الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف بالمسيلة

كلية : الحقوق والعلوم السياسية

قسم : الحقوق

رقم :.....

ميدان : الحقوق والعلوم السياسية

التخصص : قانون الجنائي و العلوم الجنائية

فرع : الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر

تحت عنوان

خصوصية التحقيق الجزائي في الجريمة المعلوماتية

من إعداد الطالبتين :

- شلالي إكرام
- عبد الكبير هاجر

تحت إشراف الأستاذ :

- أ . د . العيساوي حسين

مقروف محمد	جامعة المسيلة	رئيسا
د. العيساوي حسين	جامعة المسيلة	مشرفا ومقررا
بوبعاية كمال	جامعة المسيلة	ممتحنا

السنة الجامعية: 2024 – 2025م

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

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): تلايلي اكرام الصفة: طالب، أستاذ، باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم 210653321 والصادرة بتاريخ 2024/06/23

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

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

عنوانها: خصوصية التحقيق الجنائي في الجريمة المعلوماتية

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

التاريخ: .....

توقيع المعني (ة)

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

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): عبد الكبير هاجر الصفة: طالب، أستاذ، باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم 108123542 والصادرة بتاريخ 2022/07/24

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

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

عنوانها: خصوصية التحقيق الجنائي في الجريمة المعلوماتية.

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

التاريخ: .....

توقيع المعني (ة)

بسم الله الرحمن الرحيم

شُكرٌ وعِرفان

بسم الله الرحمن الرحيم

﴿ وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ ﴾

وصلاةً طيّبةً مباركة، تُعطر الأرواح وتُضيء القلوب، على من أُرسل رحمةً للعالمين، سيدنا محمدٍ ﷺ، صاحب الخُلق العظيم، وعلى آله وصحبه ومن سار على دربه إلى يوم الدين.

في لحظةٍ امتزج فيها الحُلمُ بالواقع، واكتملت فيها ثمرةُ الجدّ والاجتهاد، لا يسعني إلا أن أقف وقفةَ امتنانٍ صادقة، مُتوشّحةً بالشكر والعرفان، لكل من كان شعاع نورٍ في دربي، أو همسة دعمٍ في طريقي.

وإني لأبدأ كلمتي هذه باستقبالٍ يليق بمقامكم...

مرحبًا بكم يا من حضرتم، فأنرتم، وزيّنتم هذا اليوم البهيّ بحضوركم العاطر.

أتقدّم بجزيل الشكر وعظيم التقدير إلى مشرفي الفاضل الدكتور " عيساوي الحسين" ، الذي لم يبخل عليّ بعلمه وتوجيهه.

كما أرفع أسمى عبارات الشكر والعرفان إلى اللجنة العلمية الموقّرة، التي شرّفتني بتقييمها، وأسعدتني بحضورها الكريم.

ولا أنسى أن أُهدي شكري إلى كل من حضر وشاركني لحظة فرحي، فأنتم جزءٌ لا يتجزأ من هذه الفرحة التي لا تُنسى، أنتم بهجتها وسندها وذاكرتها الأجمل.

وتحية تقدير إلى طاقم الإدارة والكلية، على ما قدموه من تسهيلات ودعم طوال مسيرتي العلمية.

وكل التقدير والاحترام إلى أساتذتي الأجلاء، الذين غرسوا في نفسي بذور الطموح، وسقوها بعلمهم وتوجيههم.

وإلى كل شخصٍ آمن بي، دعمني، وساندني من قريب أو بعيد، أقول من أعماق القلب:

"من لا يشكر الناس لا يشكر الله"، فشكرًا لكم جميعًا، فبكم بعد الله تحققت الإنجازات، وبكم كان للأمل معنى.

جزاكم الله عني خير الجزاء، ورفع قدركم في الدنيا والآخرة.

هاجر إكرام

إهداء

بسم الله الرحمن الرحيم

﴿رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ﴾

وآخِرُ دعوانا أن الحمد لله ربّ العالمين، ما سلكنا هذا الطريق ولا بلغنا هذه الغاية إلا بتوفيق الله وعونه، قال تعالى:

﴿وَمَا بِكُم مِّن نِّعْمَةٍ فَمِنَ اللَّهِ﴾

فالحمد لله على ما أنعم، وله الشكر على ما وفّق، وأسأله أن يتمّ نعمته عليّ، ويجعل هذا التخرّج فاتحة خير ونور وعلم نافع.

اما بعد...

أهدي بكل حب وامتنان ثمرة تخرّجي، إلى من كانوا لي نورًا وركيزة في كل خطوة والدي العزيزين، إلى من كانا السبب -بعد الله- فيما أنا عليه اليوم، إلى من لولاهما ما وصلت، وما بلغت، وما ارتفعت، وجودكما سر دعمي، وصبركما قوتي، ودعاؤكما سلاحي.

إلى والدي العزيز

إلى من وهبني وقته وجهده واهتمامه بلا تعب، ودعمني بلا حدود... كنتَ لي النور الذي ينير دربي، والعطاء الذي لا ينتهي، جسّدتَ في أفعالك أصدق معاني التضحية، وعلّمتني أن الدنيا ميدان كفاح، وأن العلم والمعرفة هما سلاحي، زرعت في روحي مكارم الأخلاق، وكنت قدوتي في كل خُلق نبيل، رافقتَ مسيرتي خطوة بخطوة، فكنتَ بعد الله ركيزة المشوار، وسندي، وضلعي الثابت الذي لا ينكسر، أستلهم منك الإصرار والعزيمة...

فأنا أُباهي بك العالم كله، لأنك أبي، فخري، واعتزازي، الذي أرفع به رأسي عاليًا، يا أعظم رجل في حياتي، يا من سيظل اسمه محفورًا في كل نجاح أحققه، وكل حلم أبلغه...

وإلى أمي الحبيبة،

يا وطن الدفء، والحضن الذي لا يميل...

قال تعالى: ﴿وَوَصَّيْنَا الْإِنسَانَ بِوَالِدَيْهِ إِحْسَانًا﴾

وأنتِ خير مثال لتلك الوصية، وأسمى درجات البر. أنتِ اليد الحنونة التي تمسح على قلبي كلما تعثرت، والدعاء الذي لا ينقطع، والقلب الذي لا يتغيّر... يا من احتواني قلبكِ قبل حضنك، قال الحبيب ﷺ: "الجنة تحت أقدام الأمهات". وأنتِ جنتي في هذه الدنيا، وأعظم نعم الله عليّ.

هذا التتويج، وهذا النجاح، لا أقدّمه لنفسي فقط، بل هو لكما، هو ثمرة تعبكما، وسهركما، وصبركما. فشكرًا... لا تكفي، ودعائي لكما لا ينقطع، رفع الله قدركما كما رفعتماني، وبارك الله في أعماركما كما باركتما في طريقي.

إلى أخي وأخواتي

إلى من شُدّ بهم عضدي فاستقام الطريق، إلى من كانوا عمادًا لقلبي، والكتف الذي لا يميل، والنبض الذي لا يخون... منكم تعلّمت أن العائلة لا تُعوّض، وأن الأخوّة سندٌ لا يصدأ، وقد صدق قوله تعالى: ﴿سَنَشُدُّ عَضُدَكَ بِأَخِيكَ﴾. وأنتم، والله، الشدّة التي لا تلين، والدعم الذي لا يخفت. رزقكم الله سعادةً دائمة، وفرحةً لا تنطفئ.

إلى صديقاتي الغاليات،

اللائي كنّ لي عونًا في مشواري، ومدَدْنَ لي يد المساعدة كلّما احتجتُ، علّمتني أن الأُنس لا يُقاس بعدد اللقاءات، بل بصدق القلوب، وفي صحبتكنّ إستشعرت روح الآية:

﴿وَتَعَاوَنُوا عَلَى الْبِرِّ وَالتَّقْوَىٰ﴾

فجزاكنّ الله عني خير الجزاء، ورفع قدركنّ كما كنتنّ دائمًا مصدر الدعم والثبات في طريقي.

وختامًا...

الشكر موصول لنفسي الطموحة، على الصبر، والثبات، والإصرار.

الحمد لله من قبل ومن بعد،

راجية من الله تعالى أن يكون هذا التخرج بداية لطريق أعظم، وأن يبارك في علمي، وينفعني بما علمني، ويعلمني ما ينفعني، ويجعله حجة لي لا علي.

إكرام

إهداء

إلى نفسي...

شكرًا لكل لحظة صبرتِ فيها، لكل مرة نهضتِ رغم التعب، ولكل حلم تمسّكتِ به رغم كل شيء. هذا الإنجاز ثمرة جهدك وإيمانك.

إلى أمي الغالية

يا من كنتِ الدعاء الذي لا يخيب، والسند الذي لا يميل... لولاكِ لما وصلتُ إلى هنا. شكرًا على حُبك ودعمك ووجودك الدائم.

إلى أبي العزيز

دعاؤك ومساندتك كانت النور الذي أنار طريقي... شكرًا لأنك كنت القوة التي دفعتني للأمام دائمًا.

إلى إخوتي الأحبّة

كنتم الدفء في لحظات البرد، والضحكة وقت التعب... أنتم جزء من هذا الإنجاز.

إلى صديقاتي الغاليات

كنتنّ الزهر الذي زاد أيامي جمالًا... شكرًا لكل لحظة فرح، وكل كلمة دعم، وكل تواجد صادق.

وإلى كل من ساعدني، من قريب أو بعيد...

لكم مني كل التقدير والامتنان، فقد تركتم بصمة في قلبي وفي طريق نجاحي.

هاجر

قـــائمة الـــمختصـــرات:

- ق إ م وإ ج: قانون الإجراءات المدنية والإدارية الجزائري.

- ق إ ج ج: قانون الإجراءات الجزائية الجزائري.

- ج ر ج ج: الجريدة الرسمية للجمهورية الجزائرية.

- ق ع ج: قانون العقوبات الجزائري.

- ف: الفقرة,

- ط: الطبعة.

مـــقـدمـــة

مقدمــة:

في ظل الثورة الرقمية المتسارعة، أصبحت تكنولوجيا المعلومات أداة أساسية في مختلف مجالات الحياة اليومية، غير أن هذا التطور أفرز في المقابل تحديات أمنية وقانونية جسيمة، من أبرزها الجرائم المعلوماتية، التي باتت تمثل خطرًا حقيقيًا على الأمن الوطني، الاقتصادي، والاجتماعي، سواءً في الجزائر أو على الصعيد الدولي. وتشمل هذه الجرائم أفعالًا غير مشروعة مثل اختراق نظم المعلومات، الوصول غير المشروع إلى البيانات، تزوير المحتوى الرقمي، واستغلال الفضاء السيبراني في أغراض إجرامية.

ونظرًا لطابعها غير المادي، وسرعة تنفيذها، وتعقيد وسائلها، تستلزم هذه الجرائم مقاربة قانونية دقيقة تختلف عن الجرائم التقليدية، خصوصًا على مستوى التحقيق وجمع الأدلة الرقمية.

واستجابة لهذه المتغيرات، عمل المشرع الجزائري على تطوير منظومته التشريعية من خلال تعديل قانون العقوبات وقانون الإجراءات الجزائية، وإصدار قوانين خاصة، أبرزها:

- **القانون رقم 06-22** المؤرخ في 2006 يعدل ويتمم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية الجزائري، ويوسع صلاحيات التحقيق في الجرائم الرقمية، خاصة فيما يتعلق بتفتيش الأجهزة الإلكترونية وضبط الأدلة.
- **المرسوم التنفيذي رقم 06-348** المؤرخ في 2006 يحدد إجراءات التفتيش وضبط الأدلة الرقمية في الجرائم المعلوماتية، ويمنح اختصاصًا إقليميًا موسعًا لبعض الجهات القضائية لمتابعة الجرائم السيبرانية.
- **القانون رقم 09-04** المؤرخ في 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وينظم الإطار القانوني للتوقيع الإلكتروني والمعاملات عبر الوسائط الرقمية.

- **القانون رقم 18-07** المؤرخ في 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ويعزز الإطار القانوني لمواجهة الاحتيال الإلكتروني وحماية البيانات الشخصية.
- **المرسوم الرئاسي رقم 20-05** المؤرخ في 2020 يضع الإطار الوطني لأمن الأنظمة المعلوماتية لتأمين البنية التحتية الرقمية، ويتضمن إنشاء منظومة وطنية لأمن الأنظمة المعلوماتية.
- **المرسوم الرئاسي رقم 20-183** المؤرخ في 2020 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ويحدد تشكيلتها ومهامها.
- **القانون رقم 24-06** المؤرخ في 2024 يعدل ويتمم الأمر رقم 66-156 المتضمن قانون العقوبات، ويفرض رقابة أشد على الجرائم الإلكترونية، خصوصًا ما يتعلق بالقرصنة، التجسس الإلكتروني، واستغلال الأطفال عبر الإنترنت. كما يضع هذا القانون آليات دقيقة لحفظ الأدلة الرقمية واعتمادها قانونيًا، مع تشديد العقوبات في حالات المساس بالأمن القومي.

كما تم إنشاء هيئات ومصالح مختصة لمكافحة هذا النوع من الجرائم، من بينها: الفرقة الوطنية لمكافحة الجرائم المعلوماتية التابعة للدرك الوطني، الوحدة المركزية للتحريات في الجرائم السيبرانية التابعة للأمن الوطني، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي والوكالة الوطنية لأمن نظم المعلومات.

ورغم هذه المجهودات، لا تزال التحقيقات في مجال الجريمة المعلوماتية تواجه عدة صعوبات، منها تعقيد الأساليب الإجرامية، الطابع العابر للحدود، وصعوبة تتبع الجناة وإثبات الفعل الجرمي رقميًا.

إن خصوصية هذا النوع من الجرائم تستوجب التوفيق بين فعالية التحقيق من جهة، وحماية حقوق الإنسان والحريات الدستورية من جهة أخرى، وهو ما يجعل من دراسة خصوصية التحقيق الجزائي في الجرائم المعلوماتية أمرًا ضروريًا لفهم مدى جاهزية المنظومة القانونية الجزائرية في مواجهة هذه التحديات، وفعالية الأدلة الرقمية، ومشروعيتها أمام القضاء.

أهـمية الموضوع:

تنبع أهمية موضوع "التحقيق الجزائي في الجريمة المعلوماتية" من كونه يتناول إحدى أبرز الإشكاليات القانونية المعاصرة التي فرضها التطور الرقمي المتسارع، حيث أصبحت الجريمة المعلوماتية من بين أخطر التهديدات التي تواجه الأفراد والمجتمعات والدول، لما تتسم به من خصائص فنية معقدة، وطابع لا مادي، وعابر للحدود، فضلًا عن صعوبة تتبع مرتكبيها أو تحديد هوياتهم بدقة.

وفي هذا الإطار، يكتسي التحقيق الجزائي أهمية بالغة باعتباره المرحلة المركزية في التعامل مع هذه الجرائم، فهو الأداة التي من خلالها يتم جمع الأدلة الرقمية وتحليلها وفق قواعد قانونية دقيقة، تمهيدًا لإثبات الجريمة وتحديد المسؤوليات. غير أن خصوصية الجرائم المعلوماتية تفرض تحديات متعددة أمام جهات التحقيق، سواءً من حيث طبيعة الجريمة نفسها، أو خصائص الأدلة الرقمية، أو محدودية وسائل التحقيق التقليدية في مواجهتها.

من هنا، تهدف هذه الدراسة إلى تحليل الإطار القانوني والإجرائي المنظم للتحقيق في هذا النوع من الجرائم، وبيان ما إذا كانت آليات قاضي التحقيق والضبطية القضائية كافية للتصدي لهذه التحديات، إلى جانب رصد الصعوبات التقنية والقانونية المرتبطة بجمع الأدلة وقبولها أمام القضاء.

كما تكمن أهمية الموضوع في كونه يلامس واقعًا قانونيًا متغيرًا، ويطرح إشكالات حديثة في الفقه الجزائي الجزائري، مما يسهم في إثراء النقاش الأكاديمي وتقديم مقترحات عملية لتطوير

التشريعات الوطنية، بما يضمن تحقيق التوازن بين فعالية التحقيق وحماية الحقوق الرقمية في البيئة المعلوماتية.

أسباب اختـيار الموضـوع:

يرجع اختيارنا لهذا الموضوع الى ما تفرضه الجرائم المعلوماتية من تحديات حقيقية امام المنظومة التشريعية التقليدية، وذلك بسبب الطابع المستحدث والمتطور لهذه الجرائم، مما يجعل النصوص القانونية القائمة عاجزة أحياناً عن الإحاطة بها ومعالجتها بالشكل الكافي. الى جانب مجموعة من الأسباب وهي:

الأسـباب الذاتـية:

- ❖ اهتمامنا العميق بالقانون الجنائي، لا سيما في شقه المتعلق بالجرائم الحديثة التي أفرزها التطور التكنولوجي، والتي باتت تشكل تحديًا حقيقيًا للمنظومة العدلية.
- ❖ رغبتنا في التعمق أكثر في خصوصية التحقيقات في الجرائم المعلوماتية من زاوية جزائية تطبيقية، والوقوف على مدى نجاعة الآليات القانونية المعتمدة في التعامل معها.
- ❖ حرصنا على الإسهام في إثراء النقاش الأكاديمي حول الإشكالات العملية التي تواجه المحققين أثناء التعامل مع الأدلة الرقمية وضمان احترام قواعد المحاكمة العادلة.

الأسباب الموضوعية:

- ❖ التزايد المطّرد للجرائم المعلوماتية في الجزائر وتأثيرها المتنامي على الأفراد والمؤسسات وحتى على الأمن العام، ما يجعل من الضروري دراسة سبل مواجهتها قانونيًا.
- ❖ التطورات التشريعية التي شهدها القانون الجزائري، خاصة مع صدور القانون 21-11 المتعلق بمكافحة الجرائم المعلوماتية والقانون 24-06، مما يستوجب تحليل مدى فعاليتهما في مجابهة هذه الجرائم.

❖ الحاجة إلى تقييم قدرة الجهات المكلفة بالتحقيقات الرقمية على مواكبة التطورات التقنية، ومدى نجاعة الوسائل القانونية المعتمدة في إثبات الأدلة الرقمية أمام القضاء.

أهداف دراسة الموضوع:

تهدف دراستنا إلى تسليط الضوء على خصوصية التحقيق الجزائي في الجريمة المعلوماتية، من خلال تحليل الإشكالات القانونية والإجرائية التي يطرحها هذا النوع المستحدث من الجرائم في ظل التطور الرقمي المتسارع. وتتمثل الغاية الأساسية من التحقيق في الكشف عن الحقيقة وإثبات وقوع الجريمة في العالم الافتراضي، وذلك بالتعرف على الوسائل التي استخدمت في تنفيذها والظروف التي أحاطت بارتكابها. كما تهدف الدراسة إلى إبراز الأهمية المحورية للدليل الرقمي في إثبات التهمة، باعتباره الدعامة الأساسية التي يقوم عليها التحقيق المعلوماتي، خاصة في الحالات التي تكون فيها شخصية الجاني غامضة أو مجهولة بفعل استخدام تقنيات الإخفاء والتمويه الرقمي. ويسعى البحث أيضًا إلى فهم السياسة الإجرائية التي تبناها المشرع الجزائري بشأن التحقيق في الجرائم المعلوماتية، من خلال تحليل القوانين الوطنية ذات الصلة، وعلى رأسها القانون رقم 21-11 والقانون رقم 24-06، مع التركيز على الخصوصيات التي أضفاها المشرع على هذا النوع من الجرائم من حيث الإجراءات والأدلة. كما تحاول الدراسة الوصول إلى جملة من التوصيات التي من شأنها تعزيز فعالية التحقيق في الجرائم المعلوماتية، سواءً من حيث تطوير القدرات التقنية للجهات المختصة أو دعم التنسيق المحلي والدولي لمواجهة التحديات العابرة للحدود التي تفرضها هذه الجرائم.

الـدراسات الســـابقة

من بين الدراسات التي تناولت موضوع التحقيق الجنائي في الجرائم المعلوماتية، نذكر ما يلي:

- **أطروحة دكتوراة للباحث ربيعي حسين آليات البحث والتحقيق في الجرائم المعلوماتية جامعة باتنة، سنة 2016**، عالج الباحث الموضوع من خلال دراسته مدى فاعلية الآليات القانونية المستحدثة في مجال دعم أعمال البحث والتحري للكشف عن الجرائم، بينما موضوع دراستنا اقتصر على مرحلة التحقيق فقط.
- **أطروحة دكتوراه للباحثة أو مدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية جامعة محمد البشير الابراهيمي برج بوعريريج، سنة 2020-2021**، ناقشت من خلالها الباحثة ما اذا كان المشرع الجزائري قد كرس احكام قانونية تتلاءم مع خصوصية التحقيق لضمان فاعليته في مواجهة الجرائم المعلوماتية والحد من آثارها، درست الباحثة أيضا مجموعةمن الجرائم وذلك للترعف على مختلف صورها بينما تطرقنا في موضوع دراستنا الى الجانب الاجرائي المتمثل في التحقيق.
- **أطروحة دكتوراه للباحث بوقرة جمال الدين، التحقيق الجنائي في الجريمة الإلكترونية جامعة محمد بوضياف المسيلة كلية الحقوق والعلوم السياسية سنة 2024-2025**، درس فيها الجوانب الإجرائية الخاصة بمكافحة الجريمة الإلكترونية من خلال التعرف على الجهاز المكلف بالتحقيق فيها على المستويين الوطني والدولي وإبراز خصوصية الأساليب المعتمدة من خلال تحريه عن هذه الجريمة، بينما تطرقنا في موضوع دراستنا الى الجهاز المكلف بالتحقيق فيها على المستويين الوطني والدولي .

المنهجية المعـتمدة:

يعتمد البحث على عدة مناهج علمية تتكامل فيما بينها لتحليل الموضوع بشكل دقيق على:

- **المنهج الوصفي التحليلي:** يعتمد على وصف الجريمة المعلوماتية وتحليل النصوص القانونية المتعلقة بها، خاصة فيما يتعلق بإجراءات التحقيق والأدلة الرقمية.

❖ **المنهج المقارن:** تتم مقارنة التشريعات الجزائرية مع بعض الأنظمة القانونية الدولية لقياس مدى فعالية القوانين الوطنية في مواجهة الجرائم المعلوماتية

الإشكاليــة المـطروحة:

أمام خصوصية الجرائم المعلوماتية وما تطرحه من تعقيدات وإشكالات قانونية وتقنية في مرحلة التحقيق، تثار تساؤلات حول مدى استجابة التشريع الجزائري لهذه الخصوصيات، وفعالية الأدلة الرقمية في إثباتها. وبناءا على ذلك، تتمحور الإشكالية الرئيسية لهذا البحث حول:

" كيـف استطاع المشرع الجزائري التكـيف مع خصوصية التحقـيق الجزائي في الجرائم المعلوماتية، وما مدى فعـالية الأدلة الرقمية في إثبات هذه الجـرائم أمام القـضاء؟"

وللإجابة عن هذه الإشكالية، سيتم تقسيم خطة البحث إلى فصلين متكاملين، يتناول كل منهما جانبًا أساسيًا من الموضوع وهيا كالآتي:

في الفصـل الأول، نعالج الأحكام العامة للتحقيق في الجريمة المعلوماتية، من خلال تحديد الإطار المفاهيمي لها، من ناحية تعريفها قانونيًا وفقهيًا، وبيان خصائصها، وأركانها التي تبنى عليها، ثم تصنيفها وفقًا لطبيعتها.

كما يسلط الضوء على أطراف هذه الجريمة، بما في ذلك المجرم المعلوماتي بمعرفة سماته، وفئاته، ثم تحليل دوافعه، أو من جهة الضحية وما يلحق به من أذى في الفضاء الرقمي.

أما من الناحية الإجرائية، فيتناول هذا الفصل جهات التحقيق القضائية في الجريمة المعلوماتية، ويعرض اختصاصات كل من قاضي التحقيق، والضبطية القضائية.

كما يناقش الصعوبات التي تواجه التحقيق، سواءً ما تعلق بطبيعة الجريمة، أو بالجهات المتضررة، أو بجهات التحقيق.

ويسلط الضوء أيضا، على الأجهزة المختصة بالتحقيق في الجريمة المعلوماتية على المستوى الدولي والوطني.

أما **الفصـل الثانـي**، يركز على الدليل الرقمي باعتباره جوهر التحقيق في الجريمة المعلوماتية، من خلال تعريفه، وبيان خصائصه، وفروقاته بينه وبين الدليل التقليدي.

كما يتناول الفصل أساليب التحري الخاصة بالتحقيق في التشريع الجزائري سواءً الأساليب التقليدية أو الحديثة.

ويتطرق أيضًا الى التحديات التى تواجه الدليل الرقمي، من حيث الطبيعة الغير مرئية للدليل، سهولة محو أثاره أو تعديله أو تدميره، وضخامة البيانات المراد فحصها.

ويختتم بمناقشة مراحل مشروعية الدليل الرقمي أمام القضاء، من حيث مرحلتي التحريز والتحليل، وأيضاً مرحلتي العرض والقبول.

الفصل الأول: الأحكام العامة للتحقيق في الجريمة المعلوماتية.

تمـهيـــد:

مع التطور السريع في تكنولوجيا المعلومات والإتصالات، برزت الجريمة المعلوماتية كظاهرة جديدة وخطيرة، تعتمد على إستغلال الأنظمة الرقمية، والاجهزة الإلكترونية بطرق غير قانونية لتنفيذ أفعال جرمية تهدد الأفراد والمؤسسات والمجتمع ككل. ونظرًا لتعقيد هذه الجرائم وصعوبة تعقب مرتكبيها، باتت إجراءات التحقيق في الجرائم المعلوماتية تعتمد على تقنيات واساليب متقدمة تضمن كشف الفاعلين، وجمع الأدلة الرقمية بطريقة تضمن مصداقيتها أمام الجهات القضائية.

لذا اصبح من الضروري فهم طبيعة الجريمة المعلوماتية من حيث مفهومها، وخصائصها، واركانها، تصنيفاتها، وكذا اطرافها. وكذلك الاطلاع على الجهات القضائية المختصة بإجراءات التحقيق في هذه الجرائم، والصعوبات التي قد تواجه التحقيق في الجريمة المعلوماتية، مع معرفة الأجهزة المختصة بالتحقيق سواء على المستوى الدولي أو الوطني.

وفي هذا الفصل، سنقدم دراسة شاملة لهذا الموضوع إلى مبحثين:

1. المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية.
2. المبحث الثاني: الأجهزة والجهات القضائية المختصة بالتحقيق في الجريمة المعلوماتية على المستوى الدولي والوطني.

المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية.

تعد الجريمة المعلوماتية من المفاهيم الحديثة التي ظهرت نتيجة التطور التكنولوجي والإعتماد المُتزايد على الأنظمة الرقمية. ولكي نفهم طبيعة هذه الجرائم، من الضروري تحديد تعريفها بدقة، وإستعراض خصائصها، بالإضافة إلى تصنيف أنواعها، ومعرفة الأركان التي تبنى عليها الجريمة المعلوماتية، وأهم أطرافها. وذلك من خلال:

1. المطلب الأول: مفهوم الجريمة المعلوماتية.
2. المطلب الثاني: أطراف الجريمة المعلوماتية.

المطلب الأول: مفهوم الجريمة المعلوماتية.

بما أن الجريمة المعلوماتية من الجرائم الحديثة التي تجاوزت النمط التقليدي. استوجب علينا في هذا المطلب دراسة **تعريفها فقهيًا وقانونيًا**، ثم **خصائصها وأركانها**، و**تصنيفاتها المتعددة**.

الفرع الأول: تعريف الجريمة المعلوماتية.

لم يكن هناك إجماعًا على تعريف الجريمة المعلوماتية، نظرًا لما أُحيط بها من غموض وإختلاف، بسبب إرتباطها بالتطور المستمر واللامُتناهي لتكنولوجيا الإعلام والاتصال[1]. لذلك، سنحاول التفصيل في تعريفها بين الجانبين الفقهي والقانوني كما يلي:

أولاً: التعريف الفقهي للجريمة المعلوماتية: إختلف الفقهاء في تعريفها، وتعددت الإتجاهات بشأنها، فهناك من أسند التعريف على موضوع الجريمة المعلوماتية، ومنهم من أسنده على وسيلة إرتكابها، وعليه سنأخذ بعضًا من تعاريف الفقهاء حولها والمتمثلة في الآتي:

[1] عميمر عبد القادر، **التحديات القانونية لإثبات الجريمة المعلوماتية**، النشر الجامعي الجديد، الجزائر، 2021، ص: 22.

❖ عرفها الفقيه روز بلات على أنها: **"كل نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والى تحويل طريقها"**[1]

❖ ويرى الأستاذ باركار أن: **"الجريمة الإلكترونية هي كل فعل إجرامي معتمد أياً كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل"**[2].

واذا كان مفاد هذه التعريفات أن الجريمة المعلوماتية، نشاط إجرامي يستخدم فيه الحاسوب، سواءً كأداة لإرتكاب الفعل الإجرامي أو كمحل له، إلا أن عند وضع تعريفها، يجب مراعاة إعتبارات هامة، تتمثل في ما يلي:[3].

1. أن يكون التعريف مقبولا ومفهوما على المستوى العالمي.
2. أن يراعى أثناء وضع التعريف التطور السريع الذي تشهده التكنولوجيا.
3. أن يبرز التعريف دور جهاز الكمبيوتر في النشاط الإجرامي وإتمامه.

ثانياً: التعريف القانوني للجريمة المعلوماتية: لم يستخدم المشرع الجزائري مُصطلح "الجريمة المعلوماتية" بشكل مباشر، بل إعتمد مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والإتصال". وقد تم تنظيم هذه الجرائم من خلال عدة قوانين أبرزها:

1. **القانون رقم: 04-15 المتعلق بتعديل قانون العقوبات، حيث أضيف القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات.** نصت المادة 394 مكرر على تجريم الدخول أو البقاء غير المشروع في كل أو جزء من نظام المعالجة الآلية للمعطيات، أو محاولة ذلك[4]. كما جرمت المادة 394 مكرر 1 تصحيح أو بحث أو تجميع أو توفير أو

[1] الديربي عبد العال، صادق إسماعيل محمد، **الجرائم الإلكترونية**، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012، ص: 40.

[2] محمد أمين أحمد شوابكة، **جرائم الحاسب والأنترنت**، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2004، ص ـ ص: 8/9.

[3] عادل محمد أمين نائلة، **جرائم الحاسب الآلي الأقتصادية**، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2005، ص: 32.

[4] القانون رقم: 04-15 المؤرخ في: 2004/11/10، يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 1966/6/8، المتضمن قانون العقوبات، ج ر ج ج، العدد 71، الصادر في: 2004/11/10، ص: 11.

نشر أو الاتجار في معطيات مخزنة، أو معالجة، أو مرسلة عن طريق نظام معلوماتي، يمكن أن تُرتكب بها الجرائم المنصوص عليها في هذا القسم[1].

2. **القانون رقم: 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**، وقد عرفت المادة 2 منه الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية"[2]. كما عرفت نفس المادة **المنظومة المعلوماتية** بأنها: "أي نظام منفصل، أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين". و **المعطيات المعلوماتية** بأنها: "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل المنظومة المعلوماتية تؤدي وظيفتها"[3].

3. و **بموجب الأمر رقم: 21-11 المتضمن تعديل قانون الإجراءات الجزائية الجزائري، وإستحداث القطب الجزائي الوطني المتخصص في هذه الجرائم**[4]. عرف المشرع الجزائري، بموجب المادة 211 مكرر 22/ف3، الجرائم المتصلة بتكنولوجيات

[1] أنظر المادة 394 مكرر 1، المرجع السابق ، ص 12.

[2] القانون رقم: 09-04 المؤرخ في: 2009/8/5 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج ر ج ج، العدد 47، الصادر في: 2009/8/16، ص 5.

[3] أنظر المادة 2، المرجع نفسه، ص 5.

[4] الامر رقم: 21-11 المؤرخ في: 2021/08/25 المعدل و المتمم للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية الجزائري والذي بموجبه قام المشرع الجزائري باستحداث قطب جزائي وطني متخصص بمكافحة جرائم الاتصال والإعلام، المادة 211 مكرر 22 وما بعدها.

الإعلام والاتصال على أنها: "أي جريمة ترتكب أو يسهل إرتكابها باستعمال منظومة معلوماتية، أو نظام للاتصالات الإلكترونية، أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال".

من خلال ما سبق، يتضح أن المشرع الجزائري قد اعتمد تعريفات دقيقة وشاملة للجرائم الإلكترونية، مع التركيز على حماية أنظمة المعالجة الآلية للمعطيات، ومكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.

الفرع الثاني: خصائص الجريمة المعلوماتية وأركانها.

تتميز الجريمة المعلوماتية بعدة خصائص وأركان تبنى عليها سنتطرق اليها في هذا الفرع:

أولاً: خصائص الجريمة المعلوماتية: إن ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الإنترنت، جعلها تختلف عن الجرائم العادية من حيث طبيعتها، وأساليب ارتكابها. ومنه ظهرت مجموعة من الخصائص التي تميزها عن الجريمة التقليدية، مما يستدعي دراستها بشكل دقيق، ومن بين هذه الخصائص نذكر ما يلي:

1. **الجريمة المعلوماتية جريمة عابرة للحدود:** تعد جريمة عابرة للحدود لانها ترتكب عبر الأنترنت من أي مكان في العالم، وتخلف نتائجها، وقد تستهدف أفراد أو مؤسسات في دول مختلفة. مما يسبب صعوبة في تعقب الجناة قانونيًا، بسبب اختلاف القوانين بين الدول، وتعقيد التنسيق بين الجهات الأمنية الدولية. فبعد ظهور شبكات المعلومات، لم تعد هناك حدود مرئية أوملموسة تقف أمام نقل المعلومات عبر الدول المختلفة[1].
2. **الجريمة المعلوماتية صعبة الإثبات والاكتشاف:** فهي لاتترك أثرًا ماديًا ملموسًا، كما أن تحديد مكان وقوعها أو التعامل معها معقد بسبب اتساع نطاقها وضخامة البيانات[2]. وغالبا

[1] عميمر عبد القادر، المرجع السابق، ص ـ ص: 19/18.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص: 79.

ما يتم إكتشافها بالصدفة. و تعقبها يتطلب خبرة فنية عالية، وهوا مايفتقر اليه المحقق العادي للتعامل معها[1].

3. **الجريمة المعلوماتية جريمة الأذكياء:** يمتاز مرتكبو هذا النوع من الجرائم بذكاء عالٍ وقدرة على التحكم في الأجهزة الإلكترونية، مايسمح لهم بتنفيذ افعالهم بدقة واحترافية، وتحقيق أهدافهم بهدوء دون إثارة فوضى أو استعمال للعنف[2].

4. **الجريمة المعلوماتية جريمة ناعمة و سهلة الارتكاب:** لا تتطلب أي جهد عضلي أو عنف، كما هو الحال في الجرائم التقليدية، بل يكفي أن يمتلك المجرم المعلوماتي قدرة تقنية على التعامل مع جهاز الحاسوب، وتعتبر من الجرائم "النظيفة"، لانها ترتكب في صمت دون آثار مادية، بل تتمثل فقط في تغيرات رقمية داخل ذاكرة الأجهزة[3].

ثانياً: أركان الجريمة المعلوماتية:

1. **الركن الشرعي:** يقصد به وجود نص قانوني يجرم الفعل ويعاقب عليه[4]، تطبيقا لمبدأ المادة 1 من ق ع ج بقولها:"**لا جريمة ولا عقوبة أو تدابير أمن بغير قانون**"[5]. ويمنع على القاضي القياس او التوسع في تفسير النصوص الجزائية[6]. أما بالنسبة للجريمة المعلوماتية[7]، فالمشرع الجزائري أحدث في قانون العقوبات القسم السابع مكرر من الفصل الثالث، عنوان

---

[1] هشام محمد فريد رستم، **الجرائم المعلوماتية: أصول التحقيق الجنائي الفني وآليات التدريب التخصصي للمحققين**، مجلة الأمن والقانون، دبي، الامارات العربية المتحدة، العدد2، 1999، ص: 11.

[2] عميمر عبد القادر، المرجع السابق، ص: 43.

[3] سيناء عبد الله محسن، **المواجهة التشرعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية و الوطنية**، الندوة الأقليمية حول الجرائم المتصلة بالكومبيوتر، الدار البيضاء، المملكة المغربية، 2007، ص: 52.

[4] عبد الرحمان خلفي، **محاضرات في القانون الجنائي العام (دراسة مقارنة)**، دار الهدى، الجزائر، 2012، ص: 48.

[5] أنظر المادة 1 من قانون العقوبات الجزائري.

[6] اسامة أحمد مناعة وجلال محمد زغبي، **جرائم تقنية نظم المعلومات الإلكترونية**، دار النشر والتوزيع، عمان، ط3، 2014, ص: 45.

[7] أحسن بوسقيعة، **الوجيز في القانون الجزائي العام**، دار الهومة للطباعة والنشر والتوزيع، الجزائر، ط11، 2012، ص: 58.

يإسم المساس بأنظمة المعالجة الآلية للمعطيات[1]. وكذا القانون 09-04، ليؤكد المشرع الجزائري خضوعها لمبدأ الشرعية[2].

2. **الركن المادي:** يمثل المظهر الخارجي للجريمة المعلوماتية[3]، فالقاعدة انه: "**لا جريمة دون ركن مادي**" أو "**لاجريمة دون فعل**"[4]. ويشتمل فعل ونتيجة وعلاقة سببية، ولو لم تتحقق النتيجة كاملة، فيمكن أن يتحقق دون تحقق نتيجة كالتبليغ عن الجريمة قبل حدوث نتيجتها، ويتخذ في الجريمة المعلوماتية عدة صور بحسب كل فعل إيجابي مرتكب[5]، وتتمثل هذه الصور في ما يلي:

1.1. **الدخول أو البقاء في منظومة المعالجة الآلية للمعطيات أو الشروع في ذلك:** نصت المادة 394 مكرر (04-15/24-06) على نوعين من الاعتداء، وهما: الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وينطوي هذا النوع تحت ثلاثة افعال، وهي: الدخول، البقاء، والعرقلة أو التعطيل. أما النوع الثاني، فيتمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات, ويندرج تحت هذا النوع كذلك ثلاث أفعال، وهي: أفعال الإدخال، المحو، والتعديل[6].

1.2. **إدخال للمعطيات بطريق الغش:** نصت المادة 394 مكرر 1 من ذات القانون على إزالة أو تعديل المعطيات في نظام المعالجة الآلية عن طريق الغش، ومثال ذلك حالة

---

[1] أنظر قانون العقوبات الجزائري، القسم السابع مكرر من الفصل الثالث تحت عنوان المساس بالأنظمة المعالجة الآلية للمعطيات، المادة 394 مكرر الى المادة 394 مكرر 8.

[2] حمزة خضري، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، مجلة الدراسات القانونية والسياسية، الجزائر، المجلد6، العدد2، 2020، ص: 17.

[3] حمزة خضري، المرجع نفسه، ص: 174.

[4] عبد الرحمان خلفي، المرجع السابق، ص: 101.

[5] فضيلة عاقلي، **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، المؤتمر الدولي الرابع عشر الجرائم الإلكترونية، طرابلس، 2017، ص: 119.

[6] غربي جميلة، **آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماستر، تخصص قانون جنائي، قسم القانون العام، جامعة أكلي محمد أولحاج، البويرة، 2021/2020، ص: 14.

الاستخدام التعسفي لبطاقات السحب والائتمان، سواءً من صاحبها الشرعي أو عن غيره، كحالة السرقة والتزوير[1].

3. **الركن المعنوي:** يتجلى في القصد الجنائي، والذي يتحقق بتوافر إرادة بعمل غير شرعي لدى الجاني مع علمه بأن القانون يجرمه[2]. ويشمل عنصرين هما: **العلم** اي إدراك الفاعل للأمور والسلوك الإجرامي الذي يرتكبه[3]. و**الإرادة** هي اتجاه سلوك الإنسان لتحقيق النتيجة. وهو ما يظهر من خلال استعمال المشرع الجزائري لعبارات "الغش"، "العمد"، و "الإعداد للجريمة" في المواد من 394 مكرر إلى 394 مكرر 5 من ق ع ج. وبذلك تعد الجريمة المعلوماتية جريمة عمدية بإمتياز، ولا يفترض فيها عنصر الخطأ[4]. وغالبا ما تقوم على القصد الجنائي العام، لكن هذا لا يمنع ان تقوم بعض الجرائم المعلوماتية على القصد الجنائي الخاص، مثل جرائم تشويه السمعة عبر الأنترنت، وجرائم نشر الفيروسات عبر شبكة الإتصال، وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي[5].

الفرع الثالث: تصنيفات الجريمة المعلوماتية.

تتنوع تصنيفات الجريمة المعلوماتية عدة معايير معتمدة. سنتطرق إليها كما يلي:

أولاً: تصنيف الجريمة المعلوماتية حسب نوع المعطيات ومحل الجريمة: وينقسم الى:[6]

1. **الجرائم الماسة بقيمة معطيات الحاسوب:** وتشمل نوعين رئيسيين:

---

[1] امال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، دار هومة للنشر والتوزيع، الجزائر، ط3، 2007، ص: 121.

[2] أحسن بوسقيعة، **الوجيز في قانون جنائي العام**، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط11، 2014، ص: 145.

[3] علي عبد القادر القهوجي، **الحماية الجنائية لبرامج الحاسب الآلي**، دار الجامعة الجديدة، الإسكندرية، مصر، 2010، ص ـ ص: 122/120.

[4] حمزة خضري، المرجع السابق، ص: 175.

[5] بخي فاطمة الزهراء، **إجراءات التحقيق في الجريمة المعلوماتية**، مذكرة ماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر, 2013/2014، ص: 36.

[6] يزيد بوحليط، **الجرائم الإلكترونية والوقاية منها في القانون الجزائري**، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2019، ص: 60.

1.1. الجرائم التي تمس المعطيات ذاتها، مثل جرائم الإتلاف والتشويه، بالفيروسات الخبيثة.

1.2. الجرائم التي تستهدف القيمة المالية لهذه المعطيات، مثل الاحتيال للحصول على أموال بطرق غير مشروعة، أو المتاجرة غير القانونية بالبيانات، أو التلاعب بالمعلومات.

2. الجرائم الماسة بالمعطيات الشخصية: تشمل هذه الجرائم التعدي على البيانات الشخصية للأفراد، كالتجسس، التنصت، أو الدخول غير المشروع للمراسلات والمعلومات الشخصية.

3. الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظامه: مثل "قرصنة البرمجيات"، والتي تعني انتهاك حقوق الشركات التي تطور برامج مختلفة، مثل برامج الكتابة، والتخزين أو تلك التي تقدم خدمات للمستخدمين. إلا أن هناك اعتداءات تقع عليها كتقليدها أو نسخها أو إعادة بيعها دون رخصة[1].

ثانياً: تصنيف الجريمة المعلوماتية تبعاً لدور الكمبيوتر في الجريمة.

يصنف هذا النوع من الجرائم حسب ما إذا كان الكومبيوتر وسيلة لإرتكاب الجريمة، مثل الاحتيال الالكتروني او سرقة البيانات، او كان هوا الهدف نفسه مثل الهجمات السيبيرانية. ومن هذا التصنيف يظهر مفهومان:

1. جرائم التخزين: تشمل الاحتفاظ ببيانات غير مشروعة أو استخدامها لأغراض إجرامية.

2. جرائم المحتوى: كجرائم القمار، جرائم المحتوى الإباحي، أوغسيل الاموال الإلكتروني[2].

ولمواجهة الجرائم المعلوماتية، وضعت العديد من الدول قوانين متخصصة، كما أبرمت إتفاقيات دولية، ابرزها "**اتفاقية بودابست لسنة 2001**"[3]، التي تهدف إلى تنسيق الجهود العالمية لمكافحة الجرائم المعلوماتية، وقد جاء في هذه الاتفاقية ما يلي:[4]

---

[1] يزيد بوحليط ، المرجع السابق، ص 62.

[2] المرجع نفسه، ص: 64.

[3] اتفاقية بودابست، المتعلقة بالجريمة السيبيرانية، المؤرخة في: 2001/11/23.

[4] يوسف حسين يوسف، **الجريمة الدولية للأنترنت**، المركز القومي للإصدارات القانونية، القاهرة، مصر، ط1، 2001, ص 37.

1. الجرائم المرتبطة بالكمبيوتر كالتزوير المعلوماتي والتي تستهدف سرية وسلامة المعطيات والنظام، من خلال الدخول غير القانوني لهذه المعطيات وتدميرها.

2. الجرائم المرتبطة بالمحتوى الإباحي، والأفعال غير الأخلاقية.

3. الجرائم المرتبطة بحق المؤلف والحقوق المجاورة مثل قرصنة البرمجيات[1].

ثالثاً: تصنيف الجرائم تبعاً لمساسها بالأشخاص والأموال.

1. **طائفة الجرائم التي تستهدف الأشخاص:** تشمل الجرائم الغير جنسية كالقتل باستخدام الكمبيوتر، السب، جرائم الإهمال، التحريض عن الانتحار، والتهديد وغيرها، وتشمل ايضا الجرائم الجنسية كالاستغلال الجنسي للقاصر، نشر صور لأشخاص في اوضاع مخلة.
2. **طائفة جرائم الاموال:** ماعدا السرقة أو الملكية المتضمنة أنشطة الإختراق، والإتلاف.
3. **جرائم الإحتيال والسرقة وخيانة الأمانة:** كالاعتداء على الأموال الإلكترونية، سواءً عن طريق التجارة الإلكترونية أو بالدخول غير المصرح به، أو ادخال بيانات أو مسح بيانات لغرض إختلاس أموال أو تحويلها[2].

المطلب الثاني: أطراف الجريمة المعلوماتية.

نستهل هذا المطلب بالتعريف **بالمجرم المعلوماتي**، ثم **ذكر دوافع الإجرام المعلوماتي** وأخيرًا **الضحية في الجريمة المعلوماتية.**

[1] عادل عزام، **سقف الحيط جرائم الذم والقدح والتحقير المرتكبة في الوسط الإلكتروني**، دار الثقافة للنشر والتوزيع، عمان، الاردن، ط1، 2001، ص: 123.

[2] محمد طارق عبد الرؤوف الخن، **جريمة الإحتيال عبر الأنترنت الأحكام الموضوعية والإجرائية**، منشورات الحلبي الحقوقية، لبنان، ط1، 2011، ص: 20.

الفرع الأول المجرم المعلوماتي.

الجريمة المعلوماتية من اخطر الجرائم الحديثة، حيث استغل بعض المجرمين هذا التقدم بشكل سلبي لارتكابهم أفعالاً غير مشروعة، ومنه أدى الى ظهور مجرمين يمتازون بتقنيات عالية وقدرة في التعامل مع مختلف الجوانب المعلوماتية، يُطلق عليهم "المجرمين المعلوماتيين".

أولاً: تعريف المجرم المعلوماتي: يسمى أيضا بالمجرم الإلكتروني أو "الهاكر"، كما يفضل بعض خبراء أمن المعلوماتية تسميته[1]، وهو مجرم يرتكب جرائم في البيئة الرقمية مثل القرصنة، التزوير، والتهديد وغيرها، يمتاز بخبرة علمية في الحاسوب وقدرة على تنفيذ افعاله الاجرامية رقميا، كاختراق الرموز السرية لتغيير المعلومات، تقليد البرامج، أو التحويل من الحسابات باستعمال الحاسوب نفسه[2]، فالجاني في الجريمة المعلوماتية شخص طبيعي ذو أهلية قانونية ليكون محلاً لتوقيع العقاب عليه، وهو أمر لا يتصور حدوثه لشخص معنوي[3]. ويختلف المجرمين المعلوماتيين عن المجرمين التقليديين، كونهم يقضون أوقات طويلة امام الحاسوب وسلاحهم ليس نارياً او اداة حادة، وانما عقل وبرامج وفيروسات لإختراق برامج جاسوسية[4].

ثانياً: سمات المجرم المعلوماتي: يتميز بعدة سمات نذكر منها:

1. يمتاز بمهارات فنية متخصصة في الإجرام المعلوماتي، كالاختراق وتغيير المعلومات، وتقليد البرامج أو تحويل الأموال، ومحترف في استخدام الوسائل التقنية والأنترنت، والقدرة على التكيف الاجتماعي[5].

---

[1] لينا محمد الأسدي، **مدى فاعلية احكام القانوم الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)**، دار الحامد للنشر والتوزيع، الأردن، ط1، 2015، ص: 29.

[2] هدى حامد قشقوش، **جرائم الحاسب الإلكتروني في التشريع المقارن**، دار النهضة العربية، القاهرة، 1992، ص: 27.

[3] عبد الله دغش العجمي، **المشكلات العلمية والقانونية للجرائم الإلكترونية (دراسة مقارنة)**، رسالة ماجستير، كلية الحقوق، القانون العام، جامعة الشرق الأوسط، عمان، الأردن، 2014، ص: 32.

[4] هبة نبيلة هروال، **جرائم الأنترنت (دراسة مقارنة)**، أطروحة دكتوراة، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013، ص: 12.

[5] فهد عبد الله العبيد العازمي، **الإجراءات الجنائية المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2016، ص: 40.

2. يمتاز بالذكاء في استخدام التكنولوجيا الحديثة، معتمدا على القوة الذهنية لا العضلية.

3. الدراية والعلم بالظروف المحاطة بالجريمة المراد تنفيذها، وإمكانية نجاحها أو فشلها[1].

4. يمتلك السلطة المباشرة او غير المباشرة على المعلومات المستهدفة، سواءً عبر الشفرات الخاصة بالدخول الى النظام، او باستخدام الأنظمة المعلوماتية وإجراء بعض التعاملات، وقد تكون هذه السلطة مزيفة، كاستخدام شفرات دخول شخص آخر[2].

ثالثاً: فئات المجرم المعلوماتي: يصنف المجرم المعلوماتي الى الفئات التالية:

1. القراصنة أو المخترقون: وهما صنفان:

1.1. الهاكر:[3] ويطلق عليهم الهواة، وهم أشخاص يتمكنون من الدخول إلى أنظمة المعلومات والشبكات والحسابات الآلية دون ترخيص رسمي، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما بهدف اكتساب الخبرة أو بدافع الفضول أو لمجرد التحدي وإثبات الذات[4].

1.2. الكراكرز(المخترقون): هم أفراد يقومون بإختراق أنظمة المعالجة الآلية للمعلومات بهدف الوصول الى البيانات المخزنة، وذلك إما لسرقتها أو التلاعب بها أو إتلافها، لكن في الغالب يكون بدافع التحدي واثبات القدرات التقنية، وقد أثبت الواقع العملي أن الهاكر يستعين بالكراكرز إذا ما صادفه أي نوع من أنواع الحماية، وغالبًا ما يكون هدفهم تحقيق الشهرة او مقابل مادي.

---

[1] نائلة عادل محمد قورة، **جرائم الحاسب الآلي الإقتصادية (دراسة نظرية وتطبيقية)**، منشورات الحلبي الحقوقية، بيروت، 2005، ص: 52.

[2] المرجع نفسه، ص: 58.

[3] عرفت إتفاقية الأمم المتحدة إساءة استعمال تكنولوجيات المعلومات لأغراض إجرامية، رقم: (63-55) المؤرخة في: 12/04/2000، الهاكر بأنه المبرمج المتفوق جدا ولكنه يستخدم جل طاقته في الاتجاه غير شرعي لمحاولة اختراق أنظمة حاسوبية بهدف إثبات قدرته أو التباهي بها أحيانا لأهداف إجرامية.

[4] موسى مطصفى محمد، **التحقيق الجنائي في الجرائم الإلكترونية**، مطابع الشرطة، القاهرة، ط1، 2009، ص: 153.

2. **فئة المحترفين:** يمتازون بالكفاءة العلمية والمهارات التقنية، مع التنظيم والتخطيط لأنشطتهم الإجرامية، وتهدف إعتداءاتهم لتحقيق كسب مالي، أو أغراض سياسية، أو تعبير عن موقف فكري أو نظري أو فلسفي[1].

3. **فئة الحاقدين:** هم فئة لا تسعى للتفوق العلمي واثبات القدرات والمهارات، ولا لتحقيق المكاسب المادية، وإنما هدفهم هو الانتقام والثأر. ويغلب على نشاطهم استخدام تقنيات زراعة الفيروسات والبرامج الضارة، وتخريب النظام، أو اتلاف كل معطياته أو جزء منها، أو تعطيل الموقع المستهدف إن كان من مواقع الانترنت[2].

الفرع الثاني: دوافع الإجرام المعلوماتي.

من أبرز الدوافع الى إرتكاب الجريمة المعلوماتية هي كالآتي:

1. **التفوق وتحقيق الشهرة:** قد يقوم بعض الأشخاص بإرتكاب الجريمة بدافع تحقيق لذة مؤقتة أو الرغبة في التحدي والتفوق، متجاهلين الأضرار التاتجة عنها، كما أن الشعور بالنقص يمكن أن يكون دافعًا لإرتكاب الجريمة المعلوماتية ليثبت من خلاله المجرم المعلوماتي أن النقص النفسي أو الفسيولوجي لا يعيقه في التفوق في مجالات اخرى[3].

2. **الدافع المادي:** هو أكثر الدوافع المؤدية الى اقتراف الجاني للجريمة المعلوماتية، ذلك أن الربح الكبير والممكن تحقيقه من خلاله يدفع المجرم المعلوماتي لتطوير نفسه ومواكبة كل ما يطرأ على التقنيات المعلوماتية، فيسعى للإختراع وتحقيق أعلى المكاسب بأقل جهد، ودون ترك أي أثر[4].

---

[1] علي عبود جعفر، **جرائم تكنولوجيات المعلومات الحديثة الواقعة على الأشخاص والحكومة**، منشورات زين الحلبية والأدبية، لبنان، ط1، 2013، ص: 116.

[2] على حسن الطوالبة، **الجرائم الإلكترونية**، مؤسسة فخراوي للدراسات والنشر، البحرين، ط1، 2008، ص: 65.

[3] عمير عبد القادر، المرجع السابق، ص: 50.

[4] وضاح محمود حسنات ونشأت مفضي المجالي، **جرائم الأنترنت**، دار المنار للنشر، عمان، 2005، ص: 30.

3. **الحصول على معلومات جديدة:** لعل من الدوافع التى تقف وراء ارتكاب الجريمة المعلوماتية حب الاطلاع والحصول على المعلومة. وهذا الدافع حالة نفسية تصاحب مرتكبي هذه الجرائم، فتدفعه لارتكابها سواءً متعمد أو غير متعمد، لكي يرضي فضوله العلمي، ويشعر بالارتياح بمجرد تحقق هدفه من خلال الوصول الى معلومة جديدة[1].

4. **الرغبة في قهر النظام المعلوماتي:** يميل مرتكبو هذه الجريمة إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة[2]، فالمجرم المعلوماتي حين يشعر بأنه تمكن من قهر النظام، يحقق نوعًا من الانتصار النفسي، فيشعر بالفرح والسرور[3].

5. **الانتقام:** يعتبر من أخطر الدوافع، ويكون غالبًا من خلال شخص يملك معلومات عن مؤسسة أو شركة كان يعمل بها، فتعرض للحرمان من بعض حقوقه المهنية أو طرد منها، فتتولد لديه رغبة في الإنتقام، فيقوم باستغلال المعلومات التي حصل عليها من خلال عمله في هذه المؤسسة ويرتكب جريمة، من خلال حذف أو تغيير معلومات، أو زرع برامج خبيثة لتعطيل النظام أو للحصول على معلومات أو اعطاؤها لخصوم المؤسسة، أو لمساومتها في ذلك، كما قد يلجأ الى التشهير بالمؤسسة أو بالأشخاص كنوع من الانتقام من تصرفاتهم[4].

لعل هذه ابرز الدوافع لارتكاب النشاط الإجرامي على نظم المعالجة الآلية للمعطيات، مع ذلك فهي ليست ثابتة، فقد نجد جريمة واحدة لها دوافع متعددة، خاصة اذا اشترك فيها أكثر من شخص أو أكثر من جهة، حيث يسعى كل منهم لتحقيق أهدافه الخاصة[5].

---

[1] صابر بحري ومنى خرموش، **أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية**، مجلة الدراسات في سيكولوجية الإنحراف، الجزائر، العدد1، 2021، ص: 49.

[2] نهلا عبد القادر مومني، المرجع السابق، ص: 91.

[3] صابر بحري ومنى خرموش، المرجع السابق، ص: 50.

[4] عميمر عبد القادر، المرجع السابق، ص: 51.

[5] سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة ماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق، جامعة لحاج لخضر، باتنة، 2013/2012، ص: 62.

الفرع الثالث: الضحية في الجريمة المعلوماتية.

بعد أن عرفنا المجرم المعلوماتي في الجريمة المعلوماتية كطرف أول وفاعل اصلي فيها، ستنطرق للطرف الثاني والمتمثل في الضحية.

أولاً: تعريف الضحية: الضحية بشكل عام هو كل شخص طبيعي أو اعتباري أصيب بخسارة أو ضرر أو بعدوان نتيجة ارتكاب جريمة، وينتج الضحية سواءً من فعل أو امتناع عن فعل[1].

أما الضحية في الجريمة المعلوماتية فهو: "كل كيان أصابه ضرر مادي أو معنوي نتيجة لاستخدام غير مشروع لتقنية المعلومات"[2].

ثانياً: تصنيف الضحية في الجريمة المعلوماتية: يصنف إلى فئتين:

1. **أشخاص طبيعيون ضحايا الجريمة المعلوماتية:** بسبب الاستخدام المتزايد للأجهزة الذكية مثل الهواتف والحواسيب، وازدياد الإقبال على الخدمات المعلوماتية، خاصة في ظل توفر الأنترنت، أصبحت عملية استهداف الأفراد بجرائم الإلكترونية أكثر سهولة. حيث يقوم المجرمين باختراق أجهزتهم أو حساباتهم الإلكترونية، مما يؤدي الى الحصول على بياناتهم الشخصية أو صورهم، وذلك من خلال ابتزاز الضحايا عن طريق التهديد بنشر صورهم مقابل الحصول على فوائد معينة متمثلة في مبالغ مالية[3].

والملاحظ أن الكثير من الضحايا لا يبلغون عن هذه الجرائم، خوفا على سمعتهم، مما يمنح الجناة فرصة الإفلات من العقاب، بل ويشجعهم على تكرار هذه الأفعال بحق ضحايا آخرين. وقد يتأخر الضحايا في بعض الأحيان في تقديم البلاغ إلا بعد تفاقم الضرر.

---

[1] موسى مصطفى محمد، المرجع السابق، ص: 158.

[2] يحيى عطوة الزنط، المرجع السابق، ص: 258.

[3] اسماعيل بن يحيى، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة دكتوراة علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم الحقوق، ابي بكر بلقايد، تلمسان، 2021/2020، ص ـ ص: 35/34.

2. **الشخص المعنوي ضحية الجريمة المعلوماتية:** تشكل الجرائم المعلوماتية خطرًا كبيرًا على الأشخاص المعنويين، ، إذ تستهدفهم هذه الجرائم أحيانًا بشكل مباشر ضمن حملة واحدة تمس قضايا حيوية، و تمس الأمن الوطني أو المصالح الاستراتيجية للدولة. ويزيد من خطورة هذه الجرائم إحجام الضحايا عن التبليغ، خوفًا من فقدان الثقة أو السمعة، خصوصًا لدى المؤسسات المالية أو المصرفية، حيث يفضل البعض التستر على الحادثة لتجنب التأثير السلبي على صورة المؤسسة أمام المنافسين، و العملاء. وغالبًا ما يكون الأشخاص المستهدفون هم العاملون في قطاعات حيوية، ما يجعل أنظمتهم المعلوماتية عرضة لمحاولات الاختراق، والتجسس، وهو ما يضع تلك الجهات في دائرة تهديدات أمنية تستدعي رفع مستويات الحماية الرقمية وتكثيف الوعي الأمني السيبراني[1].

[1] إسماعيل بن يحيى ، المرجع السابق ، ص ـ ص: 35/34.

المبحث الثاني: الجهات القضائية المختصة بالتحقيق في الجرائم المعلوماتية.

بسبب الانتشار الواسع للجرائم المعلوماتية وخطورتها، خصوصًا على الحياة الخاصة للأفراد، سعى المشرع الجزائري الى تعديل القوانين مثل قانون العقوبات الجزائري و قانون الإجراءات الجزائية الجزائري. وإنشاء هيئات قضائية متخصصة للتحقيق فيها، وتم توسيع صلاحيات هذه الجهات المكلفة بالتحري والتحقيق، مما يتيح لها الوصول إلى الدليل الرقمي وكشف هوية الجاني، ورغم هذه الجهود، ما تزال التحقيقات تواجه عدة صعوبات. ومنه، قسمنا هذا المبحث إلى مطلبين:

1. المطلب الأول: الجهات القضائية المختصة بالتحقيق في الجرائم المعلوماتية.
2. المطلب الثاني: الأجهزة المختصة بالتحقيق على المستوى الدولي والوطني.

المطلب الأول: جهات التحقيق القضائية في الجريمة المعلوماتية.

لقد نص القانون على نظام خاص للأجهزة والجهات الخاصة بالتحقيق في مختلف الجرائم، حيث تعتبر مهمة "التحقيق الإبتدائي" من اختصاص قاضي التحقيق. كما يجوز لضابط الشرطة القضائية أيضا مباشرة بعض مهام التحقيق في بعض الجرائم، وذلك وفقاً للمادة 63 من ق إ ج ج، وبالنظر الى ان الجرائم المعلوماتية تعد من الجرائم الحديثة، تم تعديل مهام الجهات المكلفة بالتحقيق وتمديد اختصاصات كل من قاضي التحقيق وضباط الشرطة القضائية بما يتناسب مع خصوصية هذه الجرائمة السيبيرانية وتعقيداتها. وهذا ما سنعرضه من

خلال هذا المطلب: اولاً **إختصاصات قاضي التحقيق.** ثم **إختصاصات ضباط الشرطة القضائية.** اخيراً **صعوبات التحقيق في الجريمة المعلوماتية.**

الفرع الأول: إختصاصات قاضي التحقيق في الجريمة المعلوماتية.

يتميز قاضي التحقيق عن غيره من الأجهزة بصلاحيات متعددة، من أبرزها الأستقلالية، عدم الخضوع للتبعية، وغيرها. ويخضع اختصاصه لمجموعة من المعايير، تتمثل في: المعيار الشخصي، والمحلي (المكاني)، والمعيار النوعي وفقاً لما يحدده القانون.

أولاً: الإختصاص الشخصي لقاضي التحقيق: يختص قاضي التحقيق في جميع الجرائم التي يرتكبها المتهمون دون تمييز بينهم، ويُطبق مبدأ الشخصية الذي له وجهان:[1] وجه إيجابي وآخر سلبي. على كل جاني أو مجني عليه، حتى ولو ارتكبت الجريمة خارج أقليم الدولة. فالوجه الإيجابي يتمثل في أن الجاني إذا كان يحمل الجنسية الجزائرية، تسري عليه قواعد الدولة، حتى وإن إرتكب الجريمة خارج إقليم الدولة. أما الوجه السلبي يتحقق عندما يكون المجني عليه مواطنًا جزائريًا، فتُطبق قوانين الدولة على الجاني الأجنبي، حتى ولو ارتكب الجريمة خارج أراضيها، ذلك لحماية رعايا الدولة. فالمشرع الجزائري نص في المواد 583 و 584 من قانون إ ج ج، على شروط في حالة الوجه الإيجابي سواء كانت الجريمة جنحة أو جناية، أما الصورة السلبية نصت عليها المادة 588 من نفس القانون، وقد أحسن المشرع الجزائري صنعًا حين إتخذ مبدأ الحماية، وجمع بين الوجهين في الجرائم المعلوماتية، سواء كانت جنحة أو جناية، مما يمنع المجرمين الإفلات من العقاب، سواء كان المجني عليه شخصًا طبيعيًا أو معنويًا[2]، وقد إستثنى المشرع من القاعدة العامة لإختصاص قاضي التحقيق الشخصي فئتين هما: الجرائم الخاصة بالعسكريين، وجرائم الأحداث المادة 61 و 62[3] من قانون حماية الطفل15-12[4].

ثانيا: الإختصاص النوعي لقاضي التحقيق: يتحدد اختصاص قاضي التحقيق النوعي وفق نوع الجريمة وطبيعتها، إن كانت جناية أو جنحة أو مخالفة، وذلك وفقًا لما نصت عليه المادة 66 من قانون إ ج ج أن: "**التحقيق الإبتدائي**"[5] وجوبي في مواد الجنايات.

---

[1] حورية خليصة، حمزة فيروز، **خصوصية التحقيق في الجريمة المعلوماتية**، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2024/2023، ص: 7.

[2] إسماعيل بن يحي، المرجع السابق، ص .ص: 80-85.

[3] القانون رقم: 15-12 المؤرخ في: 2015/7/15، المتعلق بحماية الطفل، ج ر ج ج، العدد 39، الصادر: 2015/7/19، ص: 13.

[4] سعاد أجعود، **محاضرات في مقياس الإجراءات**، قدمت لطلبة السنة الثانية ليسانس، مطبوعة بيداغوجية، الإجراءات الجزائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تبسة، 2022، ص: 56.

[5] التحقيق الابتدائي هو "مجموعة الإجراءات القانونية، المتخذة من جانب الجهات (الأشخاص، المؤسسات) المخولة بذلك بموجب القانون المتعلقة بوقائع معينة والتي تنطوي على انتهاك الحقوق الشخصية أو العامة وذلك بناءا على إخبار أو بدون شكوى وكل ذلك من أجل معرفة الجاني والقبض عليه وتقديمه للمحاكمة العادلة لنيل جزاءه لقاء فعله الإجرامي"، براهيمي محمد ظاهر، **تنظيم التحقيق الإبتدائي في الجرائم**، دار النشر، عمان، الأردن، ط1، 2013، ص: 15.

أما في مواد الجنح، فهو إختياري ما لم يكن ثمة نصوص خاصة، كما يجوز إجراؤه في مواد المخالفات إذا طالبه وكيل الجمهورية". ومن ثم، فإن قاضي التحقيق مختص بالتحقيق في كافة أنواع الجرائم، لكن يجب التفصيل ويكون التحقيق الإبتدائي وجوبيًا في الجنايات، واختياريًا في الجنح والمخالفات، واتصاله بالملف لا يكون إلا بناءً على طلب إفتتاحي من وكيل الجكهورية، ولو تعلق الأمر بإختصاصه الوجوبي، ويتمتع وكيل الجمهورية بسلطة تقديرية واسعة في هذا المجال، خصوصًا في ما يخص الجنح التي لا ينص القانون على وجوب التحقيق فيها، وكذلك المخالفات[1] هذا يخص المتهمين البالغين. أما بخصوص الأحداث، فإن قاضي التحقيق يختص وجوبيًا بالتحقيق في الجنايات يختص بها قاضي الأحداث وحده ، أما المخالفات فيكون التحقيق فيها جوازيًا، طبقًا للمادة 64 من قانون حماية الطفل 15-12[2].

ثالثا: الإختصاص المحلي لقاضي التحقيق: يتحدد الإختصاص المحلي لقاضي التحقيق، في الحالة العادية، بمكان وقوع الجريمة أو بمكان إقامة المتهم أو مكان القبض عليه، هذا ماجاء في نص المادة 40 من ق إ ج ج، "يتحدد اختصاص قاضي التحقيق محليًا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقترافها أو محل القبض على أحد هؤلاء الأشخاص حتى لوكان القبض قد حصل لسبب آخر"[3]، ولابد من التمييز من حيث مكان إرتكاب الجريمة بين الجرائم الوقتية والجرائم المستمرة، فالجرائم الوقتية يكون محلها هو المكان الذي يقع فيه فعل التنفيذ، أما الجرائم المستمرة فكل مكان يتحقق فيه الإستمرار يعد محلاً لها، وبالنسبة للجرائم التي تتكون من عدة أفعال وتم ارتكابها في أكثر من مكان، يكون الاختصاص لجميع قضاة التحقيق الذين وقعت الأفعال ضمن دائرة اختصاصهم[4].

---

[1] عبد الرحمان خلفي، **محاضرات في الإجراءات الجزائية موجهة لطلبة السنة الثانية ل.م.د.** كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2017/2016، ص: 304.

[2] القانون رقم: 15-12، المرجع السابق، ص: 13.

[3] عبد الرحمان خلفي، المرجع السابق، ص: 304.

[4] محمد حزيط، **أصول الإجراءات الجزائية في القانون الجزائري**، دار بلقيس للنشر، الجزائر، ط3، 2022، ص: 203.

1. **معيار مكان وقوع الجريمة:** وفقًا للمادة 40/ ف1 من ق إ ج ج، في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ويمتد اختصاص قاضي التحقيق محلياً إلى المحاكم ذات الاختصاص الموسع[1]، وفقا للمرسوم التنفيذي رقم 06-348، المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[2]. فقد حدد المشرع الجزائري بموجب الأمر رقم 21-11 المتمم لق قانون الإجراءات الجزائية الجزائري [3]، في المادة 211 مكرر22 الى 211 مكرر 29 على أن "ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني، ويمارس كل من وكيل الجمهورية وقاضي التحقيق ورئيس القطب صلاحياتهم في كامل التراب الوطني" فالمشرع خرج عن القاعدة العامة في ما يخص الإختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية نظرًا لخطورتها والتي قد ترتكب من عدة أشخاص وفي مختلف الأماكن والتي قد تتعدى إلى خارج إقليم الدولة[4].
2. **معيار مكان إقامة المتهم:** يُعتمد عليه عندما يتعذر تحديد مكان وقوع الجريمة. ووفقًا لمبدأ وحدة الدعوى الجنائية، ويعود الاختصاص لقاضي التحقيق المقيم بدائرة اختصاص أحد المتهمين في حالة ما إذا ارتكبت جريمة من طرف متهمين يقيمون بأماكن مختلفة، وهذا ينطبق على الجرائم المعلوماتية أيضًا، كما أن مكان إقامة المتهم في الجريمة المعلوماتية يبين من القاضي المختص الذي ينعقد له الإختصاص المحلي لتحقيق في الجريمة المرتكبة من بين قضاة التحقيق الذين يقيمون بدائرة اختصاص المتهم.

---

[1] إسماعيل بن يحي، المرجع السابق، ص . ص: 68/67.

[2] المرسوم التنفيذي رقم: 06-348 المؤرخ في: 2006/10/5، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر ج ج، العدد 63، الصادر في :2006/10/8، ص: 30.

[3] الأمر رقم: 21-11، المرجع السابق، ص: 10/8.

[4] فاطمة الزهراء عون، **الإجراءات التشريعية المستحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري – القطب الجزائي الوطني نموذجًا**، مجلة حقوق الإنسان والحريات العامة، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، المجلد7، العدد2، 2022/12/26، ص: 563.

3. **معيار مكان القبض على المتهم:** يتجسد هذا المعيار في حالة ما إذا لم يتم تحديد مكان وقوع الجريمة المعلوماتية، أو لم يكن للمتهم محل إقامة معروف فيتم تحديد الجهة المختصة بالتحقيق من خلال تحديد القاضي المختص محليا بالتحقيق في الجريمة المعلوماتية. و لا يخرج هذا الإختصاص عن نطاق أحد قضاة التحقيق بالمحاكم ذات الاختصاص الموسع، ذلك وفقاً للمادة 40 من ق قانون الإجراءات الجزائية الجزائري. أما في حالة تعدد المتهمين، فينعقد الاختصاص لأي قاضي من قضاة التحقيق المختصين بالتحقيق مع أحد المتهمين، ويعتبر مختصا أيضا مع سائر المتهمين الآخرين. وقد يثور خلاف حول تحديد من هو القاضي المختص محليًا بالتحقيق في الجريمة المعلوماتية، إذا كانت هذه الجريمة قد ارتكبت في دائرة اختصاص قاضي تحقيق، وكان محل إقامة المتهم في دائرة اختصاص قاضي تحقيق أخر، وتم إلقاء القبض على المتهم بدائرة اختصاص قاضي تحقيق ثالث، مما يؤدي إلى طرح إشكال حول من هو القاضي المختص بالتحقيق في الجريمة المعلوماتية؟. وللإجابة عن هذا التساؤل هي أن كل قاضي تحقيق يقع أحد المعايير الثلاثة (مكان ارتكاب الجريمة، محل إقامة المتهم، أو مكان القبض عليه) ضمن دائرة اختصاصه، يعد مختصا. فالأصل أنه لا توجد أفضلية لقاضي تحقيق على قاضي[1] آخر. ومن ثم، يختص في هذه الحالة القاضي الذي رفعت الدعوى بدائرة اختصاصه قبل غيره، استنادًا على مبدأ الأسبقية[2].

الفرع الثاني: إختصاص الضبطية القضائية.

تعرف الضبطية القضائية بأنها: "فئات من الموظفين أوكل لهم المشرع مهمة جمع الإستدلالات حول الجرائم ومرتكبيها تحت إدارة وإشراف النيابة العامة، وهم ليسوا أعضاء في السلطة القضائية بل هم جهاز يتبع السلطة التنفذية"[3]. كما أن المشرع خول لهم بعض إختصاصات قاضي التحقيق في حالات معينة كحالة الإنابة القضائية، بهدف تسريع الإجراءات،

[1] إسماعيل بن يحي، المرجع السابق، ص ـ ص: 60-72.

[2] المرجع نفسه، ص: 73.

[3] علي شملال، **الجديد في شرح قانون الإجراءات الجزائية**، الكتاب الأول ، الإستدلال والإتهام، دار هومة، ط3، دون سنة، ص: 14.

نظرًا لإنشغال قاضي التحقيق[1]، ونصت المادة 84 من ق قانون الإجراءات الجزائية الجزائري على توسيع اختصاص ضباط الشرطة القضائية إلى كامل التراب الوطني والتي جاء فيها مايلي: "غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يجوز تمديد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني".

أولاً: الإختصاص النوعي لضباط الشرطة القضائية: يتمتع ضباط الشرطة القضائية[2] بإختصاص نوعي **عام**، ويشمل جميع أنواع الجرائم مهما كانت جسامتها أو طبيعتها. وقد حددها المشرع في المواد 52/51/42/18/17 وغيرها من المواد في ق قانون الإجراءات الجزائية الجزائري. كما يتمتعون بإختصاص نوعي **خاص**، و هو أن الضبطية القضائية تختص نوعيًا بالبحث والتحري في الجرائم المحددة قانونًا، كما أن المشرع حدد الفئة المنوطة بهذا النوع من الاختصاص كأعوان الجمارك، مفتشو العمل... ، وهم الذين يمارسون مهام الضبطية القضائية وفقا لقوانين خاصة.

ثانيا: الإختصاص المحلي لضباط الشرطة القضائية (المكاني): يحدد اختصاصهم المحلي ضمن حدود الدائرة التي يمارسون فيها مهامهم، اعتمادًا على ثلاث معايير: "مكان وقوع الجريمة، محل إقامة المشتبه فيه، مكان إلقاء القبض عليه"، ولا يمنح أي معيار أولوية على الآخر. و أي إجراء يقوم به أفراد الضبطية القضائية خارج نطاق إختصاصهم المحلي يعد باطلاً، وهذا ما نصت عليه المادة 16/ف1 من قانون الإجراءات الجزائية الجزائري [3].

[1] إسماعيل بن يحي، المرجع السابق، ص ـ ص: 110/109.

[2] حددت المادة 15 فئات ضباط الشرطة القضائية والتي نصت أنه يتمتع بصفة ضابط الشرطة القضائية: رؤساء المجالس الشعبية البلدية، ضباط الدرك الوطني الموظفون التابعون للأسلاك الخاصة للمراقبين، ومحافظي وضباط الشرطة للأمن الوطني ...، الأمر رقم: 21-11، المرجع السابق.

[3] علي شملال، المرجع السابق، ص: 31.

إستثناءًا من القاعدة العامة، يجوز تمديد الاختصاص المحلي لهذه الفئة وذلك في حالة الإستعجال وبطلب من السلطة القضائية، وفقاً للمادة 16 من قانون الإجراءات الجزائية الجزائري ، "إلا أنه يجوز لهم في حالة الإستعجال[1] أن يباشرو مهمتهم في كافة دائرة اختصاص المجلس القضائي"، فيما نصت ف3 من نفس المادة على مايلي: "ويجوز لهم أيضا في حالة الإستعجال أن يباشروا مهمتهم في كافة الإقليم الوطني إذا طلب منهم أداء ذلك من قاضي التحقيق المختص قانونيا ويجب أن يساعدهم ضباط الشرطة القضائية الذين يمارسون وظائفهم في المجموعة السكنية المعنية".

ومنه، فإن تمديد الإختصاص لضباط الشرطة القضائية يكون إذا طلب قاضي التحقيق ذلك ويساعده ضباط الشرطة القضائية، كما أن الإختصاص المحلي الموسع لهم يشمل كافة دائرة اختصاص المجلس القضائي، وذلك في حالة الاستعجال، وحالة الضرورة، (وحالة البحث والتحري)[2]. وفقا لشروط يمكن إستخلاصها من المادة 16 قانون الإجراءات الجزائية الجزائري ، وهي:

1. أن يمارس هذا التوسع في الإختصاص المحلي تحت إدارة وإشراف وكيل الجمهورية.
2. أن يكون قد طلب منهم ذلك وكيل الجمهورية والقاضي المختص.
3. أن يتم إخطار وكيل الجمهورية الذي تم الإنتقال إلى دائرة اختصاصه وكذا ضابط الشرطة القضائية المختص محليا[3].

كما نصت المادة 16/ ف7 قانون الإجراءات الجزائية الجزائري ، "أنه في جرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم

---

[1] يقصد بحالة الاستعجال:**"تلك الحالة التي تتطلب السرعة في اتخاذ إجراءات الضرورية قبل ضياع الآثار ومعالجتها"**، محمد حزيط، المرجع السابق، ص: 142.

[2] محمد حزيط، المرجع نفسه، ص: 142.

[3] الأمر رقم: 21-11، المرجع السابق.

تبيض الأموال، والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد إختصاص ضابط الشرطة القضائية بالبحث والمعاينة إلى كامل التراب الوطني".

بالإضافة إلى ذلك، أن الاختصاص المحلي لضباط الشرطة القضائية التابعين لمصالح الأمن العسكري، يمتد أساسًا إلى كافة الإقليم الوطني في جميع الأحوال. كما نصت المادة 24 مكرر 1/ف3 من القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته، المعدل والمتمم، على إمتداد الاختصاص المحلي إلى كامل التراب الوطني بالنسبة لضباط الشرطة القضائية التابعين للديوان المركزي لقمع الفساد، أما بخصوص الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المنصوص عليها في قانون العقوبات من المواد 394 مكرر إلى 394 مكرر 7، بالإضافة إلى النصوص الأخرى ذات الصلة، والنصوص المتعلقة بالوقاية من الجرائم المعلوماتية ومكافحتها، لاسيما القانون رقم 09-04، والنصوص التنظيمية الصادرة قصد تطبيق أحكامه، وخاصة المرسوم الرئاسي رقم 15-261، فإن ضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، يمارسون مهامهم على كامل التراب الوطني[1]. و من خلال هذا التوسع في الاختصاص، يتجنب المشرع الجزائري إنشاء هيئات قضائية جديدة، سواء كان التمديد يشمل الاختصاص المحلي أو النوعي في مواد معينة، مفضلًا الإعتماد على الجانب البشري المتمثل في القضاة، وهوا ما أدى إلى إنشاء القطب الجزائي المختصص بمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال[2]. والملاحظ أن المشرع الجزائري لم يعرف هذا القطب[3]، واكتفى بذكر مفهوم الأقطاب الجزائية المتخصصة، وتُعرف بانها: جهات قضائية متخصصة للنظر في بعض الجرائم التي حددها القانون، وليست جهات

[1] محمد بكرار شوش، **الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري**، دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، العدد 14، 2016، ص ـ ص: 319/317.

[2] إسمهان بوضياف، **الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 14، سبتمبر 2018، ص ـ ص: 371/370.

[3] بوقرة جمال الدين، عنان جمال الدين، **القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال**، مجلة الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 7، العدد 1، جوان 2022، ص: 1676.

قضائية خاصة تنشط بإجراءات قانونية خاصة تخرج عن نطاق النظام الساري المفعول[1]، إذ يخضع لنفس القواعد القانونية الجزائية المعتمدة لدى الجهات القضائية العادية، ويُعد محكمة ذات اختصاص إقليمي موسع، حيث يمارس اختصاصه العادي إلى جانب الإختصاص الموسع الذي منحه له القانون في مجموعة من الجرائم المحددة حصرًا[2]. وقد أنشئت بموجب القانون العضوي 05-11 المؤرخ في 2005/07/17 المتعلق بالتنظيم القضائي الجزائري، وتم إصداره رسميًا بموجب القانون 04-14 المؤرخ في 2004/11/10، المعدل والمتمم لق إ ج ج[3]، وتجدر الإشارة الى أن هذا القطب الجزائي المتخصص يوجد حاليًا **في الجزائر العاصمة فقط.**

الفرع الثالث: صعوبات التحقيق في الجريمة المعلوماتية.

يُعد التحقيق في الجريمة المعلوماتية أمرًا معقدًا، ومن أبرز هذه الصعوبات: عوائق مرتبطة بطبيعة الجريمة, وأخرى بالجهات المتضررة, وثالثة بجهات التحقيق.

اولاً: عوائق تتعلق بالجريمة المعلوماتية: من المعوقات المتعلقة بالجريمة المعلوماتية:

1. خفاء الجريمة، وغياب الدليل المرئي، وإفتقارها للآثار مقارنة بالجريمة التقليدية[4].
2. إعاقة الوصول الى الدليل الرقمي بسبب وسائل الحماية الفنية كإستخدام كلمات السر على المواقع، مع سهولة محوه أو تدميره في وقت قصير جداً[5].

ثانياً: عوائق تتعلق بالجهات المتضررة: وذلك راجع للأسباب التالية:

1. تعمُد أغلب الشركات والأشخاص التستر على الجريمة المعلوماتية، وعدم الابلاغ عليها مما يؤدي الى عدم التعاون مع السلطات المختصة لمكافحتها.

---

[1] وقرة جمال الدين، جمال الدين عنان، المرجع السابق، ص: 1676.

[2] نورة بن بوعبد الله، **الاختصاص القضائي الموسع في المادة الجزائية وفق القانون الجزائري**، مجلة الفكر القانوني والسياسي، الجامعة الحاج لخضر، باتنة1، المجلد 6، العدد 1، 2022، ص . ص: 970/969.

[3] نورة بو عبد الله، المرجع السابق، ص ـ ص: 971/970.

[4] يوسف جفال، **التحقيق في الجريمة الإلكترونية**، مذكرة ماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2017/2016، ص: 41.

[5] خالد ممدوح إبراهيم، المرجع السابق، ص: 65.

2. يؤدي الإستثمار في مجال نظم المعلومات الى تسابق الشركات، وتحقيق الربح من خلال تبسيط الإجراءات، مما يُصعب معرفة هوية المستخدم في حال الحاجة الى البحث والتحري[1].

ثالثاً: عوائق تتعلق بجهات التحقيق.

1. قلة الخبرة في مجال التحقيق في الجرائم المعلوماتية.
2. قد تكون شخصية تتعلق بالمحقق مثل التهيب من استخدام الكومبيوتر، واستخدام الأنترنت، وعدم الإهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية.
3. صعوبات تتعلق بالنواحي الفنية كنقص المهارة المطلوبة للتحقيق في هذا النوع من الجرائم وعدم توفر المعرفة بأساليب ارتكاب هذا النوع من الجرائم[2].

المطلب الثاني: الأجهزة المتخصصة بالتحقيق على المستوى الدولي و الوطني.

نظرا لتعقيد الجرائم المرتكبة في الفضاء الرقمي وتعدد أطرافها عبر الحدود، برزت الحاجة إلى استحداث أجهزة مختصة بالتحقيق، بما يضمن الحفاظ على الأمن المعلوماتي محليًا ودوليًا. ومنه، سنعالج هذا المطلب من خلال: **الأجهزة المختصة وطنياً**، و **الأجهزة المختصة دولياً**.

الفرع الأول: الأجهزة المختصة على المستوى الوطني.

عملت الدولة الجزائرية على تطوير آليات مكافحة الجريمة المعلوماتية عبر تأسيس أجهزة مختصة على مستوى جهازي الأمن والدرك الوطني، وإنشاء هيئات وطنية. من أبرزها:

[1] عماد بلغيث ويوسف جغلولي، **صعوبات التحقيق في الجرائم المعلوماتية**، مجلة الرسالة للدراسات والبحوث الإنسانية، مخبر سوسيولوجية جودة الخدمة المعلوماتية، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد 6، العدد 3، سبتمبر 2021، ص: 81/80.

[2] سعيداني نعيم، المرجع السابق، ص: 81.

1. الهيئات الوطنية لمكافحة الجريمة المعلوماتية:

1.1.الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والإتصال: أنشئت بموجب المادة 13 من القانون رقم 09-04[1]، وقد أسند المشرع مهمة تنظيما وتسييرها الى نص تنظيمي، ويتضح ذلك من خلال ف/2 من نفس المادة[2]. وفي هذا السياق، أصدر المشرع عدة مراسيم تبين تطور الهيئة، منها: المرسوم الرئاسي رقم 15-261، عرف الهيئة في المادة 2 بأنها: "سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل". ثم المرسوم الرئاسي رقم 19-172، أعاد تعريفها بأنها: "مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلالية المالية، وتوضع تحت سلطة وزارة الدفاع". والمرسوم الرئاسي رقم 20-183، نص على أنها: "سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة رئيس الجمهورية". والمرسوم الرئاسي رقم 21-439، أكد على أنها: "سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي لدى رئيس الجمهورية". ويستخلص منه تطور مكانة الهيئة وهوا مايعكس اهميتها في الإستراتيجية الوطنية للأمن السيبيراني، كما إنتقلت وصايتها من وزارة الدفاع الوطني الى سلطة رئيس الجمهورية، و أعيد اعتماد وصفها بمصطلح "سلطة إدارية مستقلة" بعدما كانت "مؤسسة عمومية"[3]. و بحسب المادتين 5 و6 من المرسوم الرئاسي 21-439، تتشكل الهيئة من:

[1] رجاء امدور، **خصوصية التحقيق في مواجهة الجريمة المعلوماتية**، أطروحة دكتوراة، تخصص قانون خاص، قسم الحقوق، جامعة محمد البشير الإبراهيمي، كلية الحقوق والعلوم السياسية، برج بوعريريج، 2021/2020، ص ـ ص: 91/90.

[2] المادة 13 وجاء فيها: " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته، تحدد تشكيلة الهيئة وتنضيمها وكيفيات سيرها عن طريق التنظيم" القانون رقم: 09-04 المؤرخ في: أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته، ج ر ج ج، العدد 47، سنة 2009، ص: 8.

[3] رجاء امدور، المرجع السابق، ص: 91.

❖ **مجلس التوجيه:** يترأسه الأمين العام لرئاسة الجمهورية، ويضم في عضويته ممثلين عن وزارات وهيئات أمنية عليا. بالإضافة إلى المدير العام للهيئة الذي يتولى أمانة المجلس. وحددت المادة 7 من نفس المرسوم الرئاسي مهامه والمتمثلة في:

1. مهام تخطيط الإستراتجية، والمصادقة على برنامج الهيئة.
2. إقتراح أنشطة بحث وتقييم الأعمال ودراسة التقرير السنوي لنشاطات الهيئة[1].

ينعقد مجلس التوجيه مرة واحدة في السنة، أما الدورة الإستثنائية تكون بناءً على إستدعاء من رئيسه، أو بطلب من أحد أعضائه، أو من المدير العام للهيئة، والمجلس تقريراً بعد كل دورة[2].

❖ **المديرية العامة:** يديرها المدير العام يعين بموجب مرسوم رئاسي، وتُعد وظيفته من الوظائف العليا في الدولة، ويكلف بإخطار رئيس الجمهورية إذا وقع حادث مس بأمن الدولة أو بالأعمال الإرهابية أو التخريبية، أما مايتعلق بمسائل الدفاع الوطني يخطر بها رئيس أركان الجيش الوطني الشعبي. ومن مهام المديرية مايلي:

1. إقتراح مخططات العمل للهيئة والسهر على تنفيذها، وإحترام قواعد حماية السر المهني.
2. ممارسة السلطة السلمية على مستخدمي الهيئة[3]، وضمان التسيير الإداري والمالي.
3. إعداد مشروع النظام الداخلي للهيئة ..الخ[4].

تطورات هيكلة المديرية العامة التنظيمية بناءً على مجموعة من المراسيم الرئيسية. في البداية صدر المرسوم الرئاسي رقم 15-261، حيث لم تضمن تحديدًا لمصالح المديرية العامة. غير أن الأمر تغير مع صدور المرسوم الرئاسي رقم 19-172، نص على ضم كل من المديرية

---

[1] المواد 5 و6 و7 من المرسوم الرئاسي رقم: 21-439 المؤرخ في: 2021/11/7 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته، ج ر ج ج، العدد 86، سنة 2021، ص ـ ص: 7/6.

[2] المرجع نفسه، ص ـ ص: 7/6.

[3] عرفت المادة 5 من المرسوم الرئاسي رقم: 15-261 مستخدمي الهيئة على انهم: "المستخدمون الذين يمارسون عملهم بالتوقيت الكامل في الهيئة مهما كان وضعوهم القانوني الأصلي".

[4] المواد 7 و8 و9 و10 من المرسوم الرئاسي رقم: 21-439، المرجع السابق، ص: 7.

التقنية ومديرية الإدارة والوسائل، في المواد من 11 إلى 15[1]. ثم، جاء المرسوم الرئاسي رقم 20-183 أدخل تعديلات على تنظيم المصالح ضمن القسم الثاني في المواد من 15 إلى 20 حيث تم، إلغاء المديرية التقنية، والإبقاء على مديرية الإدارة والوسائل، و مصلحة الدراسات والتلخيص، ومديرية المراقبة الوقائية واليقظة الإلكترونية، ومصلحة التعاون واليقظة التكنولوجية[2]. أما بموجب المرسوم الرئاسي رقم 21-439، استحداث الملحقة الجهوية وفق المادة 20 منه، "تكلف بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، بإذن مكتوب من السلطة القضائية وتحت رقابتها، وطبقًا للتشريع الساري المفعول. وتوضع تحت إشراف مديرية المراقبة الوقائية واليقظة الإلكترونية". وفي نفس المرسوم الرئاسي، من المواد 20 الى 33 نظم كيفية سير الهيئة الوطنية للوقاية من جرائم الاعلام والإتصال، بما في ذلك تسجيل الاتصلات الإلكترونية وفق الشروط القانونية، وضمان المديرية العامة للاستعلام التقني، والإسناد المتعدد الأشكال للهيئة، وحفظ المعلومات المستقاة أثناء عمليات المراقبة، وفق قواعد حماية المعلومات المصنفة[3] بينما حددت المادة 14 من القانون رقم 09-04 مهام الهيئة وهي:

1. تنشيط وتنسيق عمليات الوقاية والمكافحة، والمساهمة في مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات.

2. تبادل المعلومات مع الهيئات الأجنبية لجمع المعطيات والتعرف على مرتكبي الجرائم[4].

1.2. المنظومة الوطنية لأمن الأنظمة المعلوماتية: حسب المرسوم الرئاسي رقم 20-05 تعرف في المادة 2 بأنها: "أداة الدولة في مجال أمن الأنظمة المعلوماتية، وتشكل الإطار التنظيمي

[1] المرسوم الرئاسي رقم: 19-172 المؤرخ في: 2019/7/6، المتضمن تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر ج ج، العدد37، 2019.

[2] المرسوم الرئاسي رقم: 20-183، المرجع السابق، ص ـ ص: 7/8.

[3] المرسوم الرئاسي رقم: 21-439، المرجع السابق، ص ـ ص: 9/8.

[4] القانون رقم: 09-04، المرجع السابق، ص: 8.

لإعداد الإستراتجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها"[1]. اما ف2 حدد المشرع تشكيلة المنظومة حيث تتشكل من المجلس الوطني لأمن الأنظمة المعلوماتية، بالإضافة الى وكالة أمن الأنظمة المعلوماتية[2] التى تدير لجنة توجيه، وتزود بلجنة علمية، وتكلف الوكالة بعدة مهام[3] منها إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث التي تستهدف المؤسسات الوطنية، وجمع وتحليل وتقييم المعطيات المتعلقة بأمن الأنظمة لاستخلاص المعلومات الملائمة لتأمين المنشآت، بالإضافة إلى متابعة تدقيق الأمن، أما مهام المجلس فتشمل إعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة على اتفاقيات التعاون والإعتراف المتبادل مع الأنظمة المعلوماتية، وقد حددت المواد 7و 8و 9 تنظيم المجلس، أما المواد من 10 إلى 16 نصت على كيفية سيره[4].

2. **على مستوى جهاز الأمن الوطني:** تعد الشرطة القضائية من المديريات الأساسية في مصالح الأمن الوطني، إذ تجمع بين الأبعاد الإدارية، والوظيفية، والعملياتية، مما يجعلها تلعب دورًا محوريًا. وقد عززت هذه المديرية دورها عبر تطوير استراتيجية وطنية شاملة لمكافحة الجريمة، وتحسين تكوين أعوانها لمواكبة التطورات الحديثة. كما تنفذ الإنابات القضائية والأحكام الصادرة عن الجهات القضائية المختصة، كما شهدت تطورًا مستمرًا في مواجهة أشكال الجريمة المختلفة، عبر استحداث مجموعة من المصالح المتخصصة، أبرزها: نيابة مديرية القضايا الجنائية، نيابة مديرية القضايا الاقتصادية والمالية، ونيابة مديرية الشرطة العلمية والتقنية، وتضم هذه الأخيرة عدة مصالح متخصصية، منها:

---

[1] المادة 5 و 4 من المرسوم الرئاسي رقم: 20-05 المؤرخ في: 2020/01/20 المتضمن وضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر ج ج ، العدد4، الصادرة في: 2020/01/21، ص: 6.

[2] نصيرة بوحمزة، **التحقيق الجنائي في الجريمة الإلكترونية (دراسة مقارنة)**، اطروحة دكتوراة، تخصص القانون الخاص، قسم الحقوق، كلية الحقوق والعلوم السياسية، جماعة الجيلالي اليابس، سيدي بلعباس، 2022/2021، ص: 271.

[3] عرفت المادة 17 من المرسوم الرئاسي رقم: 20-05 "الوكالة مؤسسة عمومية ذات طابق إداري تتمتع بالشخصية المعنوية والإستقلالية المالية يحدد مقر الوكالة في مدينة الجزائر".

[4] حورية خليصة و حمزة فيروز، المرجع السابق، ص ـ ص: 25/24.

2.1.المصلحة المركزية لمكافحة الجرائم السيبرانية: تُعد النواة الأساسية لمكافحة الجريمة المعلوماتية، تأسست 2011 ضمن مديرية الشرطة القضائية، تم تطويرها بإضافة المصلحة المركزية لمكافحة الجرائم المعلوماتية في 2015، ومع تزايد الجرائم المعلوماتية، تم إنشاء 48 فصيلة في مصالح الشرطة القضائية الولائية، لدعم التحريات التقنية، والرقمية، والمشاركة في التحقيقات القضائية، وتحليل التهديدات السيبرانية، وتأمين الفضاء الرقمي الوطني، وتعزيز قدرات مكافحة الجريمة من خلال البحث العلمي والتقني. وتشمل أيضًا اليقظة المعلوماتية، والبحث عبر الشبكات المفتوحة عن المحتويات غير الشرعية، و تعزيز القدرات البحثية والتكوينية لعناصر الشرطة.

2.2.المخبر المركزي للشرطة العلمية: يعد هيئة متخصصة في تقديم الخبرات التقنية والعلمية في مجال[1] البحث والتحقيق وتحليل الأدلة الجنائية المتعلقة بالجريمة المعلوماتية. ويتألف كل مخبر من دائرتين رئيسيتين: **الدائرة العلمية** تختص بالتحقيقات في المجالات البيولوجية، الطب الشرعي، الكيمياء، المخدرات، التسميم، الحرائق، المتفجرات. وذلك عبر مخابر متخصصة لكل مجال. اما **الدائرة التقنية** تركز على الجرائم المرتبطة باستخدام الأسلحة، التزوير، الجرائم المعلوماتية مع معالجة كل نوع ضمن دائرة مستقلة[2]. كما أنشأت مديرية الشرطة القضائية خمسة مخابر جهوية تابعة للمخبر المركزي، في ولايات وهران، قسنطينة، ورقلة، بشار، وتمنراست. لتقديم التحليلات والخبرات العلمية اللازمة للتحقيقات القضائية، وتقديم الدعم التقني اللازم لتسيير ومعاينة مواقع الجرائم.

2.3.المكتب المركزي الوطني للإنتربول بالجزائر: يقوم بجمع المعلومات وتبادل المعلومات الجنائية مع المكاتيب الدولية، ويساهم في دعم التحقيقات والاعتقالات العابرة للحدود،

[1] بوقرة جمال الدين، **التحقيق الجنائي في الجريمة المعلوماتية**، اطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية جامعة محمد بوضياف، المسيلة، 2025/2024، ص: 112/111.

[2] حسين ربيعي، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016/2015، ص: 178.

خاصة في مجالات الجريمة المعلوماتية، الإرهاب، والجريمة المنظمة، وحسب التزايد الملحوظ في عدد القضايا التي تم التكفل بها. سجل 567 قضية سنة 2015، ليقفز العدد إلى 3522 قضية سنة 2018، وتم حل 2627 قضية بنسبة إنجاز 74.27%. كما سبق أن عالجت 73.90% قضية في 2017[1].

3. **على مستوى جهاز الدرك الوطني:** يعد قوة عسكرية مكلفة بالأمن العمومي، يمارس مهام الشرطة الإدارية، والقضائية، والعسكرية عبر كامل التراب الوطني، معتمدا وسائل التحري العلمية، والتقنية، وخبرة الأدلة الجنائية.[2] لمواجهة الجرائم المعلوماتية، وأنشأ الجهاز:

3.1. **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها:** هيئة تقنية وظيفتها المراقبة الدائمة لشبكة الإنترنت ومختلف شبكات الاتصال الإلكترونية، تساعد وحدات الدرك الوطني، والجهات القضائية، في معاينة الجرائم المعلوماتية، والبحث عن الأدلة الرقمية، والمشاركة في عمليات التحري، والتسرب الإلكتروني، والتعاون مع مختلف مصالح الأمن والهيئات الوطنية[3]. ففي سنة 2014، ساهم في معالجة ما يقارب 240 ضحية إلكترونية تشمل تهديدات، تحرش، احتيال، والاعتداء على الحياة الخاصة[4].

3.2. **المعهد الوطني للأدلة الجنائية وعلم الإجرام:** مؤسسة عمومية ذات شخصية معنوية وصبغة إدارية، واستقلال مالي، يقع مقره بالجزائر[5]، أنشئت بموجب المرسوم الرئاسي رقم 04-183، يختص بإجراء الخبرات، والفحوص العلمية بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح، بناءً على طلب من القضاء أو من السلطات المؤهلة،

---

[1] بوقرة جمال الدين، المرجع السابق، ص: 113.

[2] راجع المواد 02 و 03 و 07 و 08 من المرسوم الرئاسي رقم: 09-143 المؤرخ في: 2009/04/27 المتضمن مهام الدرك الوطني وتنظيمه، ج ر ج ج، العدد 26، 2009.

[3] حسين ربيعي، المرجع السابق، ص: 185.

[4] سعاد رابح، **ضوابط مكافحة الجريمة المعلوماتية**، مجلة القانون العام الجزائري والمقارن، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، المجلد7، العدد1، جوان 2021، ص: 280-281.

[5] راجع المواد 02 و 03 من المرسوم الرئاسي رقم: 04-183 مؤرخ في: 2004/06/26 المتضمن إحداث المعهد الومطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر ج ج، العدد41، 2004.

ويشارك في الملتقيات، والمحاضرات، والندوات على الصعيدين الوطني والدولي لتطوير قدرات مستخدمي المعهد[1]. ورغم النتائج الإيجابية التي حققتها الشرطة القضائية في مجال مكافحة الجريمة المعلوماتية، إلا أن التطور السريع لأساليب هذه الأخيرة يفرض ضرورة تعزيز الهياكل المادية، والتقنية، والتكوين المتخصص والمستمر للعناصر البشرية، إلى جانب التنسيق الدائم مع الهيئات المماثلة إقليمياً ودولياً، لضمان دعم القضاء في كشف الجرائم الإلكترونية والوصول إلى مرتكبيها."[2]

الفرع الثاني: على المستوى الدولي.

تتميز الجريمة المعلوماتية بطابع العالمية، ما جعلها عابرة للحدود، مما أضحى معه التعاون الدولي أمرًا ضروريًا لجمع الأدلة والمعلومات. ويُعد التنسيق الأمني من أهم صور هذا التعاون الدولي لمواجهة هذا النوع من الإجرام، وتجسد ذلك بإنشاء مكاتب متخصصة، أبرزها:

1. **المنظمة الدولية للشرطة الجنائية "INTERPOL"**: تعد المنظمة من اقدم واكبر هيئة شرطية دولية، تتخذ من مدينة ليون الفرنسية مقراً لها. ارتفع عدد اعضائها من177 دولة[3] الى 195 دولة. تهدف الى تعزيز التعاون بين أجهزة الشرطة لمكافحة الجرائم العابرة للحدود، خاصة الجرائم المعلوماتية والمالية المرتبطة بالتكنولوجيا الحديثة. وتعمل المنظمة على وظيفتين أساسيتين: جمع البيانات والمعلومات من مكاتبها الوطنية المنتشرة في الدول الأعضاء، وتعمل أيضا على تنسيق الجهود لتوقيف المجرمين الفارين وتسليمهم إلى الدول التي تطلبهم. انضمت الجزائر للمنظمة سنة 1963، وتولت منصب نيابة و رئاسة المنظمة خلال عهدتين من 1971 إلى 1981، كما شاركت بانتظام في جمعيات الإنتربول العامة، مما ساهم في استفادة عدد كبير من موظفي الشرطة من تكوينات متخصصة لتحسين مستواهم المهني. من ابرز إنجازات الإنتربيول في مجال مكافحة الجريمة المعلوماتية عملية

[1] راجع المادة 04، المرسوم رقم 04-183 ، المرجع السابق .

[2] بوقرة جمال الدين، المرجع السابق، ص: 115.

[3] حسين ربيعي، المرجع السابق، ص: 148.

"**Cathedral**" سنة 1998، بالتعاون مع FBI والشرطة البريطانية، حيث فككت شبكة استغلال للاطفال عبر 12 دولة. كما نظمت مؤتمرا دوليا سنة 2005 لتكوين المحققين في الجريمة المعلوماتية، والذي عرف مشاركة 30 دولة.

2. **مركز الشرطة الأوروبي "EUROPOL"**: هو جهاز أمني مقره مدينة لاهاي بهولندا، يهدف إلى تسهيل مهام رجال الشرطة داخل دول الاتحاد الأوروبي في مكافحة الجرائم العابرة للحدود، خاصة الجريمة المعلوماتية، يقدم الدعم عبر نشرات أمنية وتقارير خاصة بهويات المجرمين والأدلة التي يتم جمعها. ويعتبر من أبرز الهيئات الأستشارية عالمياً في ميدان الإجرام الإلكتروني. حيث ساهم في إنجاز دراسات متعددة حول دوافع الجريمة المعلوماتية واستشراف تطوراتها، وقد حظي بثقة اللجنة الأوروبية التي اعتمدته مركزًا إعلاميًا متخصصاً في هذا المجال[1].

3. **الأوروجست "EUROJUST"**: وهو جهاز يهدف لتقوية التصدي للإجرام، يعمل على تطوير آليات مكافحة الجريمة المعلوماتية من خلال تبادل المعلومات مع محاكم الاتحاد الأوروبي بصفة دورية[2]. و تتمثل مهامه بشكل عام في تنسيق التعاون بين السلطات القضائية للدول الأطراف، والتبليغ عن الجرائم فيما بينها. منذ 2019، عزز الإطار القانوني المنظم لعملها، مما أتاح لها صلاحيات أوسع في تبادل المعلومات وطلب من الجهات القضائية الوطنية فتح تحقيقات أو مباشرة ملاحقات، كما له علاقة وثيقة بالأوروبول الذي يزوده بالتحليلات الهامة لتعزيز فعالية التحريات على مستوى الدول الأعضاء.

4. **آلية الاتحاد الإفريقي للتعاون في مجال الشرطة "AFRIPOL"**: يعد جهاز تعاون شرطي أفريقي مقره الجزائر، ويعمل في إطار احترام السيادة الوطنية للدول الأعضاء. ويهدف إلى وضع إطار للتعاون الشرطي على المستويين الاستراتيجي والعملياتي بين أجهزة الشرطة

[1] بوقرة جمال الدين، المرجع السابق، ص: 117.

[2] حسين ربيعي، المرجع السايق، ص: 251.

الإفريقية، من خلال تسهيل التبادل في مجالات التدريب، والتكوين، وتبادل الخبرات، والممارسات، خاصة في ميادين التحقيق والتحليل الجنائيين، واستعمال التكنولوجيات الحديثة. ورغم حداثته، يرتقب أن يلعب دورًا مهمًا في مكافحة الجريمة المعلوماتية، من خلال إستراتيجيات ملائمة للواقع الأفريقي، مع السعي لتنسيق الجهود مع الأجهزة الأقليمية والدولية[1].

[1] بوقرة جمال الدين، المرجع السابق، 199/118.

خــلاصة الفصــل الأول:

استنادًا الى المعطيات القانونية يظهر هذا الفصل، واقعاً مفاده أن الجريمة المعلوماتية كونها من الجرائم المستحدثة أضحت تمثل تحدياً صارخاً للأنظمة القانونية التقليدية، لما تتسم به من طبيعة افتراضية وتعقيد تقني بالغ، سواء من حيث طبيعة ارتكابها أو بيئة حدوثها. حيث ترتكب في فضاء رقمي لا تحكمه الحدود الجغرافية ولا تواجه بسهولة بالقواعد الإجرائية الكلاسيكية.

وتطرقنا في مستهل هذا الفصل الى الإطار المفاهيمي للجريمة المعلوماتية، مبرزين تعريفها فقهياً وقانونياً، محللين خصائصها، وأركانه. ثم قمنا بتصنيفها وفقا لطبيعتها، ومحلها، ووسائل ارتكابها، مما بين أنها تتطلب جهداً علمياً وتحليلياً متقدماً لكشف مرتكبيها. كما عرضنا أطراف الجريمة، من مجرم متمكن تقنياً، إلى الضحية التى قد تكون شخصاً طبيعياً او معنوياً، إضافة الى تعدد الدوافع الإجرامية التى تعكس التحول السوسيولوجي للسلوك الإجرامي في البيئة الرقمية.

أما في الشق المتعلق بالتحقيق، فصل صلاحيات قاضي التحقيق وضباط الشرطة القضائية، مبرزين التحديات التي يواجهونها، لا سيما في ظل تطور وسائل الجريمة المعلوماتية ونقص الكفاءة الرقمية لدى بعض المحققين. واستجابة لهذا التحدي وسع المشرع الجزائري صلاحيات هذه الجهات، وأنشأ هيئات متخصصة، وهو ما كرسه في القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وغيره من القوانين الحديثة. كما لم نغفل عن دور الأجهزة الوطنية والدولية الداعمة لمسار التحقيق، والتي تساهم بشكل فعال في كشف الأدلة وتعزيز الأمن السيبراني.

ختاماً لما سبق بيانه، يمكن القول أن الجريمة المعلوماتية فرضت نفسها كواقع لا مفر منه، وأصبحت تمثل تحدياً حقيقياً للعدالة الجنائية. ومن ثم، لا بد من التمكين للمحققين بالتكوين المستمر، والتجهيزات الحديثة، وتعزيز الإطار التشريعي والمؤسساتي، والتعاون الدولي، لضمان تحقيق فعال، يواكب تطورها، ويصون حقوق الأفراد، والمجتمع في آنٍ واحد.

الفصل الثاني: الدليل الرقمي ومراحل مشروعيته أمام القضاء.

تـمهيـــــد:

بعد أن تطرقنا في الفصل الأول الى الجريمة المعلوماتية من حيث الإطار المفاهيمي والتشريعي، ننتقل في هذا الفصل الى عنصر جوهري يعد الركيزة الأساسية في إثبات هذا النوع من الجرائم، وهوا الدليل الرقمي. فبحكم الطبيعة التقنية للجريمة المعلوماتية، اضحى هذا الدليل يحتل مكانة محورية ضمن أساليب التحري الخاصة بالإثبات، بما يطرحه من خصوصيات قانونية وتقنية تميزه عن الدليل التقليدي. كما أن استخلاصه يثير تحديات تتعلق بالمشروعية، والقبول القضائي، في ظل سهولة طمسه وإتلافه. وفي هذا الفصل، سنتناول الموضوع من خلال مبحثين:

1. المبحث الأول: ماهية الدليل الرقمي وأساليب التحري الخاصة في التشريع الجزائري.
2. المبحث الثاني: التحديات التي تواجه الدليل الرقمي ومراحل مشروعيته أمام القضاء.

المبحث الأول: ماهيـة الدلـيل الرقمــي.

يستهل هذا المبحث بتسليط الضوء على الدليل الرقمي باعتباره أحد ابرز المستجدات التي فرضها التطور التكنولوجي في مجال الإثبات الجنائي، حيث أضحى هذا الدليل يلعب دوراً محورياً في الكشف عن هذا النوع من الجرائم، لاسيما تلك المرتبطة بالفضاء الإلكتروني, ومن ثم، سيتم تناول مفهوم الدليل الرقمي كخطوة أولى وأساسية ثم تحديد خصائصه، وما يميزه عن الدليل التقليدي. وأيضا أسالب التحري الخاصة. وذلك، من خلال مطلبين أساسيين:

1. المطلب الأول: مفهوم الدليل الرقمي.

2. المطلب الثاني: أساليب التحري الخاصة التقليدية والحديثة في التشريع الجزائري.

المطلب الأول: مفـهوم الدليل الرقمــي.

يفتتح هذا المطلب بتوضيح مفهوم الدليل الرقمي لما له من أهمية في التحقيقات الحديثة، مع التطرق الى أبرز خصائصه وما يميزه عن الدليل التقليدي.

الفرع الأول: تعريف الدليل الرقمي.

قبل التطرق إلى مفهوم الدليل الرقمي في إطار التحقيق الجنائي، من المهم الوقوف أولًا على المعنى اللغوي، ثم المعنى الاصطلاحي "لدليل الرقمي"، وهذا من خلال:

أولاً: التعريف اللغوي: يُقصد "بالدليل" في اللغة المرشد والبرهان. وقد عرفه الجرجاني بأنه: "ما يلزم من العلم به العلم بشيء آخر"[1]. أما "الرقمي"، فهو مشتق من الفعل رقم[2].

ثانياً: التعريف الاصطلاحي: يقصد به في الإصطلاح القانوني: كل أثر أو معلومة ذات طبيعة رقمية تستخلص من أجهزة الحاسوب أو الوسائط الإلكترونية، في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ثم تجمع و تحلل ببرامج خاصة، إذ يقدم في عدة أشكال متنوعة مثل:

[1] علي بن محمد السيد الشريف الجرجاني، **معجم التعريفات**، دار الفضيلة، ص: 91.

[2] محمد بن يعقوب الفيروز، آبادي مجد الدين، **قاموس المحيط**، دار الحديث، القاهرة، ص: 669.

النصوص المكتوبة أو الصور أو الأصوات، وغيرها من أشكال البيانات الرقمية، قصد إعتمادها أمام أجهزة تطبيق القانون[1]، لإثبات وقائع أو نفيها في إطار التحقيق أو المتابعة القضائية. و يعد من المعطيات المقبولة منطقيًا و عقليًا، والتي يتم الحصول عليها بطرق قانونية، بغرض ترجمة البيانات المخزنة في بيانات الحاسب الآلي إلى معلومات قابلة للإستخدام في أي مرحلة من مراحل التحقيق الجنائي، لإثبات حقيقة الفعل أو نسبة الفعل إلى فاعله[2].

الفرع الثاني: خصائص الدليل الرقمي والتمييز بينه وبين الدليل التقليدي.

يقوم الدليل الرقمي على خصائص ترتبط بالبيئة الرقمية التي ينشأ فيها، وهي بيئة إفتراضية تشمل جميع مكونات أجهزة الحاسوب المادية والبرمجية. وقد إنعكست هذه البيئة على طبيعة هذا الدليل، مما أضفى عليه عدة سمات تميزه عن الأدلة التقليدية، من أبرزها:

الدليل الرقمي هو **دليل علمي**، لا يمكن الحصول عليه إلا باستخدام أساليب علمية دقيقة، وهذا يعود للمنشأ الذي يكون فيه الدليل[3]. كما أنه **ذو طبيعة تقنية**، إذ يتم تجميع المعلومات والبيانات المتعلقة بنشاط الجاني باستخدام تقنيات عالية[4]. وأيضاً **يصعب التخلص منه**، إذ إن محاولات الجاني لمحو آثاره الرقمية لا تنجح غالبًا، حيث تبقى آثار النشاط مسجلة ويمكن إسترجاعها باستخدام تقنيات متخصصة[5]. أيضًا أنه **متنوع ومتطور**، إذ يشمل أنواعًا متعددة من البيانات الإلكترونية الممكن تداولها رقمياً، مثل صور ثابتة أو متحركة[6]. كما أنه **غير مرئي**، إذ

---

[1] نور الهدى محمودي، **حجية الدليل الرقمي في إثبات الجريمة المعلوماتية**، مجلة الباحث للدراسات الأكادمية، جامعة باتنة1، المجلد4، العدد2، جوان 2017، ص: 911.

[2] محمد الأمين البشري، **التحقيق في الجرائم المستحدثة**، دار الحامد للنشر والتوزيع، عمان، الأردن، ط1، ص: 234.

[3] خطوي المسعود، **خصوصية الدليل الإلكتروني**، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي، الأغواط، المجلد7، العدد1، سنة 2023، ص: 1064.

[4] عبير بعقيقي، فيصل نسيغة، **الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04**، مجلة العلوم القانونية والسياسية، جامعة محمد خيضر، بسكرة، الجزائر، المجلد9، العدد2، جوان 2018، ص: 38.

[5] المرجع نفسه، ص: 38.

[6] لعصامي آمال، بن طالب جميلة، **حجية الدليل الإلكتروني في الإثبات الجنائي وفق التشريع الجزائري**، مذكرة ماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة د. مولاي الطاهر، سعيدة، سنة 2022/2021، ص: 21.

يتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، بل إدراكها أو التعامل معها يتم من خلال أجهزة ومعدات الحاسب الآلي ونظم "Hardware"، برمجيات الحاسوب "Software". وأخيرًا، فهو **قابل للنسخ** حيث أن هذه الخاصية تقلل أو تعدم مخاطر إتلاف النسخة الأصلية، عن طريق نسخ طبق الأصل من الدليل، مما يوفر ضمانة كبيرة لحفظه من الفقد وإعتماده[1].

ورغم أن الدليل الرقمي والتقليدي كلاهما يعد دليل إثبات يعتد به في المجال الجنائي للوصول إلى الحقيقة القضائية الحقة، كما يستخلص من الجريمة، إلا أن الإختلافات بين كلا الدليلين تظهر في عدة جوانب وهذا ماسنوضحه من خلال الآتي[2]:

1. **من حيث التعريف:** الدليل التقليدي معتمد في مختلف فروع القانون "كالتجاري، والبحري.." يشمل: الإقرار، الكتابة، القرائن، واليمين الحاسمة، يلزم القاضي بالأخذ به إذا توفرت شروطه، دون أن تكون له سلطة تقديرية. اما الدليل الرقمي يستخرج من الحواسيب أو شبكات الأنترنت، يجمع ببرامج متخصصة, ويعتمد عليه في مراحل التحقيق.
2. **من حيث الإجراءات:** يتطلب الدليل التقليدي إجراءات تقليدية كالضبط، التفتيش، المعاينة، الخبرة. أما الدليل الرقمي فيحتاج إلى تقنيات خاصة حديثة مثل: حفظ البيانات، إعتراض المراسلات، والمراقبة الإلكترونية، بهدف إثبات وقوع الجريمة وتحديد شخصية مرتكبيها[3].
3. **من حيث الأنواع:** الدليل التقليدي يتضمن: الدليل الكتابي، المحاضر، المحررات، الإعتراف، الشهادة، والقرائن. في حين أن الدليل الرقمي يتضمن: صناعة الفيروسات ونشرها، سرقة أجهزة أو مكونات أو معلومات أو الغش أو التغيير في المواصفات.

---

[1] بن فريدة محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)**، مجلة الباحث للدراسات الأكادمية، كلية الحقوق والعلوم السياسية، جامعة بجاية، الجزائر، المجلد4، العدد2، جوان 2017، ص: 278.

[2] هروال أية نور الهدى، **الأدلة الرقمية في إثبات الجريمة المعلوماتية**، مذكرة ماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، 2021/2020، ص: 11.

[3] المرجع نفسه، ص: 12.

4. **من حيث القانون المطبق:** يخضع الدليل التقليدي لقانون الإجراءات الجزائية الجزائري فقط، أما الدليل الرقمي فيخضع لهذا القانون إلى جانب قوانين خاصة بالجريمة المعلوماتية كالقانون 09-04.

5. **من حيث الطبيعة والجهات المختصة:** يتولى جهاز الشرطة القضائية، جمع الدليل التقليدي والأقطاب المتخصصة تنظر في مدى قبوله، بينما يتطلب الدليل الرقمي تدخل ضبطية قضائية مختصة بالجريمة السيبيرانية، و تعددت التسميات بين شرطة الأنترنت أو الشرطة الإلكترونية.[1]

المطلب الثاني: أساليب التحري الخاصة التقليدية والحديثة في التشريع الجزائري.

تقتضي عملية إستخلاص الدليل الرقمي إتباع أساليب تحري خاصة بالتحقيق، والتى تتنوع بين أساليب تقليدية مستمدة من القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية الجزائري ، وأخرى حديثة تواكب التطور التكنولوجي. ومنه, سنسعى من خلال هذا المطلب الى ذكر الأساليب المعتمدة في التشريع الجزائري. بدءًا من: **أساليب التحري التقليدية**, ثم **أساليب التحري الحديثة.**

الفرع الأول: أساليب التحري التقليدية.

رغم خصوصية الدليل الرقمي إلا أن الجهات المختصة في الغالب ما تلجأ لأساليب التحري التقليدية المعروفة في قانون الإجراءات الجزائية الجزائري. للكشف عن الجريمة المعلوماتية. تكمن هذه الاسالب في:

1. **المعاينة:** وتعد من أهم أساليب التحري الخاصة بالتحقيق لما يمكن أن توفره من أدلة إثبات، خاصة في الجرائم التقليدية، ويطلق عليها عادة إثبات حالة الأشخاص ذات الصلة بالحادث[2]. لكن الأمر يختلف في الجرائم المعلوماتية، هذا راجع للطبيعة الخاصة للسلوك

[1] هروال آية نور الهدى، المرجع السابق، ص: 13.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص: 147.

الإجرامي، واعتبارها جريمة مستحدثة تخلف مسرح مادي. فالمعاينة المعلوماتية هي: "المشاهدة والرؤية بالعين لمكان أو شخص أو أي شيء له علاقة بالجريمة، لإثبات حالته والآثار المادية التي خلفها جراء إرتكابه الجريمة المعلوماتية، وضبط كل ما يفيد كشف الحقيقة عن الجريمة المعلوماتية المرتكبة، بهدف الحفاظ على الأدلة التقنية من التلف أو المحو أو التعديل"[1]. فهي تقدم للمحقق صورة حقيقية عن مكان وقوع الجريمة. وتختلف المعاينة في قانون الإجراءات الجزائية الجزائري عن قانون الإجراءات الإدارية والمدنية [2]، بحيث أن المعاينة يقوم بها كل من المحضر القضائي والخبير حسب المادة 146 من قانون الإجراءات الإدارية والمدنية: "يجوز للقاضي من تلقاء نفسه أو بطلب من الخصوم، القيام بإجراء معاينات أو تقييمات أو تقديرات أو إعادة تمثيل الوقائع التي يراها ضرورية مع الإنتقال إلى عين المكان إذا اقتضى الأمر ذلك"[3]، أما من خلال المادة 79 قانون الإجراءات الجزائية الجزائري: "يجوز لقاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها. ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته"[4]. فالمعاينة من إختصاص النيابة العامة وقضاة التحقيق. فبعد تلقي البلاغ عن وقوع الجريمة المعلوماتية والتأكد من البيانات الضرورية في البلاغ، يتم الإنتقال الى مسرح الجريمة لإجراء المعاينة، وينبغي على القائمين بالمعاينة التعامل مع مسرح الجريمة على أنه مسرحان هما:

1.1. مسرح مادي: يشمل كل المكونات المادية للحاسب الآلي، وقد يحتوي على أثار مادية كالبصمات أو أوراق .

[1] عيدة بلعابد، **خصوصية التحقيق في الجريمة المعلوماتية**، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بأفلو، الأغواط، جامعة د. مولاي الطاهر، سعيدة، المجلد4، العدد 6، مارس 2021، ص: 140.

[2] هروال أية نور الهدى، المرجع السابق، ص: 22.

[3] القانون رقم: 08-09 المؤرخ في: 2008/2/25، يتضمن قانون الإجراءات المدنية والإدارية، ج ر ج ج، العدد21، 2008, ص: 14.

[4] الأمر رقم: 66-155 المؤرخ في: 1966/6/8، يتضمن قانون الإجراءات الجزائية الجزائري، المعدل والمتمم، ج ر ج ج، العدد 48، 1966، المعدل والمتمم بموجب القانون رقم: 17-07، المؤرخ في: 2017/3/27، ج ر ج ج، العدد 48، لسنة2017.

1.2. مسرح رقمي: يبقى داخل العالم الإفتراضي لجهاز الحاسب الآلي، ويحتوي على جميع البيانات والمعلومات المخزنة التي تفيد التحقيق[1]

ولكي يصبح للمعاينة في مسرح الجريمة أهمية في كشف الحقيقة يجب مراعاة التالي[2]:

1. تصوير الكمبيوتر وما يتصل به من أجهزة دقيقة، وطرفية، والمحتويات التي بواسطتها أرتكبت الجرائم، مع مراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة[3].
2. العناية البالغة بملاحظة الطريقة التي أعد بها النظام وما يخلفه من آثار معلوماتية، خاصة السجلات المعلوماتية لمعرفة موقع الإتصال ونوع الجهاز[4].
3. فصل الكهرباء عن موقع المعاينة لِشل فاعلية الجاني من القيام بأي فعل من شأنه التأثير على آثار الجريمة[5].
4. اقتصار مباشرة المعاينة على فئة من المحققين ذوي الخبرة الفنية والكفاءة العلمية في مجال الكمبيوتر[6].
5. مراعاة القواعد الإجرائية لتجنب خرق مبدأ الشرعية الذي يؤدي لبطلان الدليل الرقمي[7].

2. الخبرة التقنية: وهي أيضا من أهم الأساليب التقنية التقليدية في إستخراج الدليل الرقمي. وتعرف بصفة عامة أنها المهارة المكتسبة في تخصص معين سواءً بحكم العمل في ذلك التخصص لمدة زمنية طويلة، أو عن طريق دراسات خاصة، ومنه يطلق على ذوي هذه

---

[1] هاجر طباخ، صبرينة مقلاني، **الأدلة الرقمية ودروها في الإثبات الجنائي**، مذكرة ماستر في الحقوق، تخصص إعلام آلي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2024/2023، ص: 30.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص: 172.

[3] هشام محمد فريد رستم، **الجوانب الإجرائية للجرائم المعلوماتية**، مكتبة الآلات الحديثة بأسيوط، لسنة 1994، ص: 60.

[4] خالد ممدوح إبراهيم، المرجع السابق، ص: 173.

[5] المرجع نفسه، ص: 174.

[6] حسين بن سعيد بن سيف الغافري، **السياسية الجنائية في مواجهة جرائم الأنترنت (دراسة مقارنة)**، رسالة دكتوراة في القانون الجنائي، كلية الحقوق, جامعة عين شمس، سنة 2006, ص: 356.

[7] عبد العزيز أحمد، **خصوصية التحقيق في الجريمة المعلوماتية**، مذكرة ماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق, جامعة د. مولاي الطاهر، سعيدة, 2022/2021، ص: 84.

المهارات "بالخبراء"[1]. بينما "**الخبرة القضائية**" هي إجراء للتحقيق يعهد به القاضي لشخص مختص يسمى الخبير، وذلك لدراسة واقعة أو وقائع مادية يتطلب فهمها أو إبداء رأي فني أو علمي متخصص لا يتوفر في الشخص العادي ولا يستطيع المحقق العادي الوصول إليه بمفرده[2]. وقد أولى المشرع الجزائري إهتماماً بالخبرة وإعتبرها من إجراءات الحصول على الدليل الرقمي ونظمها من المواد 143 إلى 156 قانون الإجراءات الجزائية الجزائري ، وأُسند المشرع الجزائري وفق المادة 143 من قانون الإجراءات الجزائية الجزائري ،[3] مسألة تعيين الخبير لجهات التحقيق أو الحكم بناءً على طلب من النيابة العامة أو من تلقاء نفسها أو بطلب من الخصوم، كما نصت على حماية الخبراء من أي خطر وتهديد لاسيما الجريمة المستحدثة من المواد 65 مكرر 19 الى 65 مكرر 28 قانون الإجراءات الجزائية الجزائري [4]. و تتجلى أهمية الخبير في مجال الجرائم المعلوماتية في كونه عنصرًا أساسيًا لكشف الغموض المحيط بالجريمة المعلوماتية, ففي غياب الخبير لا تستطيع الضبطية القضائية كشف الغموض، بسبب إفتقارها الكفاءة اللازمة في التعامل مع الجوانب التقنية والتكنولوجية المعقدة، مما قد يترتب عنه تدمير أو محو للدليل بسبب الإهمال[5]. ويأتي هذا إنسجامًا مع ما نصت عليه الفقرة الأخيرة من المادة 5 من القانون رقم 09-04،[6]حيث مكنت السلطات المختصة بتكليف شخص له دراية بالمنظومة المعلوماتية قصد الحصول على دلائل وكشف الجريمة. وتتجلى أهمية الخبرة في الجريمة المعلوماتية[7]، في:

1. الكشف عن الدليل الرقمي وتحديد خصائصه الفريدة.

---

[1] خالد ممدوح إبراهيم، المرجع السابق، ص: 273.

[2] محمود جمال الدين زكي، **الخبرة في المواد المدنية والتجارية: دراسة تعليمية للحكام القضاة الموضوع بندب الخبراء**، جامعة القاهرة، 1990، ص: 11.

[3] أنظر المادة 143 من قانون الإجراءات الجزائية الجزائري.

[4] أنظر المواد من 65 مكرر 19 الى 65 مكرر 28 من قانون الإجراءات الجزائية الجزائري.

[5] سعيداني نعيم، المرجع السابق، ص: 166.

[6] أنظر المادة 5/ف3 من القانون رقم: 09-04، المرجع السابق، ص: 5.

[7] خالد ممدوح إبراهيم، المرجع السابق، ص: 303/302.

2. إصلاح الدليل الرقمي وإعادة تجميعه من المكونات المادية للكمبيوتر.

3. يستخدم الخبير الخوارزميات لتأكد من أن الدليل لم يتم العبث به أو تعديله.

3. التفتيش: لم يعرف المشرع الجزائري التفتيش وتركه للفقه، وإعتبره إجراء من إجراءات التحقيق حيث نصت المادة 79 من قانون الإجراءات الجزائية الجزائري على "يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها." وكذا المادة 81 من ذات قانون على "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة." وقد كرس المشرع الجزائري التفتيش الإلكتروني للتحقيق الجنائي في الجريمة المعلوماتية بموجب المادتين 5 و 6 من قانون 09-04[1]، ويكمن الهدف من التفتيش:[2]

1. البحث عن الأدلة المتعلقة بالجريمة المعلوماتية للقبض على مرتكبيها وتقديمهم للقضاء.

2. يعد أحد إجراءات تقوية الدليل وإثبات إسناد الوقائع للمتهم أو نفيها عنه.

3. يستطيع المحقق الجنائي كشف ملابسات الجريمة من خلال التفتيش الإلكتروني وذالك بتحديد مكان، وزمان إرتكاب الجريمة، وتحديد الفاعل الأصلي، وشركائه، وكذا التعرف على الثغرات الإلكترونية والأمنية التي إستعملها الجاني ومكنته من إرتكاب الجريمة.

3.1. شروط التفتيش: لابد من مراعاة جملة من الشروط أثناء التفتيش يمكن تصنيفها إلى شروط موضوعية وأخرى شكلية[3]. بحيث تتمثل **الشروط الموضوعية في:**

1. وجود جريمة معلوماتية.

[1] انظر المادتين 5 و 6 من القانون رقم: 09-04، المرجع السابق، ص: 6.

[2] بوقرة جمال الدين، المرجع السابق، ص: 166.

[3] لعصامي أمال، بن طالب جملية، المرجع السابق، ص: 29.

2. وجود أشخاص مرتكبين للجريمة المعلوماتية أو مشاركين فيها، مع وجود قرائن تدل على وجود معدات معلوماتية لدى المتهم التي تساهم في كشف الحقيقة.

بينما الشروط الشكلية تتمثل في:

1. تسبيب الأمر بالتفتيش حيث يكون محدداً وليس شاملاً.
2. كتابة الإذن بالتفتيش في حالة الندب.
3. حضور الشخص المعني أو من ينوبه أو الشاهدان.
4. مراعاة المواعيد المحددة للتفتيش في التشريعات الإجرائية من الساعة 5:00 صباحا إلى 8:00 مساءًا، مع مراعاة الحالات الإستثنائية الواردة على سبيل الحصر في المادة 47 فقرة 2 قانون الإجراءات الجزائية الجزائري [1].

3.2. **الجزاء المترتب على عدم احترام ضوابط التفتيش:** نظم المشرع إجراء التفتيش ووضع له ضوابط يجب إتباعها صوناً للحقوق والحريات، ورتب بالمقابل البطلان على مخالفتها تكريسا لمبدأ الشرعية الإجرائية, إذ تنص المادة 48 قانون الإجراءات الجزائية الجزائري على أنه "يجب مراعاة الإجراءات المنصوص عليها في المادتين 45 و 47، ويترتب على مخالفتها البطلان". كما تؤكد المادة 44 من القانون ذاته "على بطلان التفتيش الذي يجريه عون لا يحمل صفة ضابط الشرطة القضائية، أو حال إجرائه خارج نطاق اختصاصه الإقليمي". وبالرجوع إلى أحكام المادة 05 من القانون رقم 09-04، التي أحالت بدورها إلى القواعد الإجرائية العامة، فإن أي كل مخالفة لضوابط التفتيش المذكورة يترتب عليها البطلان، فيعد التفتيش كأن لم يكن، وتسقط الأدلة المستمدة منه، ولا يمكن للمحكمة الاستناد إليها في إثبات التهمة. وأمام تشابك الحواسيب وانتشار الشبكات الداخلية والدولية، قد يمتد التفتيش إلى نظم معلوماتية أخرى غير تلك محل التفتيش، وقد يتحصل من خلالها على معلومات

[1] لعصامي أمال، بن طالب جملية، المرجع السابق، ص: 29.

تخص جهات ليست محل إشتباه. لذلك، من الضروري وجود قوانين تضبط هذه المسألة بدقة لتفادي التفتيش العام[1]، مع ضرورة تحلي المحقق الجنائي بالحيطة اللازمة أثناء أداء مهامه، واستعانته بالخبراء الفنيين عند الحاجة لتحقيق الغرض من التفتيش، مع السعي دائماً نحو تعزيز التعاون الدولي الحقيقي لتبادل الأدلة في إطارها المشروع[2].

4. **الحجز الإلكتروني:** يعد الحجز من إجراءات جمع الأدلة، وهو الهدف الرئيسي من عملية التفتيش والأثر المباشر له، ويقصد به "وضع اليد على الأشياء والمحافظة على محتوياتها لمصلحة التحقيق[3]، وتأخذ المحجوزات شكلاً مادياً عندما يتعلق الأمر بأدوات مادية مثل جهاز الحاسوب وملحقاته، الأقراص الصلبة، الطابعة، بطاقة الإئتمان، أو المعدات المستعملة في شبكة الانترنت كالمودم[4]، كما يمكن ان يشمل الحجز في البيئة الرقمية أشياء ذات طبيعة معنوية كالبيانات، المراسلات، والإتصالات الإلكترونية، وقد أثارت مسألة الحجز جدلاً فقهياً واسعاً وإختلافاً تشريعياً حول مدى إمكانية ضبط البيانات الإلكترونية[5].

4.1. **إجراءات الحجز:** نظم المشرع الجزائري عملية الحجز من خلال المادة 6 من القانون 09-04، والتي تتمكن من خلالها السلطة التي تباشر التفتيش من حجر المعطيات المفيدة في الكشف عن الجرائم و مرتكبيها[6]، وعند اكتشاف معطيات ذات صلة بالجريمة أثناء التفتيش، يجب وضعها في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية الجزائري ، مع الحرص على سلامة منظومة المعلومات محل الحجز[7]، وفي حال تعذر إجراءات الحجز

[1] بوقرة جمال الدين، المرجع السابق، ص: 180

[2] بوقرة جمال الدينن المرجع نفسه ، ص: 180.

[3] جيلالي بغدادي، **التحقيق**، الديوان الوطني للأشغال التربوية، الجزائر، ط1، 1999، ص: 152.

[4] مجدوب نوال، **الآليات الإجرائية للكشف عن الجريمة المعلوماتية**، مجلة البحوث القانونية والاقتصادية، المركز الجامعي، مغنية، الجزائر، المجلد 6، العدد 3، 2022، ص: 198.

[5] عيدة بلعابد، المرجع السابق، ص: 140.

[6] سنتير خضرة، **الآليات القانونية لمكافحة الجريمة الالكترونية**، أطروحة دكتوراة، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة احمد دراية، أدرار، 2021/2020، ص: 101.

[7] صالح شنين، **إجراءات التحري والتحقيق في جرائم تكنولوجيات الإعلام والإتصال في التشريع الجزائري القانون (09-04)**، مجلة الدراسات الحقوقية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، العدد1، 2014، ص: 283.

لأسباب تقنية، يجب على السلطة القائمة بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات أو نسخها[1]. كما يمكن للسلطة الآمرة بالتفتيش أن تأمر بإتخاذ الإجراءات المناسبة للإطلاع على المعطيات، لاسيما بتكليف شخص مؤهل لإستخدام الوسائل التقنية اللازمة لذلك[2].

4.2. الصعوبات التي تواجه المحقق في الحجز الإلكتروني:

1. ضخامة البيانات التي من الواجب فحصها.
2. الحجز أحياناً يمثل اعتداءً على حقوق الغير أو على حرمة حياتهم الخاصة مما يستوجب اتخاذ ضمانات لازمة لحماية هذه الحقوق.
3. قد توجد هذه البيانات والمعطيات في شبكات وأجهزة تابعة لدولة أجنبية مما يستدعي تعاونها مع جهات التحقيق الوطني[3].

الفرع الثاني: أساليب التحري الحديثة.

الى جانب الاساليب التقليدية نظم المشرع الجزائري أساليب حديثة تتماشى مع الجريمة المستحدثة وهذا ما سنتناوله في هذا الفرع:

1. **التسرب الإلكتروني:** اعتمد المشرع الجزائري أسلوب التسرب كأحد إجراءات التحري والتحقيق، عند تعديله لقانون الإجراءات الجزائية الجزائري بمقتضى القانون رقم 06-22[4]، حيث عرفه المشرع في المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري بقوله: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة

[1] انظر المادة 7 من القانون 09-04، المرجع السابق، ص: 7.

[2] انظر المادة 8، القانون رقم 09-04 ، ص:7.

[3] عبد العزيز احمد، المرجع السابق، ص: 91.

[4] القانون رقم: 06-22 المؤرخ في: 2006/12/20، يعدل ويتمم الأمر رقم: 66-155، يتضمن قانون الإجراءات الجزائية الجزائري، ج ر ج ج، العدد 84، الصادر بتاريخ: 2006/12/24.

بايهامهم انه فاعل معهم أو شريك لهم او خاف"[1]، ومن هذا التعريف يتبين لنا أن التسرب عملية معقدة تتطلب أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية[2]. ويمكن تصور التسرب في الجريمة المعلوماتية عن طريق ولوج ضابط أو عون الشرطة إلى العالم الإفتراضي ومشاركته في محادثات حول تقنيات إختراق شبكات الإتصال أو بث الفيروسات أو إنخراطه في مجموعات أو نوادي الهاكر، مستخدماً في ذلك أسماء

مستعارة ليظهر كأنه واحد منهم قصد الكشف عن أعمالهم الإجرامية[3].

1.1. **شروط القيام بعملية التسرب:** ولكي يكون لإجراء التسرب آثار قانونية يجب أن يتم وفق شروط شكلية وأخرى موضوعية. **تتمثل الشروط الشكلية في:**

1. الإذن القضائي وكل ما يجب أن يتضمنه من أحكام[4]، إذ لا يجوز للضابط الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من وكيل الجمهورية أو قاضي التحقيق طبقا لأحكام المادة 65 مكرر 11 قانون الإجراءات الجزائية الجزائري بقولها: "يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد اخطار وكيل الجمهورية، ان ياذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد ادناه".

[1] أنظر المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري.

[2] أنظر المادة 65 مكرر 14 الفقرة الأخيرة من قانون الإجراءات الجزائية الجزائري.

[3] براهيمى جمال، **التحقيق الجنائي قي الجرائم الالكترونية**، اطروحة دكتوراة في العلوم تخصص القانون، كلية العلوم والحقوق السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018، ص: 85.

[4] بن عنطر سيهام، المرجع السابق، ص: 97.

2. يشترط في الإذن أن يكون مكتوباً، وإلا كان هذا الإجراء باطلا، لأن الأصل في العمل الإجرائي هو الكتابي كما نصت عنه المادة 65 مكرر 15[1].

3. مدة الإذن في عملية التسرب لا يمكن ان تتجاوز 4 أشهر وهي قابلة لتجديد حسب مقتضيات التحري والتحقيق مع إصدار إذن آخر بنفس الشروط الزمنية والشكلية التي شملها الإذن الأول، غير أنه في حالة ما إذا وجد المتسرب صعوبة في الإنسحاب من الشبكة فهو يبقى لمدة قد تصل إلى ضعف المدة القانونية، ولا يمكنه الإنسحاب بنفسه فجأة من التنظيم الإجرامي دون التحضير لذلك، وإلا كان محلاً للشك[2].

في حين أن الشروط الموضوعية تكمن في:

1. كون التسرب إجراءً جديدًا وحديثًا في مجال التحري والتحقيق، فرضته ضرورات قضائية نص عليها المشرع في المادة 65 مكرر 11 قانون الإجراءات الجزائية الجزائري بأنه: "عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المنصوص عليها في المادة 65 مكرر 5 اعلاه[3]" بمعنى ان مباشرة هذا الإجراء مشروطة بوجود ضرورة ملحة لجمع البيانات والاستدلالات الجنائية، وايضا لصنف محدد من الجرائم، وعليه، فإن الدافع الأساسي لتفعيله يتمثل اولاً في الضرورة، وثانياً في طبيعة الجرائم المعنية به[4].

2. سرية عملية التسرب وهو كتمان كل سر يتعلق بالعملية، والسرية عامل يضمن عدم المساس بسلامة المتسرب من جهة، مع إبقاء النشاط الإجرامي للشبكة في سريان عادي دون أن يشك المجرم أنه تحت المراقبة من جهة اخرى، كما أن لها دور فعال في ضمان

[1] المادة 65 مكرر 15 من القانون رقم: 06-22، المرجع السابق.

[2] نصيرة بوحمزة، المرجع السابق، ص: 398.

[3] صغير يوسف، مرجع سابق، ص: 142.

[4] قريشي حمزة، **الوسائل الحديثة للبحث والتحري في ضوء القانون 06-22 (دراسة مقارنة)**، مذكرة ماجستير، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة قاصدي مرباح، ورقلة، 2012، ص: 75.

أمن وسلامة المتسرب وحسن سير العملية ،[1] ويخفي ضابط أو عون الشرطة القضائية المتسرب هويته الحقيقة وصفته أثناء القيام بالمهمة وهو عمل أجازه المشرع بنص المادة 65 مكرر16 من القانون رقم 06-22[2].

3. الجرائم التي تستدعي عملية التسرب نص عليها المشرع في المادة 65 مكرر5 من قانون 06-22 بقولها: "جرائم المخدرات أو في الجرائم المنظمة العابرة للحدود الوطنية او الجرائم الماسة بانظمة المعالجة الآلية للمعطيات او جرائم تبييض الأموال او الارهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد".

وتجدر الإشارة إلى أن هذه الجرائم المستحدثة لا تعني أنها بالضرورة حديثة، وإنما قد تكون معروفة وسائدة من قبل، لكن ثمة تغيرات كثيرة طرأت عليها سواء تعلق الأمر بنشأتها، أركانها، أو التحقيق فيها[3].

2. مراقبة الإتصالات الإلكترونية: تناول المشرع الجزائري هذا الإجراء في المادة 4 من القانون 09-04، ونص على الحالات التي تسمح باللجوء إلى الرقابة الإلكترونية.[4] بحيث ان المشرع الجزائري لم يضع تعريف لهذا الإجراء ولكن عرفه الفقه على "أن المراقبة الإلكترونية تعتمد على الإنصات والتسجيل ومحلها المحادثات الخاصة سواءً كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية واللاسلكية"[5]. ومنه،

---

[1] عنتر أسماء، **مكافحة الجرائم المستحدثة في التشريع الجزائري (التسرب نموذجاً)**، مجلة القانون العام الجزائري والمقارن، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، العدد 6، سنة 2017، ص: 79.

[2] أنظر المادة 65 مكرر16 من القانون رقم: 06-22، المرجع السابق.

[3] شيخ ناجية، **إجراء التسرب في القانون الجزائري: وسيلة لمكافحة الجرائم المستحدثة**، مجلة المعارف، جامعة البويرة، المجلد 13، العدد2، 2018، ص: 11-12.

[4] القانون رقم: 06-22، المرجع السابق.

[5] أحمد مسعود مريم، **آليات مكافحة جرائم تكنولوجيا الإعلاك والإتصال في ضوء القانون 09-04**، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013، ص: 79.

يمكن القول أن المراقبة الإلكترونية هي وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه[1]. وقد حدد المشرع الجزائري شروط الجوء لتقنية المراقبة الإلكترونية وهي:

1. وجود ضرورة تتطلب هذا الإجراء لاسيما عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الإلكترونية، وهو ما نصت عليه المادة 4 الفقرة "ج" من القانون رقم 09_04[2].

2. ان يتم تنفيذ هذه التقنية بإذن مكتوب من السلطة القضائية المختصة[3].

2.1. أشكال مراقبة الاتصالات الإلكترونية: ولها صورتان تتمثل في:

2.1.1.إعتراض المراسلات السلكية واللاسلكية: ورد ذكر إعتراض المراسلات السلكية واللاسلكية في المادة 65 مكرر 5 قانون الإجراءات الجزائية الجزائري [4]، بحيث ان المشرع الجزائري لم يقدم تعريف لهذه العملية وترك ذلك للفقه وعرفها بأنها: "إجراء تحقيقي يباشر بشكل سري، وبنتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في شكل محدد قانونا، بهدف الحصول على دليل غير مادي للجريمة، وهي بمثابة وسيلة هامة من الوسائل الحديثة للبحث والتحري تستخدمها الضبطية القضائية لمواجهة الإجرام الخطير، وتتم عبر وسائل الإتصال السلكية واللاسلكية[5]

2.1.2.اعتراض البريد الإلكتروني: يعتبر إعتراض البريد الالكتروني صورة من صور مراقبة الإتصالات الإلكترونية، ونظرًا لكونه يعتمد على شبكة الانترنت كوسيلة للتواصل فإن الطرق التقليدية لا تصلح لمراقبة البريد الالكتروني، وقد ظهرت إلى وجود أساليب

---

[1] نبيلة هروال، المرجع السابق، ص: 199.

[2] طاهر عبد المطلب، **الاثبات الجنائي لأدلة الرقمية**، مذكرة ماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2014، س: 24.

[3] انظر المادة 4 من القانون رقم: 09-04، المرجع السابق، ص: 6.

[4] أنظر المادة 65 مكرر 5 من القانون رقم: 06-22، المرجع السابق.

[5] ياسر الأمير فاروق، **مراقبة الأحاديث الخاصة في الإجراءات الجنائية**، دار المطبوعات الجامعية، الإسكندرية، ط1، 2009، ص: 150.

متطورة وقادرة على مراقبة البريد الالكتروني نذكر منها: نظام "كارنيفور" الذي تستخدمه وكالة المباحث الفيديرالية الأمريكية للتجسس[1]

3. التزامات مقدمي الخدمات:

3.1. مقدمو الخدمات: قبل مباشرة التحقيق في الجريمة المعلوماتية، يتطلب الأمر أحياناً إتخاذ بعض الإجراءات الوقائية من أجل الحفاظ على البيانات الإلكترونية المحزنة وحمايتها من التلف أو التعديل، ويكون ذلك بالزام مقدمو الخدمات بالتحفظ عليها إلى غاية تقديمها أمام السلطات المكلفة بالتحريات القضائية، وقد عرفت إتفاقية بوداست[2]، مزودو الخدمات في المادة 1 فقرة "ج" ب" "يقصد بمزود الخدمة أي كيان عام أو خاص يقدم للمستخدمين القدرة على الإتصال عن طريق نظام الكمبيوتر، وأي كيان آخر يقوم بمعالجة بيانات الكمبيوتر أو تخزينها نيابة عن مزود خدمة الإتصالات أو مستخدمي هذه الخدمة"، في حين ان المشرع الجزائري عرف مقدمو الخدمات في المادة 2 الفقرة "د" من القانون رقم 09-04 بأنها: "أي كيان عام أو خاص يقدم لمستعملى القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام الاتصالات. وأي كيام آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها"[3].

3.2. تصنيف مقدمي الخدمات: يمكن تصنيفهم إلى صنفين هما:

---

[1] تعني تسمية كارينفور بانه نظام كومبيوتري مصمم لوكالة المباحث الفيدرالية الأمريكية، وبالتعاون مع الشركة المزودة لخدمات الاترنت بتطبيق أمر محكمة بجمع معلومات محددة حول رسائل البريد الإلكتروني، أو أية اتصالات الكترونية أخرى من و الى مستخدم معين يستهدفه تحقيق ما. وتقول المباحث الأمريكية بأن اسم كارنيفور (أكلات اللحوم) وهي كلمة إنجليزية تعني أكل اللحوم، يشير إلى أن البرنامج يقوم بمضغ كافة البيانات المتدفقة عبر شبكة ما، ولكنه يقوم فعليا بالتهام المعلومات التي يسمح بها أمر المحكمة فقط. للمزيد انظر للرابطين:

.htm/ https://wwwl.epic. Org/privacy/carnivore/defalult
https://ar.wikipedia.org/wiki/كاريفوز

[2] الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، المنعقدة بمدينة بوداست، بتاريخ 2001/11/23

[3] أنظر المادة 2 من القانون رقم: 09-04، المرجع السابق، ص: 5.

1. **مقدم خدمة التوصيل:** وهو كل شخص طبيعي أو معنوي يقدم للعملاء خدمة الوصول إلى الأنترنت، حيث يزود العميل بمقتضى عقد إشتراك بالوسائل الفنية التي تمكنه من الوصول إلى الإرتباط بالشبكة والإطلاع على المواقع التي يريدها، فمهمته ذات طابع فني هو توصيل المستخدم بالشبكة العنكبوتية[1]، ويخضع مقدمو الخدمات في أنشطتهم إلى دفتر شروط محدد من قبل سلطة الضبط للبريد والمواصلات، وتوجد ثلاث شركات كبرة تهيمن في قطاع الإتصالات بالجزائر وهي شركة إتصال الجزائر "موبليس"، وشركة "جيزي"، وشركة "أوريدو" (نجمة سابقا).

2. **خدمة الإيواء:** كل شخص طبيعي أو معنوي يعهد إليه بعرض صفحات شبكة الانترنت على حاسباته الخادمة، وكان المؤجر هو متعهد الإيواء، ومحل التأجير هو الموقع على شبكة الانترنت، والمستأجر هو الذي ينشئ ما يرده من نصوص أو صور أو إنشاء روابط معلوماتية في مواقع أخرى[2] كما تجدر الإشارة إلى أن سلطة البريد والمواصلات السلكية واللاسلكية قد منحت تراخيص لعدد كبير من مزودي خدمة الانترنت ذلك لتغطية الطلب المتزايد على خدماتها، وتسهيل ولوج المستخدم اليها، وتمكن مزود الخدمة من تتبع جميع خطواته[3].

3.3. **حفظ المعطيات المتعلقة بحركة السير:** يعتبر حفظ البيانات أداء تحقيق في إطار جرائم الحاسوب والجرائم المرتبطة به، حيث تكون البيانات محلا للتلاعب، فيؤدي لضياع الدليل بسبب الإهمال في التحزين، أو حذف الدليل، لذلك يجب ان يكون المسؤول عن حفظ البيانات جدير بالثقة، ولهذا فحفظ حركة البيانات المتعلقة بالإتصالات هو أمر لازم لأنه

---

[1] عبد الفتاح بيومي حجازي، **النظام القانوني لحماية الحكومة الإلكترونية**، دار المطبوعات الجامعية، الإسكندرية، مصر، 2003، ص: 126.

[2] محمد بعجي، **التزامات مقدمي الخدمات عبر الانترنت**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 1، العدد 1، 2019، ص: 37.

[3] يزيد بوحليط، **تفتيش المنظومة المعلوماتية و حجز المعطيات في القانون الجزائري**، مجلة التواصل، المجلد 22، العدد 8، 2016، ص: 325.

هو الذي يسمح بتتبع الإتصال ومعرفة مصدره، فيكون الإجراء الأفضل من التفتيش والضبط المعلوماتي[1]. وعرف المشرع الجزائري حفظ المعطيات المتعلقة بحركة السير في المادة 2 فقرة "ه" من القانون رقم 09-04 بقوله: "اي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الإتصالات توضع مصدر الإتصال، والوجهة المرسلة إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة".

3.4. **التزامات مزود خدمات الانترنت:** يقع على عائق مزود الخدمات العديد من الإلتزامان تذكر اهمها:

1. **حفظ البيانات المتعلقة بحركة السير:** تنص المادة 11 من القانون 09-04، على مراعاة طبيعة ونوعية الخدمات، يلنزم مقدمو الخدمات بحفظ :

1.1. المعطيات التي تسمح بالتعرف على مستخدمي الخدمة.

1.2. المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.

1.3. الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال.

1.4. المعطيات المتعلقة بالخدمات التكملية المطلوبة أو المستعملة ومقدميها[2].

ومنه فإجراء الحفظ يتم بعد قيام مقدمو الخدمات بإجراء التجميع والتسجيل ثم الحفظ و ارساله للسلطات المكلفة بالتحريات القضائية، وتكتسي هذه الإجراءات أهمية بالغة كونها أداة

[1] روابح فريد، **ضمانات حرمة الحياة الخاصة أثناء إجراءات المراقبة الإلكترونية**، مجلة الأبحاث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سطيف، المجلد 2 ، العدد 2، سنة 2020، ص: 11.

[2] أنظر المادة 11 من القانون رقم: 09-04، المرجع السابق، ص: 7.

تنقيب تحري في تحديد مصدر الإتصال عن طريق أرقام الهاتف، كما توفر بيانات مرتبطة بالساعة والمدة والتاريخ المتعلق بأنواع الإتصالات غير المشروعة[1].

2.إتخاذ الاحتياطات الأمنية الكافية: من نص المادة 12 من القانون 09-04 بقولها: "زيادة على الالتزامات المنصوص عليها في المادة 11 اعلاه يتعين على مقدمي الخدمات ما يلي":

1.1. التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم، بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين أو تخزينها أو جعل الدخول إليها غير ممكن.

1.2. وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام والآداب العامة وإخبار المشتركين لديهم بوجودها.

3.الالتزام بمدة التخلص من المعطيات: بما أن حفظ المعطيات إجراء وقتي يلجأ المشرع إلى وضع التزام على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها وذلك بعد سنة إبتداءا من تاريخ التسجيل[2]، وهو ما يستفاد بمفهوم المخالفة من نص المادة 11 من القانون 09-04، "وتحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة من تاريخ التسجيل".

4.مساعدة العدالة: على مزودو الخدمات تقديم كافة البيانات التي تساهم في تحديد هوية المؤلف إلى السلطات[3]، وفي هذا السياق الزم المشرع على مزودي الخدمات بموجب المادة 11/ف1من ذات القانون بأنه: "يتعين على مقدمو الخدمات تقديم المساعدات للسلطات

---

[1] بن خليفة الهام، **الحماية الجنائية للمحررات الإلكترونية من التزوير**، اطروحة دكتوراة في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2016/2015، ص: 327.

[2] مليايني عبد الوهاب، **أمن المعلومات في بيئة الأعمال الإلكترونية**، رسالة لنيل شهادة الدكتوراة في القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2017/2016، ص: 344.

[3] مرتيز فاطمة، **الاعتداء على الحق في الحياة الخاصة عبر شبكة الانترنت** أطروحة مقدمة لنيل شهادة الدكتورة في القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة ابو بكر بلقايد ،تلمسان، 2013/2012، ص: 32/33.

المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها".

5.مسؤولية مزودو الخدمات في إهمال حفظ المعطيات: إذا أخل مزودو الخدمات بأحد الاتزامات الملقاة على عاتقه بموجب القانون 09-04، من شأنه ان يعرقل عمل السلطة المكلفة بالتحريات القضائية، فيؤدي ذلك لقيام المسؤولية الجزائية عليه، وفضلاً عن قيام المسؤولية الادارية[1]. و هو ما نصت عليه الفقرتين الاخيرتين من المادة 11 من القانون رقم 09-04[2].

المبحث الثاني: التحديات التي تواجه الدليل الرقمي ومراحل مشروعيته أمام القضاء.

يواجه الدليل الرقمي عدة تحديات في مرحلة جمعه نتيجة لطبيعته التقنية الهشة وسهولة التلاعب به، كما يشترط لاعتباره دليلًا قانونيًا احترام مراحل معينة تضمن مشروعيته. ومنه، نتناول في هذا المبحث ما يلي:

1. المطلب الأول: الصعوبات التي تواجه الدليل الرقمي.
2. المطلب الثاني: مراحل مشروعية قبول الدليل الرقمي.

المطلب الأول: المعوقات المتعلقة بالدليل الرقمي.

بما أن الدليل الرقمي يعد وسيلة أساسية لإثبات الجرائم المعلوماتية، فهو يواجه عدة صعوبات أمام سلطات التحري والتحقيق. برغم من أن المشرع الجزائري يعترف بهذا النوع من الأدلة. وعليه،

[1] مذكور عائشة، **الحماية الجنائية للعقود الإلكترونية في التشريع الجزائري**، مذكرة لنيل شهادة الماجستير في القانون، فرع قانون العقود، كلية الحقوق والعلوم السياسية، جامعة أكلى محند أولحاج، البويرة، 2018، ص:181.

[2] انظر المادة 11 الفقرتين الأخيرتين من القانون رقم: 09-04، المرجع السابق، ص: 7.

سنتناول في هذا المطلب ثلاث معوقات رئيسية: **الطبيعة الغير مرئية للدليل الرقمي، سهولة محو آثار الدليل الإلكتروني أو تعديله أو تدميره، ضخامة البيانات المراد فحصها.**

الفرع الأول: الطبيعة الغير مرئية للدليل الرقمي.

يعد عدم وجود دليل مرئي يمكن قراءته أو استيعابه من أكبر الصعوبات التي تواجه المحققين في جرائم الحاسوب بسبب أنها لا تخلف آثارا مادية توصل إلى مرتكبيها كما في الجرائم التقليدية[1]. ويتميز الدليل فيها أنه غير مرئى فهو عبارة عن نبضات إلكترونية مكونة من سلسلة من الأرقام الثنائية وتصل في حجمها وشكلها و مكان تواجدها إلى درجة شبه منعدمة وذلك ما يجعل من المستحيل الاطلاع عليها بوسائل غير تقنية تعالج هذه الذبذبات في صورة مفهومة للبشر[2].

الفرع الثاني: سهولة محو آثار الدليل الإلكتروني أو تعديله أو تدميره.

يستعمل المجرم الإلكتروني عدة أساليب وتقنيات تسمح له بإخفاء كل آثار الجريمة والتستر عليها بسهولة كبيرة، وسرعة إمكانية محو بعض التعليمات في نظام الحاسوب.

يتم محو البيانات بالكامل و بإمكانه بكبسة زر على لوحة المفاتيح أن يقوم بإلغاء الأوامر الصادرة للجهاز وهذا ما يجعل الأمر صعبا لجهات التحري في الوصول إلى الدليل الرقمي[3].

الفرع الثالث: ضخامة البيانات المراد فحصها.

إن الكم الكبير للمعلومات والبيانات المتعين فحصها من أكبر الصعوبات التي تواجه سلطات التحقيق، لذا وجب الاستعانة بخبراء فنيين في مجال الحاسب الآلي للقدرة على فحص المعلومات والبيانات الكثيرة المخزنة[4].

---

[1] عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، دار الفكر الجامعي، مصر، ط1، 2006، ص: 78.

[2] عبد الفتاح بيومي حجازي المرجع نفسه ، ص 79.

[3] بن مالك أحمد الخال إبراهيم، **دور الأدلة الرقمية في الاثبات الجنائي، مجلة العلوم الإنسانية**، جامعة تمنراست، المجلد 5، العدد 1، أفريل 2021، ص: 113/114.

[4] هاجر طباخ، صبرينة مقلاني، المرجع السابق، ص: 38.

المطلب الثاني: مراحل مشروعية الدليل الرقمي.

يعد الإثبات من التحديات التي تواجه الأجهزة الأمنية ويزداد الإثبات صعوبة في الجرائم المعلوماتية، وفي حال اكتشاف وقوع هذه الجريمة والابلاغ عنها فان إثباتها أمر يحيط به الكثير من الصعاب، مما يتطلب الكثير من الجهد والخبرة الفنية، حيث تستدعي في المقام الأول اكتشاف الجريمة المعلوماتية، ومحلها، وبيئتها ثم الإبلاغ عنها، واخذ إذن الجهات المختصة قبل القيام بالمعاينات، والتفتيش للمواقع، وذلك للبحث عن الدليل الرقمي بالطرق التقنية والفنية فالطرق التقليدية في استخلاص الأدلة يصاحبها الكثير من المشكلات العملية ويكشف التحليل العميق لهذه الطرق أن هناك بعض الخطوات يمكن إلغاؤها باستخدام نظام يقوم على تكنولوجيا المعلومات والاتصالات. وعليه، حتى يكون الدليل الرقمي مشروعاً لابد أن يمر بعدة مراحل تتمثل في كل من:

الفرع الأول: مرحلتي التحريز والتحليل.

أولا نبدأ بمرحلة التحريز حيث أنه أثناء هذه المرحلة يكون المحقق أو الخبير في وضع لا يعرف أي نوع من البيانات يمكن من خلالها الحصول على دليل جنائي رقمي وعليه الحفاظ على النظام الرقمي وكامل القيم الرقمية ليتم تحديد الضرورية منها لاستخلاص الدليل لاحقا، وكذلك يستلزم نسخ جميع البيانات المخزنة داخل الحاسب الآلي موضوع الجريمة إلى الحاسب الخاص بالمختبر الجنائي الرقمي للاعتماد عليها، بالإضافة إلى نسخ البيانات المخزنة داخل جهاز الحاسب الآلي المشكوك فيه، ثم يقدم الدليل ويعرض على المحقق للاستعانة به في عملية الاثبات[1].

[1] محمودي نور الهدى، المرجع السابق، ص: 903.

أما الأمر المهم جدا في مرحلة التحليل هو وجوب قيام الفحص والتحليل على نسخ مطابقة الأصل لعدم تغيير خصائص الملفات، حيث يتم الحفاظ بالنسخة الأصلية المضبوطة من أجل التحقيق والتدقيق على أن البيانات الموجودة مطابقة للأصل ولم يطرأ عليها أي تغيير أو حذف.

أما الهدف من وراء قيام عملية الفحص والتحليل هي استنباط ثلاثة أنواع من الأدلة:

1. دليل الإدانة، ويعد الدليل المؤكد والمستند إلى وجود فكرة معينة على ارتكاب وإسناد الجريمة محل التحقيق.
2. دليل البراءة، ويعتبر الدليل الذي يخالف فكرة ارتكاب الجريمة موضوع التحقيق.
3. دليل محايد، وهو الدليل غير المرتبط لا بالإدانة ولا بالبراءة، بل يستعان به في إثبات أنه لم يطرأ أي تعديل أو تغيير في النظام الرقمي للحاسب الآلي لاستبعاد استخدام محتوياته أو الاستعانة به كدليل.[1]

الفرع الثاني: مرحلتي العرض والقبول.

مرحلة العرض يتم من خلالها تقديم وعرض النتائج التي تم التوصل إليها عن طريق التحقيقات والفحص والتحليل الفني إلى جهة المحكمة المختصة، ويطبق على عملية هذه المرحلة النظام الجنائي المطبق في تلك الدولة ويستلزم الأمر موثوقية الأدلة الجنائية الرقمية لضمان مصداقيتها، حيث أنه يمكن توثيق الأدلة الجنائية الرقمية بالعديد من الوسائل المختلفة منها التصوير الفوتوغرافي التصوير بالفيديو والقيام بنسخ الملفات المخزنة في الأقراص أو في الحاسب الآلي. كما يستوجب أيضا تدوين التاريخ والوقت وتوقيع الشخص الذي قام بإجراء الحفظ عند حفظ الأدلة الرقمية، بالإضافة إلى اسم ونوع نظام التشغيل والمعلومات المسجلة في الملف المحفوظ وقسم البرنامج أو الأوامر التي استعملت في إعداد النسخ.

[1] عبد المطلب، ممدوح عبد الحميد، **البحث والتحقيق الجنائي الرقمي في الكومبيوتر والأنترنت**، دار الكتب القانونية، مصر، 2006، ص: 90.

أما مرحلة قبول الأدلة الجنائية الرقمية في الإثبات موقوف إلى مدى توافر هذا الدليل في النصوص القانونية بالنسبة لنظام الإثبات المحدد، وإلى مدى اقتناع القاضي الجنائي بالدليل الرقمي بالنسبة لنظام الأدلة الإقناعية[1].

وحتى يقتنع القاضي بالدليل الرقمي لابد أن تتوفر شروط تتمثل أساسا في:

1. لابد أن تكون هذه الأدلة يقينية تقترب للحقيقة الواقعية.
2. طبقا للمادة 212 من قانون الإجراءات الجزائية الجزائري ، فانه: "لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له أثناء المرافعات أو التي حصلت فيها المناقشة حضوريا، أي أنه يتم معاينة هذا الدليل شفويا[2].
3. يجب أن يكون الدليل الرقمي مشروعا أي أن طريقة الحصول على الدليل الرقمي تكون وفق الإجراءات المحددة بموجب القانون وإلا كان باطلا.[3]

[1] عبد المطلب، ممدوح عبد الحميد ، المرجع السابق ص ـ ص: 88/87.

[2] أمينة لميز ، الدليل **الرقمي كآلية لإثبات الجرائم المعلوماتية**، مجلة بحوث في القانون والتنمية، جامعة امحمد بوقرة بومرداس، الجزائر ، المجلد 2، العدد 3، سنة 2023، ص: 16.

[3] محمودي نور الهدى، المرجع السابق، ص: 920/919.

خلاصـــة الفصل الثـــاني:

بعد تحليل معمّق للفصل الثاني، تبيّن أن تطور التكنولوجيا أفرز نوعًا جديدًا من وسائل الإثبات، وهو الدليل الرقمي، الذي أصبح ضرورة في مكافحة الجرائم السيبرانية. وقد تم التطرق إلى مفهومه وخصائصه، ومميزاته المختلفة عن الدليل التقليدي، لا سيما طبيعته اللامادية وقابليته للتعديل أو المحو، مما يستدعي ضوابط دقيقة لضمان مصداقيته القانونية.

كما عالجنا بشكل مفصل أساليب التحري الخاصة في جمعها وفق التشريع الجزائري، حيث لم يكتفِ المشرع بالوسائل التقليدية كالمعاينة والتفتيش، بل استحدث آليات خاصة لمواكبة التحول الرقمي، من بينها التسرب الإلكتروني، اعتراض المراسلات، والتقاط الصور، وهي وسائل ذات طابع حساس تتطلب إذنا قضائيًا، لما تنطوي عليه من مساس بالحقوق الدستورية كسرية الحياة الخاصة.

أما عمليًا، تواجه السلطات عدة تحديات أبرزها: صعوبة الوصول للبيانات، استعمال أدوات تشفير متطورة، وانتشار برامج التخفي مثل VPN وTOR، فضلًا عن امتداد البيانات إلى خوادم أجنبية، ما يثير إشكاليات الاختصاص ويستدعي تعاونًا دوليًا فعالًا.

وقد تم التأكيد على أن قبول هذا الدليل أمام القضاء يمر بسلسلة من الإجراءات الدقيقة (التحريز، التحليل، التقديم)، ويخضع لتقدير القاضي وفق مبدأ القناعة الشخصية، مع ضرورة خلوه من العيوب الشكلية.

ختامًا، يبقى تطوير المنظومة القانونية، وتكوين الكفاءات المختصة، وتعزيز التعاون الدولي، من الركائز الأساسية لضمان فعالية التحقيق دون الإخلال بضمانات المحاكمة العادلة.

خـــاتـــمة

خـــــاتمــة:

ختامًا لهذه الدراسة المعنونة بـ"خصوصية التحقيق الجزائي في الجريمة المعلوماتية"، يتضح أن الجريمة المعلوماتية لم تعد مجرد ظاهرة إجرامية عابرة أو محلية، بل تمثل تحديًا قانونيًا وأمنيًا دوليًا جِسيمًا، يُهدد أُسس النظام القانوني والاجتماعي والاقتصادي، نظرًا لطبيعتها التقنية وتعقيداتها العابرة للحدود الوطنية.

وقد أكدت الدراسة على أن خصوصية هذه الجريمة تقتضي تكييفًا دقيقًا وشاملًا للإجراءات القانونية للتحقيق، بما يشمل جمع الأدلة الرقمية بمهنية عالية، وتوفير سرعة استجابة قانونية وتقنية، إضافة إلى تفعيل آليات التعاون القضائي والعدلي الدولي، لضمان فاعلية المحاكمة وملاحقة الجناة دون تأخير.

رغم أن الجزائر لم تنضم بعد إلى اتفاقية بودابست لعام 2001 المتعلقة بالجريمة المعلوماتية، إلا أن القانون رقم 24-06 المؤرخ في سنة 2024، الذي يعدّل ويتمّم الأمر رقم 66-156 المتضمن قانون العقوبات، يوفّر إطارًا قانونيًا لتنظيم الإجراءات القضائية ذات الصلة ومكافحة الجرائم السيبرانية. ويعكس هذا التعديل سعي الجزائر إلى ملاءمة تشريعاتها الوطنية مع المتطلبات التقنية والمعايير الدولية في مجال مكافحة الجريمة المعلوماتية.

وتحمل الدراسة الهيئات القضائية والضبطية القضائية المختصة مسؤولية كبرى في تطوير كفاءاتها التقنية والقانونية، وتلقي الدعم الفني والتدريبي المستمر، من أجل التعامل مع التحديات المستجدة التي تفرضها الجرائم السيبرانية، مع احترام صارم لحقوق الإنسان والحريات المكفولة.

ويعد تفعيل التعاون الدولي القضائي والعدلي، وتيسير تبادل المعلومات التقنية والخبرية، ركيزة أساسية لا يمكن الاستغناء عنها لمواجهة الطبيعة العابرة للحدود لهذه الجرائم، الأمر الذي يستوجب انخراطًا حازمًا للجزائر في الاتفاقيات والبروتوكولات الدولية.

وعليه، فإن ضمان فعالية التحقيق الجزائي في الجرائم المعلوماتية مرهون بإرادة سياسية قوية، ورؤية قانونية واضحة، وتنفيذ عملي متين، يوازن بين حماية الأمن السيبراني وضمانات المحاكمة العادلة، وهو ما يُعد شرطًا حتميًا لاستدامة دولة القانون في العصر الرقمي.

انطلاقًا من ما توصلت إليه الدراسة، **نوصي بما يلي:**

1. استحداث إجراءات قانونية متخصصة تتلاءم مع خصوصية التحقيق في الجرائم المعلوماتية، تشمل أساليب جمع الأدلة الرقمية وحفظها ومعالجتها، لضمان سلامة الإجراءات وموثوقية النتائج.
2. تطوير قدرات الجهات القضائية والتنفيذية من خلال برامج تكوين مستمرة ومتخصصة في مجال تقنيات المعلومات والأمن السيبراني، مع التركيز على القضاة، ورجال الشرطة القضائية، والخبراء التقنيين.
3. تجهيز الهيئات القضائية والتقنية بمعدات حديثة تسمح بتحليل البيانات الرقمية بكفاءة عالية، وتقليل زمن الاستجابة للتحقيقات المعقدة.
4. تعزيز آليات التعاون الدولي عبر الانضمام الفعلي إلى الاتفاقيات الدولية المعنية بمكافحة الجريمة المعلوماتية، وعلى رأسها اتفاقية بودابست، لتسهيل تبادل المعلومات والمساعدات القضائية التقنية.
5. تنظيم حملات توعية قانونية وتقنية لفائدة المجتمع، تبرز خطورة الجريمة المعلوماتية وطرق الوقاية منها، مما يسهم في بناء بيئة رقمية آمنة.
6. تفعيل دور الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي لتكون شريكًا فعالًا في التحقيقات الرقمية، وضمان حماية خصوصية البيانات، وتقديم الاستشارات التقنية والقانونية.

7. مراجعة دورية للإطار القانوني والتشريعي لضمان ملاءمته مع التطورات التقنية المستمرة، وتأمين إطار قانوني مرن قادر على استيعاب المستجدات والتحديات الجديدة.

8. التوازن الدقيق بين الأمن الرقمي وحماية الحقوق والحريات، عبر وضع ضوابط واضحة تمنع التجاوزات في جمع الأدلة الرقمية، وتحترم الحقوق الدستورية للمشتبه بهم والمتهمين.

"خِتاماً أُنجز هذا البحث بعون الله وتوفيقه"

"كما قال تعالى: ﴿وَقُل رَّبِّ زِدْنِي عِلْمًا﴾ [طه: 114]"

"راجين من الله القبول والسداد."

قائـمة المصادر و المراجع

أولاً/ المـــــصادر:

ـ الـقواميس والمعجم.

1. علي بن محمد السيد الشريف الجرجاني، معجم التعريفات، دار الفضيلة.
2. محمد بن يعقوب الفيروز، آبادي مجد الدين، قاموس المحيط، دار الحديث، القاهرة.

ـ الإتفاقيات والمعاهدات.

1. إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطن معتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة بتاريخ 2000/11/15, صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 2002/02/05 ج ر ج ج, العدد9, الصادرة في 20002/02/10.
2. اتفاقية بودابست، المتعلقة بالجريمة السيبيرانية، مجلس أوروبا, مجموعة المعاهدات الأوروبية, رقم185، المؤرخة في 2001/11/23.

ـ الأوامر.

1. الأمر رقم21-11 المؤرخ في 2021/08/25 المعدل و المتمم للأمر رقم 66-155 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية الجزائري، ج ر ج ج، العدد65، الصادر في 2021.
2. الأمر رقم 66-155 المؤرخ في 1966/06/8، يتضمن قانون الإجراءات الجزائية الجزائري، المعدل والمتمم، ج ر ج ج، العدد48، 1966، المعدل والمتمم بموجب القانون رقم 17-07، المؤرخ في2017/03/27، ج ر ج ج، العدد 48، الصادر في 2017.

- القوانين.

1. القانون رقم 04-15 المؤرخ في 2004/11/10، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 1966/06/8، المتضمن قانون العقوبات، ج ر ج ج، العدد71، الصادر في 2004/11/10.

2. القانون رقم 06-22 المؤرخ في 2006/12/20، يعدل ويتمم الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية الجزائري، ج ر ج ج، العدد84، الصادر في 2006/12/24.

3. القانون رقم 08-09 المؤرخ في 2008/02/25، يتضمن قانون الإجراءات المدنية والإدارية، ج ر ج ج، العدد21، 2008.

4. القانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج ر ج ج، العدد47، الصادر في 2009/08/16.

5. القانون رقم 15-12 المؤرخ في 2015/07/15، المتعلق بحماية الطفل، ج ر ج ج، العدد 39، الصادر في 2015/07/19.

- المراسيم.

1. لمرسوم الرئاسي رقم 04-183 المؤرخ في 2004/06/26 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر ج ج، العدد41، 2004.

2. المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/5، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر ج ج، العدد63، الصادر في 2006/10/8.

3. المرسوم الرئاسي رقم 09-143 المؤرخ في 2009/04/27 المتضمن مهام الدرك الوطني وتنظيمه، ج ر ج ج، العدد 26، 2009.

4. المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/8، يحدد تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، ج ر ج ج، العدد37، الصادر في 2015.

5. المرسوم الرئاسي رقم 19-172 المؤرخ في 2019/07/6، المتضمن تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والإتصال ومكافحته وتنظيمها وكيفيات سيرها، ج ر ج ج، العدد37، 2019.

6. المرسوم الرئاسي رقم 20-05 المؤرخ في 2020/01/20 المتضمن وضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر ج ج ، العدد4، الصادرة في 2020/01/21.

7. المرسوم الرئاسي رقم 20-183، المؤرخ في 2020/07/13 يتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الاغلام و الاتصال و مكافحته، ج ر ج ج, العدد40، الصادر في 2020/07/18.

8. المرسوم الرئاسي رقم 21-439 المؤرخ في 2021/11/7 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته، ج ر ج ج، العدد 86، سنة 2021.

ثانياً/ المــراجــع:

ـ الكتب.

1. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار الهومة للطباعة والنشر والتوزيع، الجزائر، ط11، 2012.

2. أحسن بوسقيعة، الوجيز في قانون جنائي العام، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط11، 2014.

3. اسامة أحمد مناعة وجلال محمد زغبي، جرائم تقنية نظم المعلومات الإلكترونية، دار النشر والتوزيع، عمان، ط3، 2014.

4. امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للنشر والتوزيع، الجزائر، ط3، 2007.

5. براهيمي محمد ظاهر، تنظيم التحقيق الإبتدائي في الجرائم، دار النشر، عمان، الأردن، ط1، 2013.

6. جيلالي بغدادي، التحقيق، الديوان الوطني للأشغال التربوية، الجزائر، ط1، 1999.

7. الديربي عبد العال، صادق إسماعيل محمد، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012.

8. عادل عزام، سقف الحيط جرائم الذم والقدح والتحقير المرتكبة في الوسط الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، الاردن، ط1، 2001.

9. عادل محمد أمين نائلة، جرائم الحاسب الآلي الأقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2005.

10. عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2003

11. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، ط1، 2006.

12. عبد المطلب، ممدوح عبد الحميد، البحث والتحقيق الجنائي الرقمي في الكومبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006.

13. على حسن الطوالبة، الجرائم الإلكترونية، مؤسسة فخراوي للدراسات والنشر، البحرين، ط1، 2008.

14. علي شملال، الجديد في شرح قانون الإجراءات الجزائية، الكتاب الاول، الإستدلال والإتهام، دار هومة، ط3، دون سنة، ص: 14.

15. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر، 2010.

16. علي عبود جعفر، جرائم تكنولوجيات المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحلبية والأدبية، لبنان، ط1، 2013.

17. عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، الجزائر، 2021.

18. فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة المجديدة، الإسكندرية، 2016.

19. لينا محمد الأسدي، مدى فاعلية احكام القانوم الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، دار الحامد للنشر والتوزيع، الأردن، ط1، 2015.

20. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، دار الحامد للنشر والتوزيع، عمان، الأردن، ط1، 2014،

21. محمد أمين أحمد شوابكة، جرائم الحاسب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2004.

22. محمد بكرار شوش، الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري، دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، العدد 14، 2016.

23. محمد حزيط، أصول الإجراءات الجزائية في القانون الجزائري، دار بلقيس للنشر، الجزائر، ط3، 2022.

24. محمد طارق عبد الرؤوف الخن، جريمة الإحتيال عبر الأنترنت الأحكام الموضوعية والإجرائية، منشورات الحلبي الحقوقية، لبنان، ط1، 2011.

25. محمود جمال الدين زكي، الخبرة في المواد المدنية والتجارية: دراسة تعليمية للحكام القضاة الموضوع بندب الخبراء، جامعة القاهرة، 1990.

26. موسى مطصفى محمد، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ط1، 2009.

27. موسى مطصفى محمد، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ط1، 2009.

28. نائلة عادل محمد قورة، جرائم الحاسب الآلي الإقتصادية (دراسة نظرية وتطبيقية)، منشورات الحلبي الحقوقية، بيروت، 2005.

29. نائلة عادل محمد قورة، جرائم الحاسب الآلي الإقتصادية (دراسة نظرية وتطبيقية)، منشورات الحلبي الحقوقية، بيروت، 2005.

30. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

31. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة بأسيوط، 1994.

32. وضاح محمود حسنات ونشأت مفضي المجالي، جرائم الأنترنت، دار المنار للنشر، عمان، 2005.

33. ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، ط1، 2009.

34. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2019.

35. يوسف حسين يوسف، الجريمة الدولية للأنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، ط1، 2001.

ـ الأبحاث الاكاديمية.

1. أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلاك والإتصال في ضوء القانون 09-04، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013.

2. اسماعيل بن يحيى، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراة علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة ابي بكر بلقايد، تلمسان، 2021/2020.

3. بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة المعلوماتية، مذكرة ماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمحد بوضياف، المسيلة، الجزائر, 2013/2014.

4. براهيمى جمال، التحقيق الجنائي قي الجرائم الالكترونية، اطروحة دكتوراة في العلوم تخصص القانون، كلية العلوم والحقوق السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018.

5. بن خليفة الهام، الحماية الجنائية للمحررات الإلكترونية من التزوير، اطروحة دكتوراة في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2016/2015.

6. بوقرة جمال الدين، التحقيق الجنائي في الجريمة المعلوماتية، اطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية جامعة محمد بوضياف، المسيلة، 2025/2024.

7. حسين بن سعيد بن سيف الغافري، السياسية الجنائية في مواجهة جرائم الأنترنت (دراسة مقارنة)، رسالة دكتوراة في القانون الجنائي، كلية الحقوق, جامعة عين شمس، 2006.

8. حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016/2015.

9. حورية خليصة، حمزة فيروز، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي.

10. رجاء امدور، خصوصية التحقيق في مواجهة الجريمة المعلوماتية، أطروحة دكتوراة، تخصص قانون خاص، قسم الحقوق، جامعة محمد البشير الإبراهيمي، كلية الحقوق والعلوم السياسية، برج بوعريريج، 2021/2020.

11. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق، جامعة لحاج لخضر، باتنة، 2013/2012.

12. سنتير خضرة، الآليات القانونية لمكافحة الجريمة الالكترونية، أطروحة دكتوراة، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة احمد دراية، أدرار، 2021/2020.

13. طاهر عبد المطلب، الاثبات الجنائي لأدلة الرقمية، مذكرة ماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2014.

14. عبد العزيز أحمد، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة ماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق, جامعة د. مولاي الطاهر، سعيدة, 2022/2021.

15. عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، القانون العام، جامعة الشرق الأوسط، عمان، الأردن، 2014.

16. غربي جميلة، آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، تخصص قانون جنائي، قسم القانون العام، جامعة أكلي محمد أولحاج، البويرة، 2021/2020.

17. قريشي حمزة، الوسائل الحديثة للبحث والتحري في ضوء القانون 06-22 (دراسة مقارنة)، مذكرة ماجستير، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة قاصدي مرباح، ورقلة، 2012.

18. لعصامي آمال، بن طالب جميلة، حجية الدليل الإلكتروني في الإثبات الجنائي وفق التشريع الجزائري، مذكرة ماستر في الحقوق، تخصص قانون جنلئي، كلية الحقوق والعلوم السياسية، جامعة د. مولاي الطاهر، سعيدة، سنة 2022/2021.

19. مذكور عائشة، الحماية الجنائية للعقود الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة أكلى محند أولحاج، البويرة، 2018.

20. مرتيز فاطمة، الاعتداء على الحق في الحياة الخاصة عبر شبكة الانترنت أطروحة مقدمة لنيل شهادة الدكتورة في القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة ابو بكر بلقايد ،تلمسان، 2013/2012.

21. ملياني عبد الوهاب، أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة لنيل شهادة الدكتوراة في القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2017/2016.

22. نصيرة بوحمزة، التحقيق الجنائي في الجريمة الإلكترونية (دراسة مقارنة)، اطروحة دكتوراة، تخصص القانون الخاص، قسم الحقوق، كلية الحقوق والعلوم السياسية، جماعة الجيلالي اليابس، سيدي بلعباس، 2022/2021.

23. هاجر طباخ، صبرينة مقلاني، الأدلة الرقمية ودروها في الإثبات الجنائي، مذكرة ماستر في الحقوق، تخصص إعلام آلي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2024/2023.

24. هبة نبيلة هروال، جرائم الأنترنت (دراسة مقارنة)، أطروحة دكتوراة، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013

25. هروال أية نور الهدى، الأدلة الرقمية في إثبات الجريمة المعلوماتية، مذكرة ماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، 2020/**2021**.

26. يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة ماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2017/2016.

ـ المقالات والمؤتمرات.

1. حمزة خضري، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، الجزائر، المجلد6، العدد2، 2020.

2. أمينة لميز، الدليل الرقمي كآلية لإثبات الجرائم المعلوماتية، مجلة بحوث في القانون والتنمية، جامعة امحمد بوقرة بومرداس، الجزائر، المجلد 2، العدد3، 2023.

3. بن مالك أحمد الخال إبراهيم، دور الأدلة الرقمية في الاثبات الجنائي، مجلة العلوم الإنسانية، جامعة تمنراست، المجلد 5، العدد1، 2021.

4. روابح فريد، ضمانات حرمة الحياة الخاصة أثناء إجراءات المراقبة الإلكترونية، مجلة الأبحاث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سطيف، المجلد2، العدد2، 2020.

5. يزيد بوحليط، تفتيش المنظومة المعلوماتية و حجز المعطيات في القانون الجزائري، مجلة التواصل، المجلد 22، العدد 8، 2016.

6. محمد بعجي، التزامات مقدمي الخدمات عبر الانترنت، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 1، العدد 1، 2019.

7. شيخ ناجية، إجراء التسرب في القانون الجزائري: وسيلة لمكافحة الجرائم المستحدثة، مجلة المعارف، جامعة البويرة، المجلد 13، العدد2، 2018.

8. عنتر أسماء، مكافحة الجرائم المستحدثة في التشريع الجزائري (التسرب نموذجاً)، مجلة القانون العام الجزائري والمقارن، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، العدد 6، سنة 2017.

9. صالح شنين، إجراءات التحري والتحقيق في جرائم تكنولوجيات الإعلام والإتصال في التشريع الجزائري القانون (09-04)، مجلة الدراسات الحقوقية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، العدد1، 2014.

10. مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، المركز الجامعي، مغنية، الجزائر، المجلد 6، العدد 3، 2022.

11. عيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بأفلو، الأغواط، جامعة د. مولاي الطاهر، سعيدة، المجلد4، العدد 6، مارس 2021.

12. بن فريدة محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)، مجلة الباحث للدراسات الأكادمية، كلية الحقوق والعلوم السياسية، جامعة بجاية، الجزائر، المجلد4، العدد2، جوان 2017.

13. صابر بحري ومنى خرموش، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية، مجلة الدراسات في سيكولوجية الإنحراف، الجزائر، العدد1، 2021.

14. عبير بعقيقي، فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04، مجلة العلوم القانونية والسياسية، جامعة محمد خيضر، بسكرة، الجزائر، المجلد9، العدد2، جوان 2018.

15. خطوي المسعود، خصوصية الدليل الإلكتروني، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي، الأغواط، المجلد7، العدد1، سنة 2023.

16. نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكادمية، جامعة باتنة1، المجلد4، العدد2، جوان 2017.

17. سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، المجلد7، العدد1، جوان 2021 .

18. نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكادمية، جامعة باتنة1، المجلد4، العدد2، جوان 2017.

19. عماد بلغيث ويوسف جغلولي، صعوبات التحقيق في الجرائم المعلوماتية، مجلة الرسالة للدراسات والبحوث الإنسانية، مخبر سوسيولوجية جودة الخدمة المعلوماتية، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد 6، العدد 3، سبتمبر 2021.

20. نورة بن بوعبد الله، الاختصاص القضائي الموسع في المادة الجزائية وفق القانون الجزائري، مجلة الفكر القانوني والسياسي، االجامعة الحاج لخضر، باتنة1، المجلد 6، العدد 1، 2022.

21. إسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 14، سبتمبر 2018.

22. بوقرة جمال الدين، عنان جمال الدين، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، مجلة الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 7، العدد 1، جوان 2022.

23. فاطمة الزهراء عون، الإجراءات التشريعية المستحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري – القطب الجزائي الوطني نموذجًا، مجلة حقوق الإنسان والحريات العامة، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، المجلد7، العدد2، 2022/12/26.

ـ الندوات والمؤتمرات.

1. سيناء عبد الله محسن، المواجهة التشرعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية و الوطنية، الندوة الأقليمية حول الجرائم المتصلة بالكومبيوتر، الدار البيضاء، المملكة المغربية، 2007.

2. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر الجرائم الإلكترونية، طرابلس، 2017.

ـ المحاضرات.

1. سعاد أجعود، محاضرات في مقياس الإجراءات، قدمت لطلبة السنة الثانية ليسانس، مطبوعة بيداغوجية، الإجراءات الجزائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تبسة، 2022.

2. عبد الرحمان خلفي، محاضرات في الإجراءات الجزائية موجهة لطلبة السنة الثانية ل.م.د. كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2017/2016.

3. عبد الرحمان خلفي، محاضرات في القانون الجنائي العام (دراسة مقارنة)، دار الهدى، الجزائر، 2012.

ـ المواقع الإلكترونية.

1. **www//:https://ar.wikipedia.org/**كارنيفور.

الفهرس

الفهرس	الصفحة
مقدمة	8-1
الأحكام العامة للتحقيق في الجريمة المعلوماتية.	
تمهيد الفصل الأول :	10
المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية.	11
المطلب الأول: مفهوم الجريمة المعلوماتية.	11
الفرع الأول: تعريف الجريمة المعلوماتية.	11
الفرع الثاني: خصائص الجريمة المعلوماتية وأركانها.	14
الفرع الثالث: تصنيفات الجريمة المعلوماتية.	17
المطلب الثاني: أطراف الجريمة المعلوماتية.	19
الفرع الأول المجرم المعلوماتي.	20
الفرع الثاني: دوافع الإجرام المعلوماتي.	22
الفرع الثالث: الضحية في الجريمة المعلوماتية.	24
المبحث الثاني: الجهات القضائية المختصة بالتحقيق في الجرائم المعلوماتية.	26
المطلب الأول: جهات التحقيق القضائية في الجريمة المعلوماتية.	26
الفرع الأول: إختصاصات قاضي التحقيق في الجريمة المعلوماتية.	26
الفرع الثاني: إختصاص الضبطية القضائية.	30

الفرع الثالث: صعوبات التحقيق في الجريمة المعلوماتية.	**34**
المطلب الثاني: الأجهزة المتخصصة بالتحقيق على المستوى الدولي و الوطني.	**35**
الفرع الأول: الأجهزة المختصة على المستوى الوطني.	**35**
الفرع الثاني: على المستوى الدولي.	**42**
خـلاصة الفصـل الأول:	**45**
الدليل الرقمـي ومـراحل مشروعيـته أمـام القـضاء.	
تمهيد الفصل الثاني	**48**
المطلب الأول: مفـهوم الدليل الرقمـي.	**49**
الفرع الأول: تعريف الدليل الرقمي.	**49**
الفرع الثاني: خصائص الدليل الرقمي والتمييز بينه وبين الدليل التقليدي.	**49**
المطلب الثاني: أساليب التحري الخاصة التقليدية والحديثة في التشريع الجزائري.	**50**
الفرع الأول: أساليب التحري التقليدية.	**52**
الفرع الثاني: أساليب التحري الحديثة.	**59**
المبحث الثاني: التحديات التي تواجه الدليل الرقمي ومراحل مشروعيته أمام القضاء.	**68**
المطلب الأول: المعوقات المتعلقة بالدليل الرقمي.	**68**
الفرع الأول : الطبيعة الغير مرئية للدليل الرقمي	**69**

الفرع الثاني: سهولة محو آثار الدليل الإلكتروني أو تعديله أو تدميره.	**69**
الفرع الثالث: ضخامة البيانات المراد فحصها.	**69**
المطلب الثاني: مراحل مشروعية الدليل الرقمي.	**70**
الفرع الأول: مرحلتي التحريز والتحليل.	**70**
الفرع الثاني: مرحلتي العرض والقبول.	**71**
خلاصــة الفصل الثـاني	**73**
خاتمة	**75**
مصادر ومراجع	**79**
الفهرس	**94**
ملخص	

الملخص:

تُمثل الجريمة المعلوماتية تحديًا قانونيًا وواقعًا متطورًا يستلزم معالجة دقيقة ضمن إطار التحقيق الجزائي، لما تنفرد به من طبيعة تقنية معقدة ووسائل تنفيذ غير تقليدية. وقد اقتضى ذلك إعادة النظر في المفاهيم الكلاسيكية للجريمة، من خلال ضبط تعريفها وبيان أركانها وخصائصها، وتحديد أطرافها من فاعل وضحية، مع الوقوف على الدوافع التي تُحرك مرتكبها.

ويُعد التحقيق في هذا النوع من الجرائم من المسائل الحساسة التي تستوجب تدخل جهات قضائية متخصصة، أبرزها قاضي التحقيق والضبطية القضائية، ضمن حدود الصلاحيات المخولة قانونًا، مع مراعاة صعوبات الواقع الرقمي الذي يُعقّد من مهام البحث والتحري. كما يُطرح التعاون القضائي والتقني، على المستويين الوطني والدولي، كضرورة ملحة لمواجهة الطبيعة العبر وطنية لهذا النمط من الإجرام.

ويشكل الدليل الرقمي محورًا جوهريًا في إثبات الجريمة المعلوماتية، نظرًا لخصوصيته التقنية، وما يتطلبه من إجراءات دقيقة تضمن حجيته أمام القضاء، سواء في مراحل جمعه وتحريزه أو تحليله وتقديمه للمحكمة، مع ضرورة احترام المبادئ القانونية الناظمة لمشروعية الدليل، حمايةً للحقوق والحريات.

بناءً على ما تقدم، يظهر جليًا أن التصدي الفعّال للجريمة المعلوماتية يفرض تطويرًا مستمرًا في آليات التحقيق، وتكاملًا بين الجوانب القانونية والتقنية، بما يُحقق الأمن القانوني ويضمن النجاعة القضائية في بيئة رقمية متغيرة.

الكلمات المفتاحية:

الجريمة المعلوماتية، التحقيق الجزائي، الدليل الرقمي، قاضي التحقيق، الضبطية القضائية، التحري الإلكتروني، الأدلة الرقمية، الخصوصية القانونية، التعاون الدولي، الأمن السيبرانيني.

Abstract:

Cybercrime represents a legal challenge and an evolving reality that requires careful handling within the framework of criminal investigation, due to its complex technical nature and unconventional methods of execution. This has necessitated a re-evaluation of classical crime concepts by defining cybercrime, identifying its elements and characteristics, determining the parties involved — both perpetrator and victim — and examining the motives driving the offender.

Investigating this type of crime is a sensitive matter that requires the intervention of specialized judicial authorities, most notably the investigating judge and judicial police, within the bounds of their legally granted powers, while taking into account the challenges posed by the digital environment, which complicates search and investigation tasks. Judicial and technical cooperation at both national and international levels also emerges as a pressing necessity, given the transnational nature of this form of crime.

Digital evidence forms a central axis in proving cybercrime, owing to its technical specificity and the need for precise procedures that ensure its admissibility in court, whether during its collection, preservation, analysis, or presentation. All of this must be done while respecting the legal principles governing the legitimacy of evidence, in order to safeguard rights and freedoms.

In light of the above, it is evident that effectively combating cybercrime requires continuous development of investigative mechanisms, as well as integration between legal and technical aspects to achieve legal security and ensure judicial efficiency in a constantly changing digital environment.

Keywords:

Cybercrime, criminal investigation, digital evidence, investigating judge, judicial police, electronic investigation, digital forensics, legal privacy, international cooperation, cybersecurity