لا يجف، إلى من كان دعاؤها الصادق نورا أنار دربي وسرا عظيما وراء كل نجاح حققته أدام الله علينا هذه النعمة "**أمي**".

إلى الذين هم النور الذي أضاء طريقي، قرات عيوني بحم التقى الدعم و التشجيع في كل خطوة نجاح، ولا تكتمل الفرحة إلا بحضورهم أحمد الله على هذه النعمة "**إخوتي**"

شكر وعرفان

أتقدم بخالص الشكر وعظيم الامتنان للجهود القيمة التي بذلها استاذي الفاضل ومشرف بحثي من هو نعم المعين والداعم طوال فترة دراستي، استفدت من ارشاداته السديدة، وملاحظاته البناة التي كان لها بالغ الأثر في إنجاز هذا العمل، جزاه الله عنا خير الجزاء وبارك فيه وفي عمله وفي كل خطوة يخطوها "**شروف مراد**"، كما لا ننسى لجنة المناقشة وعلى رأسها الرئيس وكذا المناقش فلكم منا كل عبارات الشكر والتقدير.

أقدم جزيل الشكر لعائلتي الموقرة "**عابد**" و"**جانتي**" وبالأخص "**عثماني**" الذين احاطوني بحبهم وصدق دعواتهم وزودوني بحسن نصحهم وإرشاداتهم النيرة، لهم مني كل الشكر والعرفان ما حييت وأدامكم الله لي نورا وسندا مدى الحياة وأنار دربكم.

إلى أحبائي وزملائي في المركز الجامعي من كانوا لي خير رفيق وخير معين انست بوجودهم حولي وسعدت بالعمل معكم خير صحبة وخير زمالة وبالأخص "**وسيلة، حنان**" شكركم لا يكفي لوصفكم أعانكم الله على خيره ومنه.

لكم جميعا أهدي هذا العمل المتواضع، عرفانا بالجميل وامتنانا لا ينتهي

الطالبة عابد أمينة

شكر وعرفان

الحمد لله حمد كثيرا الحثنا على طلب العلم أينما وجد والصلاة والسلام على أشرف خلقه

أتقدم بأسمى عبارات الشكر والعرفان إلى استاذي الفاضل المشرف شروف مراد على إرشاداته وتوجيهاته التي لم يبخل بها علينا يوما، والشكر إلى كل يد رافقتنا في هذا العمل سواء من قريب أو من بعيد، كما لا أنسى أن أشكر جميع الأساتذة والمؤطرين الذين قدموا لنا يد المساعدة، وعلى كل الزملاء والأساتذة الكرام بما أفادونا من علمهم.

إهداء

الحمد لله كثيرا، والصلاة والسلام على المصطفى الكريم سيد الاولين والأخرين

اهدي ثمرة هذا العمل المتواضع إلى من وهبوني الحياة والأمل والديا العزيزين وإلى إخوتي الأعزاء ورفاق الدرب، لكم منا خالص المحبة وعمق الامتنان

وإلى كل من مد لي يد العون، من قريب أو من بعيد بدعوة صادقة، راجيا من الله أن يجازيكم عني خير الجزاء.

الطالب حفش محمد الطيب

-الرموز والمختصرات:

- **ج ر ج:** الجريدة الرسمية الجزائرية
- **د.** دكتور
- **ف:** الفقرة
- **ق إ ج:** قانون الإجراءات الجزائية
- **ق ع:** قانون العقوبات
- **ط:** الطبعة
- **م:** المادة
- **م.ر:** مرسوم الرئاسي
- **IP**: بروتوكول الانترنت
- **IDS** : Intrusion Détection System
- **P**: page

المقدمة

المقدمـــــة:

يشهد العالم المعاصر تحولاً جذرياً بفعل الثورة التكنولوجية المتسارعة، التي أرست دعائم مجتمع جديد قائم على المعرفة الرقمية والتواصل اللامحدود. فقد أفرزت التكنولوجيات الحديثة، ولا سيما تكنولوجيا المعلومات والاتصالات، واقعاً مغايراً لما عهدته البشرية في العصور السابقة، إذ لم يعد الزمان أو المكان يشكّل عائقاً أمام انتقال البيانات وتبادلها. فقد أدى الانتشار الواسع للحواسيب والهواتف الذكية، والاعتماد المتزايد على شبكات الاتصال – خاصة شبكة الإنترنت – إلى نشوء بيئة رقمية مترابطة، أصبحت جزءاً لا يتجزأ من الحياة اليومية للأفراد والدول، بغضّ النظر عن درجة تحضّرهم أو تطوّرهم الاقتصادي.

وفي ظل هذا الانفجار المعلوماتي، برزت إشكاليات قانونية معقّدة تتصل بكيفية تنظيم الفضاء الرقمي، وحماية الحقوق والحريات الأساسية في بيئة افتراضية لا تخضع – في كثير من الأحيان – لحدود سيادة الدولة التقليدية. ومن هنا تبرز أهمية دراسة الإطار القانوني المنظّم لاستخدام التكنولوجيا، وتحليل مدى ملاءمته لمواجهة التحديات المستجدة، سواء على مستوى حماية الخصوصية، أو مكافحة الجرائم الإلكترونية، أو ضمان الأمن السيبراني.

تُعد الجريمة الإلكترونية من أبرز الظواهر الإجرامية المستحدثة التي أفرزتها الثورة التكنولوجية والمعلوماتية المعاصرة، إذ أضحت تشكل تهديدًا حقيقيًا يتجاوز الحدود الجغرافية، ويطال مختلف الأصعدة الاقتصادية والسياسية والاجتماعية. وقد أسهمت البيئة الرقمية المفتوحة، وما تتميز به من تعقيد وسهولة في إخفاء الهوية، في إيجاد مناخ ملائم لارتكاب أنماط جديدة من الجرائم، لم تعد مقصورة على الواقع المادي، بل امتدت إلى الفضاء السيبراني الذي يتميّز بتشابكه وامتداده العابر للحدود.

ونظرًا لحداثة هذه الجريمة، فقد تعددت التعاريف الفقهية لها دون الاتفاق على مفهوم موحد، إلا أن الإجماع انعقد على خطورتها، وضرورة مواجهتها بتشريعات وطنية وآليات دولية فعّالة. وفي هذا السياق، برزت اتفاقية بودابست لعام 2001، التي أقرها مجلس أوروبا[1]، كأول إطار قانوني دولي يسعى إلى توحيد الجهود لمكافحة الجريمة السيبرانية، من خلال تبني سياسة جنائية مشتركة وتعزيز التعاون الدولي بين الدول.

[1] اتفاقية بودابست بشأن الجريمة المعلوماتية الموقعة في بودابست بتاريخ 23 نوفمبر 2001، منشورة من قبل مجلس أوروبا، متاحة على الموقع الرسمي:
https//www.coe.int/en/web/cybercrime/budapest-convention.

وقد كانت الجزائر من بين الدول التي لم تبقَ بمنأى عن هذه التحديات، إذ تأثرت بتبعات الثورة الرقمية، مما دفعها إلى اتخاذ خطوات تشريعية ومؤسساتية تهدف إلى التصدي لهذه الجرائم، والانخراط في المساعي الدولية الرامية إلى مواجهتها، من خلال تبني استراتيجيات وآليات قانونية وتقنية للحد من آثارها السلبية.

إن من الركائز الأساسية لمنظومة العدالة الجنائية الاعتماد على مرحلة البحث والتحري في الجرائم الالكترونية والتي تعد من أحد أهم المراحل الإجرائية من شأنها كشف الحقيقة والوصول إليها، فآليات البحث والتحري الالكتروني تعتمد على مجموع من الوسائل التقنية المتطورة التي تتضمن جمع الأدلة الرقمية، تحليل البيانات، ورصد الأنشطة الالكترونية، إضافة إلى تقنيات فك التشفير، وذلك وفقا لإطار قانوني يوازن بين فعالية الإجراءات واحترام خصوصية الأفراد وحرياتهم، إلا أن هذه الآليات لا تزال تواجه تحديات متعددة وصعوبة التحقيق من الهوية الرقمية للجناة وكذا تعقيدات في إثبات المسؤولية الجنائية، فضلا عن الإشكالات الناتجة عن الطابع العابر للحدود الذي يميز هذا النوع من الجرائم وما يترتب عليه من تداخلات قانونية وقضائية بين الدول.

وقد سعت هذه الدراسة إلى استعراض أبرز الآليات المعتمدة في مجال البحث والتحري عن الجرائم الإلكترونية، من خلال مقاربة شاملة تشمل الجوانب الفنية والتقنية من جهة، والأبعاد القانونية والتشريعية من جهة أخرى، مع التركيز على الصعوبات العملية التي تواجه مختلف الجهات المختصة بتنفيذ هذه المهام. وتهدف الدراسة إلى تقييم مدى ملاءمة الإطار القانوني القائم لمواجهة التحديات المتنامية في هذا المجال، وتحليل مكامن القصور التي تظهر على مستوى التطبيق والممارسة.

وفي ظل ما تشهده البيئة الرقمية من تطورات متسارعة، بات من الضروري الوقوف عند حدود كفاءة المنظومة الحالية للتحري الإلكتروني، ومدى قدرتها على مجاراة الجرائم السيبرانية المتطورة. ومن هذا المنطلق، تسعى الدراسة إلى تقديم جملة من المقترحات العملية الكفيلة برفع مستوى فعالية الأجهزة المختصة، وتطوير الأطر القانونية بما يواكب التحولات الراهنة ويحقق التوازن بين مقتضيات الأمن الرقمي وضمانات الحقوق والحريات.

-أهمية الموضوع: تكمن أهمية الموضوع فيما يلي

- ✓ خطورة الجريمة المعلوماتية: تعتبر الجريمة المعلوماتية من أخطر الجرائم الحديثة، حيث تتميز بكونها جريمة عابرة للحدود، مما يجعلها تهدد جميع الدول بما في ذلك الدول المتقدمة في مجالات العلم والتكنولوجيا.
- ✓ التهديدات التي تطرأ على الأمن القومي: تشكل الجرائم الإلكترونية تهديدًا للأمن القومي والاستقرار الاجتماعي، فضلًا عن تأثيرها السلبي على الاقتصاد الوطني، مما يجعل التصدي لها أمرًا حيويًا.

- ✓ تأثير الجرائم الإلكترونية على المؤسسات والأفراد: تسعى الجرائم الإلكترونية إلى التأثير العميق على المؤسسات العامة والخاصة، وكذلك تهديد خصوصية الأفراد وحرياتهم في استخدام الإنترنت، ما يبرز ضرورة دراستها من منظور قانوني.
- ✓ أهمية بناء الوعي القانوني: يهدف البحث إلى المساعدة في بناء وعي قانوني لدى الباحثين والمهتمين بشأن الأسس القانونية للتحري الإلكتروني، بالإضافة إلى تحديد الضوابط والمعايير القانونية اللازمة لمكافحة هذه الجرائم.

-أسباب اختيار الموضوع:

1-الأسباب الذاتية: الرغبة والميول للبحث في هذا الموضوع ودراسته ولخصوصيته في الانتشار السريع وتطوره مع تطور البيئة المعلوماتية ووسائلها التقنية الحديثة والتي تسهل للمجرم الالكتروني في ارتكاب اعتداءاته على الدول والمؤسسات وكذا الأفراد، بالإضافة إلى حداثة الموضوع الذي أصبح يشكل خطورة بالغة على المستوى العالمي.

2-الأسباب الموضوعية: تعد الدراسة من الموضوعات ذات الأهمية المتزايدة في العصر الراهن كون الجريمة الكترونية عابرة للحدود والاقاليم فهي مفروضة على العالم حتى في بيئتها الافتراضية ما يجعلها أزمة دولية تدعوا إلى التعاون والتنسيق بوضع حلول جذرية لمكافحتها.

-أهداف الدراسة: تهدف هذه الدراسة الى ما يلي

- ✓ فهم أبعاد الدراسة وبلورة رؤية متكاملة لآليات المواجهة: تهدف هذه الدراسة إلى فهم أبعاد الجرائم الإلكترونية بشكل دقيق، والعمل على بلورة رؤية شاملة وواقعية لآليات مكافحة هذه الجرائم، ضمن إطار قانوني يحترم سيادة القانون ويضمن الحفاظ على مبادئ العدالة والمساواة.
- ✓ تبيان خصوصية الجرائم الإلكترونية والتحديات في الكشف عنها: تهدف الدراسة إلى تسليط الضوء على الخصوصية الفريدة لهذا النوع من الجرائم، والوقوف على الإشكاليات القانونية والعقبات العملية التي تعيق كشف غموض الجرائم الإلكترونية وتحقيق العدالة في قضاياها.
- ✓ البحث في الآليات القانونية لمكافحة الجرائم الإلكترونية: تهدف الدراسة إلى استكشاف الآليات القانونية الفعّالة لمكافحة الجرائم الإلكترونية، مع التركيز على التحديات الناتجة عن غياب تشريع دولي رادع بشكل كافٍ في هذا المجال، وضرورة تطوير أطر قانونية دولية تشترك فيها مختلف الدول لمكافحة هذه الجرائم التي تُرتكب باستخدام أجهزة الحاسوب والأجهزة الإلكترونية المختلفة.

-صعوبات الدراسة:

تتمثل أبرز صعوبات الدراسة في اختيار موضوع البحث ذاته، كونه يتناول مسألة حديثة لم تحظ بعد بدراسات معمقة في الأدبيات القانونية والتقنية. مما يعقد من الوصول إلى مراجع كافية تناولت هذا المجال بشكل تفصيلي. علاوة على ذلك، يرتبط موضوع الدراسة بمجال تكنولوجيا المعلومات، مما يتطلب من الباحث الإلمام التام بمكونات النظام الحاسوبي، وكذلك فهم الأنظمة المتعلقة بالمعالجة الآلية للمعلومات والشبكات الإلكترونية. هذا بالإضافة إلى التحدي الكبير في الوصول إلى بعض المصادر الأساسية، مثل التقارير السرية المتعلقة بالتحقيقات الرقمية، والتي تقتضي اتباع إجراءات قانونية معقدة للحصول على التصاريح اللازمة للوصول إليها. هذه العوامل تشكل عقبات حقيقية أمام الباحث وتقتضي استراتيجيات متخصصة لتجاوزها بشكل يتماشى مع القوانين المعمول بها.

إشكالية الدراسة:

في ظل التقدم التكنولوجي المتسارع، شهد العالم بروزاً ملحوظاً لأنماط جديدة من الجرائم التي يتم ارتكابها باستخدام الوسائل الرقمية الحديثة، والتي تعرف بالجرائم الإلكترونية. هذه الجرائم تتسم بالعديد من الخصائص التي تجعلها فريدة من نوعها، حيث تمتاز بطبيعتها المعقدة، وسرعة تطورها، إضافة إلى قدرتها على الانتشار عبر الحدود الجغرافية دون قيود. وبالرغم من الجهود المبذولة على المستوى الأمني والقضائي، إلا أن الأجهزة المعنية لا تزال تواجه صعوبة بالغة في مكافحة هذه الأنماط الإجرامية، بسبب عدم توافق الأساليب التقليدية مع احتياجات هذه الجرائم الحديثة.

في هذا السياق، تبرز إشكالية أساسية تتعلق بمدى قدرة النظام القانوني الجزائري على التكيف مع هذه الجرائم الإلكترونية المتطورة. وبالرغم من بعض المحاولات لتحديث التشريعات والقوانين المتعلقة بهذا النوع من الجرائم، فإن هناك تساؤلات جدية حول مدى فعالية الإجراءات المتبعة وكفاءتها في كشف الجناة وملاحقتهم، خصوصاً في ظل التطور المستمر للتقنيات المستخدمة في ارتكاب الجرائم الإلكترونية.

من هنا تنبع إشكالية هذا البحث، التي تتمثل في السؤال الآتي: **ما مدى كفاءة آليات البحث والتحري المستحدثة في التعامل مع الجرائم الإلكترونية ضمن التشريع الجزائري، مع تحسين قدرة النظام القانوني على مواكبة التطور التكنولوجي في هذا المجال؟**

كما تتفرع من هذه الإشكالية الرئيسية عدة إشكاليات فرعية تتطلب معالجة دقيقة خلال الدراسة:

- إشكالية ملاءمة التشريعات الحالية لمواجهة الجرائم الإلكترونية: كيف يمكن لتشريعات مكافحة الجرائم الإلكترونية في الجزائر التكيف مع التحديات التي تفرضها تقنيات الجريمة المتطورة، وهل هي كافية لملاحقة الجناة وتقديمهم للعدالة؟

- إشكالية الأدوات التقنية في التحقيق الجنائي: إلى أي مدى تعد الأدوات الرقمية المتاحة اليوم فعالة في جمع الأدلة الرقمية وتتبع الجناة في القضايا الجنائية الإلكترونية؟ وهل تفتقر الأجهزة الأمنية للقوة الفنية الضرورية لمواجهة هذه الجرائم؟
- إشكالية التعاون الدولي في مكافحة الجرائم الإلكترونية: كيف يمكن تعزيز التعاون الدولي بين الدول لمكافحة الجرائم الإلكترونية العابرة للحدود؟ وما هي العراقيل القانونية التي تعترض هذا التعاون؟
- إشكالية حقوق الأفراد في التحقيقات الإلكترونية: كيف يمكن ضمان احترام حقوق الأفراد وحرياتهم في عمليات التحقيق الجنائي المتعلق بالجرائم الإلكترونية، خاصة فيما يتعلق بالخصوصية واستخدام البيانات الشخصية؟
- إشكالية التوعية والتدريب في المجال الجنائي الإلكتروني: ما هو دور التوعية والتدريب المتخصص للمحامين والقضاة والأجهزة الأمنية في تحسين التعامل مع الجرائم الإلكترونية؟

من خلال هذه الإشكاليات الفرعية، تسعى الدراسة إلى فحص مدى فعالية الأساليب المتبعة في التحقيقات الجنائية الإلكترونية، ومدى تكاملها مع أحدث التطورات التكنولوجية، بالإضافة إلى تقديم توصيات لتطوير النظام القانوني لمواكبة التحديات المستقبلية في هذا المجال.

-منهجية البحث:

اقتضت طبيعة البحث الاستعانة بعدة مناهج تتكامل فيما بينها وهي:

- المنهج الوصفي: عند التطرق إلى المفاهيم العامة حول الجرائم الالكترونية وبيان خصائصها وشروطها وكذا وصف الآليات المستخدمة في عملية البحث والتحري عن هذا الجرائم.

- المنهج التحليلي: عند تحليل نصوص قانون الإجراءات الجزائية والمتعلقة بآليات البحث والتحري في الجرائم الالكترونية.

- المنهج الاستقرائي: اذ يعد من المناهج المساعدة في البحث، حيث يتيح تتبع واستقصاء المسائل والجزئيات المتعلقة بجوانب الموضوع، واستخلاص النتائج من ذلك.

-خطة البحث:

وحتى نتمكن من معالجة هذا الإشكالات المطروحة ارتأينا الى تقسيم الخطة للدراسة إلى فصلين معتمدين على التقسيم الثنائي للخطة، بحيث تناولنا في الفصل الأول المعنون بالإطار النظري للجريمة الالكترونية والمقسم الى مبحثين الأول متعلق بمفهوم الجريمة الالكترونية، أما المبحث الثاني فهو يتحدث على بعض التصنيفات للجرائم الالكترونية والأطراف المشاركة في تكوين الجريمة إضافة الى موقف بعض التشريعات في مواجهتها والحد منها، أما الفصل الثاني المعنون بضوابط البحث والتحري في الجرائم الالكترونية فهو يتحدث عن المحققين والأجهزة المكلفة بالبحث والتحري عن الجرائم الالكترونية

واختصاصاتها في المبحث الأول، وكذا الوسائل والإجراءات العامة والخاصة أي التقليدية والمستحدثة في الكشف عن مرتكبي الجريمة الالكترونية في المبحث الثاني.

الفصل الأول

الإطار المفاهيمي للجريمة الالكترونية

مهيـــــد:

مع التحول التدريجي المتسارع نحو الرقمنة، الذي سعى إلى انتشار التقنيات الرقمية العالية الأداء والتي أعاد تشكيلة الهياكل الاجتماعية والاقتصادية معا، أضحت التكنولوجيا وليدت هذه التحولات حيث غدت محورا أساسيا وجزء لا يتجزأ في تكوين البنية التحتية للمجتمعات الحديثة من خلال تنظيم العلاقات الإنسانية داخل الأوساط وإدارة الأنشطة اليومية، استدعى ذلك إلى نشوء فضاءات الكترونية هي ليست مجرد وسائط للتواصل والمعرفة على حد وصفها التقليدي تتيح فرصا هائلة للعمل فيها بإيجابية، بل ساحة افتراضية تستفيد من الخصائص التقنية للأنترنت وتستغل لارتكاب أنماط مبتكرة من السلوك الإجرامي، مما أفرز ظاهرة الجريمة الالكترونية بوصفها نتاجا معقدا للتفاعل بين التطور التقني من جهة والتحولات الاجتماعية والاقتصادية من جهة أخرى.

ومن هذا المنطلق سعت دراستنا في هذا الفصل إلى إبراز الإطار النظري من خلال تأصيل مفهوم الجريمة الالكترونية ولكون الجريمة حديثة النشأة يظهر الاختلاف في تحديد المصطلحات الدقيقة لها، وقد انتج ذلك عن ظهور عدة اتجاهات مختلفة الآراء، ثم بعد سننتقل لتحديد السمات التي تميز الجريمة الالكترونية عن باقي الجرائم التقليدية الأخرى، وسنتناول كذلك دراسة الأركان القانونية لهذه الجريمة والتي تعد أساسية لفهم طبيعتها القانونية وتفسير سلوك الجناة، كما يتم تسليط الضوء أيضا على التصنيفات المتنوعة التي تقع بواسطة استخدام المكونات المادية و البرمجيات الخاصة بالأنظمة المعلوماتية وغيرها، والتفرقة بين الأنواع المختلفة للجريمة بناءا على الأداة المستخدمة ووسيلة التنفيذ من خلال معرفة مدى الثغرات البرمجية، والهجمات الموجهة على الأنظمة المعلوماتية وكذا القرصنة الالكترونية، إلى جانب ذلك سيتم تناول العوامل المؤدية إلى ارتكابها ضمن سياقات اجتماعية ونفسية وتقنية من شأنها التأثير على الافراد بمختلف اطيافهم والغاية من تحقيق أهدافهم.

المبحث الأول: مفهوم الجريمة الالكترونية

أدى الاعتماد المتزايد للتقنيات الرقمية إلى بروز الجريمة الالكترونية كنوع جديد من الجرائم، مما أثار جدلا فقهيا واسعا حول تعريفها وتحديد طبيعتها القانونية، فقد تباينت الآراء بين الفقهاء حول ما إذا كانت الجريمة الالكترونية تعد شكلا مستقلا عن الجرائم أم مجرد امتداد لجرائم تقليدية بأدوات جديدة، يعنى هذا البحث بتحديد مفهوم الجريمة الالكترونية، خصائصها وتمييز مساميا تها المختلفة بالتفصيل التالي:

المطلب الأول: تعريف الجريمة الالكترونية

شهد العالم مع تطور التكنولوجية الرقمية ظهور شكل جديد من الإجرام يعرف بالجريمة الالكترونية، يتمثل في استخدام الوسائط التكنولوجية لارتكاب أفعال غير مشروعة. وقد رافق هذا التطور تحديات قانونية في التكييف والإثبات، خاصة في ظل غياب تعريف موحد لهذه الجريمة.

الفرع الأول: التعريف الفقهي للجريمة الالكترونية

- **التعريف المرتكز على الفاعل في الجريمة**

يُعرّف "دافيد تومبسن" الجرائم المعلوماتية من منظور فاعل الجريمة بأنها "جرائم يتطلب ارتكابها توافر قدرٍ من المعرفة التقنية المتقدمة لدى الجاني، ولا يُتصور تحققها دون إلمامه بمهارات استخدام الحاسب الآلي والأنظمة المرتبطة به".[2]

- **التعريف المرتكز على وسيلة ارتكاب الجريمة[3]**

يعرف الفقيه الألماني LAUS TIEDEMAUN و CARLE BENSON " على أنها "كل أشكال السلوك غير المشروع-أو الضار بالمجتمع- الذي يرتكب باستخدام الحاسوب" أما الأستاذ LESLIE DE BALL" فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية " وانها " الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية".

كم عرفها الأستاذان R. TATTY و Hand CASTELبانها " تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسب وبعبارة أخرى تلك الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر من سبل".

---

[2] د. نادية أيت عبد المالك، د. عبد القادر فلاح، **التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد04، العدد02، جامعة الجيلالي بونعامة-خميس مليانة، السنة 2019، ص 1692.

[3] معاشي سميرة، **الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية)**، مجلة المفكر العدد 17، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، جوان 2018، ص 403-402

يُعرف بعض فقهاء القانون، ومن بينهم "ميشال" و"ريدو"، الجريمة المعلوماتية بأنها نمط من أنماط السلوك الإجرامي المرتبط بإساءة استعمال أنظمة الحوسبة، ويتجلى ذلك في صور متعددة، من بينها الدخول غير المشروع إلى نظم أو بيانات الحاسوب العائدة للغير، أو استخدام وسائل الدفع الإلكتروني بغير وجه حق، إلى جانب التعدي على أنظمة المعالجة الإلكترونية للمعطيات المالية، وتزوير العناصر المادية أو البرمجية المكونة للحاسوب، فضلاً عن الاستيلاء على الجهاز المعلوماتي ذاته أو أحد أجزائه المكونة له، سواء كان ذلك بقصد التملك أو التعطيل.[4]

- **التعريف المرتكز على موضوع الجريمة[5]**

يعرف الفقيه ROSANBLATTبان الجريمة "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحول عن طريقه".

كما عرفتها **الدكتورة هدى قشقوش** بأنها " جرائم الاعتداء على الأموال المعلوماتية وهي عبارة عن الأدوات المكونة للحاسب الإلكتروني وبرامجه ومعداته".

"وقد عرّفها مكتب تقييم التكنولوجيا التابع للولايات المتحدة بأنها تلك الأفعال غير المشروعة التي تُعد البيانات الحاسوبية والبرمجيات المعلوماتية عنصراً جوهرياً في تنفيذها."[6]

الفرع الثاني: التعريف القانوني للجريمة الالكترونية

من التعاريف القانونية المشهورة للجريمة تعريف العالم سدرلاند الذي يقول فيه: " أن الجريمة هي السلوك الذي تجرمه الدولة لما يترتب عليه من ضرر على المجتمع، والذي تتدخل لمنعه بعقاب مرتكبيه"، ويرتبط تعريف الجريمة من هذه الناحية بقانون العقوبات من جهة، وبالمجتمع من جهة أخرى، فهي فعل ما يعاقب عليه المجتمع ممثلا في مشرعه، لما ينطوي عليه هذا الفعل من المساس بشرط يعده المجتمع من الشروط الأساسية لكيانه أو الظروف المكملة لهذ الشروط.[7]

عرف مؤتمر الأمم المتحدة في سنة 2000 الجريمة الالكترونية، بأنها الجريمة التي يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام الحاسوب، أو في بيئة الكترونية.

---

[4] يزيد بوحليط، **الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات–قانون الإجراءات الجزائية– قوانين خاصة**، دار الجامعة الجديدة، الإسكندرية، 2019، ص34.

[5] د. نادية أيت عبد المالك، ط.د. عبد القادر فلاح، **التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري**، المرجع السابق، ص 1693.

[6] د. يعيش تمام شوقي، **الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، سلسلة مطبوعات المخبر، مخبر أثر الاجتهاد القضائي على حركة التشريع**، الطبعة الأولى، مطبعة الرمال، جامعة محمد خيضر، بسكرة، جانفي 2019، ص19.

[7] لامية طالة، كهينة سلام، **الجريمة الالكترونية: بعد جديد لمفهوم الاجرام عبر منصات مواقع التواصل الاجتماعي**، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد 06 العدد 02، جامعة الجزائر 3، 2020، ص67.

وعرفها أيضا خبراء منظمة التعاون الاقتصادي والتنمية، الجريمة الالكترونية بأنها: كل سلوك غير مشروع أو غير أخلاقي أو غير مصر به يتعلق بالمعالجة الآلية للبيانات و/أو نقلها.[8]

إن الانتشار التي احدثته الجرائم الالكترونية واتساع نطاقها أصبح من الضروري التصدي لهذه الظاهرة التي أصبحت تمس بالأمن الوطني الأمر الذي ترتب عنه تعديل الكثير من التشريعات الوطنية والدولية وإدخال هذا النوع من الجرائم ضمن نطاق الأفعال المجرمة التي يعاقب عليها القانون وتخصيص عقوبات تحد من انتشارها واتساعها، وعلى اعتبار أن وضع وضبط تعاريف للمفاهيم القانونية لا يدخل ضمن نطاق اختصاص المشرع فإن المشرع الجزائري وبموجب تعديل قانون العقوبات سنة 2004 عمل على تجريم الجرائم الالكترونية التي أصبحت تنتشر في المجتمع الجزائري مع بداية توجهه نحو المعلوماتية والانفتاح على العالم الرقمي، واستحدث بذلك قسما خاصا بالعقوبات المطبقة على الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، ومع انتقال الجزائر نحو انتهاج استراتيجية الجزائر الالكترونية وظهور بوادر التحول الالكتروني لجميع المؤسسات والهيئات والإدارات العمومية وجد المشرع الجزائري واقعا يفرض استحداث قانون جديد أكثر عمقا لمعالجة الجرائم الالكترونية وما يتعلق بها من تجاوزات تمس الأفراد والمؤسسات فصدر بذلك سنة 2009 أول نص قانوني متعلق بالجرائم الالكترونية ومكافحتها والذي وضع من خلاله المشرع الجزائري تعريفا للجرائم الالكترونية التي اصطلح عليها بمصطلح الجرائم المتصلة بتكنولوجية الاعلام والاتصال وذلك لاستبعاد الغموض والمرونة التي تتميز بها التعاريف الفقهية لهذا النوع من الجرائم ونص بناءا على هذا بأن " **الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية**".[9]

الفرع الثالث: تسميات مختلفة للجريمة الالكترونية

- **مصطلح جرائم اقتصادية مرتبطة بالكمبيوتر**: يُطلق هذا المصطلح على فئة من الجرائم المعلوماتية التي تنصرف إلى الاعتداء على نظم المعلومات الخاصة بالكيانات الاقتصادية ومؤسسات الأعمال، وذلك من خلال الإخلال بمبادئ أمن المعلومات، ولا سيما السرية، وسلامة المحتوى، وتوافر البيانات. ومن ثم، فإن هذا التوصيف لا يستوعب كافة صور الجرائم المعلوماتية، إذ يستثني من نطاقه تلك التي تستهدف البيانات ذات الطابع الشخصي، أو التي تمس الحقوق

[8] د. عبد السلام محمد المايل، د.عادل محمد الشريجي، د.علي قابوسة، **الجريمة الالكترونية في الفضاء الالكتروني المفهوم–الأسباب–سبل المكافحة مع التعرض لحالة ليبيا**، مجلة أفاق للبحوث والدراسات سداسية، دولية محكمة، العدد 04 جوان 2019، المركز الجامعي ايليزي، ص 246.

[9] د. سمية بهلول، د. عماد دمان ذبيح، **الاليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري**، مجلة الحقوق والعلوم السياسية، العدد 13 جانفي 2020، ص141

المعنوية للمؤلفات الرقمية، فضلاً عن الجرائم المتعلقة بالمحتوى الضار أو غير المشروع. وعليه، فإن هذا التعبير يظل قاصرًا عن الإحاطة بالإطار الكلي والشامل للظاهرة الإجرامية في البيئة المعلوماتية..[10]

- **مصطلح جرائم أصحاب الياقات البيضاء:** ولان الدقة العلمية تقتضي انطباق الوصف على الموصوف فإن هذه الجرائم تتسع لتشمل أكثر من الجرائم المعلوماتية وتتصل بمختلف أشكال الأفعال الإجرامية في بيئة الأعمال بأنواعها وقطاعاتها المختلفة فان الاصطلاح لذلك لا يكون دقيقا في التعبير عن الظاهرة مع الإشارة إلى أن جرائم الكمبيوتر تتصف بهذا الوصف لكنها جزء من طوائف متعددة من الجرائم التي يشملها هذا الوصف [11]
- **مصطلح جرائم الكمبيوتر:** هي الأنشطة التي تستهدف المعلومات والبرامج المخزنة داخل نظم الكمبيوتر، وتحديدا أنشطة التزوير واحتيال الكمبيوتر وسرقة المعطيات وسرقة وقت الآلة واعتراض المعطيات خلال النقل برغم اتصال هذا المفهوم بالشبكات أكثر من نظم الكمبيوتر، إضافة للتدخل غير مصرح به لنظام الكمبيوتر ودخول غير مصرح به للشبكات.[12]
- **مصطلح جرائم الانترنت:** تُعد هذه الجرائم نمطًا من الأفعال غير القانونية التي يُعتمد في تنفيذها على الوسائط الإلكترونية أو شبكات الاتصال الرقمية، أو تُستخدم تلك الوسائط كقنوات لنقل أو بث محتواها غير المشروع، وهي بطبيعتها تتطلب خبرة تقنية متقدمة في مجال نظم المعلومات والحوسبة، سواء عند ارتكابها أو أثناء متابعتها جنائيًا".
- **مصطلح الجريمة المعلوماتية:** يطلق هذا المصطلح على أية جريمة ضد المال المرتبطة باستخدام المعالجة الآلية للمعلومات، كما تعرف بأنها: " مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب، كما تعرف أيضا بأنها مجموعة الجرائم المتصلة بعلم المعالجة المنطقية للمعلومات.[13]

المطلب الثاني: اركان الجريمة الالكترونية وخصائصها

تقوم الجريمة الالكترونية كغير من الجرائم على أركان قانونية محددة فهي ضرورية لتحديد المسؤولية الجنائية وكذا وضع السياسات القانونية والأمنية المناسبة من أجل مكافحة هذا النوع من الجرائم وفي هذا المطلب سنتطرق لعرض لك بالتفصيل إضافة إلى ذات معرفة الخصائص التي تتميز بها هذه الجريمة.

[10] أيمن عبد الله فكري، **الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية**، مكتبة القانون والاقتصاد، طبعة الأولى، الرياض، 2014، ص 87.

[11] أيمن عبد الله فكري، نفس المرجع.

[12] يزيد بوحليط، **الجرائم الالكترونية والوقاية منها في القانون الجزائري**، المرجع السابق، ص 46.

[13] لامية طالة، كهينة سلام، **الجريمة الالكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي**، المرجع السابق، ص 67

الفرع الأول: اركان الجريمة الالكترونية

أولا: الركن الشرعي

لا يمكننا الحديث عن قيام أي جريمة إذا كانت مخالفة لقواعد القانون الذي يكون أساسه تطابق السلوك والنص القانوني الذي يجرمه سواء كان النشاط فعلا أو امتناع، فلا جريمة ولا عقوبة إلا بنص، ولذا الركن عنصرين، مطابقة الفعل لنص التجريم وألا يخضع الفعل المرتكب لسبب من أسباب الإباحة، ونجد المشرع الجزائري استحدث القسم السابع مكرر بعنوان المساس بالأنظمة المعالجة الآلية للمعطيات من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال.[14]

معناه اعتراف بتجريم الفعل المرتكب وهو ما نصت عنه المادة الأولى من قانون العقوبات، أي لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون وهذا ما نقصد به مبدأ الشرعية القوانين، أما بالنسبة للجريمة المعلوماتية، فالمشرع الجزائري قد أحدث في قانون العقوبات في القسم السابع المكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات. وكذا القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وبعض النصوص الأخرى.[15]

وقد نظم المشرع الجزائري الجريمة الالكترونية من خلال القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، وأدرج كذلك أحكاما جزائية في قانون العقوبات الجزائري خاصة المواد من 394 مكرر الى 394 مكرر8، ومن خلال المادة 394 مكرر1 يتضح لنا أن المشرع جرم الدخول الى منظومة المعلوماتية وهذا ما يؤسس الركن الشرعي لهذا النوع من الأفعال.[16]

ثانيا: الركن المادي

يتكوَّن الركن المادي في الجريمة الإلكترونية من عناصر ثلاثة: الفعل الإجرامي، والنتيجة الإجرامية، والعلاقة السببية التي تربط بينهما. غير أن تحقق هذا الركن لا يستلزم دائمًا وقوع النتيجة فعليًا، إذ قد يُعتد بالفعل وحده متى كان من شأنه أن يؤدي إلى النتيجة، كما هو الحال في الإبلاغ عن الجريمة قبل اكتمال آثارها، كأن يقوم الفاعل بإنشاء موقع إلكتروني بقصد

[14] خالد شكري، أبوبكر لراشي، **التحقيق وجمع الأدلة في مجال الجرائم الالكترونية**، مذكرة لنيل شهادة الماستر علوم في القانون، كلية الحقوق والعلوم السياسية، جامعة أمحمد بوقرة بومرداس، سنة 2022-2023، ص 15

[15] أحمد عبد العزيز، **خصوصية التحقيق في الجريمة المعلوماتية**، مذكرة لنيل شهادة ماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي سعيدة، سنة 2021-2022، ص17

[16] قانون رقم 09-04 المؤرخ في 05 أغسطس 2009، يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 44.

التشهير بشخص معين دون نشره فعليًا على الشبكة، فذلك لا ينفي قيام السلوك الإجرامي، ولا يحول دون مساءلة مرتكبه. ويأخذ الركن المادي في هذا النوع من الجرائم صورًا متعددة تتفاوت باختلاف الأفعال الإيجابية المرتكبة، ومن أمثلتها جريمة التزوير المعلوماتي، التي يتحقق ركنها المادي من خلال التلاعب بالحقيقة في السجلات أو الوثائق الإلكترونية.[17]

ليكتمل الركن المادي للجريمة الالكترونية يجب أن تتوفر عناصره على النحو التالي:

-**السلوك الإجرامي:** يعد السلوك الإجرامي الأمر الذي يصدر من الفاعل ويخشى المشرع منه ضررا على الأشخاص فما لم يصدر من الفاعل نشاط في صورة من صوره لا يتدخل المشرع بالعقاب وهي أعمال خارجية تختلف باختلاف الجرائم

-**النتيجة الإجرامية:** هي الأثر الذي يترتب على السلوك الإجرامي والمقرر حمايتها

-**العلاقة السببية:** وهي الصلة ما بين السلوك الإجرامي والنتيجة الإجرامية، بحيث تثبت بأن السلوك الإجرامي الواقع هو الذي أدى إلى حدوث تلك النتيجة الضارة، على أنه يمكن لبعض صور هذه الجرائم أن يتحقق الركن المادي دون تحقق النتيجة وهو ما يطلق عليه بالجرائم الشكلية تكتفي بعنصر واحد الذي هو النشاط لقيام ركنها المادي، وفي هذه الحالة نكون أمام جريمة قائمة بحد ذاتها دون الحاجة للبحث في النتيجة المتحققة أو العلاقة السببية حتى وإن كان وجودها من طبيعة مادية فليس له أثر قانوني، كإنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة لكن بالرغم من ذلك فلا مناص من معاقبة الفاعل ومن ثم فيتخذ الركن المادي في الجرائم الالكترونية عدة صور سنتطرق لها[18]

ثالثا: الركن المعنوي

يتخذ الركن المعنوي في اغلب الجرائم بصفة عامة صورة القصد الجنائي، والذي يتحقق بتوافر إرادة بعمل غير شرعي لدى الجاني مع علمه بان القانون يجرمه، ونفس الامر ينطبق على الجريمة المعلوماتية التي يقوم ركنها المعنوي على توافر الإرادة الجرمية لدى الفاعل، وهذا ما يظهر من خلال استعمال المشرع الجزائري لعبارة "الغش" و "العمد" و"الاعداد لجريمة" في المواد 394مكرر و394مكرر 1 و 394 مكرر 2 وفي الأخير 394 مكرر 5، من ق.ع، وهذا أن دل فإنما يدل على أن الجريمة المعلوماتية جريمة عمدية بامتياز ولا يفترض فيها عنصر الخطأ. وهذا ويختلف الركن المعنوي في الجرائم المعلوماتية من جريمة الى أخرى فجريمة الدخول غير المصرح به الى نظام الحاسب الآلي تتطلب قصدا جنائيا يتمثل في علم الجاني بعناصر الركن المادي للجريمة، أي العلم بأن الولوج إلى داخل النظام بشكل غير مصرح يعد جريمة باعتبار حماية المشرع لمحل

[17] لامية طالة، كهينة سلام، **الجريمة الالكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي**، المرجع السابق، ص69

[18] خالد شكري، أبوبكر لراشي، **التحقيق وجمع الأدلة في مجال الجرائم الالكترونية**، المرجع السابق، ص15-16

الحق وهو الحاسب الآلي لما يتضمنه من برامج ومعلومات[19]، ومثال ذلك إذا قام شخص باختراق قاعدة بيانات مؤسسة بنية تدمير أو تسريب معلومات سرية، فإن توفر العلم بالفعل والإرادة فيه يشكل الركن المعنوي[20]

الفرع الثاني: خصائص ومميزات الجريمة الالكترونية

أولا: جريمة عالمية عابرة للحدود

تُصنّف هذه الجريمة ضمن الجرائم غير التقليدية التي يُرتكب فيها الفعل الإجرامي عن بُعد، دون حضور مادي مباشر للفاعل في مكان ارتكاب الجريمة، مما يُنتج انفصالًا بين محل الجريمة وشخص مرتكبها. وتُعدّ هذه السمة من الخصائص الجوهرية للجريمة المعلوماتية، والتي وصفها الأستاذ محمد محيي الدين عوض بأنها تمثل صورة مستحدثة من الجرائم ذات الطابع العابر للحدود، سواء كانت وطنية أو إقليمية أو قارية، نظرًا لقدرتها على تجاوز النطاق الإقليمي للدولة التي يُوجد بها الجاني"[21]، فهذه الميزة للجريمة، لا تستثنى أحد، فكل دول العالم مهددة بهذا النوع من الجرائم في ظل الانتشار الهائل للعمل بشبكة الاتصالات الدولية الانترنت، الأمر الذي سهل عمل مجرمي الفضاء الافتراضي في استهداف الضحية في أي زمان ومن أي مكان، وتخطت بذلك الجرائم الالكترونية كل الحدود الدولية[22]، ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون الى استخدام هذه التقنيات في خرقهم للقانون

ومثال ذلك ما قام به أحد مجرمي المعلومات وهو فليبيني الجنسية الذي قام بصنع فيروس يسمى "ILOVE YOU" عام 2000، والذي يقوم بالعديد من التغييرات الضارة بنظام الاستخدام للحواسيب الآلية، وقد انتشر هذا الفيروس في مختلف دول العالم عن طريق البريد الالكتروني حيث تسبب في خسائر تجاوزت 5.5 مليار دولار في ظرف عشرة (10) أيام، كما تم التبليغ عن 50 مليون إصابة في نفس الفترة، من جهة أخرى وحسب إحصاء قامت به شركة

[19] حمز خضري، عشاش حمزة، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، مجلة الدراسات القانونية والسياسية، المجلد 06 العدد 02، جامعة محمد بوضياف، المسيلة، جوان 2020، ص 174-175.

[20] عبد الله أوهايبية، شرح قانون العقوبات – القسم الخاص- دار هومة، الجزائر، 2016، ص 272.

[21] معاشي سميرة، **الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)**، المرجع السابق، ص 15.

[22] فتيحة حيمر، **تأثير الجريمة الالكترونية على الأمن في إفريقيا**، مجلة أبحاث قانونية وسياسية، المجلد 09، العدد01، جامعة على لونيسي البليدة 02، الجزائر، جوان 2024، ص 548.

"SYMANTEC" الأمريكية لحماية الشبكة الالكترونية فإن المعدل السنوي لكلفة الجرائم الالكترونية حول العالم تبلغ 114 مليار دولار.[23]

ثانيا: صعوبة اكتشاف الجريمة الالكترونية وإثباتها:

تتجلى صعوبة إثبات هذا النوع من الجرائم في غياب الآثار المادية المباشرة التي يمكن معاينتها أو ضبطها، وهو ما يحدّ من إمكانية تتبع الجريمة وإثباتها بالأدلة التقليدية، ويُفاقم من ذلك الطابع العابر للحدود لهذه الجرائم، مما يُعقّد من إجراءات الملاحقة القانونية. وتشير الإحصائيات إلى أن ما يتم اكتشافه من جرائم المعلوماتية لا يتجاوز 1% من مجمل الوقائع المرتكبة، في حين أن ما يتم الإبلاغ عنه من هذا الرقم ضئيل للغاية، ولا يتعدى نسبة 5%.

والوسيلة المستخدمة لارتكاب الجريمة هي نبضة الكترونية ينتهي دورها خلال أقل من ثانية واحدة، كأن الجاني يقوم بتدمير الدليل بمجرد استعماله ويقوم بذلك بكل هدوء دون إحداث أية ضجة، وذلك على خلاف الكثير من الجرائم التي نعرف[24]، لذا يستلزم احداث طرقا جديدة لإثبات الجريمة، قوامها التعليم والتدريب المتخصص المستمر لعلوم الحاسب الآلي، إذ يقتضي ذلك وجود رجل شرطة الكتروني، ومحقق الكتروني ، وقاضي الكتروني فضلا عن الخبير الالكتروني حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم، وعليه فإن الاستعانة بالخبراء تصبح حتمية لكشف وتحليل وتفسير الدليل الجنائي، الذي يثبت البراءة أو الإدانة.[25]

ثالثا: الجريمة الالكترونية جريمة خفية

توصف الجرائم الإلكترونية بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات، وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم[26]، وكإضافة لهذه الخاصية نجد أن هذه الجريمة يصعب فيها الحصول على دليل مادي، حيث تغلب الطبيعة الالكترونية على الدليل المتوفر. ولعل صعوبة كشف الدليل تزداد بصورة

[23] الطاهر زخمي، **الجرائم المعلوماتية في التشريع الجزائري وتدابير الوقاية منها، مجلة التشريع الإعلامي**، المجلد02 العدد 01، كلية علوم الإعلام والاتصال، جامعة الجزائر 3، سنة 2023، ص 6.

[24] عبد الله دغش العجمي، **المشكلات العملية والقانونية للجرائم الالكترونية (دراسة مقارنة)**، رسالة لاستكمال الحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، سنة 2014، ص 21.

[25] فاطيمة دهان–كلثوم دهان، **إجراءات البحث والتحري في الجرائم المعلوماتية**، مذكرة تخرج لنيل شهادة ماستر أكاديمي، كلية الحقوق والعلوم السياسية، جامعة غرداية، سنة 2022/2021، ص 15.

[26] رحموني محمد، **خصائص الجريمة الالكترونية ومجالات استخدامها**، مجلة الحقيقة العدد 41، جامعة أحمد دراية، أدرار، جانفي 2018، ص 441.

خاصة متى ارتكبت هذه الجريمة في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة في هؤلاء يسهل عليهم اقتراف جرائمهم دون أن يتركوا آثار تدل عليهم.[27]

رابعا: الجريمة الالكترونية جريمة ناعمة وهادئة

وعلى خلاف الجرائم التقليدية التي تستلزم في الغالب استعمال القوة البدنية أو القيام بأفعال مادية مباشرة كالقتل أو السرقة، فإن الجرائم الإلكترونية تُرتكب بوسائل غير مادية، ولا تتطلب أي مجهود عضلي يُذكر، إذ تقوم أساساً على استخدام المعرفة التقنية والمهارات الذهنية المتقدمة في مجال الحاسب الآلي والاتصالات.[28] وغالباً ما يكون الجاني في هذا النوع من الجرائم شخصاً متمرساً في التعامل مع الأنظمة المعلوماتية، ويتسم بدرجة عالية من الذكاء والتمكن التقني، ولا يُعد بالضرورة عنصراً متمرداً على النظام الاجتماعي، بل قد يقدم على ارتكاب الفعل الجرمي بدافع التسلية، أو لإثبات قدراته على تجاوز الأنظمة الأمنية، أو سعياً لتحقيق مكاسب خاصة بطرق غير مشروعة.[29]

خامسا: الجريمة الالكترونية سريعة التنفيذ

ففي غالب الأحيان يكون الركن المادي لها مجرد ضغط على مفتاح معين في الجهاز وتنفيذ الجريمة عن بعد دون اشتراط التواجد في مسرح الجريمة لذلك فهي تشكل عنصر إغراء للمجرمين [30]

سادسا: عدم وجود مفهوم مشترك للجريمة الالكترونية

لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي، أو الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية

ومن جهة نظر الباحث فإنه يفضل اصطلاح الجريمة الالكترونية للدلالة على الجرائم المرتكبة بواسطة الحاسوب والانترنت، فاصطلاح الجريمة الالكترونية عام ويشتمل وسائل الاتصال الالكتروني الحالية والمستقبلية المستخدمة في التعامل مع البيانات وتبادلها [31]

---

[27] فاطيمة دهان، كلثوم دهان، **إجراءات البحث والتحري في الجرائم المعلوماتية**، المرجع السابق، ص 15.

[28] غنية عباس، **الجريمة الالكترونية في البيئة الرقمية ومدى تأثيرها على الجريمة المنظمة العابرة للحدود الوطنية**، المجلة الجزائرية للسياسات العامة، المجلد 12 العدد 03، جامعة لونيسي على البليدة، ديسمبر 2024، ص 89.

[29] لامية طالة، كهينة سلام، **الجريمة الالكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي**، المرجع السابق، ص 75.

[30] خالد شكري، أبوبكر لراشي، **التحقيق وجمع الأدلة في مجال الجرائم الالكترونية**، المرجع السابق، ص13.

[31] عبد الله دغش العجمي، **المشكلات العملية والقانونية للجرائم الالكترونية (دراسة مقارنة)**، المرجع السابق، ص 22-23.

سابعا: الجريمة الالكترونية جريمة مستحدثة

تعد الجرائم الالكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، فلا غرابة أن تعد الجرائم الالكترونية سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها من الجرائم المستحدثة، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمها وأمن مواطنيها. [32]

ثامنا: جريمة آثارها وخيمة على الصعيد الاقتصادي

نظرا لشمول شبكة الانترنت والكمبيوتر أجهزة اقتصادية حساسة شملت أغلب معاملاتها، حيث تسببت الجرائم المعلوماتية بتكبيد هذه المؤسسات والشركات خسار مالية ضخمة نتيجة اختراق أنظمتها المعلوماتية من طرف مجرمين مختصين في هذا المجال إضافة إلى سرقة أموال كبيرة من عديد البنوك باختراق حسابات الزبائن، وتدمير نظام التشغيل أو نشر فيروسات أو إفشاء بيانات، حيث قدرت الخسائر المادية في نهاية القرن الماضي ما يقارب 500 مليون دولار في السنة حسب احصائيات المركز الوطني لجرائم الحاسوب بالولايات المتحدة الأمريكية (NCCCD)[33]

تاسعا: جريمة تتطلب خبرة فنية وتحكم في تكنولوجيا المعلوماتية أثناء التحقيق والمتابعة

نظراً للطابع الفني والتقني المعقّد الذي تتسم به الجريمة المعلوماتية، تقتضي الضرورة أن يتوفر لدى القائمين بمهام التحري والتحقيق، سواء من عناصر الضبطية القضائية أو المحققين، تأهيل متخصص في هذا النوع من الجرائم، بما يضمن مباشرتهم للإجراءات بكفاءة ومهنية عالية خلال مرحلتي البحث والاستقصاء.

كما تفرض طبيعة هذه الجرائم المتجددة مواكبة دائمة للتطورات التكنولوجية المستحدثة، والإلمام بالوسائل التقنية والإجرائية الكفيلة بمواجهتها. ويعدّ التدريب المستمر وتبادل المعارف بين المختصين، على المستويين الوطني والدولي، من المتطلبات الأساسية لبناء قدرات فعّالة في هذا المجال.

ويُعدّ تفعيل التعاون الدولي أداة استراتيجية لتطوير الكفاءات، من خلال الاستفادة من خبرات وممارسات الدول المتقدمة في التصدي للجرائم المعلوماتية. كما تلعب الخبرات العلمية والتقنية دوراً محورياً في الكشف عن الدليل الإلكتروني، مع ما

[32] عبد الله دغش العجمي، نفس المرجع، ص 25.

[33] د. بن دراح علي إبراهيم، **مطبوعة بيداغوجية بعنوان: محاضرات في الجرائم المعلوماتية**، طلبة السنة الثانية ماستر، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، سنة 2020-2021، ص 8.

يتطلبه ذلك من قدرة على تمييز طبيعته، سواء كان في شكل مستندات رقمية، برمجيات، تطبيقات، اتصالات إلكترونية، أو صور رقمية وغيرها من الوسائط الرقمية ذات الصلة.[34]

الفرع الثالث: أنواع الجريمة الالكترونية

1- **جريمة الدخول والبقاء غير المشروع في نظام المعالجة الالية للمعطيات:** بمعنى دخول الشخص إلى شبكة الإنترنت دون الحصول على إذن صريح من الجهة المخولة قانونًا بمنح هذه الصلاحية، سلوكًا إراديًا يشكل صورة من صور المساس غير المشروع بالأنظمة المعلوماتية، وذلك من خلال تجاوز وسائل الحماية التقنية بهدف الوصول إلى بيانات أو معطيات إلكترونية. وقد تناول المشرّع هذا الفعل في نص المادة 394 مكرر من قانون العقوبات، حيث جرم الدخول غير المصرح به أو البقاء غير المشروع ضمن منظومة معلوماتية دون علم أو رضا صاحب الحق، واعتبر ذلك جريمة قائمة بذاتها حتى في غياب ضرر فعلي.

2- **تخريب أو إتلاف أجهزة المعلوماتية أو احدى مكوناتها:** عن حماية شبكة المعلوماتية يستلزم التدخل لتجريم الأفعال التي تهدف إلى تخريب أو تعطيل أو إتلاف الأجهزة المادية والمتمثلة في الحاسوب أو البيانات والمعلومات الموجودة بداخله لأن علة التجريم هي حماية المعلومات والأجهزة المادية من أفعال التخريب

3- **الغش أو التغيير في مواصفات وخصائص تقنية المعلومات:** تتحقق الجريمة متى باشر الجاني سلوكاً إيجابياً ينطوي على تدليس أو احتيال، ترتب عليه إحداث تغيير في خصائص أو مواصفات نظم المعلومات أو مكوناتها أو ما يُعد في حكمها، على نحو يؤدي إلى غش تقني يُشكل تعدياً على حقوق الملكية الفكرية، ويُعدّ فعلاً مجرّماً وفقاً للأحكام القانونية الناظمة لهذا النوع من الأفعال.

4- **صناعة الفيروسات أو نشرها:** وهي وسيلة تستخدم لتدمير المعلومات والبيانات والبرامج وتعطيل شبكة المعلومات

5- **سرقة الأجهزة أو المكونات أو المعلومات وما في حكمها:** تعتبر جريمة سرقة وإخلال بحقوق الملكية الفكرية أو براءة الاختراع أو العلامات المسجلة على أساس أن محل السرقة الحاسوب ككيان مادي

6- **جرائم الإرهاب والاعتداء على الملكية الفكرية:** إن المتضرر الأول من إساءة استخدام شبكة المعلوماتية حقوق الملكية الفكرية سواء ما يتعلق منها بحقوق المؤلف أو الحقوق المجاورة والمتعلقة بالبرامج والإصدارات الخاصة بنظم المعلومات أو بالمصنفات الفكرية أو الأدبية أو الأبحاث العلمية التي باتت متاحة على شبكة المعلوماتية أو بالمصنفات الفكرية أو الأدبية أو الأبحاث العلمية التي باتت متاحة على شبكة المعلوماتية ويتم نسخها وتداولها

[34] سويسي فتيحة، **التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها**، مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية، 18 جانفي 2022، ص 9.

دون أن تنسب إلى صاحبها الأصلي وهو ما يلحق ضررا بليغا بهذه الطائفة من الحقوق التي تعرف بالذهنية أو الفكرية

7- **جرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجية:** من خلال استقراء التشريعات العربية الخاصة بمكافحة جرائم الإنترنت، يُلاحظ أن اهتمام المشرّع انصبّ بدرجة أولى على حماية أمن الدولة ومصالحها العليا، وجعل ذلك في مقدمة أولوياته عند تنظيم الفضاء الإلكتروني، في حين جاءت حماية الحقوق الفردية للمواطن في مرتبة لاحقة، وهو ما يبدو جلياً في العديد من النصوص ذات الصلة.

8- **جرائم النظام العام والآداب العامة والاتجار في الجنس البشري:** كالإخلال بالنظام العام والآداب، إنشاء أو نشر مواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام والآداب، انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة، الإساءة إلى السمعة، والدعارة والمخدرات وغسيل الأموال[35]

المبحث الثاني: الجرائم المتعلقة بالجريمة الالكترونية ودوافع ارتكابها

تشمل الجريمة الالكترونية طيفا واسعا من الأفعال الغير مشروعة نظرا للبيئة الخصبة التي انشأتها المعلوماتية والمستفيدة منها بشكل سلبي أكثر مما هو إيجابي، فمن الأفعال المشينة الاحتيال الالكتروني، سرقة الهوية ...الخ، غالبا يصعب اكتشافها والتعقب على مرتكبيها نظرا لطبيعتها المعقدة وحدودها المفتوحة في الفضاء السبيراني، كل هذا يتأتى من دوافع محيطة بالواقع المعاش لدى الجناة وأسلوب عيشهم في الحياة وكذا كيفيات تحقيق الأهداف. في هذا المبحث سنتناول كل هذا بمراحل كالتالي:

المطلب الأول: الجرائم المتعلقة بالجريمة الالكترونية

تعتمد الجريمة الالكترونية على الوسائل التقنية الحديثة كوسيلة لارتكاب الأفعال الإجرامية، ويتحقق ذلك ضمن بيئة رقمية تتوفر فيها خدمة الانترنت، والتي تعد عنصرا أساسيا لا يتجزأ من تكوين الجريمة مكتملة الأركان، في هذا المطلب سنتناول مختلف الجرائم المحتملة الوقع بواسطة الأنظمة وغيرها.

[35] لامية طالة –كهينة سلام، **الجريمة الالكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي**، المرجع السابق، ص 80-81.

الفرع الأول: الجرائم الواقعة على النظام المعلوماتي

تُعد الجرائم الموجهة ضد الأنظمة المعلوماتية من صور الأفعال غير المشروعة التي تستهدف البنية التقنية لتلك الأنظمة، وذلك من خلال الاعتداء على مكوناتها أو اختراق نظم المعالجة الآلية للبيانات باستخدام وسائل تقنية ضارة، كالفيروسات، بقصد الإضرار بوظائفها أو تعطيلها أو الوصول غير المصرح به إلى محتوياتها.

أولا: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات والشرائط والكابلات، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية كان تكون محل للسرقة وخيانة الأمانة او الإتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل، مما يترتب عليها خسائر كبيرة.[36]

ثانيا: الجرائم الواقعة على المكونات المنطقية للنظام المعلوماتي

الإعتداء على المكونات المادية للنظام المعلوماتي يتحقق إذا كان الحاسوب والأجهزة الملحقة به أو الشبكات المعلوماتية محلا للاعتداء. [37]تتحقق جريمة التعدي على المكونات غير المادية للنظام المعلوماتي عندما تكون مكونات الكمبيوتر المعلوماتية الغير عادية مثل البرامج المستحدثة والبيانات المخزنة في ذاكرة الكومبيوتر محلا أو موضعا للجريمة، والمقصود بالبرامج أو الكيان المنطقي أنه مجموعة من الأوامر التي تسمح بتشغيل جهاز الحاسب الآلي أو نظم المعلومات المخصصة لمعالجة المعلومات بهدف إنجاز عملية معينة أو إعطاء نتائج محددة.

وجرائم الاعتداء على برامج الكمبيوتر تأخذ شكلين الأول يكون في شكل الاعتداء على البرامج التطبيقية والثاني في شكل الاعتداء على البرامج التشغيل، وفيما يتعلق بالبرامج التطبيقية يشكل هذا النوع من الجرائم نسبة تقدر بحوالي 15 بالمئة من مجموعة حالات الجرائم الالكترونية، أما بالنسبة لبرامج التشغيل تتحقق الجريمة في هذه الحالة بتزويد البرامج بمجموعة من تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تتيح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي.

ثالثا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

تُشكّل البيانات المعالجة إلكترونيًا عنصراً جوهرياً في تكوين البنية الأساسية للأنظمة المعلوماتية الحديثة، إذ تمثل أحد الأصول غير المادية ذات الأهمية البالغة، ليس فقط بالنظر إلى قيمتها الاقتصادية المتزايدة، وإنما أيضاً لما تؤديه من دور حيوي في دعم اتخاذ القرار وتسيير المصالح العامة والخاصة. وبفعل هذا الدور المحوري، أضحت هذه البيانات هدفاً مباشراً وغير

[36] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، أعمال الملتقى الوطني الافتراضي، فرقة مشروع البحث التكويني الجامعي، P.R.F.U، كلية العلوم الإنسانية والاجتماعية، جامعة يحي فارس المدية، 15 مارس 2022، ص 28.

[37] نهلا عبد القادر المومني، **الجرائم المعلوماتية**، ط الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 97.

مباشر لمجموعة متنامية من الأفعال الإجرامية، التي تستهدف في جوهرها التلاعب بمحتوى هذه البيانات أو التأثير على وظيفتها، سواء من خلال الوصول غير المشروع إليها أو تعديلها أو إتلافها أو استخدامها في غير الأغراض المخصصة لها.

وتجدر الإشارة إلى أن هذه الجرائم لم تَعُد حبيسة الأشكال التقليدية المتمثلة في الاستيلاء على الأموال من المؤسسات المصرفية أو الأفراد، بل شهدت تطوراً نوعياً ومجالياً، امتد ليشمل قطاعات ذات حساسية عالية وأهمية استراتيجية، وعلى رأسها قطاع النقل البحري وأمن الموانئ. فقد أصبحت هذه الأخيرة مسرحاً محتملاً لهجمات سيبرانية معقدة، قد تُنفَّذ من قبل جماعات الجريمة المنظمة، أو من قبل فاعلين غير حكوميين ذوي توجهات إرهابية، بل وحتى من جهات مدعومة من دول معادية، تسعى إلى الإخلال بأمن واستقرار الدول من خلال استهداف بنيتها التحتية المعلوماتية.[38]

الفرع الثاني: الجرائم الواقعة على الأشخاص

ظهرت عدة أنواع خاصة من الجرائم الالكترونية الواقعة على الأشخاص كجريمة التهديد والمضايقة والملاحقة خاصة عن طريق البريد الالكتروني بإرسال رسالة خاصة للترويع والتهديد أو عن طريق وسائل الحوارات المختلفة على شبكة الانترنت: كالفايسبوك، الفايبر والواتساب وكذلك جريمة القذف والسب وتشويه السمعة للمساس بشرف الغير وكرامتهم واعتبارهم عن طريق وسائل الاتصال المباشر أو الكتابة أو عن طريق المطبوعات أو المبادلات الالكترونية (بريد الكتروني) صفحات الويب، غرفة المحادثة. كما تعتبر من أهم الجرائم الالكترونية الواقعة على الأشخاص صناعة ونشر الإباحة والجنس سواء للبالغين والأطفال خاصة، حيث يتعرض الأطفال للاستغلال الجنسي على الانترنت بأشكال متعددة انطلاقا من الصور الى التسجيلات المرئية للجرائم الجنسية العنيفة، حيث تستمر معاناتهم ما بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنت.

ويضاف الى الجرائم الالكترونية الشخصية جرائم انتحال الشخصية والتغرير والاستدراج باستخدام شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحياته أو تتخذ هذه الجريمة وجهان: انتحال شخصية الفرد وانتحال شخصية المواقع.[39]

الفرع الثالث: الجرائم الواقعة على الأموال

تُعد الجرائم المعلوماتية الواقعة على الأموال من صور الجرائم المستحدثة في المنظومة القانونية الجزائرية، والتي ظهرت نتيجة التقدم التكنولوجي المتسارع، لاسيما في مجال استخدام الحاسوب وشبكة الإنترنت. وتتمثل هذه الجرائم في سلوكيات ذات

[38] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 29.
[39] نفس المرجع، ص 27.

طابع احتيالي أو تُرتكب بالغش والتدليس، باستخدام أدوات إلكترونية وتقنيات رقمية، بهدف تحقيق منفعة مالية غير مشروعة، من خلال استهداف الأنظمة المعلوماتية، والتلاعب بمعطياتها، وتحويل الأموال إلى حسابات الجاني دون وجه حق. ويُعتبر هذا السلوك مجرَّمًا بموجب أحكام القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لاسيما في مواده من 394 مكرر إلى 394 مكرر 8 المدرجة ضمن قانون العقوبات.[40]

ومع الانتشار الواسع لاستخدام شبكة الإنترنت، أصبحت المعاملات التجارية تُدار بشكل متزايد عبر الفضاء الرقمي، مما أدى إلى تطور وسائل الدفع الإلكتروني، مثل البطاقات البنكية، والمحافظ الإلكترونية، التي تُعد أشكالاً حديثة من وسائل الوفاء ذات الطابع الرقمي. وقد أوجد هذا التطور بيئة خصبة لارتكاب أنواع جديدة من الجرائم، حيث يستغل الجناة الثغرات التقنية أو ضعف الحماية المعلوماتية للأنظمة بهدف اختراقها وسرقة البيانات وتحويل الأموال.[41]

وفي هذا الإطار، يُجرّم المشرّع الجزائري، بموجب المادة 394 مكرر 3، فعل التزوير أو التزييف أو التلاعب في المعطيات المعلوماتية المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، متى ترتب عن ذلك ضرر للغير. كما تنص المادة 394 مكرر 5 على تجريم الدخول الاحتيالي إلى منظومة معلوماتية بقصد الإضرار أو الحصول على منافع غير مستحقة، بما في ذلك الاستيلاء على أموال الغير. ويؤكد الاجتهاد القضائي الجزائري في هذا الشأن على أن ارتكاب مثل هذه الأفعال يُعد مساسًا بالذمة المالية للأفراد، وتهديدًا للأمن الاقتصادي والمعلوماتي، وهو ما يقتضي تشديد العقوبات ومواكبة التطورات التقنية لضمان فعالية الحماية الجزائية.

الفرع الرابع: الجرائم الواقعة على امن الدولة

لقد أصبحت عدة دول مهددة بفعل التطور التكنولوجي الحاصل، وتنوعت الجرائم في هذا المجال بحسب طبيعتها، زمن بين أهم الجرائم الواقعة على أمن الدولة، جريمة التجسس، جرائم الإرهاب، الجريمة المنظمة.

أولا: جريمة التجسس

التجسس هو الاطلاع على معلومات خاصة بالغير مؤمنة في جهاز آخر وليس لغير المخولين بالاطلاع عليها، وقد سهلت شبكة الانترنت الأعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية والوطنية، وتستهدف عملية التجسس في عصر المعلومات ثلاث أهداف رئيسية

[40] عزوق عبد اللطيف، **دور الشرطة العلمية في مكافحة الجريمة الالكترونية**، مذكرة لنيل شهادة ماستر أكاديمي تخصص إعلام آلي وانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، سنة 2022-2023، ص 41.

[41] خالد شكري، أبوبكر لراشي، **التحقيق وجمع الأدلة في مجال الجرائم الالكترونية**، المرجع السابق، ص 23.

وهي: التجسس العسكري، التجسس السياسي، والتجسس الاقتصادي، كما تستخدم العديد من الدول التجسس باستخدام التقنية المعلوماتية، وهذه الأنشطة تمارس من قبل دولة على دولة أو دول أخرى، أو من قبل الدول على مواطنيها، أو من قبل شركة على شركات أخرى منافسة.[42]

ومن بين الجرائم التجسس ما يلي:

1-تخريب المعلومات وإساءة استخدامها ويشمل ذلك قواعد المعلومات المكتبات تخريب الكتب تحريف المعلومات وتحريف السجلات الرسمية

2-سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطور التقني أو الصناعي أو العسكري أو تخريبها أو تدميرها...الخ

3-تزوير المعلومات ويشمل الدخول القواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب

4-تزييف المعلومات وتشمل تغيير في المعلومات على وضع غير حقيق مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها

5-انتهاك الخصوصية ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الالكترونية ونشر معلومات عنهم أو وضع معلومات تخص تاريخ الأفراد ونشرها.

6-التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.

7-التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.

8-التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل يقصد منه اغتيال شخصية الافراد أو الإساءة.

9-السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.

10-سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.

11-الدخول غير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.

12-قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.

13-قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

[42] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 138.

14-خلاعة الأطفال وتشمل نشر صور خاصة للأطفال" الجنس السياحي" للأطفال وللإناث خاصة على الشبكات بشكل عام ونشر الجنس التخيلي.

15-سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقة الائتمان.

16-التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة.

17-القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة الكترونية

18-إفشاء الأسرار وتشمل الحصول على معلومات خاصة جدا ونشرها على الشبكة

19-الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو البطاقات المالية أو البطاقات الهاتفية

20-المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما وذلك من خلال استخدام البريد الالكتروني وإرسال الرسائل

21-الإرهاب الالكتروني، يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادر هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الالكتروني.[43]

ثانيا: جرائم الإرهاب

في إطار ما يشهده الواقع المعاصر من تطور في وسائل الاتصال وتكنولوجيا المعلومات، باتت الجماعات الإرهابية تستغل الفضاء السيبراني، من خلال إنشاء مواقع إلكترونية افتراضية تمثل واجهات دعائية لها، حيث يلاحظ تزايد هذه المواقع بالتوازي مع تنامي نشاط التنظيمات الإرهابية. وتُستخدم هذه المنصات في بث رسائل تتضمن تبني عمليات إرهابية، أو في إصدار بيانات تنفي أو ترد على ما يصدر عن منظمات أو جهات رسمية، كما تُعد وسيلة فعالة لتجنيد عناصر جديدة عبر شبكة الإنترنت، من خلال أنظمة الإعلام الآلي. وتعمد تلك الجماعات إلى استهداف فئة الشباب، لاسيما من يفتقرون إلى الوعي الكافي والقدرة على التمييز، قصد استمالتهم واستغلالهم في تنفيذ مخططاتها الإجرامية، الأمر الذي يُعد من صور الجرائم المرتكبة بواسطة الوسائل التقنية، والتي يعاقب عليها التشريع الجزائري وفقاً لأحكام القانون الجنائي، لاسيما في ظل التعديلات المتعلقة بمكافحة الجرائم الإرهابية والجريمة الإلكترونية.[44]

[43] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، مرجع سابق، ص 259-260.

[44] نفس المرجع، ص 138.

ثالثا: الجريمة المنظمة

الجريمة المنظمة ليست وليدة التقدم وان كانت استفادت منه، فالجريمة المنظمة بسبب تقدم وسائل الاتصال والتكنولوجيات الحديثة أصبحت غير محدودة لا بقيود الزمان ولا بقيود المكان، وأصبح انتشارها على نطاق واسع وكبير كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة على وسائل الانترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية بسهولة، فقد اكتشفت هذه الجماعات أن استخدام شبكات الإنترنت والتكنولوجيا تستطيع أن تؤمن فرص جديدة وفوائد حية لأعمالهم وأرباح غير مشروعة عما يقومون به.[45]

الفرع الخامس: الجرائم الواقعة على البرامج الالكترونية

والمقصود هنا هو الإتلاف المنطقي أي إتلاف معلومات الحاسوب وبياناته باستخدام الطرق المنطقية والمعلوماتية وتنوع أساليب الاعتداء على المعلومات بحسب الهدف الذي يرمي الجاني الى تحقيقه ومن أبرز هذه الاعتداءات الفيروس المعلوماتي الدودة المعلوماتية، القنابل المنطقية.[46]

1- **الفيروسات:** يُعد الفيروس المعلوماتي برنامجًا خبيثًا يتميز بخصائص تقنية تُشبه إلى حد بعيد الفيروسات البيولوجية، من حيث القدرة على التسلل والتكاثر الذاتي داخل الأنظمة المعلوماتية، وإحداث أضرار متفاوتة الخطورة بوظائفها. وتتجلى خطورته أساسًا في قابليته للتعديل الذاتي، والتأثير على البرامج التي يرتبط بها، بل وقدرته أحيانًا على تمييز البرامج التي لم تُصب بعد عن تلك التي تم التلاعب بها مسبقًا، مما يعزز انتشاره بشكل منهجي داخل المنظومة المعلوماتية.

وقد ساعدت عدة عوامل موضوعية وتقنية على تسريع وتوسيع رقعة انتشار هذه البرمجيات الخبيثة، أبرزها تفشي ظاهرة القرصنة المعلوماتية، وتوافق الأنظمة التشغيلية بين مختلف الأجهزة الإلكترونية، بالإضافة إلى الانتشار الواسع لاستخدام شبكة الإنترنت في مختلف مجالات الحياة اليومية.

[45] [45] د. رقية محمودي، د. نور الهدى قدوح، نفس المرجع.

[46] عزوق عبد اللطيف، **دور الشرطة العلمية في مكافحة الجريمة الالكترونية**، المرجع السابق، ص49.

ورغم التقدم الحاصل في تطوير مضادات الفيروسات والبرامج الوقائية، إلا أن هذه الأخيرة كثيرًا ما تعجز عن التصدي للهجمات الإلكترونية المعقدة، إذ تظل الفيروسات قادرة على اختراق النظم، والوصول إلى المعطيات الحساسة، متجاوزة بذلك مختلف آليات الحماية والتأمين المعتمدة.[47]

2- **القنبلة المعلوماتية:** وتنقسم الى قسمين

أ- **القنبلة المنطقية:** ويهدف هذا الفيروس الى تدمير المعلومات عند حدوث ظرف معين مثل تدمير نظام تسيير الموارد البشرية لمؤسسة معينة عند شطب اسم أحد الموظفين من القائمة.

ب- **القنبلة الزمنية:** يعمل هذا الفيروس في ساعة محددة من يوم معين ومن أبرز الأمثلة عن ذلك فيروس Anglo Michael مايكل انجلوا وفيروس Macmag وفيروس شرنوبيل Shernobel ويتميز هذا الأخير بأنه فيروس الأول الذي يصيب المكونات المادية بالخراب والتلف الى جانب المكونات المعنوية(المعلومات) حيث اكتشف هذا الفيروس سنة 1998.[48]

3- **الدودة المعلوماتية:** هي عبارة عن نظام معلوماتي يمتاز بقدرته على التنقل عبر شبكات نقل المعلومات بهدف إعاقة عملها، والتشويش عليها عبر شل قدرتها على التبادل ...الخ وأهم ما تتميز به هذه الفيروسات الانتشار عبر الشبكات عن طريق توليد نفسها ومن أشرها الدودة التي أطلقها الطالب الأمريكي في جامعة كورنال Uninersity Cornell، روبيرت موريس سنة 1988 عبر شبكات الجامعات والشبكات العسكرية في الولايات المتحدة بتدمير الآلاف من الحواسيب وتعطيل الشبكات وكان هدفه من عذا هو إظهار ضعف مقاييس امن الشبكات قائلا " أردت أن أعرف إذا كان بإمكاني كتابة برنامج يستطيع قدر الإمكان الانتشار بشكل واسع على شبكة الانترنت" وقد حكم على روبرت سنة 1995، بالمراقبة لمدة ثلاثة سنوات وبالعمل بالخدمة الاجتماعية لمدة 400 ساعة.

لقد بات مرتكبو الجرائم المعلوماتية يجاهرون باستخدام الوسائل التقنية المتطورة كأدوات لاختراق الأنظمة الإلكترونية، دونما خشية أو تحفظ. ومثال ذلك ما تعرض له الموقع الإلكتروني التابع لإدارة الدفاع الأمريكية (Department of Defense - DOD)، وتحديدًا الصفحة الخاصة بالقوات الجوية الأمريكية، حيث أقدم أحد القراصنة في عام 1996 على اختراق الواجهة الترحيبية للموقع، مما اضطر السلطات المختصة حينها إلى إغلاق عدد من المواقع التابعة للبنتاغون

[47] الظهير الشريف، **بتنفيذ القانون رقم 07.03 المتعلق بإحداث جرائم متعلقة بنظم المعالجة الآلية للمعطيات، لا سيما المواد من 607-3 إلى 607-10 من مجموعة القانون الجنائي المغربي**، والتي تُجرّم بشكل صريح إدخال أو تعديل أو حذف المعطيات المعلوماتية داخل نظم المعالجة، وكذلك عرقلة سيرها أو إتلافها، رقم 1.07.207 صادر في 30 نوفمبر 2007، المغرب.

[48] عزوق عبد اللطيف، **دور الشرطة العلمية في مكافحة الجريمة الالكترونية**، المرجع السابق، ص 50.

كإجراء احترازي، تمهيدًا لإعادة تهيئتها باستخدام أنظمة وقاية أكثر تطورًا وأمانًا، وذلك بعد أن تبين ضعف الحماية التقنية أمام مثل هذه الهجمات الإلكترونية.[49]

المطلب الثاني: دوافع وأسباب ارتكاب الجريمة الالكترونية، الأطراف، وموقف بعض التشريعات منها

الفرع الأول: دوافع وأسباب ارتكاب الجريمة الالكترونية

إن أسباب ارتكاب الجريمة الإلكترونية راجع لعدة عوامل منها ما هو سبب ومنها ما هو دافع، فحسب ما يرى المختصون هي المحفز لارتكاب الأفعال المشينة في المجتمع وسنتطرق لعرضها على أربعة مستويات كما يلي:

أولا: دوافع ارتكاب الجريمة الالكترونية[50]

من أبرز الدوافع التي تدفع بالإنسان الى ارتكاب الجريمة الإلكترونية ما يلي:

1- **الدوافع الذاتية:** والتي تجعل من الشخص يقوم بارتكاب عدد من المخالفات نابعة من حب الاستطلاع والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات.

2- **الدوافع النفسية:** وتكون من شخص لديه خلل نفسي أو أمراض نفسية تنعكس على السلوك.

3- **الدوافع الاجتماعية:** وتتمثل في الاختراقات للأجهزة الشخصية والتعرف على نقاط الضعف لدى الآخرين.

4- **الدوافع المالية (الربح وكسب المال):** وذلك بالرغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتراف جرائمهم من أجل تحقيق المكاسب المالية.

5- **الدافع السياسي والعسكري:** التطور العلمي والتقني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الحاسوب، وبذلك أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية.

6- **الدافع القومي والوطني:** وهو أن يقوم الهاكرز بالهجوم على مواقع معادية تختلف مع قيم وعادات مجتمع ما بتدمير أو تغيير هذه المواقع، مما يؤدي إلى منعها من تهديد فكر وسلوك أفراد ذلك المجتمع.

ثانيا: أسباب ارتكاب الجريمة الالكترونية

---

[49] الحادثة موثقة ضمن تقارير الأمن السيبراني الصادرة عن وزارة الدفاع الأمريكية لعام 1996. وقد أوردتها صحيفة The Washington Post بتاريخ 18 فبراير 1996، بعنوان: "Hackers Break Into Pentagon Computer System" (المصدر: The Washington Post Archives, 1996).

[50] د. عبد السلام محمد المايل، د. عادل محمد الشريجي، د. علي قابوسة، **الجريمة الإلكترونية في الفضاء الإلكتروني: المفهوم–الأسباب–سبل المكافحة مع التعرض لحالة ليبيا**، المرجع السابق، ص 248-249.

تتعدَّد أسباب ارتكاب الجريمة الإلكترونيَّة في المجتمع لعدَّة مستويات، نذكرها كالتَّالي:

أ- أسباب ارتكاب الجريمة على المستوى المجتمعي[51]

1- **التحضر**: يعد التحضر أحد أسباب الجريمة الالكترونية عامة حيث الهجرة الكبيرة من الريف الى المدينة والى المناطق الحضرية والمدن الكبيرة وعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية باهضة التكاليف، والتي تتطلب مهارات عالية أحيانا مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية مما يجعلهم يعيشون في مدن الصفيح والاحياء الطرفية و الهامشية وكنتيجة يجد الناس أنفسهم في تنافس غير قادرين على مجازاته مما يجعلهم يلتفتون الى الاستثمار في الجريمة الالكترونية.

2- **البطالة**: ترتبط الجريمة الالكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة وتتركز البطالة بين قطاعات كبيرة من الشباب، لذا سيستثمر الذين يملكون المعرفة ذلك في النشاط الاجرامي الالكتروني.[52]

3- **الضغوط العامة**:[53] تُعدّ الأوضاع الاجتماعية والاقتصادية المتدهورة، كالفقر والبطالة وتفشي الأمية، إلى جانب التحديات الاقتصادية الهيكلية، من العوامل الأساسية التي تمارس ضغطًا متصاعدًا على المجتمع بوجه عام، وعلى فئة الشباب بوجه خاص.[54] ويُسهم هذا الواقع في توليد مشاعر من الإحباط والاغتراب الاجتماعي لدى شرائح واسعة من الأفراد، مما يدفع بعضهم إلى تبني آليات تكيّف منحرفة، تتمثل في الانخراط بسلوكيات غير مشروعة، من بينها الاتجار الإلكتروني بالبشر، والاستغلال الجنسي عبر الوسائط الرقمية، فضلًا عن ارتكاب جرائم إلكترونية متنامية، بما يُشكل تهديدًا مباشراً للنظام الاجتماعي والأمني، ويستدعي تدخلًا تشريعيًا ومؤسسيًا عاجلًا لمعالجة الأسباب الجذرية لهذه الظواهر.[55]

4- **البحث عن الثراء**: يسعى الانسان الى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة لجتفردسون وهيرشي، ويسعى الناس الى الوسائل غير المقبولة اجتماعيا لتحقيق أهداف مقبولة اجتماعيا كما ترى نظرية "الأنومي لميرتون"، فالرغبة في الثراء يواجهها صعوبات بالغة في تحقيقه بالطرق المقبولة اجتماعيا والقانونية ولذا

---

[51] مريم قويدر، **إشكالية العوالم الافتراضية المظلمة على شبكة الانترنت، قراءة إعلامية نقدية للجرائم السيبرانية الفكرية والثقافية على شبكة الويب العالمية**، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد09، العدد02، جامعة الجزائر3، الجزائر، جوان 2024، ص 393-394.

[52] لامية طالة، كهينة سلام، **الجريمة الالكترونية: بعد جديد لمفهوم الاجرام عبر منصات مواقع التواصل الاجتماعي**، المرجع السابق، ص 78.

[53] جامعة الدول العربية، إدارة الشؤون القانونية. **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**. القاهرة، 2015.

[54] United Nations Office on Drugs and Crime. Global Report on Trafficking in Persons 2020. United Nations, 2020

[55] United Nations. Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime. 2000.

يلجأ بعض الناس الى الجرائم الالكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.[56]

5- **غياب المراقبة الوالدية:** وقد نجد أن الأسرة التي تعتبر أهم حلقة في المجتمع، المسؤول الأول عن الترويج لخطاب الكراهية من عدمه عبر أبنائنا،"... حيث يبدأ الوالدان في زرع أولى البذور التي تكون شخصية الإنسان، فإما يبذروا المحبة و قبول الآخر واحترامه، وإما يبذروا الكراهية والعنصرية البغيضة التي تتحكم بعد ذلك في تصرفات الشخص ونظرته لمن حوله"، وبالرجوع للواقع الاجتماع المعاش قد نجد أن الأسرة قد ساهمت بقسط كبير في اكتساب أفرادها لسلوكيات إجرامية، خاصة في ظل توفير الهواتف الذكية للأبناء منذ الصغر و تودهم عليها، بالإضافة لعدم متابعة المواقع و البرامج التي يقصدونها، وهو ما قد يدفع بالشباب الى الغوص في متاهات هذه التكنولوجيات وخاصة عبر مواقع التواصل الاجتماعي من أجل إبراز أنفسهم أو سب وشتم الآخر، وحتى الترويج لخطابات الكراهية و التشجيع على العنف ونبذ الآخر، ومنه يمكن القول أن وظيفة الأسرة تتعدى توفير الحاجات الأساسية الخاصة بالأكل والشرب واللباس الى الرعاية النفسية و الاجتماعية للأبناء، أي قد نجد أن هناك قطيعة بين الآباء و الأبناء وهو ما قد يصعب على الأب فهم ابنه وكذا معرفة أهم السلوكيات والأفكار التي تجول في خاطره، في ظل ظهور العديد من التكنولوجيات و المواقع الافتراضية، والتي قد يرى الشاب فيها أنها تعتبر كمتنفس حقيق له بعيدا عن المراقبة الوالدية والمجتمعية.[57]

6- **ضعف إنفاذ القانون وتطبيقه في الجريمة الالكترونية**

هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الالكترونية وأساليبها وهذا لا يتوقف عند التشريعات وانما يشمل الشرطة والتحقيق والقضاء وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني كما هو الحال على المستوى الدولي فمما يشعل الجريمة الالكترونية غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقق في الجرائم الالكترونية[58]

ب- أسباب ارتكاب الجريمة على المستوى الفردي [59]

---

[56] لامية طالة، كهينة سلام، نفس المرجع.

[57] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 428.

[58] لامية طالة، كهينة سلام، **الجريمة الالكترونية: بعد جديد لمفهوم الاجرام عبر منصات مواقع التواصل الاجتماعي**، المرجع السابق، ص 79.

[59] مريم قويدر، **إشكالية العوالم الافتراضية المظلمة على شبكة الانترنت، قراءة إعلامية نقدية للجرائم السيبرانية الفكرية والثقافية على شبكة الويب العالمية**، المرجع السابق، ص 392.

1- **ضغط الذات المنخفض:** يمكن أن يكون لضغط الذات تأثير كبير على أداء الأشخاص في مجموعة متنوعة من المؤسسات المجتمعية كالمدرسة والعمل والحياة الزوجية، فالأفراد الذين يفتقرون الى ضبط الذات بشكل جيد هم ليس فقط عرضة للسلوكيات الغير ملائمة انما غالبا ما يواجهون فشلا في النجاح في مختلف جوانب حياتهم سواء في المدرسة أو العمل أو حتى في العلاقات الزوجية أو العلاقات الاجتماعية، كما تشير الدراسات أيضا الى أن الأفراد الذين يفتقرون الى ضبط الذات ويظهرون استعدادا منخفضا لتحمل المخاطر وقد يتجهون نحو تحقيق مكاسب قصيرة الآجال، وهذا التوجه يمكن أن يؤثر على سلوكياتهم بشكل سلبي خاصة في ظل الوسائط الالكترونية والانترنيت، حيث يمكن أن يسهم التفاعل مع هذه الوسائط في تسهيل أو تعزيز السلوكيات المنحرفة، بالإضافة الى ذلك فهم يتعرضون في الانترنيت الى نماذج " التعلم الاجرامية" والى تأثير الأقران الذين قد يكونون اكثر ميلا للانخراط في عالم الجريمة السيبرانية.[60]

2- **البحث عن التقدير**: تُلاحظ في بعض الحالات ارتكاب فئة من الأحداث أو الشباب حديثي السن لبعض الأفعال التي تُصنف ضمن الجرائم الإلكترونية، ويكون الدافع وراءها في الغالب هو التباهي، أو التحدي، أو الرغبة في لفت الأنظار من خلال الظهور الإعلامي، دون إدراك لطبيعة الأثر القانوني المترتب على هذه الأفعال. وغالبًا ما تتراجع هذه التصرفات مع بلوغ الفاعلين سِنّ النضج القانوني، أي بعد تجاوز مرحلة المراهقة والدخول في عقد العشرينات.[61]

3- **الفرصة:** لقد وفرت التقنيات الحديثة والانترنت فرصا غير مسبوقة لانتشار الجريمة الالكترونية، فقد ولدت بيئة قد تشكل المعلومات فيها هدفا سهل المنال ويحقق المنفعة السريعة، وبالتالي يمكن سرقتها أو سرقة محتوياتها فهي فرصة مربحة وقليلة المخاطر واحتمالية الكشف للفاعل فيها ضئيلة.[62]

4- **النشاط الروتيني**: يمكن تفسير زيادة ضحايا الجريمة الالكترونية من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية، فمع ظهور شبكة الانترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية و الترفيه والتجارة، ذلك أن التغييرات في أنشطة الناس الروتينية مثل استخدام الانترنت وشبكات التفاعل الاجتماعي مثل الفايسبوك و الايميل و المواقع وغيرها قد خلقت فرصا للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة، يرى كوهين و فيلسون أنه من المرجع أن تحدث

---

[60] مريم قويدر، نفس المرجع.

[61] شحاتة، السيد عطية. "**تعرض المراهقين للجرائم الإلكترونية عبر وسائل الإعلام الرقمي وتأثيرها.**" **مجلة** كلية الإعلام، جامعة القاهرة، 2019، ص. 45-58. و Ali, Muhammad, et al. "Understanding Cybercrime and Youth: A Perception-Based Approach." ResearchGate, 2023.

[62] لامية طالة، كهينة سلام، **الجريمة الالكترونية: بعد جديد لمفهوم الاجرام عبر منصات مواقع التواصل الاجتماعي**، المرجع السابق، ص 76.

الجريمة عندما تتلاقي ثلاثة عوامل هي الجاني المتحفز والهدف المناسب وغياب الحراسة أنه لابد من توافر هذه العوامل الثلاثة من أجل أن تحدث الجريمة وعدم وجود واحد من هذه العوامل هو كافي لمنع حدوث الجريمة.[63]

5- **الرغبة في الانتقام**: يلجأ البعض الى ممارسة الإجرام عبر مواقع التواصل الاجتماعي، ويكون ذلك لشعورهم بالظلم وانتابتهم الرغبة بالانتقام من الأشخاص والهيئات، فالانتقام عبر مواقع التواصل الاجتماعي و بالأخص الفايسبوك قد أصبح يعرف منحى تصاعدي، وبالرجوع للواقع الاجتماعي المعاش قد نجد أن بعض الافراد الذين تم تهميشهم أو حتى وصمهم من طرف أفراد مجتمعهم بصفات بغيضة تبعا لسلوك انحرافي أو اجرامي قاموا به في السابق، قد لا يتقبلوه وهو ما يجعلهم يحبون الانتقام بشتى الطرق، وكما هو معلوم أن الفايسبوك أصبح يوفر خاصية انشاء الحسابات المزيفة عبره دون طلب تأكيد هوية المستخدم، فقد يستغل هؤلاء الأشخاص المنحرفين أو المجرمين أو الذين مورس عليهم الوصم إليه، فالفايسبوك قد يساعده في الانتقام بشتى الطرق سواء التشهير بنشر الصور الشخصية، السب والقذف، إلصاق عيب بشخص ما .... الخ.[64]

ث- أسباب ارتكاب الجريمة على المستوى العالمي

1- **التحول للمجتمع الرقمي**: والذي يمتاز بتغيرات كمية في مقدار المعلومات المتدفقة ونوعيتها، فبفعل تكنولوجيا الاتصال والمواصلات فأن الصور والمعلومات تغطي كافة المعمورة بسرعة ودقة، ووجود الشبكات حيث يتم تداول المعلومات بين جميع الأطراف مثل البريد الالكتروني، الهاتف الجوال وغيرها.[65]

2- **العولمة**: لقد شكّل الفضاء الإلكتروني بيئة خصبة لنشوء أنماط جديدة من الإجرام، إذ إن هذا الفضاء، بطبيعته اللامادية، قد يتيح للأشخاص الرقميين ارتكاب أفعال جرمية لا يقدمون على ارتكابها في الواقع المادي، وذلك بالنظر إلى مركزهم الاجتماعي أو المهني. ويُعزى ذلك إلى جملة من العوامل، من أبرزها هشاشة الهوية الرقمية، وإمكانية التخفي أو انتحال الصفات، وضعف آليات التحقق والردع، الأمر الذي يُضعف الشعور بالمسؤولية القانونية ويُشجّع على السلوك الإجرامي ضمن البيئة الافتراضية.[66]

3- **الترابط الكوني**

يمكن أن يشكل ظهور الترابط العالمي في سياق تغيرات الاقتصاد والديموغرافيا عاملا مساهما في زيادة مستويات الجريمة. فوفقا لتقرير صادر عن المركز الوطني لجرائم الياقات البيضاء يتوقع أن يتضاعف عدد سكان المدن الى 6.2

---

[63] لامية طالة، كهينة سلام، نفس لمرجع، ص 77.

[64] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 429.

[65] لامية طالة، كهينة سلام، **الجريمة الالكترونية: بعد جديد لمفهوم الاجرام عبر منصات مواقع التواصل الاجتماعي**، المرجع السابق، ص 79.

[66] Solove, Daniel J. The Digital Person: Technology and Privacy in the Information Age. NYU Press, 2004 p 87.

مليار بحلول سنة 2050، ممثلا 70 في المائة من إجمالي سكان العالم والمتوقع أن يصل إلى 8.9 مليار نسمة، وقد أظهر ذات التقرير أن الانترنت قد فتحت أبوابا جديدة لفرص الجريمة السيبرانية.

بحيث يمكن للمجرمين من التواصل مع المتضررين بشكل فعال دون الكشف عن هوياتهم الرقمية، مستفيدين في ذالك من سهولة استخدام الانترنت وعدم كشف الهوية الافتراضية في هذا الفضاء الرقمي

بالإضافة الى ما سبق توفر شبكة الانترنت للمجرمين طرق فعالة وناجعة لنقل كميات هائلة من المعلومات بقدرة استيعاب عالية وسرعة فائقة، سواء عبر غرف الدردشة أو البريد الإلكتروني أو لوحات الرسائل أو حتى مواقع الأنترنت، ونتيجة لذلك يمكن لجهاز حاسوب واحد أن يوفر وسائل متعددة لارتكاب مجموعة متنوعة من الجرائم السيبرانية وتنفيذ العديد من المعاملات المالية التي تدخل في سياق النصب والاحتيال الإلكتروني على العديد من الأشخاص خاصة الذين تقل خبرتهم في هذا المجال. [67]

4- انكشاف البنية التحتية المعلوماتية الكونية

تختلف درجات هشاشة الهياكل المعلوماتية التحتية عند تعرضها للأخطار الطبيعية أو الأفعال البشرية المهملة أو غير الرشيدة، تبعًا لطبيعة تكوينها وموقعها. وقد بيّن التقرير الصادر عن الرئاسة الأمريكية بشأن حماية "البنى التحتية الحيوية" أن هناك خمس قطاعات تشترك في سمات جوهرية تجعلها أكثر عرضة للمخاطر وتستلزم حماية خاصة. وتتمثل هذه القطاعات في: قطاع الاتصالات وتكنولوجيا المعلومات، قطاع التوزيع الفيزيائي، قطاع الطاقة، القطاع المالي والمصرفي، إضافة إلى قطاع الخدمات الحيوية ذات الطابع الإنساني.[68]

ج- أسباب ارتكاب الجريمة في العالم الافتراضي

بما ان هذه الجرائم ماهي في حقيقتها الا نبضات الكترونية فإن هذا يشكل عقبة أداء أمام اكتشافها وأمام التعرف على مرتكبيها، ولكن هذا القول لا يمكن أن يؤخذ على اطلاقه أي أن هذا القول لا يعني أن بعض جرائم الحاسب الآلي لا يمكن أن يتم اكتشافها إذ بقدر ما تطورت وسائل الحاسب الآلي وانظمته تطورت الوسائل التقنية لحمايته وحماية انظمته من الاختراق والعبث بها ورصد الاعتداءات التي يتعرض وتتعرض لها أنظمة الحاسب الآلي

وبصورة عامة فإن الأسباب التي تكمن وراء ذلك أي وراء كون جرائم الحاسب الآلي تعترض سبيل اكتشافها ثمة صعوبات تعود الى جملة من الأسباب منها:

---

[67] مريم قويدر، **إشكالية العوالم الافتراضية المظلمة على شبكة الانترنت، قراءة إعلامية نقدية للجرائم السيبرانية الفكرية والثقافية على شبكة الويب العالمية**، المرجع السابق، ص 395-396.

[68] United States, Executive Office of the President. Executive Order 13010: Critical Infrastructure Protection. Federal Register, vol. 61, no. 138, 17 July 1996, pp. 37347–37350.

-قدرة الجاني على تدمير ادلة الإدانة الموجودة ضده

-عدم تخلف الاثار المادية كما هو الأمر في الجرائم التقليدية

-النشاط الاجرامي فيها لا يمكن رؤيته بالعين الجردة

-قلة خبرات لدى السلطات المسؤولة عن ضبط الجرائم والتحقق فيها

ومما زاد من خطورة جرائم الحاسب الآلي هو أن هذه الجرائم أخذت طابعا دوليا حيث لم تعد مقتصرة على النطاق الوطني وذلك بسبب سهولة الاتصال بين دول العالم اليوم، حيث جعلت أنظمة المعلومات اليوم العالم قرية لا يعترف فيها بحدود لا طبيعية و لا سياسية، غير أن انسياب هذه المعلومات متجاوزة بذلك الحدود الدولية للدول تثير الكثير من المشاكل القانونية، فلا تقتصر ما يذهب البعض على مدى مشروعية هذه المعلومات و انسيابها ومنها ما يتعلق بشروط المعلومات التي يجوز بثها عن هذا الطريق، إن كان لا ينكر هذا الجانب بل أن لها مخاطر تتعلق بالمبادئ الراسخة في القانون الجنائي وعلى وجه الخصوص فيما يتعلق بمبدأ الإقليمية.[69]

الفرع الثاني: أطراف الجريمة الالكترونية

تتطلب لوقوع الجريمة الإلكترونية أطرافا، منها ما هو مجرم معلوماتي، ضحية، وشاهد، وسنعرضها كما يلي:

أولا: المجرم المعلوماتي

يعرف الدكتور مصطفى يوسف في على انه مجرم "مختص وعلى مستوى عالي من المهارات والحرفية ولابد ان يكون على مستوى عال من التعليم الا أن ذلك كله لا ينفي عنه صفة الاجرام والمجرم المعلوماتي يحتاج لممارسة جريمته الى الولوج غير المشروع على ذاكرة الحاسب الآلي لكي يلتقط المعلومات المخزنة أو يعدل عليها".[70]

إن التطور التكنولوجي أفرز صنفا جديدا من المجرمين وهم المجرمون المعلوماتيون، يتمتعون بقدرات عالية من الذكاء والتحكم في الوسائل والاتصالات الالكترونية ويحرص المجرم المعلوماتي على إخفاء هويته باستمرار من خلال استعمال أفضل التقنيات والبرامج لذا من الصعب الكشف عنه وتحديد هويته الحقيقية وينقسم المجرمون المعلوماتيون إلى عدة أصناف من بينهم: القراصنة، الهاكرز، الهواة، المتطفلون، الكراكر..... الخ

أ-الخصائص التي يتميز بها الجاني:

[69] مريم قويدر، **إشكالية العوالم الافتراضية المظلمة على شبكة الانترنت، قراءة إعلامية نقدية للجرائم السيبرانية الفكرية والثقافية على شبكة الويب العالمية**، المرجع السابق، ص 391.

[70] فاطيمة دهان، كلثوم دهان، **إجراءات البحث والتحري في الجرائم المعلوماتية**، المرجع السابق، ص 21.

***المهارات:** حيث تعتبر المهارة من أبرز خصائص المجرم المعلوماتي ويكتسبها عن طريق ممارسته في مجال تكنولوجيا المعلومات

***المعرفة:** والمقصود بالمعرفة هي دراسة الجاني كل المحيط الذي يستهدف لارتكاب الجريمة حيث يقوم بدراسة شاملة للمحيط قبل ارتكاب جريمته، ثم يمهد كل الأفعال التي سيقوم بها ويتوقع كل المشاكل التي سيقع فيها أثناء ارتكابه لجريمته.

***الوسيلة أو الموارد:** وهو الإمكانيات التي يتزود بها الفاعل لارتكاب جريمته سواء من الحواسيب أو الهواتف أو أجهزة أخرى تكنولوجية.

***السلطة:** ويقصد بها الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته كمعرفة شفرة الدخول الى نظام معلوماتي معين، وكذلك تمكنه من وضع ملفات لا يمكن للغير قرأتها أو كتابتها أو تعديله.... الخ.

***الباعث:** هو الدافع الذي يجعل المجرم المعلوماتي يرتكب هذا النوع من الجرائم وينقسم هذا الدافع الى دافع شخصي مثل ظروف المجرم والتي تدفعه للكسب المال مثلا، أو الدوافع غير الشخصية وهي كجنون العظمة أو الانتقام أو إثبات الذات ... الخ.[71]

ب- أصناف الجاني المعلوماتي:

- **الهاكر- المخترقون-:** وهم فئة المجرمين الأقل خطورة، حيث تتوفر لديهم خبرة معتبرة في مجال الحاسوب الآلي ووظائفه ومكوناته ونظم المعلوماتية، ومعرفة البرامج التي يجرى العلم بها كالبرامج المحاسبية، ويسمون أيضا المخترقون وهم عبارة عن أشخاص متطفلون، غالبا ما يكون ارتكابهم الجرائم بدافع التحدي ودخول إلى المواقع لإثبات الذات وهم في الغالب في سن المراهقة.[72]
- **الكراكرز-المحترفون-:** يتميزون بخطورة إجرامية كبيرة مقارنة بالنوع الأول، قد يكون هدفهم الاعتداء لكسب المال وذلك من خلال الدخول إلى البنوك والمؤسسات المالية، وقد يرتكبها الجاني بهدف تحقيق أبعاد سياسية أو طرح فكرة معينة أو توجه معين، أو قد يمس منشئات ومؤسسات أخرى، فهذا النوع من الجرائم يرتكب من طرف محترفي الاجرام الالكتروني، وعادة ما يكون متطرف أو جاسوس أو محترف الأنظمة.[73]
- **الموظفون العاملون في مجال الأنظمة المعلوماتية:** بالنظر إلى طبيعة المهام المنوطة بموظفي تقنية المعلومات، وارتباطهم الوثيق بالأنظمة المعلوماتية بوصفها مجال اختصاصهم الرئيسي، وما يتمتعون به من خبرات ومهارات فنية عالية، فإن

[71] عبد العزيز أحمد، **خصوصية التحقيق في الجريمة المعلوماتية**، المرجع السابق، ص19-20.

[72] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 86.

[73] د. رقية محمودي، نفس المرجع.

بعضهم قد يستغل هذه المعرفة لارتكاب جرائم رقمية تخدم مصالحه الشخصية، لا سيما في تحقيق مكاسب مادية غير مشروعة. وتزداد خطورة هذا النوع من الجرائم عندما يكون مرتكبها موظفًا تربطه علاقة عمل مباشرة مع الضحية، إذ أن تلك العلاقة تتيح له سهولة النفاذ إلى المعلومات أو الأنظمة، مستفيدًا من مستوى الثقة الذي يحظى به في بيئة العمل..[74]

- **المجرمون أصحاب الآراء المتطرفة:** تُعد هذه الفئة من الكيانات الإرهابية أو المتطرفة التي تتكون من أفراد تجمعهم قناعات اجتماعية أو سياسية أو دينية يسعون إلى فرضها باستخدام وسائل غير مشروعة، من بينها ارتكاب أفعال إجرامية. ويتجسد نشاطهم في الغالب من خلال ممارسات عنيفة تستهدف الأشخاص والممتلكات، وذلك بقصد جذب الانتباه إلى أفكارهم. وقد أفرزت البيئة الرقمية، لا سيما عبر شبكة الإنترنت، مساحة خصبة لتمكين هذه الجماعات من الترويج لأيديولوجياتها، ونشر محتوى قد يعرّض النظام العام وأمن الدول للخطر، فضلاً عما قد يتضمنه من إساءات وتشهير.[75]
- **المجرم الرقمي في إطار الجريمة المنظمة:** تقوم جماعات الجريمة المنظمة بتبني أصحاب الكفاءات وأصحاب الخبرة والموهوبين في مجال تقنية المعلومات، وذلك بإغراقهم بالمال لينظموا إلى صفوفها وتقوم بتدريبهم وزيادة مهاراتهم في هذا المجال لخلق مجرمين متخصصين في الجرائم الالكترونية في إطار هذه المنظمات، ويمارس المجرم الرقمي في نطاق هذه المنظمات نشاطات تدر على المنظمة أرباحا هائلة فيقومون بتزوير البرامج وتقليدها واختراق شبكات المعلومات الخاصة بالدول والمؤسسات المالية الكبرى العالمية، كما يمارسون أعمال التجسس الصناعي و التجاري.[76]

ثانيا: الضحية

قد يكون ضحية الإجرام المعلوماتي أشخاصا طبيعية أو معنوية إذ أن المجرم المعلوماتي يقوم مباشرة بقرصنة الحواسيب أو الهواتف أو اختراق البريد الالكتروني أو حسابات الأفراد على منصات مواقع التواصل الاجتماعي، كما تشكل الجرائم الالكترونية التي تستهدف الأشخاص المعنوية خطرا سواء في القطاع العام أو القطاع الخاص كالشركات التجارية والبنوك،

[74] الخليفي عبد الله بن محمد، **الجرائم المعلوماتية: دراسة فقهية نظامية**، الطبعة الثانية، مكتبة الرشد، الرياض، 2021.

[75] محمد الحمادي، "**المساهمة والتحريض على الإرهاب الإلكتروني عبر وسائل التواصل الإلكتروني في القانون الإماراتي**"، مجلة البحوث القانونية والاقتصادية، العدد 4، 2023، ص 15.

[76] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 326.

الوزارات، المستشفيات.....الخ[77]، أما الأخطر فهو أن تكون بالدولة أو الواقعة بالمجال العسكري من خلال عمليات التجسس.[78]

وللضحية دورا مهم في مساعدة الجاني على ارتكابه للجريمة، حيث أن العلاقة التي تجمعهما وبحكم العمل بإمكانها أن تحدث جريمة كون الجاني يعمل لحساب الضحية ولديه مكتسبات ودراية في مجال الأنظمة المعلوماتية وكذا الثغرات الأمنية فيها، مما يجعله محل ثقة ومأمن للضحية على خبايا مؤسسته، ومثال ذلك كأن يكون هو المسؤول عن المركز المعلوماتي فيستغل مركز الثقة الذي يحوزوه والألفة التي بينه وبين هذه الأنظمة، وذلك ما حدث في إحدى القضايا أن كان الجاني يعمل مستشارا لدى أحد البنوك الكبرى وكان يتمتع بثقة مطلقة من جانب هذا البنك مكنته من الدخول في مفتاحين الكترونيين من أصل ثلاث أساسية للتحكم في التحويلات الالكترونية للنقود من بنك أخر، وتمكن بفضل قدراته في هذا المجال من الوصول إلى المفتاح الثالث، لينقل في الحال مبلغ عشرة (10) ملايين دولار إلى حساب بنكي فتح باسمه في سويسرا وقد القي القبض عليه وصدر ضده حكم السجن لمدة ست (6) سنوات.[79]

ومن الضحية أيضا ما تستهد الجرائم الالكترونية الأطفال والمراهقين الذين هم صفر خبرة في مجال الالكترونيات ويقعون ضحية غش الكتروني أو سرقة معلومات سرية عن مصاريفهم أو أموالهم، ومثال ذلك طالب في المرحلة الثانوية أسمه أحمد مولع بالألعاب الالكترونية، قام بتحميل لعبة جديدة وجذابة من موقع غير موثوق به، وعندما حاول فتح اللعبة طلب منه إدخال معلومات حساسة عن بطاقة الائتمان، ودون تفكير قام أحمد بإدخال المعلومات المطلوبة، ولكنه اكتشف بعد ذلك سرقة مبلغ كبير من حسابه البنكي. وما أكثر القصص المؤسفة التي تتردد حول الجريمة الالكترونية، وما ينتج عنها من سرقة وابتزاز وتنمر، وقرصنة ونشر شائعات، وغير ذلك.[80]

ثالثا: الشاهد المعلوماتي

تختلف الشهادة في الجريمة المعلوماتية عن تلك المعتاد الأخذ بها في الجريمة التقليدية، نظرا للبيئة الافتراضية التي ترتكب فيها هذا النوع من الجرائم وبالتالي فإن الشهود غالبا ما يكونوا من الأشخاص المحيطون بهذه البيئة اللامادية وهم الأشخاص الذين لهم دراية وخبرة في مجال تكنولوجيا المعلومات و الاتصال[81]، قفد تعددت التعاريف لدى الفقهاء فيما يخص الشهادة

---

[77] سويسي فتيحة، **التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها**، المرجع السابق، ص11.

[78] عبد الرؤوف بوديسة بجاد، **آليات التحري عن الجريمة الالكترونية في القانون الجزائري**، مذكرة لنيل شهادة ماستر مهني في الحقوق، تخصص قانون الإعلام الآلي والانترنيت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، سنة 2021-2022، ص17.

[79] خليفة محمد، **خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها**، كلية الحقوق والآداب والعلوم الاجتماعية، جامعة 08 ماي 45 القالة، د.س.ن.

[80] www-aljazeera-net.cdn.ampproject.org,28/04/2025,08:44.

[81] فتيحة سويسي، **التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها**، المرجع السابق، ص11.

فهناك من يعرفها على أنها الأقوال التي يدلي بها الخصوم أما سلطة التحقيق أو الحكم في شأن جريمة وقعت سواء تتعلق بثبوت واقعة معينة من خلال ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه عن هذه الواقعة بطريقة مباشرة وللشهادة ثلاثة أنواع:

***الشهادة المباشرة:** وهي أن يشهد الشاهد بما شاهده أو وقع تحت سمعه

***الشهادة السماعية:** هي سماع شاهد فرعي لشاهد أصلي حيث يروي عنه ما شاهده أو سمعه وهي أقل شأنا من الشهادة الأصلية المباشرة

***الشهادة بالتسامع:** وهي شهادة تختلف عن الشهادة السماعية حيث تتعلق هذه الأخير بشهادة نقلت عن شخص معين قد شاهد الأمر بنفسه، أما الشهادة بالتسامع هي نقل واقعة معينة لكنها ليست نقلا عن شخص معين بالذات وانما يتداولها الناس فيما بينهم ويقولون سمعنا أو شاهدنا عن فلان كذا وكذا من هذه الواقعة

***الشهادة الإلكترونية:** يعرف الشاهد الالكتروني على انه الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية لازمة للدخول الى نظام المعالجة الآلية للبيانات وقد يكون الشاهد مشغلو الحاسب الآلي، خبراء البرمجة، مهندسو الصيانة، مديرو النظم، المحللون.... الخ [82]

رابعا: محل الجريمة الالكترونية

***المعلومات:** تتضمن الجرائم الإلكترونية، أفعالاً غير مشروعة تستهدف أنظمة المعلومات ووسائل الاتصال الرقمية، مثل الدخول غير المشروع إلى البريد الإلكتروني والتلاعب بمحتوياته، أو الاستيلاء على البيانات والمعلومات المخزنة في المواقع الإلكترونية دون وجه حق، وهو ما يشكل مساساً صارخاً بسرية المعلومات وخصوصية الأفراد، فضلاً عن انتهاك حقوق الملكية الفكرية، مما يُدخل هذه الأفعال في نطاق التجريم المعلوماتي وفقاً للتشريعات الحديثة.[83]

***الأجهزة:** تشمل الجرائم الالكترونية في هذه الحالة تعطيل أجهزة الكمبيوتر أو تخريبها عبر إرسال الفيروسات أو البرامج التي تحوي أنظمة هجومية مما يسبب تلفا في أنظمة الكمبيوتر يؤدي لشلل كل الأنشطة المرتبطة بهذا الجهاز أو الأنظمة المرتبطة به.

[82] عبد العزيز أحمد، **خصوصية التحقيق في الجريمة المعلوماتية**، المرجع السابق، ص 24.

[83] زينب طرفي العنزي، **"الجريمة الإلكترونية في ميزان الفقه والقانون"**، مجلة الدراسات الإسلامية والبحوث الأكاديمية، العدد 99، 2022، ص 45.

ولنتصور مدى الدمار والخسائر التي ستلحق بشبكة مصاريف مرتبطة بأنظمة عبر كمبيوتر مركزي يحوي حسابات علماء، فما الذي سيحصل لو تم تعطيل الكمبيوتر المركزي أو إتلاف أنظمته؟

فمثلا في الولايات المتحدة الأمريكية أصدر مكتب التحقيقات الفيدرالي الأمريكي إنذار عاما يحذر مستخدمي الانترنت من مخاطر رسائل الكترونية جديدة، تنطوي على فخ يدفع المستخدمين الى الكشف عن بيانات حساباتهم المالية الشخصية، ليصار لاحقا الى السطو عليها

وحذرت دائرة شكاوى جرائم الانترنت التابعة للمكتب الفيدرالي، من ظهور مجموعة من الرسائل الالكترونية التي تزعم أن المتلقي قد قام بعمليات شراء لبضائع عبر الشبكة، وتستدرجه للكشف عن بيانات حساباته، وقالت الدائرة إن نموذجين من تلك الرسائل تم رصدهما، تدعي الأولى أن المتلقي قد عقد طلبية لشراء جهاز كمبيوتر عبر الشبكة، وتطلب منه في حال عدم رغبته بإتمام الطلبية الدخول الى وصلة البيانات الشخصية حول حساباته المالية، يتوجب عليه الكشف عنه لإلغاء عملية الشراء المزعومة، مرسلة كملف PDF، تحتوي على فيروس يتسلل الى جهاز الكمبيوتر الشخصي للمتلقي، ما أن يقوم بالدخول وتشغيل الرسالة لقراءتها

***الأشخاص أو الجهات:** تهدف فئة كبيرة من الجرائم الالكترونية اشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز أو السرقة أو ممارسة الفاحشة، فمثلا سرقة المال عبر الانترنت باستخدام أرقام لبطاقات مصرفية تعود للغير، أو على الفجور وممارسة الفاحشة مع قاصر عبر الانترنت، أو الإرشادات التي تحمل في طياتها تعليمات إرهابية كلها موجهة ضد أشخاص أو جهات بعينها.[84]

الفرع الثالث: موقف بعض التشريعات من الجريمة الالكترونية

أولا: موقف التشريعات الدولية من الجريمة الالكترونية

1-اتفاقية بودابست: تم إبرام أول المعاهدات المتعلقة بمكافحة الجريمة الالكترونية أو جرائم الانترنت، وكان هذا عام 2001، بعاصمة المجرية بودابست، فقد تم صياغة المعاهدة من طرف عدد كبير من الخبراء المختصين في القانون في مجلس أوروبا، وبمساعدة دول أخرى لاسيما الولايات المتحدة الأمريكية، وبعد مشاورات عديدة بين الحكومات وأجهزة الشرطة وقطع الكمبيوتر على المستوى العالم، هذا ما أدى في النهاية إلى توقيع من قبل 30 دولة بتاريخ 23 نوفمبر 2001، في العاصمة المجرية بودابست. تتكون هاته الاتفاقية من 48 مادة، وأكدت الاتفاقية على حاجة إلى إتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر، ومخاطرها على الدول، كما تضمنت عدة توصيات للدول الأعضاء لمكافحة

[84] عبد الله دغش العجمي، **المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة**، المرجع السابق، ص 35-36.

جرائم الكمبيوتر واعتبرت مرجعا لا يستهان به في ميدان محاربة الإجرام سبيراني، سواءا بالنسبة لبعض الاتفاقيات اللاحقة ذات الصلة أو بالنسبة للتشريعات الداخلية. [85]

2-**الجمعية العامة لمنظمة الأمم المتحدة:** صدر عن الجمعية العامة لمنظمة الأمم المتحدة عدة قرارات تتعلق بمكافحة الجرائم الالكترونية والتي كان أهمها القرار 121/45 لسنة 1990 المتعلق بدليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها والقرارات رقم 70/53 الصادر بتاريخ 4 ديسمبر 1998 والقرار رقم 45/54 الصادر في 1 ديسمبر 1991 والقرار رقم 28/55 الصادر في 20 نوفمبر 2000 والقرار رقم 19/56 الصادر في 29 نوفمبر 2001 والقرار رقم 53/57 الصادر في 22 نوفمبر 2002 والقرار رقم 32/558 الصادر في 18 ديسمبر 2003 حول موضوع التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي وبعض القرارات الأخرى.[86]

وفي يوم الثلاثاء 24 كانون الأول/ ديسمبر 2024 اعتمدت الجمعية العامة للأمم المتحدة اتفاقية جديدة لمنع ومكافحة الجرائم الالكترونية، في ختام عملية تفاوض استمرت خمس سنوات، تهدف هذه الاتفاقية إلى المنع ومكافحة الجرائم الالكترونية بكفاءة وفعالية أكبر من خلال التعاون الدولي وتقديم المساعدة الفنية ودعم بناء القدرات، وخاصة لدول النامية، وقد قال رئيس الجمعية فيليمون يانغ: " باعتماد هذه الاتفاقية، أصبحت في متناول يد الدول الأعضاء الأدوات والوسائل لتعزيز التعاون الدولي في منع ومكافحة الجرائم الالكترونية وحماية الأشخاص وحقوقهم عبر الانترنت"، واعتمدت الجمعية العامة القرار دون تصويت حيث تفاوضت دول الأعضاء بمداخلات من المجتمع المدني والمؤسسات الأكاديمية والقطاع الخاص، على النص لأكثر من خمس سنوات، وسيتم فتح الاتفاقية للتوقيع في حفل رسمي تستضيفه فيتنام في عام 2025، وستدخل الاتفاقية حيز التنفيذ بعد 90 يوما من التصديق عليها من قبل الدول الموقعة الأربعين.[87]

ثانيا: موقف المشرع المصري من الجريمة الالكترونية

لقد حرص المشرع المصري على مكافحة الجرائم الالكترونية في نصوصه القانونية كغيره من القوانين الأخرى، حيث ارتكز على فلسفة تشريعية تستهدف مواكبة التشريع المصري للتغيرات المتلاحقة التي تشهدها الساحة من ظهور أنماط جديدة من الجرائم المرتبطة بالتطورات التكنولوجية في وساء الاتصالات، وتحقيق التوازن بين الحماية الجنائية لحرمة الحياة الخاصة التي يكفلها الدستور والمحافظة على المعلومات وكفالة سريتها وعدم إفشائها أو التنصت عليها إلا بأمر قضائي مسبب، وبين

[85] الطاهر ياكر، **مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية**، مجلة الصدى للدراسات القانونية والسياسية، المجلد 4 العدد 4، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، 2022، ص 21-22.

[86] الطاهر ياكر، **الجرائم الالكترونية الأحكام الموضوعية والإجرائية دراسة مقارنة**، طبعة 2024، دار بلقيس للنشر، 2024، ص 159.

[87] https://news.un.org/ar/story/2024/12/1137776,03/05/2024,00:28.

مواجهة تلك الجرائم والأفعال ومكافحتها والحد من آثارها. وقد جاءت في مذكرة ايضاحية للقانون الغاية من إصدار المشرع المصري لقانون مكافحة جرائم تقنية المعلومات.[88]

تطرق المشرع المصري إلى استحداث هو كذلك قانون خاص بمكافحة الجرائم الالكترونية بموجب القانون رقم 175 لسنة 2018 المتعلق شأن مكافحة جرائم تقنيات المعلومات في المواد من 01 إلى غاية 45، حيث ركز في الباب الثالث المعنون بالجرائم والعقوبات بحصر بعض الجرائم التي تشكل خطورة على حياة الأفراد وبتشديد العقوبة على من يرتكب تلك الأفعال والمنصوص عليها في الفصل الأول تحت عنوان الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنينها، أما الفصل الثاني فقد تحدث عن الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات ، جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الالكتروني، وقد أضاف الفصل الثالث الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع، إضافة إلى الجرائم المرتكبة من مدير الموقع في الفصل الرابع و المسؤولية الجنائية لمقدمي الخدمة المعنون في الفصل الخامس، أما باقي الفصول فهي تتحدث عن العقوبات التي تأخذ الظروف المخففة للجناة وكذا الظروف المشددة. [89]

ثالثا: موقف المشرع الجزائري من الجريمة الالكترونية

لقد أبدت الجزائر التي تعتبر دولة رائدة إقليميا في مجال الأمن المعلوماتي استعدادها منذ سنوات لمكافحة الجرائم السيبرانية والمعلوماتية بشكل حازم، لذا عكفت على إعداد النصوص القانونية القادرة على إنشاء منظومة دفاعية وقائية يتم على أساسها مكافحة الأعمال الإجرامية المتعلقة بالأنترنت ومتابعة مرتكبيها قضائيا، كما تسمح بتقصي آثار المجرمين والجناة الذين يستغلون التكنولوجيا وتطبيقاتها لارتكاب أعمالا إجرامية وغير قانونية.

-فكيف ساهمت النصوص المختلفة في مكافحة ومحاربة الأجرام السيبراني أو الإجرام المعلوماتي؟

-وبعبارة أخرى كيف واجه التشريع الجزائري الجرائم السيبرانية؟

حاول المشرع الجزائري إصدار قوانين عامة وخاصة وهياكل وأجهزة للجرائم الالكترونية ومن بينها:

---

[88] د. رامي متولي القاضي، **المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون (175) لسنة 2018م مقارنا بالمواثيق الدولية والتشريعات المقارنة**، مجلة البحوث القانونية والاقتصادية، العدد 25، مارس 2021، ص 1012.

[89] المواد من 01 إلى 45 من قانون 175 لسنة 2018، **في شأن مكافحة جرائم تقنية المعلومات**، ج ر، العدد 32 مكرر (ج) في 14 أغسطس سنة 2018.

كفل الدستور الجزائري الصادر في 06 مارس 2016 حماية الأساسية والحريات الفردية وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان منها المواد 38، 44 من الدستور.

وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات وقانون الإجراءات الجزائية والتي تحظر كل مساس بهذه الحقوق.

1-قانون العقوبات:

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي حيث عدل قانون العقوبات بموجب القانون رقم 24-06 المؤرخ في 28 أبريل 2024 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، تحت عنوان:" المساس بأنظمة المعالجة الآلية للمعطيات، ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 7.[90]

2-قانون الإجراءات الجزائية:

قام المشرع الجزائري بتمديد الاختصاص المحلي لوكيل الجمهورية في مجال الجرائم الالكترونية، طبقا للمادة 37 فقرة 02 من قانون الإجراءات الجزائية.

حيث يمتد الاختصاص المحلي إذا تعلق الأمر بجرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد والتهريب.

كما تعد هذه الجرائم أيضا من الجرائم الموصوفة طيقا للتشريع الجنائي الجزائري.

بيّن المشرّع الجزائري في الفقرة السابعة من المادة 45 من القانون رقم 06-22، المعدل والمتمم لقانون الإجراءات الجزائية، خصوصية الإجراءات المرتبطة بالتفتيش الإلكتروني، موضحًا أن هذا الأخير يخرج عن الإطار التقليدي للتفتيش من حيث القواعد الإجرائية والشروط الشكلية والموضوعية المعتمدة في القانون العام. وقد أُقرّ استثناء صريح من تطبيق المادة 44 من نفس القانون في الحالات المتعلقة بالجرائم الإلكترونية، نظرًا للطبيعة التقنية والمعقدة التي تميز الأفعال الماسة بالأنظمة المعلوماتية. وفي السياق ذاته، نصت الفقرة السادسة من المادة 51 من القانون ذاته على إمكانية توقيف النظر في جريمة

[90] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 205.

المساس بأنظمة المعالجة الآلية للمعطيات، ما يعكس توجّه المشرّع نحو تبني معالجة خاصة لهذه الجرائم، تأخذ بعين الاعتبار خصوصيتها البنيوية وتحديات الإثبات المرتبطة بها.[91]

كما نص أيضا قانون الإجراءات الجزائية بموجب المادة 65 مكرر 3 فقرة 5 أنه في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن وكيل الجمهورية المختص يقوم بوضع الترتيبات التقنية دون موافقة المعني، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة.

وفي عام 2006، أدخل المشرع تعديل آخر على قانون العقوبات بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، من هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال.

وبعد التعديل الأخير لقانون العقوبات الجزائري بموجب القانون رقم 24-06 المؤرخ في 19 شوال 2024، ضمن القسم السابع مكرر من قانون العقوبات بموجب المواد من 394 مكرر إلى 394 مكرر 8 فقد تم تشديد العقوبة أكثر من ذي قبل.

وبعد التعديل الأخير لقانون العقوبات الجزائري بموجب القانون رقم 16-02 المؤرخ في 19 يونيو 2016، ضمن القسم السابع مكرر من قانون العقوبات بموجب المواد من 394 مكرر إلى 394 مكرر 8.

وضمن نطاق الفصل الثالث الخاص بالجنايات والجنح ضد الأموال، من بين هذه الجرائم: الغش أو الشروع فيه في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات، حذف أو تغيير للمعطيات المنظمة، إدخال أو تعديل في نظام المعطيات، تصميم أو بحث أو تجميع أو توفير أو نشر أو حيازة أو إفشاء أو استعمال المعطيات، تكوين جمعية أشرار.[92]

3-صدور قانون رقم 09-04:

عمليا، سعت الجزائر إلى استدراك الفراغ القانوني من خلال تعزيز منظومتها التشريعية خاصة منذ 2009، بحيث سن المشرع الجزائري القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بتاريخ 05 أوت 2009.

---

[91] القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-155 **المتضمن قانون الإجراءات الجزائية**. الجريدة الرسمية، العدد 84، 24 ديسمبر 2006، ص 3-19.

[92] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 205

يحتوي هذا القانون على 19 مادة موزعة على 06 فصول مستمدة من الاتفاقيات الدولية. كما جاء مطابق للتشريعات الوطنية لاسيما تلك المتعلقة بمحاربة الفساد وتبييض الأموال وتمويل الإرهاب، حيث نص القانون رقم 09-04 وبموجب الفصل الخامس منه على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

ومن أبرز مهام الهيئة الوطنية تعزيز التعاون القضائي والأمني على الصعيدين الإقليمي والدولي، فضلاً عن إدارة وتنسيق الجهود الوقائية والعمليات الميدانية ذات الصلة بمكافحة الجرائم السيبرانية. كما تتولى الهيئة تقديم الدعم الفني والتقني للسلطات القضائية والأمنية المختصة، ويجوز تكليفها بإجراء خبرات قضائية متخصصة في حال وقوع اعتداءات إلكترونية تستهدف سلامة المنظومة المعلوماتية للدولة، متى كان من شأن تلك الاعتداءات تهديد المؤسسات الدستورية، أو إلحاق الضرر بأمن الدفاع الوطني، أو الإضرار بالمصالح الاستراتيجية للاقتصاد الوطني.[93]

وذلك بالتعاون مع جهات قضائية أخرى منها المعهد الوطني للأدلة الجنائية وعلم الإجرام والمديرية العامة للأمن الوطني مكافحة الجريمة الالكترونية ذات البعد الدولي من خلال انضمامها للمنظمة الدولية للشرطة الجنائية INTERPOL

علاوة على ذلك يجب التنويه بالجهود التي تقوم بها الجزائر منذ جانفي 2015 من أجل تكييف إطارها التشريعي والتنظيمي من خلال تبني مجموعة من القوانين الهامة منها الخاصة بالتوقيع والمصادقة الالكترونية التي من شأنها تطوير الخدمات المقدمة غبر الانترنت مثل الإدارة الالكترونية، التجارة الالكترونية وكذا البنوك الالكترونية، فضلا عن سعي الجزائر الحثيث إلى إرسال قاعدة قانونية لاستخدام التكنولوجيات الجديدة للإعلام والاتصال في تطوير قطاع العدالة.[94]

خلاصة الفصل:

وفي ختام هذا الفصل، يتبين لنا أن الجريمة الالكترونية تمثل أحد أبرز التحديات المعاصرة التي تواجه المنظومات القانونية في مختلف الدول، بالنظر الى طبيعتها المستحدثة وتطور وسائل ارتكابها بشكل متسارع بفضل الطفرة التكنولوجية. وقد

[93] الهيئة الوطنية للأمن السيبراني ومهامها في حماية الفضاء الرقمي." الجريدة الرسمية للدولة، العدد 45، 2023، ص 12.

[94] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 206.

سعينا في هذا الفصل إلى الإحاطة بالإطار النظري للجريمة الإلكترونية، من خلال التعريف بها، وبيان خصائصها، وتمييزها عن غيرها من الجرائم التقليدية عن طريق السمات الخاصة بالمجرم المعلوماتي والأفعال الاجرامية التي يقوم بها، إضافة الى تصنيف صورها المختلفة.

وقد أظهر وصفنا في هذا الإطار الى تعدد الجرائم الالكترونية لتشمل طيفا واسعا من الأفعال الإجرامية، من أبرزها: اختراق الأنظمة، الاحتيال عبر الانترنت، الابتزاز الالكتروني، التزوير المعلوماتي، الاعتداء على المعطيات الشخصية ونشر المحتويات غير القانونية عبر الشبكات الرقمية كل هذه الجرائم الالكترونية تتفرع منها جرائم أخرى ذات كفاءة عالية من التطور. كما تتعدد الأطراف المتدخلة في هذه الجرائم بين فاعل مباشر، ومساهم أو شريك، وقد يكون الضحية إما فردا، مؤسسة أو حتى دولة نفسها، ما يجعل هذه الجرائم أكثر تعقيدا من حيث البنية والعلاقات.

وفي السياق الجزائري، لم يبق المشرع بمنأى عن هذه التحديات، حيث بادر الى إدراج نصوص قانونية لمكافحة الجرائم الالكترونية ضمن قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها (القانون رقم 09-04 لسنة 2009). كما عمل على تحديث الإطار القانوني عبر تعزيز التعاون القضائي الدولي، ووضع آليات تقنية وأمنية تهدف الى الكشف عن مرتكبي هذا النوع من الجرائم مع الاعتراف بصعوبة إثباتها وتعقيد إجراءات تتبعها بالطرق التقليدية.

ويمهد هذا الإطار النظري للانتقال إلى دراسة الجوانب القانونية والتنظيمية والعملية لمكافحة هذه الجرائم، وهو ما سيتم التطرق إليه في الفصول اللاحقة، بالتركيز على آليات المواجهة، والجهود الوطنية والدولية المبذولة في سبيل الحد من هذا الخطر الرقمي المتنامي.

الفصل الثاني

ضوابط البحث والتحري في الجريمة الالكترونية

تمهيـــــد:

إن التهديدات التي تثيرها الجرائم الالكترونية أضحت أكثر خطورة على الأمن العام، وذلك بسبب التطورات التكنولوجية المتسارعة والانتشار الواسع لاستخدامات الانترنت والذي ترافق مع الاستغلال الغير مشروعة للفضاء الرقمي من قبل مجرمين باتوا يسعون لتخريب الأنظمة المعلوماتية بطرق جد معقدة ويصعب اكتشافها بالوسائل التقليدية، وهذا ما يشكل تحديا كبيرا للأجهزة العدالة. ومن هنا تبرز أهمية وضع ضوابط واضحة ومحددة لعمليات البحث والتحري بالاعتماد على وسائل أكثر حداثة وبالاستعانة إلى محققين متخصصين ذوي كفاءات عالية يمتلكون خبرة ومهارات أكثر تطورا بالإضافة إلى القدرة على مواكبة مثل هاته الجرائم وفهم طبيعتها المتغيرة باستمرار، وكذا تحقيق التوازن بين فعالية الإجراءات الأمنية من جهة، وضمان احترام حقوق الأفراد وحرياتهم الأساسية من جهة أخرى، وفي هذا السياق إرتأينا دراسة الضوابط الخاصة بالبحث والتحري في هذا الفصل بحيث تشمل الجوانب القانونية والتقنية التي يجب مراعاتها أثناء جمع الأدلة، وتحليلها، واستخدامها في الإجراءات القضائية وذلك لضمان نزاهة التحقيق وعدالة المحاكمة.

يتناول هذا الفصل في المبحث الأول السمات والخصائص التي ينبغي ويجب أن يتصف بها المحقق في الجرائم الالكترونية، والتي تقتضي الإلمام بالجوانب التقنية، والتحليلية، والقدرة على التعامل مع الأدلة الرقمية وفهم الإطار القانونية المتعلقة بهذه الجرائم، فدور المحقق في هذا المجال لا يقتصر على جمع الأدلة فقط بل يتعين عليه تحليلها وفهم السياق الذي ارتكبت فيه الجريمة، ما يتطلب إعدادا خاصا ومهارات متقدمة كما سنعرض الاختصاصات الخاصة بالضبطية القضائية بمختلف الجواني وعلى المستوى العالمي، وكعنصر أخر سنتطرق لمعرفة الأجهزة التي كلفت لعملية البحث والتقصي عن الجرائم الالكترونية على المستويين الدولي والوطني

أما المبحث الثاني، فسيتم عرض إجراءات ووسائل البحث والتحري في الجرائم الالكترونية، مع التركيز على آليات جمع الأدلة الرقمية، والتقنيات الحديثة المستخدمة في تتبع الجناة.

المبحث الأول: المحققين في الجرائم الالكترونية واختصاصاتهم

يعد المحققين في الجرائم الالكترونية من الخبراء المختصين في تتبع الأنشطة الإجرامية التي ترتكب في العالم الرقمي، فهم يتمتعون بمهارات تقنية عالية تمكنهم من الكشف بسهولة عن المجرمين، كما تتنوع اختصاصاتهم لتشمل التحقيق في جرائم الاختيال المالي، الهجمات السبيرانية على الأنظمة الحكومية الخاصة...الخ، وفي هذا المبحث سندرس عن الموضوع بالتفصيل:

المطلب الأول: المحققين في الجريمة الالكترونية

الفرع الأول: التعريف بالمحقق في الجرائم الالكترونية

تعدّدت التعريفات الفقهية للمحقّق الجنائي في إطار القانون الجنائي، وقد عرّفه بعض الفقهاء بأنه: "شخص أو موظف عام، أو من يكلف بخدمة عامة، يمتلك التأهيل القانوني والخبرة الفنية، ويقوم باتباع إجراءات ووسائل مشروعة تهدف إلى الكشف عن الحقيقة، من خلال جمع الأدلة التي تُثبت وقوع الجريمة، وتحديد كيفية ارتكابها، ودوافعها، والتوصل إلى الجناة.[95]

كما عرفه البعض بأنه" من عهد إليه القانون التحقيق في الجرائم بموجب الصلاحيات المخولة له من أحكام القوانين الشكلية" وذهب بعض آخر من الفقه بتعريفه بأنه" أي أعضاء النيابة العامة أو قضاة التحقيق أو أي شخص يعهد إليه بموجب القانون مباشرة بعض إجراءات أو كل الإجراءات المتعلقة بالتحقيق"[96]، وعرف آخر المحقق بأنه" كل من عهد إليه بتحري الحقيقة في الحوادث الجنائية وتحقيقها وكشف غموضها وجمع الأدلة ضد الجاني تمهيدا لمحاكمته". [97]

أما تعريف المحقق الجنائي في الجرائم الالكترونية بأنه" **الشخص المكلف بالبحث عن الحقيقة في الجريمة الالكترونية لكشف فاعلها وجمع أدلة البراءة أو الإدانة ضدهم تمهيد لإحالتهم إلى المحكمة ويتحدد دورهم بتنفيذ إجراءات القانون الملقاة كل على حسب اختصاصه سواء في دائرة اختصاصه المكاني، أو على المستوى الدولة"[98]**

فالمحقق الجنائي هو الشخص القائم بأعمال إجراءات التحقيق الجنائي ولا يختلف تعريف المحقق في الجرائم التقليدية (العادية) عن تعريفه في الجرائم الالكترونية، فالفرق هنا في نوعية الجريمة وليس في المحقق، ويتضح من التعريفات السابقة أن الاختلاف

---

[95] د. براهيم محمد طاهر، **تنظيم التحقيق الابتدائي في الجرائم الالكترونية**، دار وائل للنشر، عمان، ط1، 2013، ص 53.

[96] د. مجيد خضر السبعاوي، أ. مولان قادر أحمد، **الضرورة الإجرائية في مرحلة التحقيق الابتدائي (دراسة تحليلية مقارنة)**، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص 148.

[97] د. حسن صادق المرصفاوي، **المرصفاوي في المحقق الجنائي**، منشأة دار المعارف الإسكندرية، 1977، ص 27.

[98] د. محمد أنور عاشور، **المبادئ الأساسية في التحقيق الجنائي العملي**، عالم الكتب، القاهرة، 1987، ص 15.

راجع إلى الاختلاف في نطاق النظر إلى عمل المحقق أو تحديده من حيث ما يقوم به المحقق من إجراءات ووسائل في حين اتجهت التعريفات من حيث مهام عمله والأعمال المنوط القيام بها ويخرج من هذه التعريفات:

- المحقق الجنائي، بصفة عامة هو شخص قائم بأعمال التحقيق الجنائي ولا يختلف تعريفه في الجرائم الالكترونية عن تعريفه في الجرائم التقليدية، فالفرق كما أشرنا في نوعية الجريمة المرتكبة وليس في شخص محقق
- الاختلاف في هذه التعريفات يرجع إلى الاختلاف في عمل المحقق أو تحديده فقد عرفه الفقهاء من حيث ما يقوم به المحقق من إجراءات ووسائل، في حين عرفه فقهاء آخرون من حيث النظر إلى مهام عمله والأمور المنوط القيام بها.
- أن هناك قاسم مشترك بالاتفاق بين هذه التعريفات على أن المحقق شخص قانوني محدد بموجب القانون وحدد له وظائفه وواجباته المكلف بها فيتولى عموما المحقق في كل الأحوال جمع الحقائق معتمدا على الوسائل العملية والفنية من أجل بلوغ أهداف منها:

1-كشف غموض الجريمة بغرض اثبات حقيقتها ووقوعها

2-معرفة هوية المتهم وتحديد مكان القبض عليه

3-تحضير الأدلة للإثبات ضد المتهم وتقديمه للمحاكمة

4-التقنيات المستخدمة في ارتكابها

5-الأسباب والدوافع المحتملة لارتكابها منذ نشوئها والتفكير بها والتحضير لها على أدلة ووقائع.[99]

فالتحقيق فن استخلاص أمور مخفية من أمور ظاهرة فله خمس ملكات: (ملكة الادراك، ملكة الانتباه، ملكة الاستنتاج، وملكة النقد والحكم) وله من الأساليب المعاصرة ما يلي:

- المعلومات الارشيفية والرسمية والاستدلالية التي يراد بها وجهة المحقق وتحديد خطواته على مهارته والدهاء والخبرة في انتزاع الحقائق وربطها بين الأفكار ومعلومات التحقيق دون المساس بقرينة البراءة لدى المتهم وحقه في الدفاع
- استجماع الآثار المادية وهي تطبيق أساليب العلوم الطبيعية في تسجيل الآثار المادية للجريمة[100]

كما توكل مهمة التحقيق في الجرائم الالكترونية الى نوعين من المحققين:

[99] محمد صلاح، محمد عبد المنعم، **الجرائم الالكترونية وتحدياتها دراسة مقارنة**، رسالة دكتورة، كلية الحقوق، جامعة المنصورة، 2005، ص 234.

[100] د. سلطان الشاوي، **أصول التحقيق الإجرامي**، المكتبة القانونية للتوزيع، بغداد 1900، ص11.

النوع الأول: نوع يمثل الخبرة الفنية المتخصصة في أنظمة أجهزة الكمبيوتر والأجهزة الأخرى المرتبطة بها حيث يتم الاستعانة بهم في جميع مراحل ضبط الجرائم واكتشافها والتحقيق فيها بالإضافة الى تقديم الأدلة الجنائية أمام سلطات التحقيق بالطريقة والكيفية التي تم ارتكابها.

النوع الثاني: نوع يمثل الكفاءة المتخصصة في مجال التحقيق الجنائي لما يتصف به من قدرة ومكونات شخصية تمكنه من استنتاج الحقائق للوصول إلى أدلة يستند إليها في إقامة رفع الدعوة الجنائية.[101]

الفرع الثاني: فرق البحث والتحري في الجرائم الالكترونية

ان التحقيق الابتدائي في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص وأحد بمفرده حتى ولو كانت المضبوطات هي مجرد حاسب شخص وأحد، ولذلك فإنه يفضل أن يتعاون عدة محققين في إنجاز مهمة التحقيق والعثور على الأدلة.

ويجب أن يتشكل فريق التحقيق من فئتين وأخصائيين ذوي خبرة في مجال الحاسوب والانترنت، ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الالكتروني بشكل خاص، لهؤلاء المحققين ان يستعينوا بخبراء في مجال الحاسوب والانترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة. وإن أسلوب عمل كل فريق يستخدم في التحقيق كثيرا من أنواع الجرائم، إلا أنه يأخذ عملية خاصة في الجرائم المعلوماتية لما تتطلبه من مهارات فنية وخبرات متنوعة قد لا تتوفر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمر ضروريا، ما يتطلب الاستعانة ببعض خبراء مسرح الجريمة التقليدية، مثل خبير البصمات وخبير التصوير الذين يعتبرون من الخبراء الأساسين في معظم أنواع الجرائم.

وعلى هذا الأساس يمكن تقسيم فريق التحقيق في هذا النوع من الجرائم الى فئتين:

الفئة الأولى: وتتمثل في الأشخاص الذين يتصل عملهم مباشرة بجرائم الحاسب الآلي والانترنت ولا يمكن التحقيق في أي جريمة تنتمي الى هذه النوعية من الجرائم إلا بهم فوجودهم ضروري في مسرح الجريمة، ويمكن تحديد أعضاء هذه الفئة على النحو التالي:

1-قائد الفريق أو المحقق الرئيسي: يشترط فيمن يُسند إليه التحقيق في جرائم الحاسب الآلي والإنترنت أن يكون من ذوي الكفاءة العالية والخبرة الممتدة في العمل التحقيقي، وأن يكون ملماً إلماماً دقيقاً بالجوانب التقنية المرتبطة بهذا النوع من

[101] خالد علي نزال الشعار، **التحقيق الجنائي في الجرائم الالكترونية**، بحث مقدم لاستيفاء متطلبات الحصول على درجة دكتوراة في الحقوق، كلية الحقوق، جامعة المنصورة، ص 27.

الجرائم. ويتولى هذا المحقق إدارة موقع الحادث بصفة كاملة، ويوزع الأدوار على أعضاء الفريق، ويشرف على تنفيذ الإجراءات التحقيقية، مع التنسيق مع الجهات ذات الصلة، واتخاذ ما يلزم من قرارات تتطلبها طبيعة التحقيق ومساره.[102]

2- محقق جنائي: شخص أو أكثر بحسب ظروف الجريمة لديه خبرة ومعرفة بوسائل وأساليب التحقيق وإجراءاته، مع إلمامه بطبيعة جرائم الحاسوب والإنترنت وكيفية التعامل مع الأدلة الرقمية فيتولى التفتيش عن الأدلة وأخذ إفادة الأشخاص ذوي العلاقة في مسرح الجريمة.

3-خبير حاسب آلي وشبكات: شخص أو أكثر بحسب الظروف يجمع بين المعرفة بعلوم الحاسوب والشبكات وبين الإلمام بإجراءات التحقيق الجنائي وأساليبه وكيفية التعامل مع مسرح الجريمة ويكون مسؤول عن رفع وتحريز الأدلة الجنائية الرقمية بالطريقة الفنية المناسبة التي لا تؤثر على سلامة الدليل وصلاحيته لإقامة الدعوة والعرض على المحكمة.

4-خبير تدقيق حسابات: متخصص في المراجعة المحاسبية وعلى درجة من الخبرة في التعامل مع الأنظمة البرمجية المستخدمة في المؤسسات المصرفية والآليات المختلفة التي بواسطتها تبادل النقد الالكتروني، ويعمل مع خبير الحاسب الآلي والشبكات على تحديد أسلوب الجريمة وما إذا كان هناك تلاعب في الأنظمة المتضررة بالإضافة إلى تقدير الخسائر المادية الناتجة عن الجريمة.

5-خبير تصوير: يتولى تصوير مسرح الجريمة كما هو متبع في جميع الجرائم فيعمل على تصوير كل المواقع داخل مسرح الجريمة وخارجه وتصوير أدلة الجريمة بالتصوير الفوتوغرافي والفيديو.

6-خبير بصمات: لرفع البصمات من مسرح الجريمة كإجراء عام في معظم الجرائم مع التركيز على المكونات المادية للحواسيب والشبكات المتضررة أو المشتبه بوجود صلة لها بالجريمة، خاصة لوحة المفاتيح والفارة، وذلك بعد اتخاذ الاحتياطات الفنية اللازمة من طرف خبير الحاسوب.

7-خبير رسم تخطيطي: يقوم بعمل رسم تخطيطي (كروكي) لمسرح الجريمة بطريقة فنية دقيقة مستخدما مقياس مناسب للرسم، بما يوضح تقسيماته وأماكن تواجد الأدلة والأشخاص فيه.[103]

الفئة الثانية: وهي تمثل الأشخاص الذين قد يتطلب ظروف مسرح الجريمة تواجدهم، إلا أن دورهم ليس وثيق الصلة بالطبيعة الخاصة بجرائم الحاسب الآلي، وقلما يخلو مسرح أي جريمة مهما كان نوعها من وجودهم مثل أفراد حماية وتأمين

---

[102] الرويلي، ماجد بن عبد الله. **التحقيق الجنائي في الجرائم المعلوماتية: دراسة مقارنة**، المركز العربي للبحوث القانونية، الرياض، 2021.

[103] يومايلة ابتسام، **مناهج التحقيق الجنائي في ظل تفشي الجريمة الرقمية**، مذكرة مقدمة لنيل شهادة ماستر أكاديمي تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، 2020-2021، ص 19.

المسرح وأفراد القبض وأفراد التحريات وغيرهم وتحديد الأعضاء نوعا متروك لتقدير المحقق على ضوء المعلومات المتوافرة لديه عن الجريمة وحسب ما تفرضه طبيعة مسرح الجريمة وحجمها وظروفها.[104]

المطلب الثاني: اختصاصات الضبطية في البحث والتحري

إن الجوهر الأساسي في منظومة العدالة هو الضبطية القضائية، التي خول لها القانون ممارسة مهامها وفقا لما يقتضيه، فقد تم تحديد من خلاله الأشخاص من لهم صلاحيات القيام بعملية البحث والتحري عن الجرائم، وجمع الأدلة اللازمة لكشف الجناة وتقديمهم للعدالة. تمارس الضبطية المهام والصلاحيات بحسب دوائر الاختصاص والتي سنتطرق لتوضيحها كما يلي:

الفرع الأول: دائرة الاختصاص الضبطية القضائية

إن الركيزة الأساسية في منظومة العدالة الجنائية هي الضبطية القضائية، خولت لها بعض الإجراءات القانونية التي تهدف عن كشف الجرائم وضبط مرتكبيها وتقديمهم للعدالة، فتلك الإجراءات هي من صلاحياتهم وفي دائرة اختصاصهم إما على المستوى المحلي أو الإقليمي أو النوعي، وسنتطرق لشرح كلا منها كما يلي:

أولا: الاختصاص المحلي

يخول لضباط الشرطة القضائية، استنادًا إلى أحكام الفقرتين الأولى والثانية من المادة 16 من القانون رقم 06-22 المتعلق بالإجراءات الجزائية، ممارسة مهام البحث والتحري ضمن نطاقهم المحلي المحدد بحسب الحدود الجغرافية التي يمارسون فيها وظائفهم الاعتيادية. غير أنه، وفي حالات الاستعجال، يمكنهم مباشرة تلك المهام ضمن دائرة المجلس القضائي التابعين له. كما يجوز لهم، في ذات الإطار، تنفيذ أعمال البحث والتحري على المستوى الوطني إذا ما تلقوا تكليفًا بذلك من قاضي التحقيق المختص. أما في مجال مكافحة الجريمة المعلوماتية، فإن الفقرة الرابعة من نفس المادة تمنحهم صلاحية العمل على امتداد كامل الإقليم الوطني، للقيام بأعمال البحث، والتحري، والمعاينة، على أن يتم ذلك تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميًا، مع ضرورة إبلاغ وكيل الجمهورية المختص إقليميًا بالإجراءات المتخذة.[105]

ثانيا: الاختصاص الإقليمي

أجاز المشرع الجزائري تمديد الاختصاص الإقليمي دون عناء التنقل إلى مكان تنفيذ الإجراءات، بما يعرف بالتفتيش عن بعد والذي ينطوي على الدخول إلى المنظومة المعلوماتية محل التفتيش أو منظومة معلوماتية أخرى يمكن الدخول عليها

[104] يومايلة ابتسام، نفس المرجع، ص20.

[105] حسين ربيعي، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة مقدمة لنيل شهادة دكتوراة تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2015-2016، ص 202.

انطلاقا من المنظومة الأولى، تحتوي على المعطيات المبحوث عنها، وذلك من قبل السلطات القضائية المختصة وكذلك ضابط الشرطة القضائية بعد إعلام السلطة القضائية (ف 02- م05- القانون 09-04 المتعلق بمكافحة الجرائم المعلوماتية)، وهو الإجراء الذي يسمح بربح الوقت والجهد من خلال اختصار الإجراءات المتعلقة بتمديد نطاق الاختصاص وتعويضه بإجراءات ذات طابع تقني وفني تهدف إلى إحراز الأدلة بأسرع وقت ممكن.[106]

ثالثا: الاختصاص النوعي

يُقصد بالاختصاص النوعي الصلاحية المخولة لضابط الشرطة القضائية في مباشرة أعمال البحث والتحري بحسب طبيعة الجريمة المرتكبة. وقد فرّق المشرع الجزائري بين اختصاص عام، يمنح لبعض فئات الضبط القضائي سلطة التدخل في كافة أنواع الجرائم دون تمييز، وبين اختصاص خاص، يُسند لفئات محددة من الضبطية القضائية بشأن جرائم ذات طبيعة خاصة، كجرائم المساس بأمن الدولة، والجرائم العسكرية، والجرائم الجمركية. وبذلك، فإن الاختصاص النوعي قد يتخذ طابعاً موسعاً يتيح لعضو الضبط القضائي التعامل مع مختلف الجرائم، أو طابعاً مقيداً يقتصر على نوع محدد منها.[107]

الفرع الثاني: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجية الاعلام والاتصال

يعد القطب الجزائي الوطني المختص في مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال هيئة قضائية متخصصة في الجزائر، فهو من أحدث الأقطاب زيادة إلى الأقطاب الجزائية الأخرى، أنشأ بهدف التصدي للجرائم التي باتت تشكل تهديدا على المستوى الفردي والمؤسساتي وكذا الأمن، يختص بمتابعة قضايا عدة أهمها الجرائم الالكترونية، وسنتفرع للتعرف عليه فيما يلي:

أولا: نشأة القطب

استحدث المشرع الجزائري بموجب الأمر رقم 11/21 المؤرخ في 25 غشت 2021، المعدل والمتمم لقانون الإجراءات الجزائية، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في الباب السادس المعنون بذات العنوان والذي يحتوي على المواد من 211 مكرر 22 إلى مكرر 29 من نفس الرقم، ويتواجد هذا القطب على مستوى محكمة مقر مجلس القضاء الجزائر، وتم الإقرار بدستوريته بموجب القرار رقم 389 المؤرخ في 24 أوت 2021 بحيث يختص بالمتابعة والتحقيق في الجرائم المعلوماتية.[108]

---

[106] حسين ربيعي، نفس المرجع، ص 203.

[107] عبد القادر بن عبو، **شرح قانون الإجراءات الجزائية الجزائري**. ط. 2، دار هومة، 2020.

[108] أنظر المادة 211 مكرر 22 من ق.إ.ج.

ثانيا: دوافع استحداث القطب الجزائي:

القطب الجزائي هو جهة قضائية تختص بالنظر في الجرائم المذكورة في المادة 211 مكرر 24، وبالتالي تم استحداث هذا القطب خصيصا لمواجهة الجريمة المنظمة لاسيما الجرائم السيبرانية، ذلك أنه بات من الضروري استحداث هذا النوع من الهيئات القضائية، لمواجهة التهديدات التي تواجه الدولة والمجتمع فيما يخص الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، التي أصبحت تحتل المرتبة الأولى من حيث الجرائم المرتكبة وذلك لسهولة ارتكابها وصعوبة إثباتها لهذا يظهر جليا دوافع وخلفيات استحداث القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وذلك من حيث:

- تزايد حجم الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والتي أضحت من الجرائم العابرة للحدود الوطنية بحكم التطور التكنولوجي الهائل في تقنيات المعلوماتية.
- تعقد وصعوبة مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال استدعى استحداث قطب جزائي لمكافحة هذه الجرائم.
- ضرورة تجاوز الاختصاص الإقليمي للمحاكم التي تستند عليه في الجرائم التقليدية، والعمل على اعتماد جهات قضائية ذات اختصاص وطني.
- عدم قدرة القضاء الجنائي الغير متخصص في مواجهة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، وبالتالي محاربة الجريمة السيبرانية التي تحتاج لقضاء متخصص ذو خبرة وكفاءة، حتى يتسنى لهم الكشف عن مرتكبي الجريمة من خلال استجواب الجناة، وبالتالي بات من الضروري الاستناد على قضاء جنائي متخصص في مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.
- خصوصية الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وصعوبتها وتعقدها، جعل المشرع ينظر إليها من خلال تخصيص جهة قضائية أكثر تطورا ماديا وبشريا للحد من هذه الجرائم، ذلك أن واقع هذه الجرائم حتم على الدولة أن تتدخل بشكل متميز وتفرض سلطتها العقابية من خلال استحداث القطب الجزائي.
- ضرورة تجاوز الاختصاص الإقليمي للمحاكم التي تستند عليه في الجرائم التقليدية، والعمل على اعتماد جهات قضائية ذات اختصاص وطني.

- ضرورة التعاون الدولي بين الدول لمكافحة الجرائم السيبرانية دفع المشرع الى استحداث القطب الجزائي الوطني.[109]

الفرع الثالث: الأجهزة المكلفة بالبحث والتحري عن الجرائم الالكترونية على المستوى الوطني والدولي

إن التوسع الحاصل في استخدامات الانترنت مع التطورات التكنولوجية الحديثة لوسائل الإعلام والاتصال التي تمس مختلف جوانب الحياة، جعلت الأمة في تحديات أمنية معاصرة انتجت جرائم الكترونية لها القدرة على اختراق الحدود الجغرافية، لذا استدعى هذا التطور ضرورة إنشاء وتعزيز أجهزة متخصصة في البحث والتحري عن هذه الجرائم سواء على المستوى الوطني أو الدولي، وسنعرض هذا بالتفصيل فيما يأتي:

أولا: الأجهزة المكلفة بالبحث والتحري عن الجرائم الالكترونية على المستوى الوطني

أ- الضبطية القضائية

1-على مستوى جهاز الشرطة: وبغرض توسيع هذا النظام المتخصص وتعميمه على كافة جهات الوطن، شرعت المديرية ذاتها في إنشاء ثلاث مخابر إضافية في كل من بشار، ورقلة وتمنراست، والتي توجد حاليًا في طور الإنجاز. وتجدر الإشارة إلى أن المخبرين الجهويين للشرطة العلمية في قسنطينة ووهران يتضمنان وحدة تقنية متخصصة تحت مسمى "دائرة الأدلة الرقمية والآثار التكنولوجية"، تُعنى بالتحقيق في الجرائم ذات الطابع الإلكتروني، وتُشكّل هذه الدائرة نواة عمل فني متقدم يتكون من ثلاثة أقسام وظيفية رئيسية، وهي:

- ✓ قسم تحليل واستغلال المعطيات الرقمية المستخلصة من الحواسيب وشبكات الاتصال،
- ✓ قسم فحص البيانات الرقمية المستخرجة من أجهزة الهاتف النقال،
- ✓ قسم تحليل الأصوات، ويُعتمد في أداء هذه المهام على تجهيزات تقنية عالية الدقة، مخصصة لاستغلال الأدلة الرقمية بما يتماشى مع المعايير الدولية في مجال التحقيق الجنائي الرقمي.[110]

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

---

[109] د. رقية محمودي، د. نور الهدى قدوح، **الجرائم الإلكترونية في المجتمع الجزائري**، المرجع السابق، ص 90.

[110] المديرية العامة للأمن الوطني، **التقرير السنوي لنشاطات الشرطة العلمية ومكافحة الجريمة الإلكترونية**، الجزائر، 2023، ص 45.

ب- مركز الوقاية من جرائم الاعلام الآلي والجريمة الالكترونية

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم الالكترونية عن طريق المرسوم الرئاسي رقم 15-261 ومقره بئر مراد رايس، وهو تابع لمديرية الأمن للدرك الوطني، وقد حددت المادة الأولى منه تشكيلة وتنظيم سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.[111]

1-التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال هي مؤسسة عمومية ذات طابع إداري مستقلة بذاتها ولها صلاحياتها الكاملة كما تتمتع بالشخصية المعنوية والاستقلال المالي، هذه الهيئة توضع تحت سلطة وزارة الدفاع الوطني، فقد استحدثت بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته وحسب ما جاء في نص المادة 13 بأنه "تنشأ هيئة وطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال ومكافحته تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم"، وقد صدر التنظيم في 2019 الخاص م.ر 172/19 المؤرخ في 06 يونيو 2019 والذي يحدد تشكيلة الهيئة وكذا كيفيات سيرها وتنظيمها، [112]كما حددت المادة 03 من الرسوم الرئاسي 172/19 مقر الهيئة والمتواجدة في الجزائر العاصمة.[113]

2-اختصاص الهيئة: حسب ما جاء في نص الفقرة الثانية02 من المادة 04 من المرسوم الرئاسي 15-261 المهام الأساسية التي تكلف بها الهيئة وهي على سبيل الحصر مهام الهدف منها هو الوقاية من الجرائم المعلوماتية، ومكافحة هذه الأخيرة من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية وأبرز مهام هذه الهيئة هي:

- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الأعلام والاتصال ومكافحته.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية.

---

[111] د. نادية أيت عبد المالك، ط. د. عبد القادر فلاح، **التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري**، المرجع السابق، ص 1696.

[112] سهيلة بوزبرة، **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: بين المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية**، المجلة النقدية للقانون والعلوم السياسية، المجلد 17 العدد 02، كلية الحقوق والعلوم السياسية، جامعة تيزي وزر، 2022، ص 561.

[113] انظر المادة 03 من المرسوم الرئاسي 172/19 المؤرخ في 03 شوال 1440 الموافق ل/ 06 يونيو الذي **يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها**، ج.ر العدد 37، المؤرخة في 2019/06/09.

- ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماسة بأمن الدولة وذلك تحت سلطة قاضي مختص وذلك كاختصاص حصري.
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مسارها من أجل استعمالها في الإجراءات القضائية.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المعلوماتية.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا المعلومات.
- تنفيذ الطلبات الصادرة عن الدول الأجنبية وتطوير سبل التعاون والتبادل معها.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.[114]

3-تشكيلة الهيئة: تتكون الهيئة مما يلي:

- **هيئة الإدارية:** تتشكل الهيئة من لجنة مديرة إضافة إلى مديرية عامة، تتشكل اللجنة المديرة من الوزير المكلف بالعدل رئيسا إضافة إلى الوزير المكلف بالداخلية والوزير المكلف بتكنولوجيات الإعلام والاتصال وقائد الدرك الوطني وكذلك المدير العام للأمن الوطني، وممثلين أحدهما عن رئاسة الجمهورية والأخر عن وزارة الدفاع يكملها قاضيان من المحكمة العليا، أما المديرية العامة فيرأسها مدير عام يعين بموجب مرسوم رئاسي، وتتجلى مهام هذه المديريات في ضبط برامج عمل الهيئة ودراسة مشروع الميزانية وتقديم تقارير خاصة بنشاط الهيئة، وبالتالي فهي لا تسهم في الإجراءات الخاصة بالوقاية أو بمكافحة الجرائم المعلوماتية.[115]
- **الهيئة التقنية:** تضم الهيئة التقنية ما يلي:

-مديرية المراقبة الوقائية واليقظة الالكترونية: تتحدد تشكيلتها في مجموعة من ضباط واعوان الشرطة القضائية المختصين في مجال مكافحة الجرائم المعلوماتية، من سلك الأمن الوطن وكذلك الدرك الوطني والمصالح العسكرية للاستعلام والأمن، يعينون بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل والدفاع والداخلية، يساعدهم مستخدمي الدعم التقني والإداري من نفس الأسلاك.

-مديرية التنسيق التقني: وتتمثل مهامها في الدور الوقائي والإعلامي من خلال:

- ✓ إنجاز الخبرات القضائية في مجال اختصاص الهيئة.
- ✓ تكوين قاعدة معطيات تحليلية للإجرام المعلوماتي.

[114] حسين ربيعي، **آليات البحث والتحقيق في الجرائم المعلوماتية**، المرجع السابق، ص 172-173.

[115] حسين ربيعي، **آليات البحث والتحقيق في الجرائم المعلوماتية**، نفس المرجع، ص 175.

- ✓ إعداد الإحصائيات الوطنية للإجرام المعلوماتي.
- ✓ تسيير المنظومة المعلوماتية وإدارتها.[116]

ج: المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني

تم تأسيس هذا الجهاز بموجب م.ر رقم 04-183 المؤرخ في 26 جوان 2004، ويُعد خطوة مؤسساتية محورية في إطار تحديث منظومة العدالة الجنائية في الجزائر، نظراً لاعتماده على تقنيات علمية متقدمة في ميدان التحريات الجنائية ومكافحة الجريمة المنظمة. وقد ساهم التزامه بنظام إدارة الجودة في حصوله على شهادات اعتماد معترف بها وطنياً ودولياً، ما عزز من موثوقيته وكفاءته على المستويين الداخلي والخارجي.[117]

-مهام المعهد:

- ✓ إنجاز الخبرات والتحاليل بناء على طلبات القضاة، المحققين والسلطات المؤهلة
- ✓ الدعم التقني للوحدات أثناء التحقيقات المعقدة
- ✓ تصميم بنوك معطيات وإنجازها وفقا للقانون
- ✓ المشاركة في الدراسات والبحوث المتعلقة بالوقاية والتقليل من كل أشكال الإجرام
- ✓ المساهمة في تحديد سياسة جنائية مثلى لمكافحة الإجرام
- ✓ المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة
- ✓ العمل على ترقية البحث التطبيقي وأساليب التحريات الفعالة في ميدان علم الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي
- ✓ المشاركة في تنظيم دورات تحسين المستوى والتكوين

كما يلعب المعهد الوطني للأدلة الجنائية وعلم الإجرام دورا فعالا في مجال مكافحة الجرائم السيبرانية إذ تكلف دائرة الإعلام الآلي والالكتروني:

-بمعالجة وتحليل وتقديم كل دليل الكتروني لفائدة أجهزة العدالة

-تقديم مساعدة تقنية للمحققين في التحقيقات المعقدة

[116] حسين ربيعي، نفس المرجع، ص 176.

[117] المرسوم الرئاسي رقم 04-183 المؤرخ في 26 جوان 2004، **المتضمن إنشاء الهيئة الوطنية**، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 41، المؤرخ في 30 جوان 2004، ص 6.

-السهر على تأمين اليقظة التكنولوجية من أجل تحيين المعارف والتقنيات والطرق المستعملة في الخبرات العلمية.[118]

ومنذ إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، تبنى المعهد نظام إدارة الجودة، مما مكنه من الحصول على شهادة الاعتماد على المستويين الوطني والدولي بمهارته التقنية والتنظيمية وكذا في مجال الأدلة الجنائية من خلال الاعتماد على 56 طريقة تحليلية وفق المعيارين الدوليين إيزو 17020 وإيزو 17025 من قبل هيئة الاعتماد الجزائرية ALGERAC.[119]

هـ: المنظومة الوطنية لأمن الأنظمة المعلوماتية

لقد استحدث المشرع الجزائري المنظومة الوطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، والتي تعد الإطار التنظيمي لإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها، وتوضع لدى وزارة الدفاع الوطني، طبقا لأحكام المادة 3 من المرسوم 20-05 أعلاه تتضمن المنظمة الوطنية لأمن الأنظمة المعلوماتية، من مجلس وطني لأمن الأنظمة المعلوماتية ووكالة الأمن الأنظمة المعلوماتية نتطرق لهما تباعا.

1-المجلس الوطني لأمن الأنظمة المعلوماتية:

أ-يتشكل المجلس طبقا لأحكام المادة 5 من المرسوم الرئاسي 20-05 من:

- وزير الدفاع رئيسا
- ممثل عن الرئاسة الجمهورية
- ممثل عن الوزير الأول
- الوزير المكلف بالشؤون الخارجية
- الوزير المكلف بالعدل
- الوزير المكلف بالمالية
- الوزير المكلف بالطاقة
- الوزير المكلف بالاتصالات
- الوزير المكلف بالتعليم العالي
- المدير العام لوكالة الأنظمة المعلوماتية بصفة استشارية

[118] سويسي فتيحة، **التكييف القانوني لجرائم المعلوماتية والإشكالات العلمية المترتبة عنها**، المرجع السابق، ص 16.

[119] أنظر الموقع الرسمي لوزارة الدفاع الوطني www.mdn.dz

كما يمكن للمجلس أن يستعين بأي شخص أو مؤسسة من شأنه تنويره في أعماله.[120]

ب– مهام المجلس: حددت المادة 4 من المرسوم الرئاسي رقم 20-05 مهامه الآتي:

-البت في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها.

-دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها.

-دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليها.

-الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية.

-الموافقة على تصنيف الأنظمة المعلوماتية.

-الموافقة على سياسة التصديق الالكتروني للسلطة الوطنية للتصديق الالكتروني

-اقتراح ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية عند الحاجة.

-يبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية [121]

2–وكالة أمن الأنظمة المعلوماتية:

طبقا لما جاء في أحكام المرسوم الرئاسي 20-05 المتعلق بأمن الأنظمة المعلوماتية في تعريفه للوكالة بأنها مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية يقع مقرها بالجزائر العاصمة.

تعتبر الوكالة طبقا لأحكام المادة 17 من المرسوم الرئاسي 20-05 أعلاه مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية مقرها الجزائر

–مهام الوكالة: حددت المادة 18 من نفس المرسوم الرئاسي مهام الوكالة والمبينة كالتالي:

- ✓ تحضير عناصر الاستراتيجية الوطنية في مجال امن الأنظمة المعلوماتية وعرضها على المجلس.
- ✓ تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المحددة من قبل المجلس.
- ✓ إجراءات تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية الي تستهدف المؤسسات الوطنية.
- ✓ السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية.
- ✓ متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية.

---

[120] فتيحة حزام، **حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم 05–20**، مجلة الحقوق والعلوم الإنسانية، المجلد الثالث عشر، العدد الثالث، جامعة بومرداس، أكتوبر 2020، ص181.

[121] خالد شكري، أبوبكر لراشي، **التحقيق وجمع الأدلة في مجال الجرائم الالكترونية**، المرجع السابق، ص 34.

- ✓ ضمان اليقظة التكنولوجية في مجال الأنظمة المعلوماتية.
- ✓ إعداد وتحيين خارطة للأنظمة المعلوماتية المصنفة
- ✓ إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية.

كما يتولى أدارة الوكالة لجنة توجيه وتزود بلجنة علمية، كما يكلف بتسييرها مدير عام وتتوفر على مركز وطني عملياتي الأمن الأنظمة ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطته.[122]

ثانيا: الأجهزة المكلفة بالبحث والتحري عن الجرائم الالكترونية على المستوى دولي

أ-الشرطة الأوروبية أو الأوروبول: جهاز يكون على مستوى الاتحاد الأوروبي تم إنشاؤه في لكسمبورغ عام 1992 ومقره في مدينة لاهاي بهولندا، ليكون حلقة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال الجرائم الإرهابية والمخدرات والجريمة المنظمة، وكذلك الإجرام المعلوماتي، ويهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشرطة لمختلف الدول الأعضاء، وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة ومنها الجريمة المعلوماتية وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه اسم (système de signalement en ligne de la criminalité sur internet) في سنة 2010 بغرض التنسيق أكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الأعضاء.[123]

ب-الأوروجيست (Eurojest): هو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، تم إنشاؤه عام 2002 وينعقد اختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الإتحاد الأوروبي، ويعد الأروجيست وحدة للتعاون وحدة للتعاون القضائي، مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيق ومباشرة متابعات جزائية.

جـ-الفريبول (Afripol): هي أكبر منظمة شرطة في القارة الأفريقية المكونة من قوات الشرطة بـ 41 دولة أنشئت بمبادرة من الدولة الجزائرية يوم 2015/12/13 مقرها الرئيسي الجزائر العاصمة، وتم الإعلان رسميا عن بداية نشاطها يوم 2017/07/06 بمناسبة اجتماع مسؤولي أجهزة الشرطة للدول الافريقية الأعضاء في الاتحاد الافريقي المنعقد بالجزائر،

---

[122] أنظر المادة 17-18 من المرسوم الرئاسي 05-20 المؤرخ في 24 جمادى الأول عام 1441 الموافق لـ 20 جانفي 2020 **يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية**، الجريدة الرسمية العدد 04 المؤرخة في 26 جانفي 2020.

خالد شكري، لراشي أبوبكر، **التحقيق وجمع الأدلة في مجال الجرائم الالكترونية**، المرجع السابق، ص 35.

[123] عبد العزيز أحمد، **خصوصية التحقيق في الجريمة المعلوماتية**، المرجع السابق، ص52.

وتكمن مهام الافريبول في مضاعفة رصيد التعاون الشرطي الإقليمي والدولي، وتحديد السياسة العامة لشرطة الجنائية وتوفير تكوين وإعادة تأهيل مختلف أجهزة الشرطة الافريقية، التي تشهد تأخر وضعف على مستوى الأداء وكذلك تعزيز قيام سلم والأمن والاستقرار في القارة الأفريقية، وإيجاد الحلول الفاعلة للجرائم التي توجهها بعض الدول الأفريقية مثل جرائم الإرهاب والمخدرات والجرائم المعلوماتية.[124]

المبحث الثاني: إجراءات ووسائل البحث والتحري في الجرائم الالكترونية

يعد ظهور الجريمة الالكترونية من المستجدات الحديثة التي من شأنها خلق تهديدات تمثل تحديا معقدا أمام أجهزة العدالة الجنائية، لما تطرحه من صعوبات تقنية وقانونية تعيق فاعلية أدائها، الأمر الذي يفرض ضرورة تبني آليات وأساليب حديثة في مجلات البحث والتحري دون التخلي عن الاستفادة من الاليات التقليدية، وفي هذا المبحث سنعرض الاليات التقليدية والحديثة معا من خلال المطلب المبينة:

المطلب الأول: الإجراءات المتعلقة بالجريمة الالكترونية

الفرع الأول: الإجراءات العامة للبحث والتحري في الجرائم الالكترونية

أولا: المعاينة

1-تعريف المعاينة:

وهي رؤية العين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة ومعاينة مسرح الجرائم المعلوماتية، ويجب التفرقة بين حالتي معاينة الجرائم الواقعة على مكونات الحاسوب، كشاشة العرض الأقراص.... ومعاينة الجرائم الواقعة على المكونات غير المادية كفحص مسار الانترنت، معاينة أنظمة الاتصال بشبكة الانترنت.[125]

2-اجرءات المعاينة التقنية:

أ-الانتقال إلى مسرح الجريمة:

تتم المعاينة في الجريمة الالكترونية المرتكبة عبر الانترنت أو بواسطة الحاسب الآلي كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية، إلا أن الانتقال هناك لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني، ومن بين التدابير الفنية والتحفظية التي تساعد المحقق على المعاينة الالكترونية هي كالآتي:

---

[124] عبد العزيز أحمد، **خصوصية التحقيق في الجريمة المعلوماتية**، نفس المرجع، ص 53.

[125] د. نادية أيت عبد المالك، ط.د. عبد القادر فلاح، **التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري**، المرجع السابق، ص 1697.

-الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد وموقع الأجهزة الالكترونية وشبكاتها وسائر ملحقاتها والنهايات الطرفية المتصلة بها المتوقع مداهمتها.

-توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة يمكن الاستعانة بها في الفحص، التشغيل، الضبط والتأمين وحفظ المعلومات.

-التحفظ على محتويات سلة المهملات ومستندات الادخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.

-إعداد فريق من المتخصصين وأهل الخبرة في مجال تكنولوجيا الإعلام الآلي للاستعانة بهم عند الحاجة.

ب-تأمين مسرح الجريمة: تعتبر عملية تأمين مسرح الجريمة من الخطوات الأساسية التي تساهم في تحقيق العدالة وتوفير الأدلة اللازمة لإثبات الجريمة أو تبرئة المتهمين. إن أهمية تأمين مسرح الجريمة تتمثل في الحفاظ على الأدلة الجنائية وتحليلها بشكل دقيق، حيث أن أي تلاعب أو تغيير في موقع الجريمة يمكن أن يعيق جمع الأدلة ويؤثر سلباً على مسار التحقيقات. لذلك، فإن الإجراءات التي يتم اتخاذها عند وصول السلطات إلى مكان الحادث تُعتبر حيويّة لضمان سلامة المعلومات والأدلة المتوافرة.

علاوة على ذلك، يتيح تأمين مسرح الجريمة لفريق التحقيق القدرة على العمل في بيئة منظمة، مما يسهل عملية توثيق المشهد وتحديد منطقة البحث. يشمل ذلك وضع شريط تحذيري لتحديد الحواجز، وتوثيق الأماكن التي وُجدت فيها الأدلة مثل الدماء أو الأداة المستخدمة في الجريمة. هذه الإجراءات لا تقتصر فقط على حماية الأدلة، بل تساهم أيضًا في بناء صورة واضحة عن ملابسات الجريمة، مما يسهل لاحقًا إجراء المقابلات مع الشهود أو المشتبه بهم.

ومن أجل ضمان حماية وتأمين لمسرح الجريمة الواجب مراعاة بعض الضوابط التالية:

- تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

-إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف، حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها وتأمينها.

-إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي يكفل تنفيذها على الوجه الأكمل.

-أن تقتصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر فيهم الكفاءة العملية والخبرة الفنية في مجال الحواسيب.[126]

3-نطاق المعاينة الالكترونية:

أ-معاينة مكونات الحاسب: تعتبر الحواسيب مصدرا غنيا بالأدلة الرقمية خاصة الحواسيب الشخصية، التي يمكن اعتبارها أرشيف لسلوك الأفراد ونشاطاتهم ورغباتهم لذلك إن عملية فحص هذه الحواسيب تمثل نقطة البداية في الكشف عن خفايا الجريمة الالكترونية باعتبارها وسيلة لتنفيذ الجريمة أو محل وقوعها، والمعروف أن الحاسب الآلي يقوم في تركيبه على ثلاثة عناصر أساسية هي القطع الصلبة"hard ware" والقطع المرنة أو البرمجيات "soft ware" وكذلك المعطيات أو البيانات أو المعلومات "données informatique" وهو العنصر الذي يتوزع بين القطع الصلبة والبرمجيات وتعتمد طريقة الفحص على طريقتين أساسيتين الأولى هي الفحص الذاتي من خلال قيام الحاسب ذاته بفحص مكونات وتقديم تقرير كاملا إلى صاحب الفحص وهذه العملية تتطلب تقنيات ومهارات فنية عالية أما الطريقة الثانية وهي الفحص بواسطة حاسب آخر وأجهزة تقنية عالية للبحث في جزئيات الحاسب.

ب-معالجة أنظمة الاتصال بشبكة الانترنت: أحيانا لا تكفي معاينة مكونات الحاسب الآلي لاستخلاص الدليل الالكتروني إنما يتطلب من المحقق فحص أنظمة اتصال الحاسب بشبكة الانترنت كذلك، وهي تلك الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة للاتصال بالأنترنت أو ما يعرف ببروتكول الانترنت والنظام الأمني للشبكات وكذلك فحص الخادم" le serveur".[127]

ثانيا: التفتيش

1-تعريف التفتيش الالكتروني: عرفه الدكتور علي حسن محمد الطوالبة بأنه" البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة، ونسبتها إليه، أو هو البحث الدقيق والاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، سواء كان مسكنا أو جهاز حاسوب، وأنظمة، والانترنت".[128]

---

[126] د. ليندة بومحراث، ط.د. عبد النور سعيداني، **إجراءات البحث والتحري في الجرائم الالكترونية**، أعمال الملتقى الوطني الافتراضي الجرائم الالكترونية في المجتمع الجزائري تشخيص الواقع وتحديات الأمن السيبراني، طبعة الأولى، جامعة يحي فارس المدية، 15 مارس 2022، ص 140.

[127] خالد شكري، أبوبكر لراشي، **التحقيق وجمع الأدلة في مجال الجرائم الالكترونية**، المرجع السابق، ص 41-42.

[128] كمال حفصاوي، عمر مخلوف، **التفتيش الالكتروني بين ضرورة التحقيق والحق في سرية المراسلات والاتصالات**، مجلة الباحث للدراسات الأكاديمية، المجلد 11، العدد01، 2024، ص 332.

كما يعرف بأنه" إجراء من إجراءات التحقيق الغرض منه البحث عن الأدلة المادية والرقمية المتعلقة بالجريمة عن طريق الوصول والنفاذ إلى وسائل تقنية المعلومات والشبكات المعلوماتية وأنظمة المعالجة الالكترونية للبيانات، وذلك بهدف إثبات ارتكابها أو نسبتها الى المتهم وفقا لإجراءات قانونية محددة.[129]

2-شروط التفتيش الالكتروني: للتفتيش الالكتروني شروط شكلية وشروط موضوعية

أ-الشروط الشكلية:

- **الإذن بالتفتيش:** عموما بحسب ما جاءت به المادة 44 من ق إ ج بأنه" لا يجوز لضابط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء متعلقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش" وقد أضاف في الفقرة الثالثة من نفس المادة بحيثيات الإذن وذلك بوصف الجريمة وموضوع البحث وعنوان الأماكن التي سيتم زيارتها وتفتيشها وإجراء الحجز فيها، وأضاف في الفقرة الرابعة " تنجز هذه العملية تحت الاشراف المباشر للقاضي الذي اذن بها والذي يمكنه عند الاقتضاء ان ينتقل الى عين المكان للسهر على احترام القانون.[130]
- **محضر إجراءات التفتيش:** يجب على ضابط الشرطة القضائية المكلف بعملية التفتيش أن يحرر محضر مفصل عن سير عملية التفتيش، ولا يشترط القانون في المحضر شكل معين، وبالتالي لصحة محضر تفتيش نظم الحاسوب لا يشترط سوى ما تستوجب 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 والانترنت الذي تم الاستعانة به في مجال الخبرة الفنية الضرورية، وتحرير محضر عن عملية التفتيش هي لازمة وذلك لتمكين الجهات القضائية المختصة بنظر مدى احترام الإجراءات المتطلبة في عملية التفتيش ومن ثم رقابتها على شرعية الإجراء.[131]

ب-الشروط الموضوعية:

1-وجود سبب للتفتيش: ويتأتى سبب اجراء التفتيش بالأوضاع التالية:

---

[129] خالد ممدوح إبراهيم، **إجراءات التفتيش في الجرائم المعلوماتية (دراسة مقارنة)**، دار الفكر الجامعي، الطبعة الأولى، 2021، ص31.

[130] انظر مادة 44 من ق.إ.ج.

[131][131] كمال حفصاوي، عمر مخلوف، **التفتيش الالكتروني بين ضرورة التحقيق والحق في سرية المراسلات والاتصالات**، مرجع سابق، ص 339.

- ✓ **وقوع جريمة معلوماتية:** يشترط أن تكون الجريمة وقعت فعلا، فلا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة مستقبلة ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل، إلا أنه بالرجوع الى نص المادتان 04 و05 من القانون رقم 09-04 يتبين أن المشرع الجزائري قد أجاز إمكانية اللجوء إلى تفتيش النظام المعلوماتي إما للوقاية من حدوث جرائم أو حالة توفر معلومات عن احتمال وقوع جرائم معينة.[132]
- ✓ **توجيه التهمة إلى شخص وإسنادها إليه:** من مبررات التفتيش الموضوعية وجود قرائن قوية تدعو للاعتقاد بأن شخص أو أشخاص بعينهم قاموا بارتكاب جريمة الكترونية، سواء بوصفهم فاعلين أصليين أو شركاء في الجريمة أو حائزين على أشياء تتعلق بالجريمة التي دلت على وقوعها أمارات وقرائن حتى يبرر المساس بحرية الأشخاص المراد تفتيشهم وتفتيش ممتلكاتهم وأجهزتهم الالكترونية.[133]
- ✓ **توفر أدلة مادية تكشف الجريمة:** لابد أن تتوفر لدى المحقق أسباب كافية على أنه يوجد في مكان أو لدى الشخص المطلوب تفتيشه أدوات استخدمت في الجريمة المعلوماتية أو أشباء متحصلة منها أو مستندات الكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم أو غيره، وذلك حتى يأذن بالتفتيش بقدر يبرر تعرض التفتيش لحرمة الشخص في حريته ومسكنه في سبيل كشف اتصاله بالجريمة المعلوماتية.[134]

2-محل التفتيش: يجب أن يكون التفتيش محلا والمتمثل إما في الشخص أو المكان ويشترط موضوع التفتيش المحل أن يكون محددا أو قابلا وأن يكون مشروعا، أي يرد على محل جائز قانونا،[135]والشخص بوصفه محلا لتفتيش النظام المعلوماتي للكمبيوتر قد يكون من مستغلي أو مستخدمي الكمبيوتر أو من خبراء البرامج سواء أكانت برامج نظام أو برامج تطبيقات، وقد يكون من المحللين أو من مهندسي الصيانة والاتصالات، أو من مديري النظم المعلوماتية، أو من أي أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حاسب آلي محمولة أو تلفونات متصلة بجهاز المودم أو المستندات، أما المقصود بالمنازل وما في حكمها لتفتيش النظام المعلوماتي كافة محل الإقامة أو المأوى والملحقات المخصصة لمنافعها والتي يشغلها الشخص سواء بصفة دائمة أو مؤقتة وسواء كانت ثابتة أم متنقلة، متى ما وجدت فيها

---

[132] يوسف صغير، **التفتيش كآلية لإثبات جرائم نظم المعلوماتية**، المجلة النقدية للقانون والعلوم السياسية، المجلد 17 العدد 04، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2021، ص 603.

[133] مخلوف علمي، د. ليندة بومحراث، **ضوابط التفتيش في الجرائم الالكترونية**، مجلة المعيار، المجلد 28 العدد 1، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، 2024، ص 394.

[134] فاطمة مرنيز، **التفتيش الافتراضي كإجراء استدلالي في ضوء القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها دراسة مقارنة**، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 10 العدد 02، المركز الجامعي أحمد زبانة، غليزان، 2021، ص 241.

[135] يوسف صغير، **التفتيش كآلية لإثبات جرائم نظم المعلوماتية**، المرجع السابق، ص 602.

مكونات الكمبيوتر سواء كانت مكونات مادية أو منطقية أو شبكات اتصال خاص، وعملية التفتيش هنا تخضع لذات شروط وقواعد إجراءات تفتيش المنازل. [136]

3-إجراءات التفتيش الالكتروني:

-الكمبيوتر محل التفتيش الالكتروني: يعتمد التفتيش الالكتروني على الحاسوب فهو محله، بحيث تحدث في هذا الأخير عملية التفتيش بواسطة مكوناته المادية والمعنوية وسنوضحها كالتالي:

أ-تفتيش المكونات المادية: يحدث التفتيش في المكونات المادية للحاسوب بالتحديد في القطع الصلبة والبرمجيات، وكذا شبكات الاتصال بعدية Networks Télécommunication سلكية ولا سلكية محلية ودولية، بالإضافة الى الأشخاص والأماكن المرتبطة بالكمبيوتر وشبكات الاتصال[137]

ب-تفتيش المكونات المعنوية: أثار التفتيش في هذه الحالة جدلا فقهيا كبير حول صلاحيات المكونات المعنوية لأن تكون محلا للتفتيش باعتبار البيانات الالكترونية أو البرامج في ذاتها تفتقر ال مظهر ملموس[138]، فذهب رأي في الفقه إلى جواز ضبط البيانات الالكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما نص على إصدار الإذن بضبط "أي شيء"، فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة، بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الكمبيوتر بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد تتركز في البحث عن الأجهزة المادية أو أي مادة معالجة بواسطة الكمبيوتر.

وفي مقابل هذين الرأيين يوجد رأي آخر نأي بنفسه عن البحث عما إذا كانت كلمة "شيء" تشمل البيانات المعنوية لمكونات الكمبيوتر أم لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العلمي والذي يتطلب أن يقع الضبط على بيانات الكمبيوتر إذا اتخذت شكلا ماديا.[139]

ان موقف المشرع الجزائري من التفتيش الالكتروني قد تم التطرق اليه في نص المادة 5من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بحيث أجاز للسلطات القضائية

---

[136] خالد ممدوح إبراهيم، **إجراءات التفتيش في الجرائم المعلوماتية دراسة مقارنة**، المرجع السابق، ص 49.

[137] خالد ممدوح إبراهيم، **إجراءات التفتيش في الجرائم المعلوماتية دراسة مقارنة**، نفس المرجع، ص 84-85.

[138] كاهنة آيت حمودة، **البحث والتحري الجنائي في مسرح الجريم الالكترونية**، مجلة الفكر القانوني والسياسي، المجلد السابع، العدد الأول، جامعة حسيبة بن بوعلي، الشلف، 2023، ص 188.

[139] خالد ممدوح إبراهيم، نفس المرجع، ص 98.

المختصة وكذا ضابط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها بغرض التفتيش ولو عن بعد.[140] وقد تطرق في تفصيل إجراءات التفتيش الالكتروني في حالة ارتباط حاسوب المتهم بمنظومة معلوماتية داخل الإقليم الوطني وكذا خارجه في الفقرتان 2و3 من نفس القانون بحيث أجاز بتمديد الإجراءات بحثا عن المتهمين في الجريمة.

الفرع الثاني: الإجراءات الخاصة للبحث والتحري في الجرائم الالكترونية

أولا: المراقبـــة

1-تعريف المراقبة:

تعني المراقبة عند الفقه" وضع شخص أو وسائل نقل أو أماكن أو مواد تحت رقابة سرية ودورية، بهدف الحصول على معلومات لها علاقة بالشخص محل الاشتباه، أو بأمواله، أو بالنشاط الذي يقوم به".[141]

وتعني المراقبة الالكترونية ذلك الإجراء المتعلق بالتحريات الخاصة حول مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر.[142]

لم يتطرق المشرع الجزائري إلى إعطاء تعريف خاص بمصطلح المراقبة الالكترونية بل اكتفى بذكرها في الظروف الملائمة لاستخدامها وفي الحالات التي يجوز العمل بها كإجراء وذلك في المواد 03 و04 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وفقا لمستلزمات التحريات والتحقيقات القضائية التي تخص الجرائم الالكترونية.

2-شروط المراقبة:

لقد قيد المشرع الجزائري مجموعة من الشروط، حيث لا يمكن أن يقوم بهذا الاجراء إلا ضباط الشرطة القضائية وهم الأشخاص المحددين في المادة 15 ق إ ج وتحت سلطتهم أعوان الشرطة القضائية، وتتطلب المراقبة من القائم بها الذكاء،

---

[140] كاهنة آيت حمودة، **البحث والتحري الجنائي في مسرح الجريم الالكترونية**، المرجع السابق، ص 188.

[141] وردة شرف الدين، **مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري**، مجلة المفكر، العدد الخامس عشر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، جوان 2017، ص542.

[142] د. الطاهر ياكر، **الجرائم الالكترونية الاحكام الموضوعية والإجرائية (دراسة مقارنة)**، المرجع السابق، ص113.

سلامة الحواس وسرعة البديهة واللياقة البدنية وحسن التصرف وغيرها من الصفات، وذلك ضمانا لصحة الإجراءات ليس من الناحية القانونية وإنما المادية، كما يتعين على ضابط الشرطة القضائية إخبار وكيل الجمهورية المختص إقليميا بطلب كتابي يلتمس فيه تمديد اختصاصه الإقليمي عبر كامل الوطن للقيام بعمليات المراقبة، ويمكن لوكيل الجمهورية الاعتراض على ذلك باعتباره المشرف على أعمال جهاز الشرطة القضائية وعدم السماح بهذا الإجراء إذا لم تكن هناك مبررات لذلك.

ولأن المراقبة إجراء يترك آثاره على حقوق الأفراد فهو يخص الأشخاص والأموال والأشياء وكذلك عائدات الإجرام، فإنه لا يتقرر إلا بإذن كتابي (ترخيص) من وكيل الجمهورية، يكون بموجبه ضابط الشرطة القضائية أو العون تحت سلطته ملزمان باتباع الطرق القانونية خلال المهمة المسندة لهما، مع التقيد بالهدف المقصود.[143]

3-الحالات التي يجوز فيها اللجوء الى المراقبة الالكترونية:

وفق ما جاءت به المادة 04 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإن الحالات التي يمكن فيها القيام بعملية المراقبة الالكترونية قد ذكرت على سبيل الحصر كالتالي:

- يمكن القيام بعمليات المراقبة وفق ما تقتضيه المادة3 من نفس القانون للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- تستخدم عملية المراقبة الالكترونية في حالة الضرورة لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية
- تستخدم في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة

كل هاته الحالات لا يمكن اتخاذ عملية المراقبة الالكترونية فيها إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" من نفس المادة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته المنصوص عليها في المادة 13 من نفس القانون، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

[143] زليخة التجاني، **المراقبة كإجراء للبحث والتحري عن الجرائم**، مجلة أبحاث قانونية وسياسية، المجلد 07، العدد 01، جامعة الجزائر1، جوان 2022، ص 1190.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.[144]

ثانيا: اعتراض المراسلات

1-تعريف اعتراض المراسلات:

عرفه القضاء بأنه" التصنت على المكالمات وهو تقنية يتم من خلالها الاعتراض عن طريق ربط خط هاتفي لشخص ما مع اللجوء الى تسجيل المكالمات في أشرطة مغناطيسية"، ويقصد بذلك الاستماع خلسة الى الحديث الخاص عبر الهاتف الثابت أو النقال، وذلك عن طريق المراقبة لشخص أو أكثر من المشتبه فيهم عن بإستراق السمع للمحادثات التي تتم عبر الخطوط والإشارات التليفونية، إذ يتطلب أمر المراقبة التصنت على المكالمات وسماعها وحفظها الكترونيا، لأنه من غير المتصور مراقبة المحادثات ومعاينتها دون سماعها والتصنت عليها.[145]

2-شروط اعتراض المراسلات الالكترونية:

أ-ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ: طبقا للمادة 65 مكرر 05 من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية هذا الإجراء وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقدير فائدة إجراء الاعتراض وجديته وملاءمته لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا، وعملية تنفيذ إجراء اعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به وذلك من خلال قيام ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بإعداد محضرا عن كل عملية اعتراض للمراسلات وكذا عن عمليات وضع الترتيبات التقنية لهذا الغرض، ويذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

ب-تحديد طبيعة المراسلة ومدة الاعتراض: وهذا ما يفهم صراحة من نص المادة 65 مكرر 07 التي نصت على أنه يجب أن يتضمن الإذن باعتراض المراسلات كل العناصر التي تسمح بالتعرف على الاتصالات أو المراسلات المطلوب

[144] أنظر المادة 04 من القانون 04/09 المؤرخ 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر العدد 47 المؤرخة في 16 غشت 2009.

[145] د. الطاهر ياكر، **الجرائم الالكترونية الاحكام الموضوعية والإجرائية (دراسة مقارنة)**، المرجع السابق، ص 107.

اعتراضها، كما أن المشرع قد استوجب ألا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الإذن وفقا لمقتضيات التحري والتحقيق.[146]

3-طرق اعتراض المراسلات الالكترونية:

يعتبر البريد الالكتروني أهم وسيلة تقنية في مجال التراسل الالكتروني ومن ثم فعملية الاعتراض تنصب عليه، ومن المعلوم أن كل رسالة الكترونية يظهر فيها معلومات عامة مثل تاريخ إنشاء الرسالة وتاريخ تلقيها وكذا عنوان المرسل وعنوان المرسل إليه ولكن هذه المعلومات ليست كافية لمعرفة المرسل إذ بإمكان هذا الأخير إطلاق رسالته من صناديق بريد مسجلة بأسماء وهمية، كما أن هناك وسائل تتيح للمرسل أن يرسل رسالته دون أن يظهر فيها عنوان بريده الالكتروني الصحيح لذلك لابد من الحصول على المزيد من المعلومات التي يمكن العثور عليها في حاشية رسائل البريد الالكتروني والتي يطلق عليها مصطلح E-mail Header وهي أول خطوة للبدء في التحري عن مرسل الرسالة الالكترونية وهذه الحاشية لا تظهر بصورة مباشرة وإنما يتطلب الأمر من المستخدم إجراء بعض الخطوات للحصول عليها. أو من خلال IP يمكن من خلالها الاستدلال على صاحب الرسالة ويصبح بعد ذلك من السهل الحصول على المزيد من المعلومات عن المرسل وذلك بإدخال رقم IP في بعض المواقع التي يقوم بالكشف عن مصدر الرسالة والمكان الجغرافي الذي أرسلت منه وكذا مزود الخدمة الذي يتعامل معه مرسل الرسالة ويكون بذلك من السهل تمام اعتراض هذه المراسلات والاطلاع على محتواها دون علم مرسلها.[147]

ثالثا: التسجيل الصوتي

1-تعريف التسجيل الصوتي:

يمكن تعريفها على أنها " عبارة عن ترجمة للتغييرات المؤقتة لموجات الصوت الخاصة بالكلام أو الموسيقى إلى نوع آخر من الموجات أو التغيرات الدائمة، ويكون التسجيل عادة بواسطة آلة تترجم موجات الصوت إلى اهتزازات خاصة"، وتكون التسجيلات هي التي يتم كتابتها بواسطة الآلة الرقمية ومنها الرسائل عبر البريد الالكتروني والبيانات المسجلة بأجهزة الحاسب الآلي. وتتخذ أدوات التسجيل الصوتي أنواع عديدة منها أجهزة الاتصال السلكي الخارجي أو اللاسلكي والميكروفونات الصغيرة التي لا يتعدى حجمها عود ثقاب، وميكروفونات الليزر وكذلك الميكروفونات المسمارية.[148]

رابعا: التقاط الصور

---

[146] فاطيمة دهان، كلثوم دهان، **إجراءات البحث والتحري في الجرائم المعلوماتية**، المرجع السابق، ص58.

[147] عبد الرؤوف بوديسة بجاد، **آليات التحري عن الجريمة الالكترونية في القانون الجزائري**، المرجع السابق، ص 64.

[148] كاهنة آيت حمودة، **البحث والتحري الجنائي في مسرح الجريمة الالكترونية**، المرجع السابق، 184.

1-تعريف التقاط الصور:

يقصد بإجراء التقاط الصور تثبيت الصور على مادة حساسة وتثبيت الصورة يعني تركيزها بسرعة خاطفة ثم أخذها عن طريق جهاز معد لذلك، وعليه إجراء التقاط الصور هو عبارة عن معاينة مادية مرئية لحالة شخص أو عدة أشخاص على الوضعية التي كانوا عليها وقت التصوير، وهي تربط الزمان والمكان والأشخاص في وقت واحد وقد تمتد إلى الدليل المادي للجريمة وإلى محيطها.[149]

ويعرف التقاط الصور بأنه أسلوب جديد للبحث والتحري استحدثه المشرع الجزائري ضمن أحكام المادة 65 مكرر5 من قانون الإجراءات الجزائية، ويقصد به في الفقه المراقبة المرئية التي تتم بوضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط الصور لشخص أو عدة أشخاص يتواجدون في مكان خاص، حيث يستعمل فيه ضباط الشرطة القضائية أجهزة التقاط الصور الفوتوغرافية التي تسمح بضبط المشتبه فيهم أثناء ارتكابهم للجريمة مع تحديد مكان وزمان التقاطها من أجل استعمالها كأدلة إثبات أمام المحاكم الجنائية.[150]

ومن ثمة فإن إجراء التقاط الصور هو عبارة عن مراقبة بصرية تتم من خلال كاميرات وأجهزة خاصة تلتقط الصور والصوت لوضعية شخص أو عدة أشخاص على الحالة التي كانوا عليها، وهي عبارة عن معاينة مادية مرئية لحالة شخص أو عدة أشخاص في وقت واحد، وقد تمتد إلى الدليل المادي للجريمة وإلى محيطها.[151]

2-شروط التقاط الصور: لعملية التقاط الصور شروط شكلية وأخرى موضوعية، وسنتطرق لعرض ذلك كما يلي:

أ-الشروط الشكلية: وتتمثل فيما يلي

-إذن وكيل الجمهورية أو قاضي التحقيق قبل مباشرة العملية: حسب ما نصت عليه المادة 65 مكرر5 من قانون الإجراءات الجزائية فعند وقوع إحدى الجرائم المذكورة ضمن نفس المادة يجوز لوكيل الجمهورية أو لقاضي التحقيق أن يأذن باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بمعنى لابد من وجود إذن مسبق قبل البدء بهذه العمليات.

-ضرورة أن يكون الإذن مكتوب: يجب أن يكون الإذن مكتوب ويسلم لضابط الشرطة القضائية المكلف بالعمليات وهو يعطي الحق لحامله الاستعانة بأهل الخبرة.

-محاضر العمليات: يجب تحرير محضر يرسل إلى قاضي التحقيق عند كل مرحلة على حدا وبشكل منفصل ولا يتم الانتظار إلى بلوغ المرحلة النهائية، حيث يشمل كل محضر تاريخ وساعة بداية العملية ونهايتها ويرفق محضر يتضمن وصفا أو نسخة

---

[149] عبد الرؤوف بوديسة بجاد، نفس المرجع، ص 68.

[150] د. الطاهر ياكر، **الجرائم الالكترونية الاحكام الموضوعية والإجرائية (دراسة مقارنة)**، المرجع السابق، ص108.

[151] د. الطاهر ياكر، نفس المرجع.

من المراسلات والصور والمحادثات وإذا كانت المكالمات أو المحادثات بلغة أجنبية يتم ترجمتها من طرف مترجم يتم تسخيره لهذا الغرض.[152]

ب–الشروط الموضوعية: وتتمثل الشروط الموضوعية فيما يلي:

–السلطة المختصة بإجراء العملية: وكيل الجمهورية أو قاضي التحقيق بالرغم من أنه لا يقوم بهذا الاجراء بنفسه، إلا أنه يجري تحت إشرافه ومراقبته المباشرة.

–وقت ومكان إجراء العمليات: لم يضع المشرع الجزائري قيود زمنية ولا مكانية لهذه الإجراءات الخاصة حيث أجازها في أي وقت من ليل أو نهار وفي أي مكان عام أو خاص باستثناء السفارات والقنصليات الأجنبية التي لا يمكن أن تخضع لهذه العمليات.

–عدم مسؤولية القائم والمشرف على هذه العمليات: إن الاعتداء على الحياة الخاصة بتسجيل الأصوات واعتراض المراسلات والتقاط الصور ودخول مساكن بغير إذن صاحبها وتسلق الجدران ليلا وفتح الاقفال وغيرها كلها أفعال مجرمة، إلا أنها لا تعتبر كذلك إذا ما تمت في إطار إجراءات البحث والتحري الخاصة وبإذن من وكيل الجمهورية أو قاضي التحقيق.

–ضرورة اللجوء إليها: لابد أن توجد ضرورة ماسة تستدعي اللجوء إلى القيام بهذه الإجراءات إضافة إلى وقوع جريمة من الجرائم السبعة المذكورة بنص المادة 65 مكرر 5 من قانون الإجراءات الجزائية وهي وجود دلائل قوية ونسبتها الى المتهم.[153]

خامسا: التسريب

1–تعريف التسريب:

يقصد بالتسريب حسب ما نصت عليه المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري التسرب على أنه: "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".[154]

---

[152] مختار خداوي، **إجراءات البحث والتحري الخاصة في التشريع الجنائي الجزائري**، مذكرة تخرج لنيل شهادة الماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة د. الطاهر مولاي، سعيدة، 2015–2016، ص 38–39.

[153] مختار خداوي، **إجراءات البحث والتحري الخاصة في التشريع الجنائي الجزائري**، المرجع السابق، ص 38.

[154] كاهنة آيت حمودة، **البحث والتحري في مسرح الجريمة الالكترونية**، المرجع السابق، ص 190.

2-شروط التسرب:

أ-الشروط الشكلية: وتنحصر الشروط الشكلية للتسرب في الإذن وما يجب أن يتضمنه فلا يمكن أن يباشر ضابط الشرطة القضائية عملية التسرب بمفرده دون إذن من قبل الجهات القضائية وهذا ما نصت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية، ويجب أن يكون الإذن مكتوبا وإلا كان الإجراء باطلا، كما يجب أن يتضمن ذكر هوية الضابط الذي تتم على يديه عملية التسرب وتحديد المدة المطلوبة في عملية التسرب والتي لا يتجاوز إجراء التسرب 04 أشهر تحدد حسب المقتضيات

ب-الشروط الموضوعية: الأول يتمثل في تحديد نوع الجريمة والتي يجب ألا تخرج عن الجرائم التي حددتها على سبيل الحصر المادة 65 مكرر 5(4) أما الشرط الموضوعي الثاني فهو أن يكون الإذن التسرب مسببا، فمن خلال التسبب تتبين العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن وكذا العناصر التي دفعت ضابط الشرطة القضائية للجوء إلى هذا الإجراء والتي تكون ضمن موضوع طلبه الإذن، لذلك فكان لزاما عند إصدار الإذن بالتسرب سواء من طرف وكيل الجمهورية أو من طرف قاضي التحقيق إظهار جميع الأدلة بعد تقدير العناصر المعروضة عليه من طرف ضابط الشرطة القضائية.[155]

3-طرق التسرب في مجال الجريمة المعلوماتية:

يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات الكترونية فيها، أو اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم مستخدما في ذلك أسماء أو صفات هيئات مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام الهاكر للموقع، من اجل القيام بعملية التسرب فقد أجاز المشرع استعمال أساليب وطرق خاصة أتاحت بدورها إمكانية اللجوء إلى استخدام عدد الوسائل والتقنيات هي في الأصل ليست مسموح بها قانونا لأنها تعتبر مساسا لمبدأ حرمة الحياة الخاصة غير انه لكل قاعدة استثناء وهو ما فعله المشرع الجزائري عندما تدخل بواسطة القواعد الإجرائية ليقيد أحيانا هذه الحرمة للحياة الخاصة.[156]

[155] فاطيمة دهان، كلثوم دهان، **إجراءات البحث والتحري في الجرائم المعلوماتية**، المرجع السابق، ص 55.

[156] فاطيمة دهان، كلثوم دهان، نفس المرجع.

المطلب الثاني: وسائل البحث والتحري في الجرائم الالكترونية

الفرع الأول: الدليل الرقمي كمصدر لإثبات الجريمة

أولا: تعريف الدليل الالكتروني

1-تعريف اللغوي: الدليل لغة يعرف بأنه: ما يستدل به، برهان، بينة، حجة، شاهد، علامة.[157]

2-**تعريف الاصطلاحي**: يعرَّف الدليل في الاصطلاح بأنه الوسيلة التي يُستدل بها على أمر آخر، إذ يفضي استخدامه إلى انتقال العقل من حالة الشك إلى حالة اليقين، وصولًا إلى إدراك الحقيقة التي كانت محل تردد أو غموض.[158]

وقد وردت عدة تعاريف بشأن الدليل الالكتروني منها ما يلي:

" الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة"، أو أنه الجزء المؤسس على الاستعانة بتقنية المعالجة الآلية للمعلومات، والذي يؤدي إلى إقناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الانترنت.[159]

يعرف كذلك بأنه" ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وبأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصالات من خلال إجراءات قانونية وفنية لتقديمها إلى القضاء بعد تحليلها عمليا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال وبأصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة.[160]

ثانيا: خصائص الدليل الالكتروني

1-الدليل الالكتروني دليل علمي: يحتاج دليل إلى البيئة التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فإن ما ينطبق على الدليل العلمي ينطق الدليل الالكتروني، الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن هي قاعدة أن القانون مسعاه العدالة أو العلم فمسعاه الحقيقة: Science Seeks Truth،Law Seeks Justice، وإذا كان الدليل العلمي له منطقه الذي يجب ألا يخرج عليه من حيث أنه يجب عدم

---

[157] حسين ربيعي، **آليات البحث والتحقيق في الجرائم المعلوماتية**، المرجع السابق، ص 261.

[158] علي بن محمد الجرجاني، **التعريفات: تحقيق إبراهيم الأبياري**، دار الكتاب العربي، 1985، ص. 83.

[159] حسين ربيعي، **آليات البحث والتحقيق في الجرائم المعلوماتية**، المرجع السابق، ص 261.

[160] حسين طاهري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية المحاكمة الالكترونية (دراسة تحليلية مقارنة مدعمة بالفقه والقضاء المقارن)**، دار الولاء للطباعة والنشر الترجمة والتوزيع، أم البواقي الجزائر، 2023، ص255.

تعارضه مع القاعدة العلمية السليمة، فإن الدليل الالكتروني له ذات الطبيعة إذ يجب ألا يخرج الدليل العلمي عما توصل إليه العلم الرقمي وإلا فقد معناه.[161]

2-الدليل الالكتروني من طبيعة تقنية: فهو مستوحاة من البيئة التي يعيش فيها وهي البيئة الرقمية أو التقنية، وتتمثل هذه الأخيرة في إطار الجرائم الالكترونية في العالم الافتراضي، وهذا العالم كامن في أجهزة الحاسب الآلي والخوادم والمضيفات والشبكات بمختلف أنواعها، فالأدلة الرقمية ليست مثل الدليل المادي، فلا تنتج التقنية سكينا يتم به اكتشاف القاتل أو اعترافا مكتوبا أو بصمة أصبع ...، وإنما تنتج التقنية نبضات رقمية تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان.[162]

3-الدليل الالكتروني متنوع ومتطور: إن مصطلح الدليل الالكتروني يشمل جميع البيانات والمعلومات الرقمية التي يمكن تداولها رقميا بمختلف أشكالها وأنواعها، سواء كانت هذه الأدلة متعلقة بالحاسب الآلي أو غيرها من الأجهزة أو شبكة الانترنت أو شبكات الإتصال السلكية واللاسلكية ومنه فالآثار الرقمية المستخلصة من الحاسب الآلي أو شبكة الانترنت، تكون ثرية جدا ومتنوعة بما يحتويه من معلومات عن وقائع قد تشكل جريمة ما، وترتقي إلى أن يصبح دليل براءة أو إدانة ومن بين هذه المعلومات صفحات المواقع الالكترونية المختلفة، البريد الالكتروني، النصوص والصور والفيديوهات الرقمية، الملفات المخزنة في الكمبيوتر الشخصي والمعلومات المتعلقة بمستخدم شبكة الانترنت وغيرها.[163]

4-الدليل الالكتروني صعب التخلص منه: تعد هذه الخاصية من أهم خصائص الدليل الالكتروني بل يمكن اعتبارها ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة التقليدية، حيث يمكن التخلص بكل سهولة من الأوراق والأشرطة المسجلة إذا حملت في ذاتها إقرار بارتكاب شخص لجرائم وذلك بتمزيقها وحرقها، كما يمكن التخلص أيضا من بصمات الأصابع بمسحها من موضعها، كما أنه في بعض الدول الغربية يتم التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة. وإذا كان الأمر كذلك بالنسبة للأدلة التقليدية فإن الحال غير ذلك للأدلة الالكترونية، ذلك أن موضوع التخلص من الدليل الالكتروني باستخدام التخلص من الملفات في الحاسب الآلي أو الانترنت كخاصية Delete،Remove،Erase، لا تعد

---

[161] نصيرة بوحزمة، **التحقيق الجنائي في الجرائم الالكترونية (دراسة مقارنة)**، رسالة مقدمة لنيل شهادة دكتورة في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، 2021-2022، ص 189.

[162] نصيرة بوحزمة، نفس المرجع، ص 190.

[163] حنان عكوش، **خصوصية الدليل الالكتروني**، مجلة الفكر القانوني والسياسي، المجلد السابع العدد الأول، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي الاغواط، 2023، ص 1056.

من العوائق التي تحيل دون استرجاع الملفات المذكورة، إذ تتوافر برمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغائها أو إزالتها من الكمبيوتر.

ويترتب على هذه الخاصية مسائل هامة في القانون أبرزها مسألة التخلص من الدليل، فإذا اثبت الخبير التقني مثلا أن مرتكب الجريمة استخدم برمجيات للتخلص من الأدلة، فإنه يمكن إدانته بالنصوص القانونية التي تجرم مثل هذه الأفعال، وهنا ينبغي تقوية عناصر النصوص القانونية التي تجرم التخلص من الأدلة بتخصيص منطق فيها يجعل التشديد وجوبا فيها حال وجود علاقة بين التخلص من الأدلة وبين العالم الرقمي.[164]

5-الدليل الالكتروني دليل غير ملموس يتميز بالخفاء: الدليل الالكتروني ليس دليلا ماديا ملموسا، فهو -أي الدليل الإلكتروني- تلك المجالات المغناطيسية أو الكهربائية، ومن ثم فإن ترجمة هذا الدليل وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل إن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الالكترونية الى الهيأة التي يمكن الاستدلال بها على معلومة معينة. وبمعنى آخر، إن هذه الأدلة خفية لا يمكن رؤيتها، حيث تتكون من مجموعة نبضات كهربائية ومغناطيسية غير ملموسة، ولا يمكن إدراكها بالحواس الطبيعية للإنسان، أي عدم وجود آثار مادية يمكن متابعتها، وهي خطيرة وصعبة الاكتشاف من حيث مكان وقوعها أو مكان التعامل معها بسبب اتساع نطاقها وضخامة البيانات.[165]

6-الدليل الالكتروني ذو طبيعة رقمية ثنائية (0-1): ليس للدليل الالكتروني هيئة واحدة، وإنما له خاصية الالتصاق بمفهوم تكنولوجيا المعلومات من حيث تكوينه، أذ يتكون من تعداد غير محدود لأرقام ثنائية موحدة في الواحد(1) والصفر(0) والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه، فالكتابة مثلا في العلم الرقمي ليس لها الوجود المادي الذي تعرفه في شكل ورقي، وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فأي شيء في العالم الرقمي يتكون من الصفر والواحد، وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة، وأما تكوين معطياته فإنها تختلف من حيث الحجم والموضوع، إذ كمية (1-0) في ملف يمكن أن تختلف عن الحجم في ملفات أخرى.[166]

---

[164] نصيرة بوحزمة، **التحقيق الجنائي في الجرائم الالكترونية (دراسة مقارنة)**، المرجع السابق، ص 190

[165] بندر عقاب جفين كميخ حطاب الدويش، **خصائص وأنواع الدليل الالكتروني في الكويت ودول المقارنة**، المجلة القانونية علمية محكمة، المجلد 16 العدد 3، كلية الحقوق، جامعة عين شمس، مايو 2023، ص 826.

[166] نصيرة بوحزمة، نفس المرجع، ص 192.

ثالثا: أنواع الأدلة الرقمية

تتعدد وتتنوع الأدلة الرقمية على النحو الآتي:

-الأدلة الرقمية المستخرجة من مسرح الجريمة الافتراضي: ويقصد بها الأدلة الرقمية أو التكنولوجية المستخرجة من الحاسبات الآلية والخوادم المستخدمة في إتمام تنفيذ الفعل الإجرامي في مراحله المختلفة ومثالها:

- الرقم التعريفي IP Address
- سجلات الحفظ داخل الحاسبات والخوادم وهي المعنية تستخدم الإجراءات وكافة الأنشطة التي سبق اتخاذها من قبل مستخدم الانترنت.
- البريد الالكتروني (e-mail)، وهي الرسائل الالكترونية المتبادلة من المتهم والمجني عليه. وتشير إلى ما تم بينهما من مراسلات واتفاقات ووعود وتهديدات.

ويمكن طباعة هذه الأنواع من الأدلة الرقمية من خلال الحواسب الآلية أو الخوادم وبأساليب فنية خاصة تمكن من تحديد هوية القائم بالفعل الإجرامي، وتكون الطباعة في صورة رسائل الكترونية أو ملفات نصية من Log File تظهر الرقم التعريفي (IP).[167]

-الأدلة الرقمية المستخرجة من الأجهزة بعد ضبطها: وفي حال نجاح جهود الأجهزة الأمنية والفنية في تحديد هوية المتهم وضبطه بناء على إذن من النيابة العامة التي تأمر كذلك بضبط جهاز الحاسب الآلي أو الأجهزة المستخدمة في تنفيذ الجريمة، يمكن في هذه الأحوال، ومن خلال الفحص الفني لهذه الأجهزة استخراج عدد من الأدلة الرقمية على النحو التالي:

- نصوص مستخرجة من ذاكرة الحاسب، ويتضمن تلك النصوص بعض المعلومات أو الصور أو البيانات الخاصة -مثلا- بكروت ائتمان تم تجميعها من خلال بعض الصفحات المزيفة التي يستخدمها الجاني للإيقاع بالمجني عليه.
- صور مستخدمة في ذاكرة الحاسب يتم استخراجها من خلال برامج ذات تقنية خاصة بفحص الأجهزة الرقمية وتشير إلى بعض الإجراءات والخطوات التي قام بها المتهم لتنفيذ أو إخفاء معالم جريمته.

[167] حسين طاهري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية المحاكمة الالكترونية (دراسة تحليلية مقارنة مدعمة بالفقه والقضاء المقارن)**، المرجع السابق، ص 254.

- وسائل البريد الالكتروني (e-mail) المتبادلة بين المتهم والمجني عليه، والتي تشير إلى سابقة تبادلها الرسائل وما تضمنته الرسائل الالكترونية للمتهم من احتيال أو تهديد أو ابتزاز أو انتحال صفة.[168]

رابعا: وسائل جمع الدليل الرقمي

1-برنامج معالجة الملفات: وهو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصل، يستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضغوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

2-برنامج النسخ: وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر وهو برنامج مفيد للحصول على التوازي أو على التوالي وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها.

3-قرص بدء تشغيل الكمبيوتر: وهو قرص يمكن المحقق من تشغيل الكمبيوتر إذا كان نظام التشغيل فيه محميا بكلمة مرور ويجب أن يكون القرص مزودا ببرنامج مضاعفة المساحة فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.

4-برامج كشف الدسك: ويمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد، ونسخة خاصة بالشرطة.

5-برامج الاتصالات: وهو يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.[169]

خامسا: دور الدليل الرقمي في الاثبات الجنائي

أ-حجية الدليل الإلكتروني

1-مشروعية الدليل الرقمي: يتسع ويضيق قبول الدليل الرقمي تبعا للمبادئ التي تقوم عليها أنظمة الاثبات السائدة، وفي هذا الصدد نجد المشرع الجزائري كغيره من المشرعين أفرد نصوص تحفز القاض على قبول أو عدم قبول أي دليل بما في

[168] حسين طاهري، نفس المرجع، ص 255.

[169] نادية غرباوي، **أساليب البحث والتحري في الجرائم المعلوماتية**، مذكرة تخرج لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، 2016-2017، ص45.

ذالك الدليل التقني. كما ان حرية الاثبات في المسائل الجزائية من المبادئ المستقرة في نظرية الإثبات، وبذلك اقر المشرع الجزائري مبدأ حرية الإثبات الجزائي في المادة 212 من قانون الإجراءات الجزائية، حيث نصت على أنه يجوز اثبات الجرائم لبأي طريقة من طرق الاثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكما تبعا لاقتناعه الشخصي، ومن بين مبررات الأخذ بمبدأ حرية الإثبات ظهور الأدلة العلمية الحديثة التي كشف عنها العلم الحديث في إتيان الجريمة ونسبها إلى المتهم، كبصمة الصوت والبصمة الوراثية.

ويتجلى الدور الإيجابي للقاضي الجزائي في الجريمة الالكترونية في عنصرين هامين هما:

- توفر الدليل من خلال البحث عن الدليل باستعمال السلطات المخولة له قانونيا، حيث يستطيع أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إليه، من خلال الإفصاح عن كلمات المرور والشفرات الخاصة بتشغيل البرنامج.
- سلطة الأمر بتفتيش نظم الحاسوب بجميع مكوناته بحثا عن الدليل الرقمي.[170]

2-مصداقية الدليل الرقمي: زاد ظهور الدليل التقني من دور الإثبات العلمي، الذي كان دور الخبراء فعال في ذلك وهذا بالنظر إلى الجرائم الالكترونية، وللخبرة التقنية أهمية في استخلاص الدليل التقني التي لها دور في البحث عن مصداقيته في مجال المعالجة الالية للمعلومات.

ب- الضوابط المتعلقة بالدليل الرقمي:

تتمثل أهم الضوابط المستمدة من الدليل الرقمي في سلطة القاضي الجزائي في تقديره لهذا الدليل، وهي تستمد من ضرورة الاقتناع بالأدلة الرقمية الصحيحة، وضرورة مناقشته لها في الجلسة مع وجود أصل الدليل في أوراق الدعوى المعروضة في المحكمة.[171]

[170] د. نادية أيت عبد المالك، ط. د. عبد القادر فلاح، **التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري**، مرجع سابق، ص 1701.
[171] د. نادية أيت عبد المالك، ط. د. عبد القادر فلاح، نفس المرجع، ص 1702.

الفرع الثاني: الوسائل المستخدمة في التحري وجمع الأدلة

أولا: الوسائل المادية

1-عناوين IP، MAC، البريد الالكتروني وبرامج المحادثة

يُعد عنوان الإنترنت (IP Address) أحد العناصر الجوهرية في بنية الشبكة المعلوماتية، حيث يضطلع بمهمة توجيه حزم البيانات إلى وجهاتها المحددة ضمن الشبكة العالمية. ويُشبه هذا العنوان في طبيعته عنوان البريد التقليدي، إذ يمكّن أجهزة التوجيه والشبكات الوسيطة من إيصال الرسائل إلى الأجهزة المستقبِلة بدقة. ويُمنح كل جهاز متصل بالإنترنت عنوانًا فريدًا يتكوّن عادة من أربعة مقاطع رقمية، كل منها يتكون من عدد من الخانات، ليشكل ما مجموعه اثنتي عشرة خانة كحد أقصى. وتدل المقاطع الأربعة على معلومات محددة؛ فالمقطع الأول يشير إلى الموقع الجغرافي، والثاني يعبّر عن مزود الخدمة، والثالث عن مجموعة الحواسيب المرتبطة، أما الرابع فيُخصص للجهاز الذي تم الاتصال من خلاله. وعند وقوع حوادث اختراق أو أنشطة تخريبية، فإن الخطوة الأولى للتحقيق غالبًا ما تتمثل في تعقّب عنوان الجهاز لتحديد مصدر الهجوم. ومن جهة أخرى، يستطيع مزود الخدمة مراقبة هذا العنوان في حال توفر الأجهزة والبرمجيات المناسبة لذلك. كما يمكن للمستخدم نفسه الاطلاع على عنوان الجهاز عند الاتصال المباشر، خصوصًا في أنظمة تشغيل Windows، وذلك عبر إدخال الأمر (Winpcfg) ضمن نافذة التشغيل، حيث يظهر عنوان IP الخاص. ويجدر التنويه إلى أن هذا العنوان قد يتغير مع كل اتصال جديد بالشبكة، وفقًا لنوع التهيئة المستخدمة.[172]

2-البروكسي Proxy:

ويكون عمله كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة Cache Memory. وتقوم الفكرة في البروكسي على تلقيها مزود البروكسي طلبا من المستخدم الباحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، ثم يقوم بإعادة إرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية. وفيما إذا لم يتم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين IP. ومن أهم مزايا مزود البروكسي أنه يمكن للذاكرة Cache الاحتفاظ بتلك العمليات

[172] Doll Barbara, Understanding IP Addresses: Everything You Ever Wanted to Know, TechNet, Microsoft, 2021

التي تمت عليها مما يجعل دوره قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.[173]

3- برامج التتبع: تساهم البرامج الأمنية المتخصصة في الكشف عن محاولات الاختراق الرقمي من خلال تحليل البيانات المتعلقة بالهجمات الإلكترونية، وتحديد هوية الجهة المهاجمة، إن أمكن وتقوم هذه البرامج بتوليد تقرير مفصل يُعرض على المستخدم المتضرر، يتضمن وصفا للحادثة، وتاريخ وقوعها، وعنوان بروتوكول الإنترنت (IP) المستخدم في الاختراق، فضلا عن تحديد مزوّد خدمة الإنترنت الذي ينتمي إليه المخترق، ومنافذ الاتصال المستعملة أثناء تنفيذ الهجوم، بالإضافة إلى معلومات تقنية أخرى تُستخدم في التتبع والتحقيق الرقمي.[174]

4- نظام كشف الاختراق Intrusion Détection System: تُعرف أنظمة كشف التسلل، والتي يُشار إليها بالاختصار IDS، بأنها برامج متخصصة ترصد الأنشطة الجارية على أجهزة الحاسوب أو عبر الشبكات. وتُنجز هذه المهمة من خلال تحليل حزم البيانات أثناء تنقلها في بيئة الشبكة، بالإضافة إلى مراقبة ملفات نظام التشغيل المعنية بتسجيل الأحداث فور وقوعها. وتعتمد هذه الأنظمة على مقارنة ناتج التحليل بمجموعة من السمات التي تُعد مؤشرات معيارية للهجمات الإلكترونية، والتي يُطلق عليها في المجال التقني مصطلح "التوقيعات". وفي حال تطابق أي من هذه التوقيعات مع نشاط جارٍ، يقوم النظام بإشعار مسؤول الشبكة فورًا من خلال وسائل متعددة، مع توثيق كافة البيانات المرتبطة بالحادثة في سجلات إلكترونية مخصصة. وتُعد هذه البيانات ذات أهمية كبيرة لفرق التحقيق الإلكتروني، إذ تُسهم في تحديد نمط الهجوم، وأسلوبه، وربما مصدره.[175]

5-نظام جرة العسل Honey Pot: نظام مصمم خصيصا لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أية بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعا خاطئا بسهولة الاعتداء على هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز آخر في الشبكة، في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء، وتحليلها وبالتالي اتخاذ اجراء وقائي فعال وهذه المعلومات التي تم جمعها تفيد في تحليل أبعاد الجريمة في حال وقوعها ومد فريق التحقيق بالعديد من البيانات التي توضح معالم الجريمة.[176]

---

[173] خالد علي نزال الشعار، **التحقيق الجنائي في الجرائم الالكترونية**، المرجع السابق، ص38.

[174] أحمد غانم، **أمن الشبكات وأنظمة المعلومات**، ط. 2، دار الفكر الجامعي، 2020، ص 135.

[175] Peltier, Thomas R. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Auerbach Publications, 2016.

[176] خالد علي نزال الشعار، **التحقيق الجنائي في الجرائم الالكترونية**، المرجع السابق، ص 39.

6-أدوات تدقيق ومراجعة العمليات الحاسوبية Auditing Tools: إن عمل هذه الأدوات مراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسوب معين وتسجيلها في ملفات خاصة يطلق عليها logs والكثير من هذه الأدوات تأتي مصممة في أنظمة التشغيل بعد إعدادها للعمل، وهنا ما يقوم به مدير الشبكة أو النظام بتفعيلها وإعدادها للعمل في وقت مبكر وسابق لارتكاب الجريمة حتى يستطيع أن يقوم بتسجيل المعلومات التي قد يكون لها علاقة بالحادثة وتساعد في كشف أسلوب الجريمة وشخصية مرتكبها. والمثال عليها أداة Event Viewer لبيئة النوافذ، وأداة Syslogd لبيئة يونيكس.[177]

7-أدوات الضبط: إن جهاز التحقيق وجمع الاستدلالات تحتاج لضبط ماديات الجريمة وإثبات وقوعها والمحافظة على الأدلة لتقديم الجاني للنيابة العامة، لذا فإن هناك أدوات تساعد في ضبط الجريمة الالكترونية، كبرامج الحماية وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وبرامج التصنت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات، ومراجعة قاعدة البيانات، وبرامج النسخ الاحتياطي، والتسجيل وغيرها من الأدوات مثل CONTENT MANGEMETNT، MNM4، IDS.

8-الوسائل التي تساعد على التحقيق: تُعتبر الوسائل التقنية الحديثة من الأدوات الجوهرية في مجال التحقيقات الجنائية الرقمية، لا سيما عند التعامل مع الجرائم الإلكترونية التي تتضمن محاولات لإتلاف الأدلة أو حذفها. وتشمل هذه الوسائل مجموعة من البرامج المتخصصة، مثل برامج استرجاع البيانات من الأقراص الصلبة التالفة، وتجاوز كلمات المرور، بالإضافة إلى أدوات الضغط وفك الضغط، والبحث عن الملفات سواء كانت مرئية أو مخفية. كما تُستخدم برامج تشغيل الأجهزة ونسخ البيانات والبرمجيات التي تتيح الكتابة على الأقراص الصلبة في استخراج المعلومات الرقمية، حتى تلك التي يُعمد إلى حذفها نهائياً. وتساهم هذه الأدوات في حفظ مسرح الجريمة الرقمي وتمكين الجهات المختصة من تحليل الأدلة الإلكترونية بكفاءة.[178]

9-أدوات فحص ومراقبة الشبكات: وهي أدوات تستخدم في فحص بروتوكول TCP/IP وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها، ومنها:

- ✓ برامج Visual Rloute: وهو برامج تلتقط أي عملية فحص عملت ضد الشبكة، فيقوم بتقديم أجوبة تبين البيانات التي حدث فيها مسح، والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان IP أو اسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

[177] خالد علي نزال الشعار، نفس المرجع.

[178] القحطاني عبد الله بن عبد العزيز، **الأدلة الإلكترونية في الإثبات الجنائي**، دار جامعة نايف للنشر، الرياض، 2018، ص 85 إلى ص 110.

- ✓ أداة التتبع Tracer: ترسم مسار بين جهازين تظهر فيه كل التفاصيل عم مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها الوقت والفترات التي قضاها، وتسمح كذلك برؤية المسار الذي اتخذه IP من مضيف إلى آخر، وتستخدم هذه الأداة الأخيرة Time To Live(TTL) التي تكون ضمن IP لكي تستقبل من كل موجه رسالة وبذلك يكون هو العدد الحقيقي للوثبات. ويتم بذلك تحديد وبشكل دقيق المسار الذي تسلكه الرزمة. وهذه الأداة تستخدم في الأساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها، إذ أنه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيح ونقاط الضعف، ولكن يمكن أيضا من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها.
- ✓ أداة التفحصNEW STAT: هي أداة لفحص حالة الاتصال الحالي للبرتوكول TCP/IP وتقوم بالعديد من المهام لعرض جميع الاتصالات الحالية، ومنافذ التصنت، وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لدول التوجيه.[179]

ثانيا: الوسائل الإجرائية

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثانية والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

- ✓ افتقار الأثر: يمكن تقصي الأثر بطرق عدة سواء عن طريق بريد الكتروني ثم استقباله، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.
- ✓ الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.
- ✓ الاستعانة بالذكاء الاصطناعي، من خلال استنساخ النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الالكترونية وفق برامج صممت خصيصا لهذا الغرض
- ✓ مراقبة الاتصالات الالكترونية: لم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الاتصالات الالكترونية، على عكس بعض التشريعات التي عرفتها مثل التشريع الأمريكي والكندي.[180]

[179] عبد الرؤوف بوديسة بجاد، **آليات التحري عن الجريمة الالكترونية في القانون الجزائري**، المرجع السابق، ص40.

[180] د.عز الدين عثماني، **إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية**، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد الرابع، جانفي 2018، ص 55.

الفرع الثالث: مشروعية وسائل البحث والتحري في الجرائم الالكترونية

قد أقر المشرع الجزائري في تعديل دستور 2020 في نص المادة 47 على أنه، " لكل شخص الحق في حماية حمايته الخاصة وشرفه، لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت، لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية، حماية الأشخاص عند معالجة المعطيات ذات الطباع الشخصي حق أساسي، وبإسقاط ما سبق بيانه على التشريع الجزائري لاسيما قانون الإجراءات الجزائية وقانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال أن المشرع حاول إمساك مسطرة العدالة من النصف، بحيث أراد الحفاظ على حق الجماعة في توقيع العقاب وعدم إفلات المجرمين منه، ومن جهة أخرى قرر مجموعة من الضمانات والشروط التي يجب اتباعها من قبل الضبطية القضائية ونطاق تطبيقها.[181]

وإذا هذه الإجراءات الحديثة التي تتصف بطابع المشروعية، وضع المشرع مجموعة من الضمانات يمكن لنا إجازها في النقاط التالية:

-أن يكون المساس بحقوق الشخصية الفردية، وفقا للقانون.

-أن ينظم القانون ضمانات شكلية وموضوعية دقيقة ومفصلة، يلتزم القائمون بالتحري والتحقيق إتباعها.

-أن يكون الإذن الصادر بإتخاذه مكتوبا ومسببا، تحديد مدة الإجراء المتخذ، نطاق الجرائم التي يتخذ بشأنها، ضرورة الحفاظ على السر المهني.

-أن يكون تقرير الإجراء قد دعت إليه الضرورة، خاصة إذا كنا بصدد الجرائم التي تتسم بالخطورة والتعقيد والتي تمس الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة.

-أن يتم تحديد الجرائم الخطيرة على سبيل الحصر والتي يمكن اتخاذ بصددها تلك الإجراءات الماسة بحقوق الإنسان.[182]

[181] عبد الرؤوف بوديسة بجاد، **آليات التحري عن الجريمة الالكترونية في القانون الجزائري**، المرجع السابق، ص 71.

[182] وردة شرف الدين، **مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري**، المرجع السابق، ص 554.

خلاصة الفصل الثاني:

يتبن في ختام هذا الفصل أن عملية البحث والتحري عن الجرائم الالكترونية تختلف عن غيرها من الجرائم التقليدية، سواء من حيث الوسائل المعتمدة أو من حيث القيود القانونية المفروضة، وذلك بالنظر إلى الطبيعة التقنية المعقدة لهذه الجرائم، وسرعة تطورها، وامتدادها عبر الحدود الجغرافية. وقد برزت الحاجة الى إيجاد توازن دقيق بين فعالية الأجهزة الأمنية في كشف مرتكبي هذه الجرائم، وضمان احترام الحقوق والحريات الأساسية والمعطيات الشخصية.

وقد تطرق هذا الفصل إلى أهم الضوابط القانونية والإجراءات التي تحكم عمليات التحري الرقمي، بدءا الأجهزة المكلفة بعملية البحث مرورا إلى كيفية جمع الأدلة الالكترونية ووصولا إلى دور الهيئات المختصة في مكافحة هذا النوع من الإجرام وذلك وفق ما تم تسليط الضوء على موقف المشرع الجزائري من هذا الإجراءات من خلال النصوص القانونية –خصوصا ما تعلق بالقانون 09-04- والخاص بتنظيم تلك الإجراءات بشكل يكفل الفعالية القانونية دون المساس بضمانات المحاكمة العادلة.

وتأسيسا على ما سبق، فإن نجاح جهود التحري في مجال الجريمة الالكترونية يظل مرهونا بمدى تأهيل الجهات المكلفة بالتنفيذ تقنيا وقانونيا، وتحديث النصوص باستمرار، وتعزيز التعاون الدولي، باعتبار أن هذه الجرائم تتخطى الحدود الوطنية وتتطلب استجابة مشتركة ومتكاملة.

الخاتمة

خاتمـــــــــــــة:

استنادًا إلى ما تم استعراضه من تحليل دقيق في هذا البحث حول آليات البحث والتحري في الجرائم الإلكترونية، تبين أن هذا النوع من الجرائم قد أبرز تباينًا فقهيًا واضحًا في تحديد المصطلحات القانونية المرتبطة به، حيث يتفاوت تحديد هذه المصطلحات وفقًا لاختلاف المذاهب القانونية، وهو ما يعكس عدم استقرار في المسميات القانونية المتفق عليها. إلا أن ما يظل مشتركًا بين كافة الاتجاهات الفقهية هو اعتبار الأفعال المرتكبة في هذا السياق من الأفعال الإجرامية التي يجب مكافحتها والحد من انتشارها، نظرًا للضرر الكبير الذي تسببه للمجتمع.

ويرجع هذا التباين في الفهم إلى التطور السريع والمتزايد في تكنولوجيا المعلومات، وهو ما أدى إلى ظهور أنماط جديدة من الجرائم يصعب تصنيفها ضمن المفاهيم التقليدية للجرائم. وقد تناول هذا البحث الخصائص التي تميز الجرائم الإلكترونية عن الجرائم التقليدية، لاسيما من حيث الطبيعة اللامادية لهذه الجرائم، ما يعقّد عملية اكتشافها وضبط أدلتها، فضلًا عن أن الجاني في هذا السياق لا يحتاج إلى التواجد المادي في موقع الجريمة، إذ تتم الجرائم عبر بيئات افتراضية غير محددة الهوية، مما يزيد من صعوبة تعقب الجناة وملاحقتهم.

كما تناول موضوع البحث الأنماط المختلفة لهذه الجرائم وخصائص الجناة ودوافعهم التي تميزهم عن الجناة التقليديين، مما يستدعي تطوير التشريعات القانونية لتمكين الأجهزة المعنية من مواجهة هذا النوع من الجرائم بفعالية، واتخاذ تدابير قانونية قادرة على الحد من آثارها السلبية على الأمن الاجتماعي والاقتصادي

حيث يتضح من خلال الدراسة أن التحولات الجديدة التي شهدتها مجالات البحث والتحقيق في الجرائم الإلكترونية قد أبرزت الدور البارز الذي تلعبه الوسائل التقنية في العصر الرقمي الحالي. فقد أصبح من الواضح أن انتشار الأنشطة غير القانونية في الفضاء الرقمي يشكل تهديداً مباشراً على الأمن القومي والاقتصادي والاجتماعي، بل والعالمي، لما تسببه من اختراقات لأنظمة حساسة، مثل سرقة المعلومات الاستراتيجية، وتقويض الثقة في التعاملات الإلكترونية. بالإضافة إلى ذلك، فإن الأضرار المالية الكبيرة التي تصيب المؤسسات والشركات بمختلف أنواعها تساهم في زيادة خطورة هذه الجرائم وتهديداتها، حيث تمس سرية البيانات الشخصية وتؤثر سلباً على استقرار المجتمعات. كما أن الجرائم الإلكترونية لم تعد مقتصرة على مناطق معينة، بل أصبحت تتجاوز الحدود الجغرافية، مما يخلق تحديات كبيرة أمام الجهات القانونية. وهذا يفرض الحاجة إلى تعاون دولي مستمر، بالإضافة إلى تحديث التشريعات والإجراءات الوقائية بشكل دوري.

لقد تم التطرق خلال دراسة موضوع البحث الأبعاد القانونية والفنية والتقنيات الحديثة المعتمدة في إجراءات البحث والتحري التي تجريها الضبطية القضائية وكذا الأجهزة المكلفة بالتقصي عن مثل هاته الجرائم الخطرة في إطار تشريعي يحث على المبادئ القانونية التي تحكم جمع الأدلة الرقمية وحجيتها في إقناع القاضي بمدى مشروعيتها أثناء إجراءات المحاكمة، كما تناولنا الجوانب الفنية التي تستدعي من الأجهزة الأمنية توفر خبرات والدراية بالتقنيات والعلم بها المتعلقة بكيفية استخراج المعلومات الرقمية من الأجهزة والشبكات بأساليب علمية دقيقة تضمن الحفاظ على سلامة الدليل، ومن ناحية أخرى تقنية استعرضنا الوسائل التي تواكب التطور الحديث للتكنولوجيات المعاصرة والتي تعتمدها الأجهزة الأمنية، مثل تقنيات تتبع المواقع الجغرافية الالكترونية، وتحليل حركة البيانات، وفك التشفير الخاص بالمعلومات وكذا البرمجيات المتخصصة في رصد النشاطات الإجرامية عبر الشبكة وكبح انتشارها وتوسعها، كل هذا يتطلب السرعة في العمل للقبض على الجناة قبل لجوئهم لحظر أفعالهم وبذلك نكون أمام صعوبات تستلزم استخدام طرق بديلة للكشف عن الجريمة.

ومن خلال ما تم التطرق إليه في دراستنا نتوصل إلى مجموعة من النتائج والتوصيات نوردها على النحو التالي:

أ- النتائج:

بعد تناولنا لموضوع آليات البحث والتحري في الجرائم الالكترونية من مختلف جوانبه، تم التوصل إلى عدد من النتائج والتي سنوردها على النحو التالي:

1- تطور آليات البحث والتحري: تمكّن الجهات المختصة من استخدام وسائل وتقنيات عصرية لرصد الجرائم الإلكترونية، مثل تتبع عناوين الـ IP وتحليل الأدلة الرقمية.

2- التعاون مع مزودي خدمات الإنترنت: يعد التعاون مع مزودي خدمات الإنترنت أداة أساسية في الكشف عن الجرائم الإلكترونية وتحقيق العدالة.

3- التحديات القانونية في رصد الجرائم الإلكترونية: رغم توفر وسائل تقنية متقدمة، إلا أن هناك غموضًا قانونيًا حول كيفية استخدامها في التحقيقات، مما يعرقل فعالية تنفيذ القوانين.

4- التعاون الدولي: يعزز التعاون الدولي في مكافحة الجرائم الإلكترونية، ولكنه يعاني من نقص التنسيق بين الأجهزة الأمنية والعدلية على الصعيد العالمي.

5- الاختراقات الأمنية وتطبيقات الفيروسات: تؤدي عمليات الاختراقات ونشر الفيروسات إلى تهديد نظم المعلومات، ما يستدعي تعزيز التنسيق بين الدول والمنظمات المعنية بالأمن السيبراني.

6- نقص التشريعات المواكبة للتطور التكنولوجي: تفتقر العديد من الدول إلى تشريعات تواكب التغيرات السريعة في التكنولوجيا، ما يؤدي إلى فجوة بين الجريمة الإلكترونية والنظام القانوني.

7- الغموض في تحديد مفاهيم الجريمة الإلكترونية: عدم وضوح بعض المفاهيم القانونية الأساسية المتعلقة بالجريمة الإلكترونية، مثل اختراق الأنظمة الإلكترونية والوصول غير المشروع إلى الحسابات الشخصية.

8- قصور التشريعات في مواجهة الجرائم الحديثة: بعض التشريعات التقليدية لا تتضمن وسائل تقنية حديثة، مثل الاستفادة من الثغرات الأمنية في البرمجيات لتحقيق أغراض غير قانونية.

9- تعقيدات في الإثبات الجنائي: تواجه الأجهزة القانونية صعوبة في إثبات الجرائم الإلكترونية نظرًا للغموض في التشريعات ولصعوبة تأمين الأدلة الرقمية في المحاكم.

10- تحديات في استخدام الوسائل الرقمية: تعاني الأجهزة الأمنية من صعوبة في استخدام وسائل التحري الرقمية المعترف بها قانونًا، بسبب محدودية الأدوات التقليدية وعدم وجود معايير دقيقة لضمان موثوقية الأدلة الرقمية.

11- الحاجة لتحديث التشريعات الوطنية: تفتقر العديد من التشريعات الوطنية إلى الآليات القانونية التي تحمي الأفراد من الجرائم الإلكترونية المستحدثة، مما يستدعي تحديث القوانين بما يتناسب مع التطورات التكنولوجية.

12- عدم كفاية التدريب في مجال التحقيقات الرقمية: لا يزال هناك نقص في التدريب المتخصص لأفراد الأمن والعدالة في مجال التحقيقات الرقمية، مما يؤثر سلبًا على فعالية التحقيقات في الجرائم الإلكترونية.

13- المسؤولية القانونية للمؤسسات التقنية: تنشأ إشكالات قانونية في تحديد مسؤولية الشركات التقنية في الحماية من الجرائم الإلكترونية، حيث أن بعض التشريعات لا تعكس المسؤوليات الواضحة لهذه الشركات في هذا المجال.

14- تزايد الأنشطة الإجرامية عبر الحدود: تؤدي الطبيعة العابرة للحدود للجرائم الإلكترونية إلى تحديات في تنفيذ الإجراءات القضائية، ما يفرض الحاجة إلى تفعيل اتفاقيات دولية أكثر فعالية للتعاون في مكافحة هذه الجرائم.

15- تأثير الجرائم الإلكترونية على الاقتصاد العالمي: تؤدي الجرائم الإلكترونية، بما في ذلك سرقة البيانات والتحايل على أنظمة الدفع، إلى خسائر اقتصادية كبيرة على المستوى الدولي، ما يتطلب استجابة قانونية منسقة لحماية المصالح الاقتصادية.

ب- التوصيات:

من خلال دراستنا توصلنا إلى مجموعة من التوصيات التي تتماشى مع التطورات الحديثة في مجال الجريمة الإلكترونية وتعكس أهمية تحديث القوانين والآليات المتبعة لمواكبة التحديات السيبرانية الجديدة، نوردها على النجو التالي:

1- تعزيز البنية التحتية الرقمية لمنظومة الأمن السيبراني: في ضوء الثورة المعلوماتية المتسارعة التي تشهدها المجتمعات، وما يصاحبها من ظهور جرائم إلكترونية جديدة تختلف عن تلك المرتكبة بالطرق التقليدية، يصبح من الضروري العمل على بناء بنية تحتية رقمية متكاملة تسهم في دعم الأجهزة الأمنية في إجراء عمليات البحث والتحري بفعالية. يقتضي ذلك تحديث وتطوير التجهيزات التقنية والبرمجيات المتخصصة في تحليل الأدلة الرقمية، واستخدام أدوات متقدمة لتتبع الأنشطة السيبرانية، إضافة إلى اعتماد تقنيات الذكاء الاصطناعي في استخبار المصادر وجمع البيانات.

2- استحداث وحدات شرطية وقضائية متصلة وطنياً ودولياً: من الضروري إنشاء وحدات متخصصة في التحقيقات السيبرانية على مستوى وطني ودولي، بحيث تضم كوادر متعددة التخصصات تشمل محققين جنائيين ذوي خبرة في التعامل مع الجرائم الرقمية والأدلة الرقمية، إلى جانب مهندسي شبكات معلوماتية، ومتخصصين في القانون السيبراني. يجب أن تكون هذه الوحدات مزودة بأحدث التقنيات اللازمة لاكتشاف الأدلة الرقمية وتحليلها، مع مراعاة المعايير الدولية لضمان قبول الأدلة في الإجراءات القضائية.

3- تحديث التشريعات لمواكبة تطورات الجريمة الإلكترونية: في ظل التطور المستمر للجريمة الإلكترونية، يتعين تحديث التشريعات القانونية بشكل دوري لتواكب أحدث التوجهات والأساليب المستخدمة في ارتكاب الجرائم عبر الإنترنت. يجب أن تشمل التعديلات القانونية تعزيز الآليات القانونية المتعلقة بالتحقيق والمقاضاة في الجرائم الرقمية، وضمان حماية حقوق الأفراد في البيئة الإلكترونية.

4- تعزيز التعاون الدولي في مكافحة الجريمة السيبرانية: بالنظر إلى الطبيعة العابرة للحدود للجرائم الإلكترونية، ينبغي تعزيز التعاون بين الدول من خلال اتفاقيات دولية ملزمة في مجال مكافحة الجريمة السيبرانية، بما في ذلك تبادل الخبرات والمعلومات وتوحيد الإجراءات القانونية لمكافحة هذه الجرائم.

5- إطلاق حملات توعية على مستوى المجتمع: من الضروري إطلاق حملات توعية مستمرة للمواطنين والشركات على حد سواء بشأن مخاطر الجرائم الإلكترونية وسبل الوقاية منها. تشمل هذه الحملات تعزيز فهم الجمهور لأهمية الحفاظ على أمن المعلومات وتدابير الحماية الرقمية.

6- إدخال برامج تدريبية متخصصة في الأمن السيبراني: يجب إنشاء برامج تدريبية مستمرة لجميع الفئات المعنية، من موظفي الجهات الحكومية والأمنية إلى المحامين والقضاة، بهدف رفع مستوى الكفاءة في التعامل مع الجرائم الإلكترونية وأدوات التحليل السيبراني.

7- إنشاء مراكز استجابة فورية لحوادث الأمن السيبراني: يجب أن يتم إنشاء مراكز استجابة فورية متخصصة في الحوادث السيبرانية على مستوى كل دولة، تقوم بتوفير الدعم الفوري والموارد التقنية للتعامل مع الهجمات الإلكترونية، بالإضافة إلى التنسيق مع الجهات الأمنية المختصة.

8- تعزيز دور القطاع الخاص في مكافحة الجرائم الإلكترونية: يجب على الجهات الحكومية والشركات الخاصة العمل سوياً لتطوير استراتيجيات مشتركة في مكافحة الجرائم الإلكترونية، بما يشمل تبادل المعلومات، تطوير حلول تكنولوجية مشتركة، وإقامة شراكات استراتيجية لتعزيز الأمان الرقمي.

في الأخير نأمل من المشرع الجزائري أن يبادر إلى استدراك النقائص والعيوب التي لحقت تقنين آليات البحث والتحري في الجرائم الالكترونية، وأن يسعى إلى تكملت أعماله المستحدثة في هذا الموضوع. ونتمنى أن نكون قد أجبنا عن الإشكالية المطروحة، ويفيد هذا البحث كل من اطلع على محتوياته، آملين أن نكون قد قدمنا الإضافة العلمية المرجوة، سائلين من الله العلي القدير التوفيق والسداد.

قائمة المصادر

والمراجع

الكتب

1) الجرجاني علي بن محمد، التعريفات: تحقيق إبراهيم الأبياري، دار الكتاب العربي، 1985.

2) الخليفي عبد الله بن محمد، الجرائم المعلوماتية: دراسة فقهية نظامية، مكتبة الرشد، الرياض، 2021.

3) القحطاني عبد الله بن عبد العزيز، الأدلة الاكترونية في الإثبات الجنائي ، دار جامعة نايف للنشر، الرياض، 2018.

4) المومني نهلا عبد القادر، الجرائم المعلوماتية، ط الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010.

5) بن عبو عبد القادر، شرح قانون الإجراءات الجزائية الجزائري، الطبعة الثانية، دار هومة، 2020.

6) خالد ممدوح إبراهيم، إجراءات التفتيش في الجرائم المعلوماتية (دراسة مقارنة)، الطبعة الأولى، دار المفكر الجامعي، 2021.

7) د. حسن صادق المرصفاوي، المرصفاوي في المحقق الجنائي، منشأة دار المعارف الإسكندرية، 1977.

8) د. سلطان الشاوي، أصول التحقيق الإجرامي، المكتبة القانونية للتوزيع، بغداد 1900.

9) د. محمد أنور عاشور، المبادئ الأساسية في التحقيق الجنائي العلمي، عالم الكتب، القاهرة، 1987.

10) د.ابراهيم محمد طاهر، تنظيم التحقيق الابتدائي في الجرائم الالكترونية، الطبعة الأولى، دار وائل للنشر، عمان، 2013.

11) د.فكري أيمن عبد الله، الجرائم امعلوماتية (دراسة مقارنة في التشريعات العربية والأجنبية)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، بلا تاريخ.

12) د.ياكر الطاهر، الجرائم الالكترونية الاحكام الموضوعية والإجرائية (دراسة مقارنة)، طبعة 2024، دار بلقيس للنشر، دار البيضاء الجزائر، 2024.

13) د.يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، سلسلة مطبوعات المخبر، مخبر أثر الاجتهاد القضائي على حركة التشريع، الطبعة الأولى. مطبعة الرمال، جانفي 2019.

14) طاهري حسين، إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية المحاكمة الالكترونية (دراسة تحليلية مقارنة مدعمة بالفقه والقضاء المقارن)، دار الولاء للطباعة والنشر الترجمة والتوزيع، أم البواقي الجزائر، 2023.

15) غانم أحمد، أمن الشبكات وأنظمة المعلومات، الطبعة الثانية، دار الفكر الجامعي، 2020.

16) يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات–قانون الإجراءات الجزائية–قوانين خاصة، دار الجامعة الجديدة، الإسكندرية، 2019.

الاطروحات والمذكرات الماجستير والماستر:

أ- الاطروحات:

1) بوحزمة نصيرة، الجنائي في الجرائم الالكترونية (دراسة مقارنة)، رسالة مقدمة لنيل شهادة دكتورة في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، سيدي بلعباس، 2021-2022.

2) ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتورة تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2015-2016.

3) محمد صلاح، محمد عبد المنعم، الجرائم الالكترونية وتحدياتها (دراسة مقارنة)، رسالة مقدمة لنيل شهادة دكتورة، كلية الحقوق، جامعة المنصورة، 2005.

ب- مذكرات الماجستير:

1) د.غش العجمي عبد الله، المشكلات العملية والقانونية للجرائم الالكترونية (دراسة مقارنة)، رسالة لاستكمال الحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.

ت- مذكرات الماستر:

1) بوديسة بجاد عبد الرؤوف. (2022-2021). آليات التحري عن الجريمة الالكترونية في القانون الجزائري. مذكرة لنيل شهادة ماستر مهني في الحقوق تخصص قانون الإعلام الآلي والانترنت. برج بوعريريج: كلية الحقوق والعلوم السياسية، جامعة محمد ابشير الابراهيمي، 2021-2022.

2) خداوي مختار، إجراءات البحث والتحري الخاصة في التشريع الجنائي الجزائري، مذكرة تخرج لنيل شهادة ماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي، سعيدة، 2015-2016.

3) دهان فاطمة، دهان كلثوم، إجراءات البحث والتحري في الجرائم المعلوماتية، مذكرة تخرج لنيل شهادة الماستر أكاديمي، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2021-2022.

4) شكري خالد، لراشي أبوبكر، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية. مذكرة لنيل شهادة الماستر علوم في القانون، كلية الحقوق والعلوم السياسية، جامعة أمحمد بوقرة، بومرداس، 2022-2023.

5) عبد العزيز أحمد، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة ماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي، 2021-2022.

6) عزوق عبد اللطيف، دور الشرطة العلمية في مكافحة الجريمة الالكترونية، مذكرة مقدمة لنيل شهادة ماستر أكاديمي تخصص إعلام آلي و الانترنت، كلية الحقوق والعلوم السياسية بودواو، جامعة أمحمد بوقرة، بومرداس، 2022-2023.

7) غرباوي نادية، أساليب البحث والتحري في الجرائم المعلوماتية مذكرة مقدمة لنيل شهادة الماستر،كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، 2016-2017.

8) يومايلة ابتسام، مناهج التحقيق الجنائي في ظل تفشي الجريمة الرقمية، مذكرة مقدمة لنيل شهادة ماستر أكاديمي تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، 2020-2021.

المجلات العلمية:

1) التجاني زليخة، المراقبة كإجراء للبحث والتحري عن الجرائم، مجلة أبحاث قانونية وسياسية، المجلد 07، العدد 1، جوان 2022.

2) الحمادي محمد، المساهمة والتحريض على الإرهاب الالكتروني عبر وسائل التواصل الالكتروني في القانون الإماراتي، مجلة البحوث القانونية والاقتصادية، العدد 04، 2023.

3) السيد عطية شحاتة، تعرض المراهقين للجرائم الالكترونية عبر وسائل الإعلام الرقمي و تأثيرها، *مجلة كلية الإعلام*، 2019.

4) الطاهر ياكر، مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، المجلد 4 العدد 4، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، 2022.

5) العنزي زينب طرفي، الجريمة الالكترونية في ميزان الفقه والقانون، مجلة الدراسات الإسلامية والبحوث الاكاديمية، العدد 99، 2022.

6) آيت حمودة كاهنة، البحث والتحري الجنائي في مسرح الجريمة الالكترونية، مجلة الفكر القانوني والسياسي، المجلد07، العدد1، 2023.

7) بندر عقاب جفين حطاب الدويش، خصائص وأنواع الدليل الالكتروني في الكويت ودول المقارنة، المجلة القانونية علمية محكمة، المجلد 16 العدد 3، كلية الحقوق، جامعة عين شمس، مايو 2023.

8) بوزيرة سهيلة، الهيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: بين المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد02، 2022.

9) بومحراث ليندة، علمي مخلوف، ضوابط التفتيش في الجرائم الالكترونية، مجلة المعيار، المجلد28، العدد1، 2024.

10) حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم 20-05، مجلة الحقوق والعلوم الانسانية، المجلد13، العدد03، أكتوبر 2020.

11) حفصاوي كمال، مخلوف عمر، التفتيش الالكتروني بين ضرورة بين ضرورة التحقيق والحق في سرية المراسلات والاتصالات، مجلة الباحث للدراسات الأكاديمية، المجلد11، العدد01، 2024.

12) حيمر فتيحة، تأثير الجريمة الالكترونية على الأمن في افريقيا، مجلة أبحاث قانونية وسياسية، المجلد 09، العدد01، جوان 2024.

13) خمز خضري، عشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، جوان 2018.

14) د.الشريجي عادل محمد، د.قابوسة علي، د.المايل عبد السلام، الجريمة الالكترونية في الفضاء الالكتروني: المفهوم-الأسباب-سبل المكافحة مع التعرض لحالة ليبيا، مجلة أفاق للبحوث والدراسات سداسية، دولية محكمة، 04 جوان 2019.

15) د.بهلول سمية، د.دمان ذبيح عماد، الاليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، العدد، 13 جانفي 2020.

16) د.دمان ذبيح عماد، د.بهلول سمية، الاليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، العدد، مجلة الحقوق والعلوم السياسية، 13 جانفي 2020.

17) د. رامي متولي القاضي، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون (175) لسنة 2018م مقارنا بالمواثيق الدولية والتشريعات المقارنة، مجلة البحوث القانونية والاقتصادية، العدد 25، مارس 2021.

18) د.عادل محمد الشريجي، د.ع السلام محمد المايل، د.علي قابوسة. (بلا تاريخ). الجريمة الالكترونية في الفضاء الالكتروني المفهوم-الأسباب-سبل المكافحة مع التعرض لحالة ليبيا. مجلة أفاق للبحوث والدراسات سداسية، دولية محكمة.

19) رحموني محمد، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة العدد 41، جانفي 2018.

20) زخمي الطاهر، الجرائم المعلوماتية في التشريع الجزائري وتدابير الوقاية منها، مجلة التشريع الإعلامي، المجلد 02 العدد 01، 2023.

21) شرف الدين وردة، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة المفكر، العدد15، جوان 2017.

22) صغير يوسف، التفتيش كآلية لإثبات جرائم نظم المعلوماتية، المجلة النقدية للقانون والعلوم السياسية، المجلد17، العدد04، 2021.

23) ط.د.فلاح عبد القادر، د.أيت عبد المالك نادية، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد 04، العدد02، 2019.

24) طالة لامية، سلام كهينة. (2020). الجريمة الالكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي. مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد 06 العدد 02، جامعة الجزائر 3، 2020.

25) عباس غنية، الجريمة الالكترونية في البيئة الرقمية ومدى تأثيرها على الجريمة المنظمة العابرة للحدود الوطنية، المجلة الجزائرية للسياسات العامة، المجلد 12 العدد 03، جامعة لونيسي على البليدة، ديسمبر2024.

26) عكوش حنان، خصوصية الدليل الالكتروني، مجلة الفكر القانوني والسياسي، المجلد السابع العدد الأول، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي الاغواط، 2023.

27) قويدر مريم، إشكالية العوالم الافتراضية المظلمة على شبكة الانترنت، قراءة إعلامية نقدية للجرائم السبيرانية الفكرية والثقافية على شبكة الويب العالمية، مجلة الرسالة للدراسات والبحوث الانسانية، الجلد 09 العدد 02، جوان 2024.

28) قويدر مريم، إشكالية العوالم الافتراضية المظلمة على شبكة الانترنت، قراءة إعلامية نقدية للجرائم السبيرانية الفكرية والثقافية على شبكة الويب العالمية، مجلة الرسالة للدراسات والبحوث الانسانية، الجلد 09 العدد 02، جوان 2024.

29) مرنيز فاطمة، التفتيش الافتراضي كإجراء استدلالي في ضوء القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها (دراسة مقارنة)، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 10، العدد02، 2021.

30) محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، بدون اسم المجلة، كلية الحقوق والآداب والعلوم الاجتماعية، جامعة 08 ماي 45 قالمة.

31) معاشي سميرة، الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية. مجلة المفكر، العدد 17، جوان 2018.

القوانين والمراسيم

أ- القوانين الوطنية:

1) القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-155 المؤرخ في 8يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج ر ج العدد 84 المؤرخ في 24 ديسمبر 2006.
2) القانون رقم 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
3) المرسوم الرئاسي رقم 04-183 المؤرخ في 26 جوان 2004، المتضمن إنشاء الهيئة الوطنية، ج ر ج، العدد 41، المؤرخ في 30 جوان 2004.
4) المرسوم الرئاسي 172/19 المؤرخ في 03 شوال 1440 الموافق ل/ 06 يونيو 2019 الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها.
5) المرسوم الرئاسي 05-20 المؤرخ في 24 جمادى الأول عام 1441 الموافق لـ 20 جانفي 2020 يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر ج، العدد 04 المؤرخة في 26 جانفي 2020.

ب- القوانين الدولية:

1) الطهير الشريف، بتنفيذ القانون رقم 07-03 المتعلق بإحداث جرائم متعلقة بنظم المعالجة الآلية للمعطيات، لاسيما المواد من 3-607 إلى 10-607 من مجموعة القانون الجنائي المغربي.
2) قانون 175 لسنة 2018، في شأن مكافحة جرائم تقنية المعلومات، ج ر، العدد 32 مكرر (ج) في 14 أغسطس سنة 2018.

التقارير:

1) جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، إدارة الشؤون القانونية، القاهرة، 2015.
2) د.مجيد خضر السبعاوي، أ. مولان قادر أحمد، الضرورة الإجرائية في مرحلة التحقيق الابتدائي (دراسة تحليلية مقارنة)، المركز القومي للإصدارات القانونية، القاهرة، 2017.
3) سويسي فتيحة، التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها، مداخلة مقدمة خلال الندوة البحثية، مركز البحوث القانونية والقضائية، 18 جانفي 2022.
4) الرويلي ماجد بن عبد الله، التحقيق الجنائي في الجرائم المعلوماتية (دراسة مقارنة)، المركز العربي للبحوث القانونية، الرياض، 2021.

5) الحادثة موثقة ضمن تقارير الأمن السيبراني الصادرة عن وزارة الدفاع الأمريكية لعام 1996. وقد أوردتها صحيفة The Washington Post بتاريخ 18 فبراير 1996، بعنوان: " Hackers Break Into Pentagon Computer System" (المصدر: The Washington Post Archives, 1996).

6) المديرية العامة للأمن الوطني، التقرير السنوي لنشاطات الشرطة العلمية ومكافحة الجريمة الالكترونية، الجزائر، 2023.

7) الهيئة الوطنية للأمن السيبراني ومهامها في حماية الفضاء الرقمي." الجريدة الرسمية للدولة، العدد 45، 2023.

ملتقيات:

1) د.محمودي رقية، د.قدوح نور الهدى، الجرائم الالكترونية في المجتمع الجزائري، أعمال الملتقى الوطني الافتراضي، فرقة مشروع البحث التكويني الجامعي P.R.F.U، 15 مارس 2022.

محاضرات:

1) د. بن دراح على إبراهيم، مطبوعة بيداغوجية بعنوان: محاضرات في الجرائم المعلوماتية، طلبة السنة الثانية ماستر، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، 2020-2021.

المواقع الالكترونية:

1) الموقع الرسمي لوزارة الدفاع الوطني www.mdn.dz.
2) www-aljazeera-net.cdn.ampproject.org,28/04/2025,08:44.
3) https://news.un.org/ar/story/2024/12/1137776,03/05/2024,00:28.

المراجع باللغة الأجنبية:

1) Ali, Muhammad, et al. "Understanding Cybercrime and Youth: A Perception-Based Approach." ResearchGate, 2023.
2) Doll Barbara, Understanding IP Addresses: Everything You Ever Wanted to Know, TechNet, Microsoft, 2021.
3) United Nations Office on Drugs and Crime. Global Report on Trafficking in Persons 2020. United Nations, 2020.
4) United Nations. Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, 2000.
5) United States, Executive Office of the President. Executive Order 13010: Critical Infrastructure Protection. Federal Register, vol. 61, no. 138, 17 July 1996, pp. 37347–37350.

6) Solove, Daniel J. The Digital Person: Technology and Privacy in the Information Age. NYU Press, 2004.

فهرس

المحتويات

فهرس المحتويـــــــــات

ملخص الدراسة:

تعنى هذه الدراسة ببحث آليات التحري والاستقصاء في الجرائم الإلكترونية، من خلال معالجة شاملة تجمع بين البعد النظري والتطبيقي. في الشق النظري، تم التطرق إلى تعريف الجريمة الإلكترونية وبيان خصائصها، مع استعراض صورها المختلفة وتحليل الدوافع المتنوعة لارتكابها، سواء كانت تقنية أو اجتماعية أو نفسية. أما في الجانب التطبيقي، فقد ركزت الدراسة على الجهات المختصة بمكافحة هذا النوع من الجرائم، مبيّنةً حدود اختصاصها والمهام التي تقوم بها، لا سيما فيما يتعلق بجمع المعلومات وتتبع الأدلة الرقمية. كما تم الوقوف على الوسائل القانونية والفنية المعتمدة في إجراءات البحث والتحري، مع إبراز التحديات التي تواجه السلطات المختصة في هذا السياق، خصوصًا ما يرتبط بخصوصية البيانات الإلكترونية وحجية الأدلة الرقمية. وتخلص الدراسة إلى ضرورة تعزيز الإطار القانوني وتحديث آليات العمل بما يواكب تطور الجريمة الإلكترونية.

الكلمات المفتاحية: الجرائم الإلكترونية، محققون مختصون، الإجراءات الجنائية، الأدلة الرقمية.

This study focuses on investigating the mechanisms of investigation and inquiry in cybercrimes through a comprehensive approach that combines both theoretical and practical dimensions. In the theoretical section, the study addresses the definition of cybercrime, its characteristics, and explores its various forms, analyzing the diverse motivations behind committing such crimes, whether technical, social, or psychological. On the practical side, the study focuses on the authorities responsible for combating these types of crimes, outlining their jurisdictional limits and the tasks they perform, particularly in relation to gathering information and tracking digital evidence. The study also examines the legal and technical methods used in research and investigation procedures, highlighting the challenges faced by the relevant authorities, especially concerning the privacy of electronic data and the admissibility of digital evidence. The study concludes with the necessity of strengthening the legal framework and updating operational mechanisms to keep pace with the evolution of cybercrime.

Keywords: Cybercrimes, Specialized Investigators, Criminal Procedures, Digital Evidence.