جامعة قاصـــــدي مرباح ـ ورقلة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر أكاديمي

الميدان: الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص : قانون جنائي وعلوم جنائية

عنوان المذكرة

التحقيق الرقمي في مواجهة جرائم الفضاء الالكتروني

من إعداد الطالبتين :

قسوم رحاب

صالحي تسنيم

إشراف الاستاذ :

أ. بن فردية محمد

أعضاء لجنة المناقشة :

الاسم و اللقب	الرتبة العلمية	الصفة
نجاة صالحي	أستاذ محاضر قسم ب	رئيساً
محمد بن فردية	أستاذ التعليم العالي	مشرفاً
ياسين بن عمر	أستاذ محاضر قسم ب	مناقشاً

السنة الجامعية : 2025 – 2026

جامعة قاصـــــدي مرباح ـ ورقلة
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر أكاديمي

الميدان: الحقوق والعلوم السياسية

الشعبة : الحقوق

التخصص : قانون جنائي وعلوم جنائية

عنوان المذكرة

التحقيق الرقمي في مواجهة جرائم الفضاء الالكتروني

من إعداد الطالبتين :

قسوم رحاب

صالحي تسنيم

إشراف الاستاذ :

أ. بن فردية محمد

أعضاء لجنة المناقشة :

الاسم و اللقب	الرتبة العلمية	الصفة
نجاة صالحي	أستاذ محاضر قسم ب	رئيساً
محمد بن فردية	أستاذ التعليم العالي	مشرفاً
ياسين بن عمر	أستاذ محاضر قسم ب	مناقشاً

السنة الجامعية: 2025 – 2026.

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة قاصدي مرباح ورقلة

التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لانجاز بحث

(ملحق القرار الوزاري رقم 1082 المؤرخ 27 ديسمبر 2020 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها)

أنا المدعي أسفله،

إسم ولقب الطالب	التخصص	رقم بطاقة التعريف الوطنية	تاريخ الاصدار
1. شوم رحاب	قانون جنائي	100310890346 0008	2023.06.27
2. صالحي تسنيم	قانون جنائي	110031089002840000	2024.09.30

المسجل (ة) بكلية الحقوق والعلوم السياسية بورقلة قسم الحقوق

و المكلف (ة) بانجاز أعمال بحث مذكرة ماستر، عنوانها:

التحقيق الابتدائي في جريمة جرائم الفضاء الالكتروني

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

التاريخ: 16 ماي 2026

شوهد للمصادقة على الإمضاء
16 ماي 2026

1. توقيع المعني (ة)
2. توقيع المعني (ة)

شكر

الحمد لله حمداً كثيراً طيباً مباركاً فيه، نحمده سبحانه وتعالى ونشكره على نعمه التي لا تُعد ولا تُحصى، واقتداءً بقوله: "وَلَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ"، وعملاً بقول نبيه محمد صلى الله عليه وسلم: "من لا يشكر الناس لا يشكر الله"

الحمد لله الذي وفقنا لإتمام هذا العمل، والذي بنعمته تتم الصالحات.

نتقدم بخالص عبارات الشكر والتقدير والامتنان إلى الأستاذ المشرف الأستاذ بن فردية، الذي كان نعم المؤطر والموجّه، على ما قدمه من توجيهات علمية قيمة ونصائح سديدة، وعلى سعة صدره وصبره ومرافقته العلمية طوال إنجاز هذه المذكرة، فله منا كامل الاحترام والتقدير.

كما نتوجه بجزيل الشكر إلى كافة أساتذة كلية الحقوق، الذين كان لهم الفضل في تكويننا العلمي والأكاديمي، والذين بذلوا جهودًا عظيمة في سبيل إيصال العلم والمعرفة، فكانوا خير منارة نهتدي بها في مسيرتنا الجامعية.

ولا يفوتنا أن نتقدم بالشكر والتقدير لكل من ساهم من قريب أو بعيد في إنجاز هذا العمل، ولو بكلمة طيبة أو دعاء صادق.

فإليهم جميعًا أسمى عبارات الشكر والامتنان.

إهداء

إلى نبع الحنان الغزير، وفيض الأمان الكبير... أمي،

إلى تلك التي كانت دعواتها ترافقني في كل خطوة، والتي علّمتني أن الأحلام العظيمة لا تولد إلا من الصبر والتعب، أهديكِ ثمرة هذا الجهد.

إلى الأحرار في دنيا العبيد... أبي،

إلى الرجل الذي كان سندًا ثابتًا لا يميل، والذي علّمني أن الكرامة مبدأ، وأن النجاح الحقيقي يُبنى بالشرف والتواضع والثبات.

إلى إخوتي... الذين يشبه وجودهم الطمأنينة،

والذين كانوا دائمًا مصدر قوة ودعم في كل مراحل الطريق.

إلى عائلتي الكريمة،

إلى كل من حمل لي المحبة والدعاء، وكان لي سندًا وأمانًا وسببًا للاستمرار.

إلى أصدقائي وزملائي الذين تقاسموا معي تعب الطريق وجمال اللحظات.

إلى الأستاذ الدكتور خويلدي السعيد،

تقديرًا لقيمته العلمية الراقية، ولما تركه علمه وأسلوبه من أثر جميل في نفسي، فكان مثالًا للرقي العلمي والأخلاقي.

إلى السيد النائب العام سعيدي أنور،

إلى من اجتمعت فيه هيبة المنصب مع نبل الأخلاق، والذي ترك حضوره في نفسي احترامًا يسبق الكلام.

إلى القاضي عطايلية عبد الله،

عرفانًا بمكانته العلمية والمهنية، وتقديرًا لما يجسده من صورة مشرّفة لرجل العدالة.

إلى قضاة محكمة ورقلة وقضاة مجلس قضاء ورقلة،

حَمَلة رسالة الحق، الذين تبقى للعدالة بفضلهم هيبتها وقيمتها.

وإلى كل من آمن بي، ولو بكلمة،

وإلى كل من كان أثرًا طيبًا في رحلتي،

أهدي هذا العمل المتواضع، الذي كُتب بالتعب، وكبر بالأمل، وحمل بين سطوره شيئًا من القلب قبل الحبر.

الطالبة رحاب قسوم.

إهداء

بسم الله الرحمن الرحيم

الحمد لله رب العالمين، والصلاة والسلام على خاتم الأنبياء والمرسلين.

إلى "نفسي" التي صمدت رغم كل العثرات... هذا الإنجاز ليس مجرد فخر، بل هو عرفان بصبر طويل، ووعدٌ مني بأن المسيرة مستمرة مهما بلغت التحديات.

إلى من كانت النور الذي يبدد ظلمات دروبي، والدافع الذي يقويني في لحظات ضعفي، اليد التي لم تخذلني يوماً؛

إلى أمي الغالية، حفظها الله وأطال في عمرها... هذا النجاح ثمرة دعائك، وكل ما سأحققه هو لكِ.

إلى من آمن بي وبقدراتي، وكان سنداً وعوناً لي طوال مسيرتي؛

إلى أبي العزيز، رعاه الله وبارك في عمره.

إلى من تقاسموا معي لحظات التعب والسهر، وكان وجودهم نعمة لا تقدّر؛

إلى إخوتي الأعزاء.

إلى أختي ومعلمتي الدكتورة سمية صالحي،

التي لم تكن مجرد أستاذة، بل كانت السند والداعم الحقيقي طوال سنوات دراستي، رافقتني بعلمها وأخلاقها وحرصها الدائم على توجيهي ومساندتي.

إليكِ أهدي هذا النجاح عرفاناً بفضلكِ الكبير، وتقديراً لكل ما قدمتِه لي من دعم وتشجيع كان له الأثر البالغ في مسيرتي العلمية

إلى من جعلوا الأيام أصعبها أهون، والضحكات أجمل...إلى أصدقائي الأوفياء.

إلى كل من علمني وجهاً لوجه، أو وجهني بكلمة، إلى عائلتي الكبيرة، وإلى كل من ترك أثراً في هذا العمل.

أهدي هذا الجهد المتواضع، لا كخاتمة لمشوار، بل كبداية لما هو أجمل وأفضل بإذن الله.

الطالبة تسنيم صالحي

مقدمة

مقدمة

شهد العالم خلال العقود الأخيرة تطورًا تكنولوجيًا متسارعًا مسَّ مختلف جوانب الحياة، حيث أصبحت التكنولوجيا الرقمية والأنظمة المعلوماتية عنصرًا أساسيًا في مختلف المعاملات اليومية، سواء في المجالات الاقتصادية أو الاجتماعية أو الإدارية أو الأمنية، الأمر الذي ساهم في تسهيل المعاملات وتسريع تبادل المعلومات والبيانات بصورة لم يشهدها العالم من قبل. غير أنّ هذا التطور لم يقتصر على الجوانب الإيجابية فحسب، بل صاحبه تطور مماثل في الأساليب الإجرامية، إذ لم تعد الجريمة تقتصر على صورتها التقليدية المعروفة، وإنما امتدت إلى البيئة الرقمية والفضاء الإلكتروني، فأصبحت العصرنة والرقمنة تشمل حتى النشاط الإجرامي، مما أدى إلى ظهور نوع جديد من الجرائم يُعرف بجرائم الفضاء الإلكتروني، والتي أصبحت من أخطر الجرائم المستحدثة في العصر الحديث وأكثرها تعقيدًا.

وتُعد الجريمة الإلكترونية صورة متطورة للجريمة التقليدية، غير أنها تختلف عنها من حيث الوسيلة وطبيعة التنفيذ، إذ تُرتكب باستخدام الوسائل المعلوماتية والأنظمة الإلكترونية أو تستهدفها بصورة مباشرة، ومن أبرز صورها جريمة الدخول أو البقاء غير المشروع داخل الأنظمة المعلوماتية، والتي تقوم على اختراق الأنظمة الإلكترونية أو الولوج إليها دون ترخيص قانوني، قصد الحصول على بيانات أو معلومات أو تعطيل الأنظمة أو المساس بسرية المعطيات الإلكترونية، وهو ما يشكل اعتداءً خطيرًا على أمن المعلومات والأنظمة الرقمية. كما تتميز هذه الجرائم بعدة خصائص تجعلها أكثر خطورة من الجرائم التقليدية، من

بينها السرعة في التنفيذ، وصعوبة اكتشاف مرتكبيها، وسهولة إخفاء آثارها أو محوها في وقت قصير، إضافة إلى طابعها العابر للحدود، مما يجعل مكافحتها من أكبر التحديات التي تواجه أجهزة العدالة الجنائية.

ويختلف المجرم الإلكتروني عن المجرم التقليدي، إذ يكون غالبًا شخصًا يتمتع بذكاء تقني وخبرة واسعة في مجال الإعلام الآلي والبرمجيات والشبكات الإلكترونية، تمكنه من استغلال الثغرات التقنية واختراق الأنظمة المعلوماتية بطرق دقيقة يصعب اكتشافها، كما يستطيع تنفيذ أفعاله الإجرامية دون الحاجة إلى التواجد المادي بمكان الجريمة، الأمر الذي يزيد من صعوبة تعقبه والوصول إليه. وفي المقابل، أصبح التحقيق في هذا النوع من الجرائم يتطلب محققًا رقميًا يتمتع بمهارات تقنية وقانونية عالية، وقادرًا على التعامل مع الوسائط الإلكترونية وتحليل المعطيات الرقمية واستخراج الأدلة الإلكترونية بطريقة علمية وقانونية تحافظ على سلامتها وحجيتها أمام القضاء.

وقد فرضت هذه الخصائص المميزة للجرائم الإلكترونية تحديات كبيرة أمام أجهزة العدالة الجنائية، التي وجدت نفسها أمام نمط إجرامي يختلف جذريا عن الجرائم التقليدية من حيث الوسائل والآليات المستعملة في ارتكابه، فالجريمة الإلكترونية قد ترتكب في ثوان معدودة دون الحاجة إلى التواجد المادي بمكان الجريمة، كما يمكن أن تمتد آثارها إلى عدة دول في وقت واحد، الأمر الذي يصعب من عملية تحديد الاختصاص القضائي والجهة المخولة بالتحقيق والمتابعة.

كما أن الطبيعة غير المادية للأدلة الرقمية تجعلها أكثر عرضة للتلف أو التغيير أو الحذف، سواء بشكل متعمد من طرف الجاني أو نتيجة أخطاء تقنية، وهو ما يفرض على جهات التحقيق التدخل السريع واتخاذ الإجراءات اللازمة للمحافظة على هذه الأدلة وضمان سلامتها. وتزداد هذه الصعوبات مع اعتماد بعض المجرمين على وسائل متطورة لإخفاء هوياتهم الحقيقية، كاستخدام الشبكات الافتراضية الخاصة(VPN) وتقنيات التفشير وبرامج إخفاء الآثار الرقمية.

وأمام هذه التحديات، لم يعد من الممكن الاعتماد على وسائل التحقيق التقليدية وحدها في مواجهة هذا النوع من الجرائم، بل أصبح من الضروري تطوير آليات حديثة تتلاءم مع البيئة الرقمية، وتسمح بالكشف عن الأدلة الإلكترونية وجمعها وتحليلها وفق أساليب علمية دقيقة تحافظ على حجيتها القانونية. ومن هنا برز التحقيق الرقمي كأحد أهم الوسائل المستحدثة التي اعتمدتها التشريعات الحديثة لمواجهة الجرائم الإلكترونية والتصدي لمخاطرها المتزايدة.

وأمام هذا التطور الخطير في الجريمة الإلكترونية، أصبحت إجراءات التحقيق التقليدية عاجزة عن مواكبة هذا النوع من الجرائم، خاصة وأنها لا تخلّف في الغالب آثارًا مادية ملموسة كالجرائم العادية، بل تكون آثارها في شكل بيانات رقمية قابلة للإتلاف أو التعديل أو الإخفاء بسهولة، وهو ما استوجب ضرورة اعتماد وسائل حديثة للتحقيق تعتمد على التكنولوجيا والوسائط الرقمية، الأمر الذي أدى إلى ظهور ما يُعرف بالتحقيق الرقمي،

والذي يُقصد به مجموعة الإجراءات التقنية والقانونية التي تهدف إلى جمع الأدلة الرقمية وتحليلها واستخراجها وحفظها بطريقة قانونية تسمح بالكشف عن الجرائم الإلكترونية والوصول إلى مرتكبيها.

وقد أدى هذا الواقع إلى بروز التحقيق الرقمي كحتمية تفرضها متطلبات مكافحة الجرائم الإلكترونية، حيث أصبح يشكل أحد أهم الأدوات الحديثة التي تستعين بها أجهزة إنفاذ القانون في البحث عن الأدلة الرقمية وتتبع الأنشطة الإجرامية المرتكبة عبر الفضاء الإلكتروني.

ويعتمد التحقيق الرقمي على مجموعة من الإجراءات والأساليب التقنية التي تمكن من جمع البيانات الإلكترونية وتحليلها واستخراج المعلومات ذات القيمة الإثباتية، مع الحرص على المحافظة على سلامة الدليل الرقمي وعدم المساس بمحتواه.

وتكمن أهمية التحقيق الرقمي في قدرته على الوصول إلى أدلة قد يصعب أو يستحيل الحصول عليها بالوسائل التقليدية، خاصة في جرائم التي ترتكب عبر الشبكات المعلوماتية أو تستهدف الأنظمة الإلكترونية. كما يسمح بتتبع الأنشطة الإجرامية والكشف عن هوية الجناة وتحديد أساليبهم الإجرامية، الأمر الذي يساهم في دعم جهود العدالة الجنائية وتحقيق الأمن المعلوماتي.

غير أن فعالية التحقيق الرقمي تبقى مرتبطة بمدى توفر الإمكانيات التقنية والكفاءات البشرية المؤهلة، إضافة إلى وجود إطار قانوني يضمن مشروعية الإجراءات المتخذة ويحافظ

في الوقت نفسه على الحقوق والحريات الأساسية للأفراد. ولذلك اتجهت العديد من التشريعات الحديثة إلى تطوير قواعد قانونية خاصة بالتحقيق الرقمي والأدلة الإلكترونية لمواكبة التطور المتسارع لتكنولوجيات الإعلام والاتصال.

الدراسات السابقة

ركزت أغلب الدراسات السابقة على الجريمة الإلكترونية من حيث مفهومها وخصائصها وصورها وآثارها وسبل مكافحتها، إلا أنها لم تتناول بصورة معمقة موضوع التحقيق الرقمي في مواجهة هذا النوع من الجرائم، خاصة من حيث الإجراءات والأساليب الحديثة المعتمدة في التحري والتحقيق باغي صبرينة، وقريقة غادة، مرحلة التحقيق في الجرائم الالكترونية في ظل التشريع الجنائي الجزائري، مذكرة ماستر في القانون، المركز الجامعي عبد الحفيظ بوالصف، ميلة2024-2025.

بن عنطر سهام، التحقيق الجنائي في الجرائم الالكترونية، مذكرة ماستر، جامعة مولود معمري تيزي وزو، 2023، طبيعة الدليل الرقمي، والضمانات القانونية المتعلقة بحمايته ومشروعية استخراجه واستعماله. ومن هنا تتجلى القيمة العلمية لهذه الدراسة، باعتبارها لا تقتصر على دراسة الجريمة الإلكترونية فقط، وإنما تتناول جانبًا إجرائيًا وتقنيًا بالغ الأهمية يتمثل في التحقيق الرقمي ومدى فعاليته في مواجهة جرائم الفضاء الإلكتروني.

أهمية الموضوع

تتجلى أهمية الدراسة في تسليط الضوء على التحديات القانونية والتقنية التي تعترض إجراءات التحقيق الرقمي، وبيان مدى كفاية القواعد القانونية المعمول بها لمواكبة التطورات التكنولوجية المتسارعة، بما يساهم في تعزيز فعالية العدالة الجنائية في مواجهة جرائم الفضاء الالكترونية وتحقيق التوازن بين متطلبات مكافحة الجريمة وحماية الحقوق والحريات الفردية.

ولا تقتصر أهمية التحقيق الرقمي على الجانب الإجرائي فحسب، بل تمتد إلى كونه وسيلة أساسية لتحقيق التوازن بين متطلبات مكافحة الجريمة الإلكترونية وحماية الحقوق والحريات الفردية. فكلما تم احترام الضوابط القانونية أثناء جمع الأدلة الرقمية ومعالجتها، ازدادت ثقة الافراد في العدالة الجنائية وتعززت مشروعية الإجراءات المتخذة في مواجهة المجرمين الإلكترونيين.

كما يكتسي التحقيق الرقمي أهمية خاصة بالنسبة للقضاء الجزائري، في ظل تزايد المستمر لاستخدام الوسائل الإلكترونية في مختلف المجالات، وما يترتب على ذلك من ارتفاع في معدلات الجرائم المرتبطة بالأنظمة المعلوماتية.

وهوما يستدعي تطوير آليات البحث والتحري وتعزيز التكوين المتخصص لأعوان الضبطية القضائية والخبراء المختصين في المجال الرقمي.

أسباب وأهداف الدراسة

يرجع اختيار هذا الموضوع إلى الانتشار الواسع للجرائم الإلكترونية والتطور المستمر لأساليب ارتكابها، مما أثار العديد من الإشكالات القانونية والإجرائية المتعلقة بكيفية التحقيق فيها وإثباتها، خاصة في ظل قصور بعض الإجراءات التقليدية عن مواكبة طبيعتها التقنية. كما تهدف هذه الدراسة إلى توضيح مفهوم التحقيق الرقمي وبيان أهم الإجراءات والأساليب الحديثة المعتمدة فيه، إضافة إلى دراسة الدليل الرقمي ومدى حجيته القانونية والضمانات المقررة لحمايته، فضلًا عن محاولة تقييم فعالية التحقيق الرقمي في مواجهة جرائم الفضاء الإلكتروني.

الإشكالية

ونظرًا للطبيعة الخاصة التي تتميز بها جرائم الفضاء الإلكتروني، وما تطرحه من صعوبات في الكشف عن مرتكبيها والوصول إلى الأدلة المرتبطة بها، أصبح التحقيق الرقمي من أهم الوسائل الحديثة التي تعتمد عليها الجهات المختصة في البحث عن الدليل الإلكتروني واستخراجه وتحليله. غير أنّ فعالية هذا النوع من التحقيق تبقى محل تساؤل في ظل التطور المستمر للأساليب الإجرامية الرقمية، الأمر الذي يثير الإشكالية التالية:

ما مدى فعالية التحقيق الرقمي في متابعة وكشف الجرائم الالكترونية.

المنهج المعتمد

تم الاعتماد في هذه الدراسة على المنهج الوصفي باعتباره الأنسب لوصف ظاهرة الجريمة الإلكترونية وبيان خصائصها وخطورتها، إضافة إلى المنهج التحليلي من خلال تحليل النصوص القانونية المتعلقة بالتحقيق الرقمي والدليل الرقمي وبيان مدى فعاليتها في مواجهة جرائم الفضاء الإلكتروني.

صعوبات الدراسة

ولعل أبرز الصعوبات التي واجهت هذه الدراسة لم تتمثل في نقص المراجع أو ضيق الوقت، وإنما ارتبطت أساسا بطبيعة الموضوع ذاته، باعتباره من المواضيع الحديثة والحساسة التي تجمع بين الجانب القانوني والتقني، الأمر الذي تطلب الإلمام بمفاهيم دقيقة ومتجددة باستمرار بفعل التطور التكنولوجي السريع. كما أن موضوع التحقيق الرقمي في مواجهة جرائم الفضاء الإلكتروني يُعد من المواضيع الواسعة والمتشعبة التي تثير العديد من الإشكالات القانونية والعملية، مما جعل الإحاطة بكافة جوانبه ضمن إطار مذكرة ماستر أمرًا بالغ الصعوبة.

تقسيم الدراسة

تم تقسيم موضوع الدراسة إلى فصلين، حيث خُصص الفصل الأول لدراسة إجراءات وأساليب التحقيق الرقمي في مواجهة جرائم الفضاء الإلكتروني، مع التطرق إلى أهم الآليات الحديثة والتعاون الدولي في هذا المجال، بينما خُصص الفصل الثاني لدراسة الدليل الرقمي وبيان حجيته القانونية والضمانات المقررة لحمايته في إطار التحقيق في الجرائم الإلكترونية.

الفصل الأول:

الاجراءات والاساليب الدولية للتحقيق الرقمي

تمهيد

يعد التحقيق في الجريمة الالكترونية من أبرز التحديات التي فرضها لتطور التكنولوجي الحديث، إذ أفرزت البيئة الرقمية أنماطا إجرامية جديدة تختلف عن الجرائم التقليدية من حيث الوسيلة وطبيعة الدليل، وسرعة ارتكاب الفعل الاجرامي وانتشاره عبر الحدود. الامر جعل أساليب التحقيق التقليدية تواجه صعوبات عملية وقانونية في الكشف عن مرتكبي الجرائم وإثباتها.

وأمام التحديات، اتجهت التشريعات الحديثة الى تطوير آليات التحقيق وتوسيع نطاقها بما يتلاءم مع خصوصية الجريمة الالكترونية، من خلال استحداث إجراءات تقنية حديثة تسمح بتتبع النشاط الاجرامي الرقمي وجمع الأدلة الالكترونية بفعالية، مع الحرص على احترام الضمانات القانونية وحماية الحقوق والحريات، كما برزت أهمية التعاون الدولي باعتباره عنصرا أساسيا لمواجهة الجرائم الالكترونية التي غالبا ما تتجاوز الحدود الوطنية وتمتد آثارها الى عدة دول.

وعليه، يقتضي البحث في هذا الفصل دراسة مختلف الآليات المعتمدة في التحقيق في الجريمة الالكترونية، سواء من خلال الإجراءات المعتمدة داخليا أو عبر صور التعاون الدولي التي تهدف الى تعزيز فعالية الملاحقة والتحقيق في هذا النوع من الجرائم.

المبحث الأول: إجراءات التحقيق الرقمي

ان خصوصية الجريمة الالكترونية وما تتميز به من طابع تقني فرضت على جهات التحقيق ضرورة الاعتماد على وسائل وأساليب تتلاءم مع طبيعتها، خاصة وان الدليل في هذا النوع من الجرائم يكون في الغالب دليل رقمي سريع الزوال وسهل التعديل أو الاخفاء، ورغم أهمية الإجراءات التقليدية في مباشرة التحقيق والمحافظة على الشرعية الإجرائية، الا

أن التطور التكنولوجي أظهر محدودية هذه الإجراءات في بعض الحالات، الامر الذي استوجب تدعيمها بإجراءات حديثة أكثر فعالية وقدرة على مسايرة البيئة الرقمية.

ومن هذا المنطلق، أصبح التحقيق في الجريمة الالكترونية يقوم على الجمع بين الإجراءات التقليدية التي تشكل الأساس القانوني للتحقيق، والإجراءات المستحدثة التي أفرزها التطور التقني، وذلك بهدف الوصول الى الأدلة الرقمية والكشف عن مرتكبي الجرائم الالكترونية في إطار قانوني يحقق التوازن بين فعالية التحقيق وضمان الحقوق والحريات.

وعليه سنتطرق في هذا المبحث الى الإجراءات التقليدية للتحقيق الرقمي في (المطلب الأول) والإجراءات المستحدثة للتحقيق الرقمي في (المطلب الثاني).

المطلب الأول: الإجراءات التقليدية للتحقيق الرقمي

تعد الإجراءات التقليدية الأساس الذي تقوم عليه عملية التحقيق الجنائي، باعتبارها الوسائل القانونية التي خولها المشرع لجهات التحقيق من أجل البحث عن الحقيقة وجمع الأدلة وكشف عن مرتكبي الجرائم، ورغم ارتباط هذه الإجراءات أساسا بالجرائم التقليدية، الا انها تبقى ذات أهمية في مجال الجريمة الالكترونية، غير أن تطبيقها في البيئة الرقمية يثير عدة صعوبات مرتبطة بطبيعة الدليل الالكتروني وخصوصية الوسائل المستعملة في ارتكاب الجريمة.

وعليه سنتطرق في هذا المطلب الأول الى المعاينة في الوسط الرقمي في (الفرع الأول)، والتفتيش الرقمي في (الفرع الثاني)، الضبط الرقمي في (الفرع الثالث)، الخبرة التقنية (الفرع الرابع).

الفرع الأول: المعاينة في الوسط الرقمي

تعد المعاينة من أولى الإجراءات التي يباشرها ضابط الشرطة القضائية فور اكتشاف الجريمة، كما انها "رؤية بالعين لمكان أو شخص أو أي شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"[1].

وبالرجوع إلى نص المادة78 الفقرة 03 من قانون الإجراءات الجزائية25-14، فإن المشرع الجزائري أجاز المعاينة عندما يتعلق الأمر بجرائم تكنولوجيات الإعلام و الاتصال[2].

وكذا الحال في حال وقوع جريمة من الجرائم المنصوص عليها في القانون18-07المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي، فإنه بالإمكان القيام بمعاينة المحلات والأماكن لتي تتم فيهم معالجة المعطيات الشخصية[3].

[1] محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، الطبعة السابعة،2002، ص233.

[2] المادة78 من القانون رقم 25-14المؤرخ في9صفر1447الموافق3غشت2025، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد54، الصادر في2025، "يلاحظ ان المشرع الجزائري استعمل في قانون الإجراءات الجزائية الملغى مصطلح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، غير انه في قانون الإجراءات الجزائية الجديد (25-14) استبدله بمصطلح جرائم تكنولوجيات الإعلام والاتصال، وهو مصطلح أوسع يعكس تطور البيئة الرقمية وتعدد الوسائل المستعلمة في ارتكاب الجريمة".

ويُلاحظ أن المشرع الجزائري لم يكتفِ فقط باستعمال مصطلح جرائم تكنولوجيات الإعلام والاتصال في قانون الإجراءات الجزائية الجديد، بل عزز ذلك باستحداث آليات قضائية متخصصة لمواجهة هذا النوع من الجرائم، من خلال النص على القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك بموجب المواد من 335 إلى 342 من قانون الإجراءات الجزائية، وهو ما يعكس إدراك المشرع لخطورة الجرائم الإلكترونية وخصوصيتها، وضرورة توفير أجهزة وآليات متخصصة تتماشى مع طبيعتها التقنية المعقدة."

[3] المادة49 من القانون رقم18-07 المؤرخ في25 رمضان عام1439 الموافق10يونيو سنة2018، المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، الجريدة الرسمية للجمهورية الجزائرية، لعدد34، سنة2018.

ونظرا للطبيعة العابرة للحدود للجرائم المعلوماتية، فقد تستلزم عملية المعاينة التعاون الدولي لجمع الأدلة الرقمية، وهذا ما نصت عليه المادة16من 09-04 التضمن الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال[1].

غير ان المعاينة في المجال الرقمي لا تنصب على مكان مادي، وانما يمتد الى ما يعرف بمسرح الجريمة الإلكترونية، الذي يتمثل في جهاز الحاسوب، هاتف ذكي، تصوير الشاشات، حفظ البيانات الظاهرة، وكدا ضبط عناوين بروتكول الإنترنت المرتبطة بالنشاط الإجرامي. وتقتضي هذي العملية دقة تقنية عالية الجودة لتفادي إتلاف البيانات او تغيرها، خاصة وأن [2]الدليل الرقمي سريع الزوال والإتلاف كما انه قابل للمحو أو التعديل فيه في أي لحظة، ويتم اجراء المعاينة التقنية لمسرح الجريمة الإلكترونية عن طريق التعامل في هذا الإطار على انه مسرحان هما:

1.المسرح تقليدي: يقع خارج بيئة الحاسوب والأنترنت بحيث يقتضي معاينة المكونات

المادية للأجهزة التي تم بيها ارتكاب الواقعة فقد يترك فيها الجاني آثار عدة، كالبصمات وكل مما يعتبر من المكونات المادية ذات الطابع المادي المحسوس للأدلة المادية وعليه فإنه تطبق نفس القواعد المتعارف عليها في المعاينة التقليدية للأدلة المادية.

2. المسرح افتراضي: ويقع داخل البيئة الإلكترونية، الذي يتكون من بيانات رقمية غير مادية موزعة عبر الأنظمة والشبكات. وانطلاقا من هذه الخصوصية، تملك الضبطية القضائية المختصة (المصالح التقنية للأمن والدرك الوطنيين) وكذا سلطة التحقيق صلاحية

[1] المادة16من القانون 09-04المؤرخ في14شعبان عام1430الموافق5غشت سنة2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] بو قصة إيمان و، بدايرية يحي، "أثر خصوصية إجراءات التحقيق في الجرائم المعلوماتية على حجية الدليل الرقمي في الإثبات "، مجلة الحقوق والحريات، جامعة محمد خيضر بسكرة، المجلد 13، العدد02، جوان2025،ص 534_535.

مباشرة إجراءات المعاينة الفنية للأنظمة المعلوماتية، دون اشتراط الانتقال المادي لمكان تواجد الأجهزة[1].

وهو ما أكدته الممارسة الميدانية من خلال مقابلة أجراها الباحث مع السيد قاضي التحقيق لدى محكمة ورقلة، حيث أشار الى إمكانية قيام القاضي بمباشرة المعاينة الرقمية لمنصات محل التحقيق مباشرة من مكتبه، لضمان السرعة والفعالية في التحصيل الرقمي، مع الاستعانة بتقرير الخبرة القضائية المتخصصة في الأمن السيبراني[2].

ونظرا لخصوصية واختلاف مسرح الجريمة الإلكترونية ينبغي إتباع عدة قواعد فنية والمتمثلة في:

. تحديد موقع المعاينة والجمع القبلي للمعلومات، بحيث يعد مقر مزود خدمة الإنترنت من أفضل الأماكن التي يمكن من خلالها معاينة فنية دقيقة[3].

. تشكيل فريق من الخبراء المتخصصين تقنيا، بناء على امر قضائي، نظرا للخصوصية التي تتمتع بها أماكن تخزين البيانات[4].

ومن الإجراءات التي يتعين إتباعها عند إجراء المعاينة ما يلي:

. القيام بتصوير جهاز الحاسب الآلي الذي ترتكب عن طريقه الجرائم وما قد يتصل به من أجهزة طرفية ومحتوياته وأوضاع المكان الذي يوجد به بصفة عامة مع العناية بتصوير أجزاءه الخلفية وملحقاته الأخرى[1].

---

[1] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، ص84.

[2] مقابلة شفوية اجراها الباحث مع السيد قاضي التحقيق لدى محكمة ورقلة، حول المعاينة الرقمية، بتاريخ2026/01/18، على الساعة15:00زوالا.

[3] عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة عين شمس،2004 ص895

[4]نبيلة هبه هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2013، ص220.

.العناية البالغة بملاحظة الطريقة التي يتم بها إعداد النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها بشبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج الى النظام أو الموقع[2].

الفرع الثاني: التفتيش الرقمي

التفتيش هو إجراء من إجراءات التحقيق الأساسية، يقوم به موظف مختص طبقا للإجراءات المنصوص عليها قانونا، في محل يتمتع بالحرمة[3]، فغاية التفتيش هو كشف ما تحتويه نظم الحاسوب من خفايا إجرامية، ولتفتيش قواعد تتمثل في القواعد موضوعية وهي وقوع جريمة

وان يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به، اما القواعد الشكلية لتفتيش نظام الحاسوب ان يكون التفتيش مسبب وان ينجر التفتيش باستخدام الوسائل التقنية الحديثة [4].

وقد تبنى المشرع الجزائري في القانون09-04المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، في المواد06، 07، 08، إجراءات خاصة

[1] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط،1994، ص60.

[2] سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية(الإنترنت)، دار النهضة العربية، القاهرة، 2007، ص290.

[3] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، طبعة01، دار الفكر الجامعي، الإسكندرية، 2009، ص77.

[4]باغي صبرينة وقريقة غادة، مرحلة التحقيق في الجرائم المعلوماتية في ظل التشريع الجنائي الجزائري، مذكرة ماستر في القانون، معهد الحقوق، المركز الجامعي عبد الحفيظ بو الصوف، ميلة، 2025/2024، ص89-90.

بضبط البيانات تحت عنوان حجز المعطيات المعلوماتية[1]، إذ يترتب عن التفتيش حجز المنظومة المعلوماتية في حالة اكتشاف السلطة التي تباشر إجراء التفتيش عن وجود معطيات مخزنة تفيد في الكشف عن الجريمة، ففي هذه الحالة من الممكن أن تحجز المنظومة كلها، أو ان يحجز جزء منها وذلك بالاعتماد على إجراءات متمثلة: في انه، يجوز للسلطة المختصة اثناء التفتيش نسخ المعطيات المخزنة على دعامات التخزين الإلكترونية القابلة للحجز، سواء كانت هذه المعطيات محل البحث أو كانت ضرورية لفهمها.

كما يمكن اللجوء إلى استعمال وسائل تقنية لإعادة تشكيل المعطيات أو معالجتها بما يسمح بالاستفادة منها في إجراءات التحقيق الجنائي الرقمي، شريطة عدم المساس بمضمونها[2].

وفي حال تعذر اجراء الحجز لأسباب تقنية، يتعين اتخاد التدابير التقنية اللازمة لمنع الوصول على المعطيات أو نسخها من طرف الأشخاص غير المرخص لهم باستعمال المنظومة المعلوماتية. بحيث يهدف هذا الاجراء الى الحفاظ على الأدلة الرقمية في بيئتها الإلكترونية، ومنع أي محاولة لطمسها أو إخفائها، بما يضمن فعالية إجراءات التفتيش[3].

ونظرا لخصوصية الجريمة المعلوماتية، فان التفتيش فيها يحتاج الى تقنيات خاصة، لكون محل التفتيش يقع على الحاسوب والشبكات، وذلك لسهولة إخفاء المعطيات وصعوبة تحديد مكانها، كون ان الجريمة الإلكترونية من الجرائم التي تعد عابرة للحدود، وعليه لابد من معرفة صلاحية كل من شبكات الحاسوب ومكوناته، وقابليتها للتفتيش.

[1] المواد06، 07، 08، من القانون09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،

[2] المادة06من نفس القانون.

[3] المادة07من نفس القانون.

تتكون نظم الحاسوب من مكونات مادية (hardware)ومكونات منطقية (software)، محل التفتيش كما تربطه بغيره من الحاسبات اتصال بعديه على المستوى المحلي أو الدولي [1].

أولا: تفتيش مكونات الحاسوب المادية

الواقع ان التفتيش الواقع على المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء يتصل بجرمية إلكترونية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها،[2] ويخضع التفتيش فهذه الحالة للقواعد العامة المقررة قانونا، إلا أنه يجب مراعاة مكان تواجد المعدات، سواء كانت في الأماكن الخاصة أو الأماكن العامة، إذ يمثل المعيار المكاني حجز الزاوية في تحديد الضمانات القانونية الواجبة عند التفتيش، فإذا كانت في مكان خاص كمسكن المتهم أو أي مكان غير مفتوح للعموم، فإنه لصحة الإجراء يجب الالتزام والتقيد بالشروط المنصوص عليها وبنفس الضمانات المقررة قانونا، بحيث يجب الحصول على الموافقة الكتابية لصاحب المسكن[3]، ومراعاة ميعاد التفتيش[4]، إلا أن المشرع الجزائري قد أورد استثناءات في تطبيق ضمانات على بعض الجرائم من بينها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث أجاز التفتيش في كل محل سكني أو غير سكني وفي أي ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص[5]. فالمشرع هنا غلب المصلحة العامة لتحقيق العدالة على الحق في حرمة الحياة الخاصة ومستودع الاسرار أي المصلحة الخاصة، وتبريرا لذلك يعود لخطورة الجريمة الإلكترونية وما تتسم به أدلتها الرقمية من سرعة الزوال وقابلية التلاشي، فضلا عن الاحترافية لمرتكبيها.

---

[1] اشرف عبد القادر قنديل، الاثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، الأسكندرية ص130.

[2] عائشة بن قارة مصطفى، مرجع سابق، ص88.

[3] أنظر المادة 97، من قانون الإجراءات الجزائية، (25-14).

[4] أنظر المادة78 من نفس القانون.

[5] أنظر المادة97، فقرة3 من نفس القانون .

أما بخصوص تفتيش الأنظمة المعلوماتية المتواجدة في الأماكن العامة، فإن خضوعها للتفتيش يرتبط قانونا بالحلات التي يباح فيها تفتيش الأشخاص المتواجدين بها أو الحائزين لها، حيث يتم الإجراء وفقا لذات الضوابط والضمانات الإجرائية المقررة لتفتيش الأشخاص في هذا السياق[1].

ثانيا: تفتيش مكونات الحاسوب المعنوية

تتمثل المكونات المعنوية للحاسوب في أنظمة الكومبيوتر والبيانات المخزنة فيه، وعليه فإن احكام قانون الإجراءات الجزائية الخاصة بالتفتيش تتناسب مع هذه المكونات المعنوية، باعتبارها انها قابلة للضبط والتخزين في وسائط مادية أو طبعها على دعائم ورقية[2]. ويتضح موقف المشرع الجزائري من خلال نص المادة05 من القانون09-04 على إجازة تفتيش المنظومات المعلوماتية وقد نصت على انه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في اطار قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد الى منظومة معلوماتية او جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلومات[3].

فالتفتيش في هذه الحالة على درجة من الخطورة تتعلق بالتفتيش عن بعد، نتيجة للطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أداة عبر شبكات حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، وهو ما يزيد الامرا تعقيدا باعتبار ان الشبكة المعلوماتية ممتدة عبر انحاء العالم[4].

---

[1] عائشة بن قارة مصطفى، مرجع سابق، ص90.

[2] حليم رامي، إجراءات استخلاص لدليل في الجرائم المعلوماتية، مجلة دفاتر البحوث العلمية، المجلد09، العدد01، جامعة البليدة2، الجزائر2021، ص231.

[3] انظر المادة05، من القانون 09-04.

[4] جليلة بلعلمي ومزري صالح، الدليل الرقمي والاثبات الجنائي، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة،2022/2021، ص16.

ميز المشرع الجزائري في إجراءات تفتيش المنظومات المعلوماتية بين فرضيتين بحسب مكان تواجد المعطيات الرقمية، فالحالة الأولى تتعلق بالولوج الى بيانات مخزنة في منظومة مرتبطة بالنظام يقع داخل الاقليم الوطني، بينما تخص الحالة الثانية البيانات المخزنة في أنظمة تقع خارج الإقليم الوطني[1].

وفي كلتا الحالتين، اقر المشرع اجراء سمح للسلطات المختصة وضباط الشرطة القضائية بمباشرة التفتيش دون اشتراط اذن قضائي مسبق، وإنما الا كتفاء بإخطار السلطة القضائية المختصة، نظرا لخصوصية الدليل الرقمي وسرعة تلاشيه[2].

والتفتيش العابر للحدود لا يعد انتهاكا لسيادة الدولة الأجنبية، بل يندرج ضمن مقتضيات التعاون الدولي والاتفاقيات الثنائية، شريطة الالتزام بمبدأ المعاملة بالمثل والقواعد الدولية الودية[3].

الفرع الثالث: الضبط الرقمي

ان الغاية من التفتيش هو ضبط الأدلة التي تفيد في كشف الحقيقة، وعلى ذلك فإن ضبط الأشياء المتعلقة بالجريمة هي الأثر المباشر للتفتيش[4].

وضبط في نطاق الإجراءات الجزائية يقصد به: الحصول على الأشياء ذات صلة بجريمة وقعت ويفيد في كشف حقيقتها وسبتها الى المتهمين، غير ان الضبط في الجرائم الالكترونية يختلف عن الضبط في الجرائم الأخرى من حيث المحل، وذلك بسبب ان الأول يرد على

---

[1] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، جامعة الوادي، العدد05، جوان2012، ص167.168.

[2] انظر المادة05، ف2، من القانون09-04.

[3] انظر المادة05، ف3، نفس القانون.

[4] بوعناد فاطمة الزهراء ، مشروعية الدليل الالكتروني في مجال الاثبات الجنائي، أطروحة دكتوراه، جامعة سيدي بلعباس2013.2014، ص143.

أشياء ذات طبيعة معنوية وهي البيانات، المراسلات والاتصالات الالكترونية، اما الثاني فيرد على أشياء ذات طبيعة مادية كالمنقولات والعقارات، وقد اثارت البيانات المعنوية جدل حول مدى امكانية ضبطها، ويرجع السبب في ذلك ان الضبط حسب الأصل لا يرد الا على الأشياء المادية[1].

أجاز المشرع الجزائري حجز المعطيات حيث نص انه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها فيجوز في هذه الحالة ان يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احراز طبقا للقواعد المقررة في قانون الإجراءات الجزائية، كما انه يجب في جميع الأحوال السهر على سلامة هذه المعطيات وعدم المساس بمحتواها[2].

وأضاف المشرع الجزائري انه في حال اذا كانت عملية الحجز مستحيلة لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات لمنع الوصول ال المعطيات الموجودة في المنظومة المعلوماتية أو القيام بنسخها[3]، كما يمكن لهذه السطلة ان تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ويكون ذلك عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك [4].

بمجرد وضع السلطات المختصة يدها على الأجهزة والوسائط المعلوماتية، تبرز ضرورة تقنية وقانونية تتمثل في الحفاظ على سلامة المحتوى الرقمي من التلف او التعديل، وهوما

[1] عائشة بن قارة، مرجع سابق، ص 114.

[2] انظر المادة06من القانون09-04.

[3] انظر المادة07من نفس القانون.

[4] انظر المادة08 من نفس القانون .

يستوجب اتباع خطوات فنية دقيقة لضمان حجية الدليل، وتتمثل اهم هذه الإجراءات فيما يلي:

1. طريقة النسخ (copy):

تعتمد هذه الطريقة في استنساخ البيانات الرقمية المضبوطة بدقة، وذلك باستخدام برمجيات مخصصة مثل) برامج (laplink تتيح هذه التقنية نقل البيانات من الأجهزة المحجوزة وتخزينها على وسائط خارجية (أقراص مدمجةcdأو (dvdتابعة لجهة الضبط، مع ضرورة الاحتفاظ بنسخة احتياطية لتفادي ضياع الأدلة أو تلفها.

2. أسلوب التجميد:

يقصد به شل حركة النظام المعلوماتي ومنع التعديل عليه، وذلك عبر ضغط الملفات والبيانات لتقليص حجمها وتسهيل حفظها على أقراص الليزر، مع ضمان بقاء خصائصها الاصلية سليمة، ولضمان فعالية هذا الاجراء، يجيب الالتزام بالضوابط التالية:

أ. عدم الاكتفاء بنسخ البيانات بل ضبط الدعائم الاصلية الحاملة لها[1].

ب. حجب الوصول الى البيانات المضبوطة أو سحبها من النظام المعلوماتي وفقا للمعايير الدولية، خاصة إذا كانت البيانات تتضمن خطر أو ضرر للمجتمع[2].

حدد المشرع الجزائري ضوابط حجز الأدلة بحيث أن الاحراز والوثائق المحجوزة لا يتم فتحها إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا[3]، وعليه فإن الاطلاع على

[1] بوعناد فاطمة زهرة، مرجع سابق، ص147.146

[2] انظر المادة19فقرة3من اتفاقية بو دابست، موقعة في23نوفمبر 2001

[3] انظر المادة160 قانون الإجراءات الجزائية25-14.

المستندات المراد حجزها مخول فقط لقاضي التحقيق أو ضابط الشرطة القضائية الذي نابه قبل حجزها ووضعها في احراز مختومة ويحرر محضر بضبطها[1].

الفرع الرابع : الخبرة الرقمية

تعتبر الخبرة القضائية من اهم اجراءات التحقيق الجنائي الرقمي، بحيث تفرض الطبيعة التقنية المعقدة التي تتسم بها الجرائم المعلوماتية، الى جانب خصوصيتها ضرورة الاستعانة بالخبرة المتخصصة، لاسيما في الإجراءات المعقدة المرتبطة بالتحقيق في الأشرطة الممغنطة واستنطاق البرامج، الرقمية منها وهذا راجع لصعوبة هذه المسائل التي يتعذر على المحقق الالمام بها بمفرده، مما يستدعي تدخل اهل الخبرة من ذوي الاختصاص لمعالجتها بكفاءة[2] .

والخبرة في مجال المعلوماتية تكون بتحري الحقيقة عن طريق جمع المعلومات من الأدلة الرقمية وتحصيلها من خوادم الموقع ومن جهاز المعتدى عليه بعد التوصل الى تحديده ثم يقوم الخبير بعملية تحليل رقمي لها لمعرفة كيفية تع اعدادها البرمجي ونسبتها الى مسارها الذي اعدت فيه، ومن ثمة تحديد عناصر حركتها لتوصل بذلك الى معرفة بروتوكول الانترنت للحاسب الذي صدرت منه النبضات الالكترونية[3].

[1] انظر المادة09من القاون 09-04.

[2] غدامسي موسى، السياسة التشريعية الجزائرية لحماية النظام العام والآداب العامة في البيئة الرقمية، مداخلة مقدمة ضمن المحور الثاني: الآليات القانونية لحماية النظام العام والآداب العامة في البيئة الرقمية، كلية الحقوق والعلوم السياسية، جامعة أحمد بوقرة بومرداس، ص13.

[3] جليلة بلعلمي وصالح مزري، مرجع سابق، ص19

كما يتولى الخبير الرقمي استخراج الأدلة الرقمية من الأجهزة او المنصت الالكترونية دون التسبب في تلفها أو فقدانها، من خلال استخدام مهارات تقنية متقدمة مثل فك الشيفرات، استرجاع البيانات، تتبع حركة الجاني داخل البيئة الافتراضية[1].

كما ان المشرع الجزائري أجاز للسلطة المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[2] .

ترك المشرع لقاضي التحقيق حرية ندب خبير واحد أو أكثر، الا انه في مجال الخبرة التقنية يجوز تعدد الخبراء، فمجال تقنيات الحاسوب ونظمه واسع ومتعدد وبالتالي يصعب وجود خبير متخصص له دراية كاملة[3].

نظم المشرع الجزائري أعمال الخبرة، باعتبارها من إجراءات استنباط الأدلة الرقمية الجنائية، انه لجهات التحقيق أو الحكم عندما تعرض عليها مسألة ذات طابع فني ان تأمر بندب خبير إما بناء على طلب من النيابة العامة، أومن تلقاء نفسها أو من الخصوم.[4] ومن واجبات الخبير حلف اليمين قبل أداء مهامه، وكذا الاستجابة للطلبات التي قد وجهت اليه أثناء عملية الخبرة كتليفه بإجراء أبحاث معينة او سماع أي شخص معين باسمه قد يكون قادر على مدهم بالمعلومات ذات الطابع الفني، كما يجب ان تحدد للخبير مهلة لإنجاز

[1] باغي صبرينة و قريقة غادة، مرجع سابق، ص96

[2] المادة5 ف3من القانون 09-04.

[3] المادة243، قانون الإجراءات الجزائية 25-14.

[4] المادة239 نفس القانون.

مهمته وفي حال عدم إيداع الخبير للتقارير جاز استبداله، وبعد انتهاء الخبير من ابحاثه وفحوصاته يعتين عليه اعداد تقرير متضمن ما توصل اليه من اعمال ونتائجها[1].

إضافة الى واجبات الخبير التقنية يجي أيضا قواعد فنية تحكم عمله والمتمثلة في: الالمام بتركيب الحاسب ونظمه، طبيعة البيئة التي يعمل في ظلها الحاسب من حيث التنظيم وكذا تحديد أماكن التخزين والوسائل المستخدمة في ذلك، وقدرة الخبير على اتقان ما أمر به دون ان يترتب على ذلك تدمير الأدلة المتحصل عليها وكذلك التمكن من نقل ادلة الاثبات غير المرئية وتحويلها الى ادلة مقروءة مع إثبات ان المخرجات الورقية لهذه الأدلة تتطابق مع ما هو مسجل على الحاسب أو النظام أو الشبكة [2].

المطلب الثاني: الإجراءات المستحدثة لتحقيق الرقمي

تعد الإجراءات المستحدثة من أهم الآليات التي فرضها التطور التكنولوجي في مجال التحقيق الرقمي الجنائي، إذ استحدث المشرع لمواجهة الجرائم الالكترونية والكشف عن مرتكبيها بفعالية أكثر.

وتتميز هذه الإجراءات بطابعها التقني واعتمادها على وسائل حديثة تسمح بتتبع النشاط الاجرامي، وذلك بما يتلاءم مع خصوصية الجريمة الالكترونية وطبيعة الفضاء الرقمي.

وعليه سنتطرق في هذا المطلب الى التسرب الالكتروني في (الفرع الأول)، اعتراض المراسلات في (الفرع الثاني)،المراقبة الالكترونية في (الفرع الثالث)، الحفظ والافشاء العاجلان للمعطيات الالكترونية (الفرع الرابع).

[1] انظر المواد قانون الإجراءات الجزائية.249،24،244،241

[2] بوقصة إيمان وبدايرية يحي، مرجع سابق، ص540

الفرع الأول: التسرب الالكتروني

هو تقنية من تقنيات التحري والتحقيق الخاصة، تقوم على قيام ضابط أو عون من الشرطة القضائية بالتغلغل داخل وسط أو جماعة إجرامية، تحت اشراف جهة قضائية مختصة، وذلك عبر إخفاء هويته الحقيقية واعتماد صفة مستعارة، بهدف كسب ثقة المشتبه فيهم ومراقبتهم من الداخل، والكشف عن أنشطتهم الاجرامية وجمع الأدلة المتعلقة بها.

يقصد بالتسرب بشكل عام هو قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية او جنحة بإيهامهم انه فاعل معهم أو شريك لهم أو خاف.[1] ويتم اللجوء لهذا الاجراء عندما تقتضي ضروريات التحري والتحقيق في الجرائم المنصوص عليها حصرا في نص المادة114 من قانون الإجراءات الجزائية، والتي من ضمنها الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، فيلاحظ ان القانون رقم09-04يكمل قانون الإجراءات الجزائية في حصره للجرائم المعنية بالتسرب، وذلك من خلال نص المادة02 منه التي تنص على انه يقصد في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال، جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات.

تتجلى عملية التسرب الالكتروني كآلية إجرائية مستحدثة في قدرتها على التكيف مع الطبيعة الافتراضية للجرائم المتصلة بتكنولوجيات الاعلام والاتصال، فبموجب هذا المفهوم القانوني، ينتقل ضابط الشرطة القضائية من أساليب التحقيق التقليدية الى اختراق الفضاء السيبراني عبر التخفي بأسماء مستعارة داخل غرف الدردشة ومنصات النقاش الرقمية، وتكمن الرابطة الجوهرية هنا في ان الجريمة الالكترونية بطبيعتها العابرة للحدود والمختفية خلف الشاشات، تفرض على المتسلل محاكاة السلوك الاجرامي الرقمي لضمان ادماجه، فيظهر بمظهر

[1] انظر المادة121، قانون الإجراءات الجزائية

المستخدم العادي لمراقبة الحوارات المتعلقة مثلا بدعارة الأطفال او بث الفيروسات واختراق الشبكات، [1]وتبرز خصوصية هذا الاجراء في الجانب التقني، حيث لا يكتفي المتسلل بالمراقبة، بل يسعى لاستدراج الجناة)الهكرز(للكشف عن أساليبهم في اقتحام المواقع، أو الخوض في نقاشات مباشرة حول محتويات غير قانونية، وهو ما يجعل التسرب الأداة الأكثر فعالية لكسر حاجز السرية الرقمية وكذا ضبط الأدلة في حالة التلبس، بما يتماشى مع الطبيعة التقنية والمعقدة لهذا النوع من الجرائم.

تعد تقنية التسرب من الوسائل الإجرائية الاستثنائية التي استحدها المشرع لمواجهة الجرائم المستعصية، وقد أحاطها بمجموعة من الضوابط الموضوعية والشكلية، وتتمثل هذه الشروط فيمايلي:

أولا: الشروط الموضوعية: تتمثل هذه الشروط في

1.ضرورة اللجوء للتسرب

يعتبر عنصر الضرورة الركيزة الأساسية لاعتماد أسلوب التسرب، حيث لا يتم اللجوء اليه إلا عندما تقتضي مقتضيات التحري أو التحقيق ذلك، وتتجلى هذه الضرورة في الحالات التي يصعب فيها الوصول الى الحقيقة أو الى الجناة باستخدام الوسائل التقليدية للبحث والتحري.

وبناء عليه، أجاز المشرع لوكيل الجمهورية أو قاضي التحقيق صلاحية الاذن بمباشرة هذه العملية بعد إخطار مسبق.[2]

2.طبيعة الجريمة

[1] اشرف عبد القادر قنديل، مرجع سابق،ص157.

[2] انظر المادة120، من قانون الإجراءات الجزائية.

لم يفتح المشرع نطاق إعمال تقنية التسرب أمام كافة الأنماط الاجرامية، بل حصرها على فئات محددة تتميز بالخطورة البالغة والتعقيد الفني، وفي سياق الجرائم الالكترونية يبرز هذا الشرط كضابط جوهري بالنظر الى خصوصية الجريمة الالكترونية.[1]

ثانيا: الشروط الشكلية :وتتمثل هذه الشروط في

1.الاذن

لا يمكن مباشرة عملية التسرب الابعد الحصول على إذن مسبق من وكيل الجمهورية أو قاضي التحقيق، شريطة اخطار النيابة العامة بذلك، وبناء عليه لا يجوز لضابط الشرطة القضائية القيام بعملية التسرب الا بعد الحصول على الاذن الصريح، ويشترط في هذا الاذن ان يكون مكتوب، وهو شرط جوهري نص عليه القانون، حيث يجب ان يتضمن جميع البيانات الأساسية، كهوية الجهة المصدرة له، وتحديد طبيعة الجريمة محل التحقيق، بالإضافة الى ذلك ينبغي ان يكون الاذن مسبب، أي يبين الأسباب التي دفعت الى اللجوء لأجراء التسرب.

2. مدة التسرب

بالرجوع الى نص المادة 124 من قانون الإجراءات الجزائية نجد ان المشرع قد حدد مدة التسرب بأربعة4 أشهر قابلة لتجديد مرة واحدة وذلك عند مقتضيات التحري والتحقيق، وعدم كفاية المدة الأولى التي حددها القانون[2].

الفرع الثاني: اعتراض المراسلات

[1] انظر المادة114، من نفس القانون.

[2] قيشاح نبيلة، التسرب كآلية للتحري والتحقيق في الجريمة المنظمة، جامعة تبسة، ص74.73, وانظر المادة124، قانون الإجراءات الجزائية.

يقصد باعتراض المراسلات ذلك الاجراء القانوني الذي يخول للسلطات القضائية المختصة، وبناء على إذن مسبق تتبع المراسلات والاتصالات التي تتم بين الأشخاص، سواء كانت سلكية أو لاسلكية أو حتى الكترونية، مع إمكانية تسجيلها أو نسخها أو الاحتفاظ بها، وذلك بهدف كشف الحقيقة وجمع الأدلة في إطار البحث والتحقيق في الجرائم، ويتم وفقا لذلك اعتراض المراسلات التي تكون عبارة عن بيانات قابلة للإنتاج، أو التوزيع، أو التخزين، أو الاستقبال، أو العرض[1].

وفي سياق الجريمة الالكترونية، يكتسي اجراء اعتراض المراسلات أهمية بالغة، نظرا لان هذا النوع من الجرائم يقوم أساسا على تبادل البيانات والمعلومات عبر الشبكات الرقمية، فالجناة يعتمدون على وسائل الاتصال الالكترونية للتخطيط لجرائمهم، والتنسيق فيما بينهم وتنفيذ أفعالهم، بل وحتى لإخفاء أثارها، وهو ما يجعل من اعتراض هذه المراسلات مدخلا أساسيا لكشف الجريمة الالكترونية.

ويلاحظ ان المشرع الجزائري لم يضع تعريف لاعتراض المراسلات، بل اكتفى بتنظيمه من خلال تحديد صوره وشروط اللجوء إليه[2]،وتتمثل هذه الشروط في:

أولا: الحصول على إذن قضائي مسبق ومسبب: لا يجوز المباشرة إجراءات الاعتراض الا بعد استيفاء الشروط التالية:

1.الجهة المختصة: يجب أن يصدر الإذن عن سلطة القضائية المختصة (وكيل الجمهورية أو قاضي التحقيق).

2.التعريف بالعملية :يجب ان يوضع الاذن بدقة ماهي المراسلات المستهدفة، ونوع الاتصالات التي سيتم رصدها وتسجيلها، مع تعيين الموقع أو الأجهزة المعنية بالعملية، كما

[1] غدامسي موسى، مرجع سابق، ص340.

[2] انظر المادة114، قانون الإجراءات الجزائية.

يجب أن يحدد في الإذن الفترة الزمنية المخصصة لعملية الاعتراض، والتي ينبغي الا تتجاوز أربعة أشهر كحد اقصى، مع بقاء إمكانية التجديد قائمة وفقا لما تراه السلطة القضائية مناسب.

ثانيا: تسبيب اللجوء الى اعتراض المراسلات: اي وجود مبرر قانوني وضرورة تستدعي القيام بهذا الاجراء الاستثنائي، حيث يشترط وكيل الجمهورية أو قاضي التحقيق تقديم أسباب جدية تبرهن على أن الاعتراض سيؤدي الى كشف ملابسات الجريمة وتحديد الجناة.

ثالثا: تحديد الجرائم محل الاعتراض: إن الاستعانة بتقنيات اعتراض المراسلات ليست مطلقة، بل هي محصورة في أنواع معينة من الجرائم دون غيرها لأغراض التحقيق، وهذه الجرائم على سبيل الحصر ومن بينها الجرائم المتصلة بتكنولوجيات الاعلام والاتصال[1].

رابعا: سرية الإجراءات وكتمان السر المهني: يجب ان تنفذ عملية الاعتراض في سرية مطلقة وبمعزل عن علم الشخص المشتبه فيهم أو مالكي الأماكن المستهدفة لضمان نجاح الاجراء، وبالتوازي مع ذلك يتوجب على كافة الأطراف المعنية بالتنفيذ الالتزام التام بواجب كتما السر المهني وعدم إفشاء أي معلومات يتم الاطلاع عليها[2].

الفرع الثالث: المراقبة الالكترونية

تعد مراقبة الاتصالات الالكترونية أداة قانونية وتقنية متطورة تتمثل في رصد وتتبع كافة المراسلات والبيانات المتداولة عبر الشبكات الرقمية، وذلك بهدف جمع الأدلة والمعلومات حول الأنشطة المشبوهة في الفضاء السيبراني، ويتمثل دورها الفعال في كونها الوسيلة الاستباقية الأهم للوقاية من الجرائم الالكترونية ومكافحتها، حيث تتيح للهيئات المختصة،

[1] بن عنطر سهام، التحقيق الجنائي في الجرائم الالكترونية، مذكرة ماستر، جامعة مولود معمري تيزيوزو، 2023، ص ص101.102.

[2] انظر المادة76، قانون الإجراءات الجزائية.

تحت إشراف القضاء القدرة على اختراق السرية التي يعتمد عليها مرتكبو الجرائم المعلوماتية، وكشف أساليبهم.

لقد استحدث المشرع هذا الاجراء بموجب المادة03 من القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، فيلاحظ ان لم يتطرق لي تعريف المشرع المراقبة الالكترونية، بل اكتفى بتحديد مفهوم الاتصالات الالكترونية في المادة02 من نفس القانون سالف الذكر، على "انها تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة وسيلة الكترونية". [1]وتكتسي المراقبة الالكترونية للاتصالات دور فعال في مواجهة الجريمة الالكترونية، وذلك من خلال تمكين جهات التحقيق من رصد السلوك الاجرامي في بيئته الرقمية قبل ضياع آثاره أو حذف بيانته، مما يساهم بفعالية في كشف الجرائم الالكترونية وتحديد مرتكبيها وتفكيك الشبكات الاجرامية الالكترونية.

أولا: الشروط الموضوعية لإجراء مراقبة الاتصالات الالكترونية: اقر القانون لمراقبة الاتصالات الالكترونية مجموعة من الضمانات التي انفرد بها القانون09-04 والمتمثلة في:

انه لتحقيق الغرض من عملية اللجوء الى المراقبة الالكترونية أقر المشرع اللجوء الى هذا الاجراء في حالات استثنائية المنصوص عليها في المادة04 من نفس القانون، وذلك لما لها من اعتداء على حق الانسان في سرية حياته الخاصة واتصالاته الشخصية، بغرض الوصول حقيقة الجريمة والكشف عن مرتكبها.[2]

[1] حليم رامي، مرجع سابق ص237.

[2] بوقصة ايمان وبدايرية يحي، مرجع سابق، ص542.

ومن مقتضيات التحريات والتحقيقات فانه يتم اللجوء الى اجراء المراقبة الالكترونية للاتصالات، متى تطلبت مستلزمات التحقيق الى ذلك، بحيث ان المشرع جعل من هذا الاجراء وسيلة وقائية للحماية من وقوع جرائم معينة[1].

ولجوء الى المراقبة الالكترونية يكون حتى بعد وقوع الجريمة، بغرض كشف مرتكبي الجريمة لان الإجراءات التقليدية اثبتت قصورها في كشف مرتكبي الجريمة الالكترونية، مما دفع بالمشرع الى استحداث هذا الاجراء لمواكبة التطور التقني للجريمة.

ثانيا: الشروط الشكلية لمراقبة الاتصالات الالكترونية:

اشترط المشرع لجواز اللجوء الى مراقبة الاتصالات الالكترونية ، توافر مجموع من الشروط لحماية حقوق الافراد وضمان عدم التعسف في استعمال هذا الاجراء، حيث نصت المادة04 من القانون09-04 على ضرورة صدور إذن قضائي مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق المختص، مع تحديد طبيعة الجريمة والاتصالات محل المراقبة، كما ان مدة هذا الاجراء هي 06اشهر قابلة للتجديد وفق نفس الشروط الشكلية والالزامية، وذلك تحت اشراف السلطة القضائية المختصة، بما يضمن مشروعية الاجراء وتحقيق التوازن بين فعالية التحري وحماية الحياة الخاصة[2].

الفرع الرابع: الحفظ والافشاء العاجلان للمعطيات الالكترونية

يقصد بإجراء الحفظ العاجل للمعطيات الالكترونية قيام السلطات المختصة بإلزام الأشخاص المختصة أو الجهات الحائزة للبيانات الالكترونية بحفظها بصورة فورية، حماية لها من الضياع أو التعديل أو الحذف، وذلك قصد تمكين جهات التحقيق من الاستفادة منها كدليل في الكشف عن الجريمة الالكترونية ومرتكبيها، ويكتسي هذا الاجراء أهمية بالغة خاصة

[1] انظر المادة03، من القانون09-04.

[2] اتفاقية بودباست لمكافحة الجرائم المعلومايتة، الموقعة في 23 نوفمبر 2001.

بالنظر الى الطبيعة السريعة والقابلة للمحو التي تتميز بها المعطيات الرقمية، اما الافشاء العاجل للمعطيات الالكترونية، فيتمثل في إلزام مزودي خدمات الاتصالات أو الأشخاص الحائزين للبيانات بالكشف السريع عن المعطيات المحفوظة ، بما يسمح بتتبع مصدر الاتصالات أو تحديد هوية المستخدمين المرتبطين بالنشاط الاجرامي، الامر الدي يساهم في تسريع إجراءات التحري والتحقيق في الجرائم الالكترونية.

يعتبر هذا الاجراء من الإجراءات المستحدثة الفعالة، بحيث تلزم مزودي خدمة الانترنت على تقديم المساعدة للتحقيق في جريمة معلوماتية، من خلال حفظ البيانات والمعلومات، أو إفشاء أي معلومة مهمة لمساعدة رجال الضبطية القضائية، بحيث في حال عدم التزامهم فإنه تترتب عليهم قيام مسؤوليتهم الجزائية. [1]

وبذلك فإن السلطة القضائية بعد إصدارها أمر بالحفظ العاجل لمعطيات المرور، يمكنها أن تلزم مقدمي الخدمات بالكشف الفوري عن تلك المعطيات، أو عن جزء منها، ووضعها تحت تصرف الجهات المكلفة بالتحقيق، بحيث يتم هذا الاجراء بشكل مستعجل قبل التلاعب أو تلف البيانات، وعليه فإن هذا الاجراء يمكن سلطات التحري من كشف هوية الأطراف المتورطة[2].

وقد حدد المشرع لمقدمي الخدمات حفظ:

المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات الطرفية المستعملة للاتصال بالإضافة الى الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

[1] انظر المادة10، من القانون09-04.

[2] باغي صبرينة وقريقة غادة، مرجع سابق، ص111.

وكذلك المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها[1]. ولعملية إجراء حفظ أو إفشاء معطيات المرور شروط تتمثل في:

أولا: احترام مدة الحفظ:

يعتبر الحفظ العاجل إجراء قانوني مؤقت تفرضه السلطة المختصة على مزود الخدمة، حيث تكون مدة الحفظ للبيانات والمعلومات الالكترونية سنة واحدة تبدا من تاريخ تسجيل البيانات، وبمجرد انتهاء هذه الفترة يتوجب على مزود الخدمة حذفها، بحيث ان مخالفة هذا الالتزام ترتب عقوبات صارمة تتراوح بين الحبس من(6أشهر الى 5سنوات)وغرامات مالية من(50.000دج الى500.0000دج)، مما يعكس جدية المشرع في ضبط هذا الاجراء[2].

ثانيا: التزام خاص بمقدمي خدمة الانترنت:

يتعين على مقدمي خدمة الانترنت، التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، ووضع ترتيبات تقنية تسمح بحصر إمكانية الدخول الى الموزعات التي تحوي معلومات مخالفة لنظام العام أو الآداب العامة وإخبار المشتركين بذلك[3].

المبحث الثاني: الأساليب الدولية للتحقيق في الجرائم الالكترونية

إن التطور السريع لتكنولوجيا الاعلام والاتصال وما نتج عنه من انتشار واسع لاستعمال الأنظمة المعلوماتية، أدى الى ظهور الجريمة الالكترونية كأحد أخطر الجرائم الحديثة، بالنظر لما تتميز به من طابع عابر للحدود وصعوبة اكتشاف مرتكبيها أو تتبع أدلتها الرقمية. وهو ما جعل إجراءات التحقيق التقليدية غير كافية لوحدها لمواجهتها، الامر

[1] انظر المادة11، من القانون09-04.

[2] المادة11، الفقرة الأخيرة، من نفس القانون.

[3] انظر المادة12، من القانون09-04.

الذي دفع بالتشريعات الحديثة الى استحداث إجراءات خاصة تتلاءم مع طبيعتها التقنية، بهدف تسهيل الكشف عن هذه الجرائم وجمع الأدلة المتعلقة بها.

غير أن فعالية هذه الإجراءات قد تبقى محدودة في بعض الحالات، خاصة عندما تمتد الجريمة الى أكثر من دولة أو تكون الأدلة الرقمية موجودة خارج الإقليم الوطني، مما أبرز الحاجة الى اعتماد أساليب دولية قائمة على التعاون والتنسيق بين الدول لمكافحة هذا النوع من الاجرام. وفي هذا الإطار، أصبح التعاون الدولي والتعاون القضائي الدولي من أهم الآليات المعتمدة في التحقيق ومكافحة الجريمة الالكترونية، من خلال تبادل المعلومات والخبرات، وتسهيل إجراءات جمع الأدلة الرقمية، وتسليم المجرمين، وتنفيذ الانابات القضائية الدولية.

لذا سيتم التطرق في هذا المبحث الى التعاون الأمني الدولي في (المطلب الأول)، ثم التعاون القضائي الدولي في (المطلب الثاني).

المطلب الأول: التعاون الأمني الدولي للتحقيق في الجرائم الالكترونية

نظرا للطبيعة العابرة للحدود التي تتميز بها الجريمة الالكترونية، أصبح التعاون الأمني الدولي ضرورة حتمية لمواجهتها والحد من مخاطرها، خاصة وأن مرتكبي هذه الجرائم يستغلون التطور التكنولوجي والفضاء الالكتروني لتنفيذ افعالهم من دول مختلفة وبطرق يصعب كشفها، لذلك اتجهت الدول الى تعزيز التنسيق والتعاون بين أجهزتها الأمنية من خلال تبادل المعلومات والخبرات التقنية وتعقب المجرمين الالكترونين.

اذا سيتم التطرق في هذا المطلب الى تعريف التعاون الأمني وأساسه في (الفرع الأول)، ثم صور التعاون الأمني الدولي في مجال التحقيق الرقمي والجهود المنظمة الدولية للشرطة الجنائية في (الفرع الثاني).

الفرع الأول: تعريف التعاون الأمني الدولي وأساسه

أولا: تعريف التعاون الأمني وأهميته

تعد ظاهرة التعاون الأمني الدولي ضرورة استراتيجية وحتمية قانونية في ظل العصر الرقمي، حيث يعرف بأنه تضافر الجهود الدولية المشتركة وتبادل الدعائم بين الوحدات الدولية، سواء كانت دولا أو منظمات، ويعرف أيضا على أنه حلقة وصل استراتيجية تهدف الى تبادل الخبرات، والمعلومات، والمساعدات التقنية والقانونية بين دولتين أو أ كثر، قصد التصدي للظواهر الاجرامية التي استغلت ثغرة العولمة لتطوير أساليبها.

ان هذا المفهوم يتجاوز فكرة الملاحقة الشرطية التقليدية، ليمتد الى منظومة متكاملة من العمل الوقائي والقمعي.

وتتجل أهمية هذا التعاون عند النظر الى التحولات النوعية في طبيعة الجريمة، فالدولة الوطنية، مهما امتلكت من ترسانة أمنية متطورة تبقى عاجزة بنيويا عن احتواء الجرائم التي تخطط في قارة ن وتنفذ في قارة ثانية، وتحقق آثارها في قارة ثالثة.

هنا يصبح التعاون الأمني الدولي هو المعدل الموضوعي لقوة الاجرام المنظم، فمن خلال أجهزة مثل "الإنتربول' و"إلافريبول " والاتفاقيات الثنائية، يتم خلق فضاء أمني موحد يسمح بتدفق المعلومات بسرعة تفوق سرعة انتقال الجريمة نفسها، وكذلك تبرز هذه الأهمية بشكل استثنائي في مجال الجريمة الالكترونية، التي ألغت الحدود الجغرافية، بحيث لا يمكن تتبع الجناة أو استرجاع الأدلة الرقمية المشفرة دون وجود بروتكولات تعاون تلزم الدول بتبادل البيانات والولوج المشترك لقواعد المعلومات [1].

ثانيا: أساس التعاون الأمني الدولي في التحقيق الرقمي

[1] معتوق محمد أكلي وعاشور سهام، التعاون الدولي في مكافحة الجريمة الالكترونية، مذكرة ماستر، جامعة برج بوعريريج، 2023، ص40.

تتجسد فعالية التحقيق في الجرائم الالكترونية في قدرة المنظومة الدولية على تفعيل تنسيق مؤسساتي رفيع المستوى، يتجاوز العوائق الجغرافية ليربط بين الأجهزة الأمنية وآلياتها المختلفة على الصعيدين الإقليمي والدولي، وهذا التنسيق ليس مجرد تبادل روتيني للمعلومات، بل هو استراتيجية تهدف الى محاصرة الجريمة من خلال التكامل التقني والعملياتي.

ويستند هذا التعاون في جوهره الى أساس قانوني واتفاقي متين، يتمثل في المعاهدات الثنائية والمتعددة الأطراف التي تمنح إجراءات التحقيق العابرة للحدود مشروعيتها القانونية، كما يمتد هذا الأساس ليشمل التعاون التقني وبناء القدرات، عبر تكثيف البرامج التدريبية المشتركة لتمكين مهارات المحققين في التعامل مع الأدلة الرقمية المعقدة[1].

الفرع الثاني: صور التعاون الأمني الدولي في مجال التحقيق الرقمي والجهود المنظمة الدولية للشرطة الجنائية

أولا: صور التعاون الأمني الدولي في مجال التحقيق الرقمي

يعد التعاون الأمني الدولي الركيزة الأساسية لضمان فعالية التحقيق الرقمي، اذ يتيح تجاوز العقبات التقنية والقانونية العابرة للحدود، وتتبع الأدلة الالكترونية الهشة وتأمينها وضبطها قبل ضياعها، مما يستلزم تظافر الجهود الدولية عبر عدة صور تضمن مشروعية ونجاعة التحقيق الجنائي في الفضاء السيبراني، وتتمثل في:

1.الربط الشبكي للاتصال وتبادل المعلومات: تعتبر سرعة تدفق المعلومات حجز الزاوية في ملاحقة الجريمة المعلوماتية، وهو ما فرض ضرورة إيجاد كيانات دولية (مثل المنظمات الدولية والإقليمية) تأخذ على عاتقها تطوير قنوات اتصال فورية، يهدف هذا الربط الشبكي الى تمكين سلطات التحقيق والملاحقة من التواصل اللحظي لتبادل البيانات والمعطيات

[1] بن عنطر سهام، مرجع سابق، ص106.

المتعلقة بالجرائم المرتكبة، مما يساهم في تسريع وتيرة التحقيق من هوية الجناة وتتبع آثارهم الرقمية عبر مختلف الأنظمة الوطنية.

2.تبادل المعاونة لمواجهة الازمات والمواقف الحرجة أثناء التحقيق: نظرا لتفاوت التقني والتشريعي بين الدول، قد تواجه بعض أجهزة العدالة الجنائية عقبات في مواجهة جرائم الكترونية كبرى تفوق إمكانياتها أو تحدث بشكل مفاجئ (كوارث سيبرانية). لذا تبرز هذه الصورة من التعاون كآلية لتكثيف الجهود وتظافر الجهود الدولية لمساعدة الدول الأقل جاهزية تكنولوجيا، وضمان توفير الخبرات الفنية الازمة لإجراء التحقيقات الرقمية المعقدة في الوقت المناسب، قبل استفحال الضرر أو ضياع الأدلة.

3.القيام بالعمليات الشرطية والأمنية المشتركة: تعد هذه الصورة الأكثر تقدما في ملاحقة مجرمي المعلوماتية عبر "الشبكة العنكبوتية"، حيث تشمل تنسيق عمليات ميدانية تهدف الى تعقب الجناة وتفتيش الأنظمة الحاسوبية العابرة للحدود بحثا عن الأدلة الرقمية، وتساهم هذه العمليات المشتركة ف تمكين المحققين من القيام ب عمليات التفتيش والضبط الرقمي وفق معايير فنية، مما يؤدي الى تحويل البيانات المبعثرة الى أدلة جنائية مقبولة قانونا.[1]

ثانيا: جهود المنظمة الدولية للشرطة الجنائية الانتربول في مجال التعاون الأمني:

تتمحور جهود منظمة الانتربول حول إرساء دعائم متينة لعمليات التحقيق الرقمي على المستوى الدولي، من خلال تعزيز قنوات الوصل بين الأجهزة الأمنية الشرطية لضمان سرعة تتبع المجرمين المعلوماتيين وضبط الأدلة الالكترونية، بدقة عالية حيث تضطلع المكاتب المركزية الوطنية بدور محوري في تأمين تبادل لحظي للبيانات الجنائية عبر منظومة اتصالات، تتيح للمحققين النفاذ المباشر لقواعد البيانات التقنية، وتتجلي نجاعة هذا التنسيق في النجاحات المحققة ضمن التحقيقات الرقمية المشتركة، كالعملية الدولية التي تمت

[1] صون آسيا، التعاون الدولي في مكافحة الجرائم الالكترونية، مذكرة ماستر، جامعة مستغانم، 2022، ص71.

بالتنسيق مع المباحث الفيدرالية الامريكية لتتبع وتحليل فيروس "دودة الحب" في الفلبين، وهو ما يؤكد أن الوصول الى نتائج ملموسة في التحريات السيبرانية لا يتوقف عند الجاهزية التقنية للأجهزة الأمنية فحسب، بل يمتد ليشمل ضرورة تكاتف الجهود الدولية وإثارة الوعي بمخاطر هذه الجرائم لضمان بيئة رقمية أكثر امان[1].

المطلب الثاني: التعاون القضائي الدولي في الجرائم الالكترونية

نظرا للطبيعة العابرة للحدود التي تتميز بها الجريمة الالكترونية، أصبح التعاون القضائي الدولي ضرورة أساسية لضمان فعالية التحقيق والمتابعة القضائية لهذا النوع من الجرائم، خاصة في الحالات التي يكون فيها الجاني أو الأدلة الرقمية موجودة خارج الإقليم الوطني.

لذلك اتجهت الدول الى تعزيز التعاون بين سلطاتها القضائية من خلال الانابات القضائية الدولية، وتسليم المجرمين، وتبادل المساعدة القضائية قصد تسهيل إجراءات التحقيق وجمع الأدلة الرقمية.

يهدف هذا التعاون القضائي الدولي الى تحقيق تنسيق فعال بين الدول بما يضمن عدم إفلات مرتكبي الجرائم الالكترونية من العقاب.

الفرع الأول: المساعدة القضائية والتحقيقات المشتركة في مجال الجريمة الالكترونية

أولا: المساعدة القضائية المتبادلة في مجال الجريمة الالكترونية

يمثل التعاون القضائي الركيزة الأساسية للتنسيق بين السلطات القضائية عبر، الدول ويهدف بشكل رئيسي الى تفعيل الإجراءات الجنائية الرقمية، بدءا من مرحلة التحقيق والمحاكمة

[1]بن عنطر سهام، مرجع سابق،ص108.

وصولا الى تنفيذ الاحكام، الغاية الأسمى من هذا التعاون هي محاصرة الجريمة وضمان عدم إفلات الجناة من العقاب نتيجة اختلاف الحدود الجغرافية والقوانين الوطنية.

وقد أولت الاتفاقيات الدولية (كاتفاقية الأمم المتحدة لمكافحة الجريمة) أهمية بالغة لهذا النوع من المساعدة، حيث ألزمت الدول الأطراف بتقديم أقصى درجات الدعم القانوني المتبادل في التحقيقات القضائية، كما كرس المشرع الجزائري في القانون رقم09-04، معتبرا أن التحريات والتحقيقات الجارية لجمع الأدلة في الجرائم الالكترونية تقع ضمن صلب مهام السلطات المختصة.

تتخذ المساعدة القضائية بين الدول عدة اشكال إجرائية يكن حصرها في:

1.تبادل المعلومات: حيث تلتزم الدول بتقديم الوثائق والمستندات التي تطلبها السلطات القضائية أو الأمنية الأجنبية، بم في ذلك بيانات الاتهام الموجهة للرعايا في الخارج، والاطلاع على السوابق القضائية للجناة[1].

2.نقل الإجراءات: في إطار التعاون القضائي الدولي في مجال التحقيق الرقمي وفعاليته في مواجهة الجرائم الالكترونية، أجاز المشرع اتخاذ إجراءات جنائية في إقليم دولة أخرى بناء على مبدا المعاملة بالمثل وتوافر شرط التجريم المزدوج، وكل ذلك يصب في مصلحة العدالة ويهدف لضمان سير التحقيقات في البيئة أكثر ملاءمة للوصول الى الحقيقة[2].

ثانيا: التحقيقات المشتركة في مجال الجرائم الالكترونية

تفرض الطبيعة الخاصة للجرائم الالكترونية ضرورة حتمية للتعاون القضائي الدولي، نظرا لطابعها العابر للحدود، مما يستوجب تشكيل فرق تحقيق مشتركة تضم الجهات المختصة في كافة الدول التي شهدت مسرح الجريمة أو جزء من نشاطها.

[1] هادي زياده، آليات التعاون الدولي في مكافحة الجريمة السيبرانية، مذكرة ماستر، جامعة مستغانم،2023، ص43.42.

[2] انظر المادة17، من القانون 09-04.

يبرز نموذج "محاربي شمال أوروبا (الفايكنغ)" كمثال حي على نجاح هذا التنسيق، ففي يونيو2009 تكاتفت أجهزة الشرطة في اربع دول للإطاحة بهذه المجموعة التي كانت تدير شبكة دولية لاستغلال الأطفال عبر الانترنت، وأسفرت العملية عن ضبط 50شخصا متورطا في تداول محتويات غير قانونية، الا انه رغم ما يحققه هذا النوع من التحقيقات من توحيد الجهود وتعزيز الامن الجماعي، يبقى الواقع العملي لايزال يواجه تحدي البطء في الإجراءات، مما يستدعي ضرورة اعتماد كوادر مؤهلة أكثر تقنية لضمان سرعة كشف الغموض المحيط بالجرائم الرقمة، ومن ثمة تدعيم ركائز التعاون القضائي الدولي لمواجهة هذه المخاطر[1].

الفرع الثاني: الانابة القضائية الدولية

تعد الانابة القضائية الدولية من أرقى وأهم آليات التعاون الدولي المعاصر، حيث تهدف الى تفعيل الحماية القانونية العابرة للحدود من خلال استكمال إجراءات التحقيق التي تقع خارج النطاق الإقليمي للقاضي الوطني، وتبرز نجاعة هذه الآلية بشكل جلي في مواجهة الظواهر الاجرامية المتطورة، خاصة الجرائم المعلوماتية، وتظهر فعالية الانابة القضائية الدولية من خلال تمكين القاضي الوطني من التعويل على نتائج التحريات الرقمية التي تجريها سلطات قضائية أجنبية، مما يضمن استمرار الدعوى العمومية وعدم توقفها أمام الحواجز الجغرافية[2].

خلاصة الفصل الأول

[1] بن عنطر سهام، مرجع سابق، ص116.

[2] معتوق محمد أكلي وعاشور سهام،مرجع سابق،ص43

في ختام هذا الفصل، يتبين أن التحقيق الرقمي في مواجهة الجرائم الالكترونية أصبح يعتمد على مقاربة شاملة تجمع بين تطور الوسائل الإجرائية الداخلية والانفتاح على آليات التعاون الدولي، وذلك بالنظر الى خصوصية هذا النوع من الجرائم التي تتميز بالسرعة والتعقيد، وتجاوز الحدود الإقليمية.

فمن جهة، لم تعد الإجراءات التقليدية وحدها كافية لضبط هذا النوع من الجرائم، رغم دورها الأساسي في تكريس الشرعية الإجرائية وضمان حقوق الأطراف، وقد استدعى ذلك تبني إجراءات أكثر مرونة وتطور تقوم على توظيف الوسائل التقنية الحديثة في البحث وجمع الأدلة الرقمية وحفظها وتحليلها، بما يتلاءم مع طبيعة الفضاء الرقمي.

ومن جهة أخرى، أضحت الأساليب الدولية للتحقيق في الجرائم الالكترونية بمختلف صوره، ضرورة حتمية في مواجهة الجريمة الالكترونية، سواء من خلال التنسيق الأمني بين الأجهزة المختصة أو عبر آليات التعاون القضائي التي تسمح بتبادل المعلومات وتنفيذ الانابات القضائية الدولية، وهو ما يعزز فعالية التحقيق ويحد من الإفلات من العقاب.

وبناء عليه، يمكن القول ان التحقيق في الجريمة الالكترونية يقوم اليوم على توازن دقيق بين تحديث الإجراءات الداخلية وتفعيل الأساليب الدولية للتحقيق، بما يضمن مواجهة فعالة لهذا النوع من الجرائم في إطار يحترم الضمانات القانونية ويواكب التطور التكنولوجي المتسارع.

الفصـــــــل الثانـي:

الآثار القانونية للتحقيق الرقمي

والضمانات الإجرائية المقررة له

تمهيد:

ساهم التطور الرقمي في بروز التحقيق الرقمي كوسيلة حديثة لمواجهة الجرائم الإلكترونية، لما له من دور فعال في كشف الحقيقة والوصول إلى الأدلة التقنية. غير أن هذا التطور لم يخلُ من آثار قانونية وإجرائية مهمة، خاصة فيما يتعلق بحجية الدليل الرقمي وضمانات مشروعية الحصول عليه حفاظاً على الحقوق والحريات الفردية.

وأمام هذا التطور، لم يعد الدليل في صورته التقليدية كافيًا لمواجهة الجرائم المرتكبة في البيئة الرقمية، بل برز ما يُعرف بالدليل الرقمي باعتباره أداة إثبات ذات طبيعة خاصة، تقوم على بيانات ومعلومات إلكترونية قابلة للاستخراج والتحليل بوسائل تقنية متخصصة. غير أن خصوصية هذا الدليل من حيث قابليته للتعديل والنسخ وسهولة إتلافه تثير إشكالات قانونية دقيقة تتعلق بمدى حجيته وشروط قبوله أمام القضاء.

ومن جهة أخرى، فإن إجراءات البحث والتحري في المجال الرقمي قد تمسّ بشكل مباشر حقوقًا أساسية، كحرمة الحياة الخاصة وسرية المراسلات وحق الدفاع...، مما يستوجب إحاطتها بجملة من الضمانات القانونية التي تكفل عدم الانحراف بها عن مبدأ الشرعية الإجرائية.

ويعود الاهتمام المتزايد بالتحقيق الرقمي إلى التحول العميق الذي شهدته المجتمعات المعاصرة نتيجة الانتشار الواسع لتكنولوجيات الإعلام والاتصال، حيث أصبحت مختلف الأنشطة الاقتصادية والإدارية والاجتماعية تعتمد بشكل متزايد على الأنظمة المعلوماتية والوسائط الرقمية.

وقد ترتب عن هذا التحول ظهور أنماط جديدة من الجرائم استهدفت البيانات والأنظمة الإلكترونية أو استعملت الوسائل الرقمية كأداة لارتكابها، الأمر الذي فرض على أجهزة العدالة الجنائية البحث عن آليات أكثر فعالية تتلاءم مع خصوصية البيئة الرقمية.

كما أن الأدلة المرتبطة بهذا النوع من الجرائم تختلف عن الأدلة التقليدية من حيث طبيعتها وطرق حفظها واستخراجها، فهي غالبا ما تكون في شكل بيانات أو سجلات إلكترونية تحتاج على وسائل تقنية متخصصة للكشف عنها وتحليلها. ولذلك أصبح نجاح التحقيق في الجرائم الإلكترونية مرتبطا بمدى القدرة على التعامل الصحيح مع الدليل الرقمي، منذ مرحلة جمعه وحفظه إلى غاية تقديمه أمام الجهات القضائية المختصة.

ومن هذا المنطلق، برزت أهمية الدليل الرقمي باعتباره حجر الأساس في إثبات الجرائم الإلكترونية، إذ يساهم في كشف حقيقة الوقائع وتحديد هوية الجناة وربطهم بالأفعال الإجرامية المنسوبة إليهم، غير أن الاعتماد على هذا الدليل يثير العديد من المسائل القانونية المتعلقة بحجيته وشروط قبوله ومدى تمتعه بالقوة الثبوتية اللازمة في المجال الجنائي.

وتأسيسا على سبق، فإن دراسة الدليل الرقمي والضمانات القانونية المرتبطة به أصبحت من المسائل الجوهرية في مجال التحقيق الرقمي، لما لها من أثر مباشر على فعالية مكافحة الجرائم الإلكترونية من جهة، وضمان احترام الحقوق والحريات الأساسية من جهة أخرى. الامر الذي يبرز الحاجة إلى الوقوف على مختلف الجوانب القانونية والفنية التي تحكم هذا النوع من الأدلة وتحدد قيمته في الإثبات الجنائي.

وعليه، يهدف هذا الفصل إلى تأصيل المفهوم القانوني للدليل الرقمي وبيان خصائصه وإطاره التشريعي (المبحث الأول)، ثم تحليل الضمانات التي تحكم إجراءات التحقيق فيه (المبحث الثاني)، في محاولة للكشف عن مدى تحقيق التوازن بين مقتضيات الفعالية في مكافحة الجريمة الرقمية ومتطلبات حماية الحقوق والحريات الأساسية.

المبحث الأول: الإطار القانوني للدليل الرقمي

يعتبر الدليل الرقمي كوسيلة من وسائل الإثبات غير المادية، ويرجع ذلك لسبب الطبيعة الفنية والتقنية للجرائم المعلوماتية عند ارتكابها خاصة الجرائم السرية، كما أن محاولة الجاني لطمس الدليل المادي للجريمة يزيد من صعوبة إثبات الجريمة، وهذا ما يؤدي إلى استخدام نوع جديد من البيانات لمحاكاة الفعل الإجرامي عُرفت باسم الدليل الرقمي أو الدليل الإلكتروني، حيث أصبحت المحاكم تأخذ هذا الدليل ليس فقط في القضايا ذات الطبيعة الإلكترونية بل حتى في القضايا العادية وبعض الجرائم التقليدية خاصة في حالات المسح والحوسبة الإلكترونية وتحديد وفحص مسرح الجريمة.

المطلب الأول: مفهوم الدليل الرقمي

تعددت التعريفات الاصطلاحية للدليل الرقمي وإن كانت في مجملها تجتمع في نقطة محددة تتعلق بالبيئة الالكترونية لهذا الدليل الحديث، مع تميزه بجملة من الخصائص.

وعليه سيتم التطرق في هذا المطلب الى تعريف الدليل الرقمي وتمييزه عن الأدلة التقليدية في (الفرع الأول)، خصائص الدليل الرقمي في (الفرع الثاني)، والطبيعة القانونية للدليل الرقمي وحجيته في الإثبات الجنائي في (الفرع الثالث).

الفرع الاول: تعريف الدليل الرقمي وتمييزه عن الأدلة التقليدية

أولاً: تعريف الدليل الرقمي

الدليل الرقمي:" هو الدليل المأخوذ من أجهزة كمبيوتر في شكل موجات ونبضات مغناطيسية أو كهربائية يمكن تجميعها و تحليلها بواسطة برامج تطبيقات و تكنولوجيات

خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الرسوم من أجل اعتماده أمام أجهزة تطبيق القانون[1].

كما يعرف بأنه " الدليل الذي يجد له أساساً في العالم الافتراضي إلى الجريمة"[2].

أيضاً هناك تعريف آخر يشير إلى أن الدليل الرقمي هو مجموعة من الوقائع المثبتة أو المسندة كدليل إلكتروني "الأرقام أو الرموز أو الأقراص الإلكترونية" والذي يؤدي إلى إقناع قاضي الموضوع بثبوت ارتكاب شخص ما جريمة ما عبر الإنترنت أو عبر استخدامه للحاسوب أو أي جهاز إلكتروني آخر[3].

ويُعرَّف الدليل الرقمي كذلك بأنه: "الدليل المستمد من النظم البرمجية المعلوماتية وأجهزة ومعدات الحاسب الآلي وشبكات الاتصال، والذي يتم الحصول عليه وفق إجراءات قانونية وتقنية، ثم إخضاعه للتحليل العلمي قصد تقديمه أمام القضاء"[4].

ونستخلص مما سبق أن الأدلة الجنائية الرقمية هي عبارة عن مجموعة من البيانات الرقمية التي تتكون من مجموعة من الأرقام والحروف والرموز التي تمثل مختلف المعلومات والمعطيات، بما فيها النصوص المكتوبة والرسومات والخرائط والصور والفيديوهات وغيرها من الروابط المعلوماتية التي تنطوي على بيانات خاصة بالأفراد أو الأشخاص المعنوية والهيئات، تكون مخزنة في أجهزة الحاسوب وملحقاتها من ديسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات كالطابعات والفاكس أو متنقلة عبر شبكات الإتصال والأنترنت،

[1] عيدة بلعابد، "الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية "، مجلة أفاق علمية ، جامعة سعيدة، الجزائر، العدد 1 المجلد 11 ، السنة 2019 ص 137 .

[2] عمر محمد أبوبكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، دار النهضة العربية، القاهرة، 2004م. ص969 .

[3] يس حسن محمد عثمان ، الدليل الرقمي وأثره على الدعوى الجنائية ، مجلة العلوم القانونية والاجتماعية،جامعة زيان عاشور بالجلفة ، الجزائر، العدد 3 المجلد 5 ، سبتمبر 2020،ص318.

[4] عائشة بن قارة مصطفى، مرجع سابق، ص 52-53

والتي يمكن تجميعها وتحليلها بإستخدام برامج وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبها".

ثانيا: تمييز الدليل الرقمي عن الأدلة التقليدية

- إن مخاطر إتلاف الدليل الرقمي تقل أو تعدم تقريبا، لأنه يمكن نسخ الدليل الأصلي مرة أخرى من جهاز الكمبيوتر عدة مرات، حيث تتطابق طريقة النسخ مع طريقة الإنشاء، بينما لا يمكن نسخ الدليل التقليدي إطلاقا.[1]
- إن إستخدام التطبيقات والبرامج الصحيحة يكون من السهولة تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل، بينما يمكن تغيير الدليل التقليدي دون أن يظهر هذا التغيير.[2]
- إن هناك إمكانية إعادة الدليل الرقمي إلى حالته الأصلية بعد تحطيمه أو محوه من ذاكرة الكمبيوتر و ذلك بإعادة إسترجاعه من خلال القرص الصلب للكمبيوتر، بينما قد توجد صعوبة كبيرة لإسترجاع الدليل التقليدي بعد إتلافه .[3]

الفرع الثاني: خصائص الدليل الرقمي

يتميز الدليل الرقمي بمجموعة من الخصائص نوردها فيما يلي:

أولاً: الدليل الرقمي دليل غير ملموس

يتميّز الدليل الرقمي بكونه غير ملموس في أصله، إذ يتمثل في بيانات ومعلومات ذات صيغة رقمية مجردة، ولا يمكن إدراكها بشكل مادي إلا عبر استعمال أجهزة الحاسوب والوسائط التقنية المناسبة والبرمجيات الخاصة. كما يتسم هذا النوع من الأدلة بسرعة التعامل

[1] انظر المادة 7 من القانون 09-04 ،مرجع سابق .

[2] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الرقمي في الجرائم الكمبيوتر و الانترنت، دارالكتب القانونية ، مصر ، سنة 2006 ص 89 .

[3] المرجع نفسه ، ص89 .

معه وسهولة تداوله، إلى جانب صعوبة القضاء عليه نهائياً، حيث إن محاولة الجاني حذف أو إتلاف هذا الدليل قد تترك آثاراً رقمية يمكن تتبعها واستغلالها ضده كقرينة إثبات[1].

ثانياً: الدليل الرقمي دليل متطور

إن التطور المتسارع الذي يشهده العالم اليوم في مجال التكنولوجيا والاتصالات أدى إلى تنوع الدليل الرقمي وتعدد صوره بشكل مستمر، الأمر الذي فرض ضرورة مواكبة هذا التطور بوسائل حماية فعالة. لذلك لم تعد الحماية القانونية وحدها كافية، بل أصبح من الضروري تدعيمها بحماية تقنية وفنية تضمن سلامة البيانات والمعلومات الرقمية.

وفي هذا الإطار، تعتمد كبرى المواقع والمنصات الإلكترونية على أنظمة حماية متطورة لإحاطة بياناتها المخزنة بسياج أمني وتقني، بهدف منع أي ولوج غير مشروع إليها، سواء كان الغرض من ذلك تدمير البيانات أو تعديلها أو الاطلاع عليها أو نسخها بطرق غير قانونية، وهو ما يعكس الأهمية المتزايدة التي أصبحت تحظى بها حماية الدليل الرقمي في البيئة الإلكترونية الحديثة[2].

ويُعد الدليل الرقمي من الأدلة التي تتسم بالتطور المستمر، نظراً لارتباطه الوثيق بالتقدم التكنولوجي في البيئة الرقمية. فمع التطور المتسارع في مجالات الإعلام الآلي ووسائل الاتصال، يتجدد هذا الدليل ويتطور من حيث أشكاله ووسائل الحصول عليه، مما يجعله دليلاً ديناميكياً يتكيف مع التحولات التقنية الحديثة.

ثالثاً: صعوبة إتلاف الدليل الرقمي

[1] بن الطيبي مبارك، رحموني محمد، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية ، مجلة القانون والعلوم السياسية، جامعة أحمد دراية، أدرار العدد 2 المجلد 5 ، سنة 2019 ص23.

[2] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي ، جامعة الإسكندرية، العدد 24، مصر، 1992، ص30-40

تُعتبر صعوبة التخلص من الدليل الرقمي أحد أهم خصائص الدليل الرقمي على الإطلاق بل إنه يمكن إعتبارها ميزة يتمتع بها الدليل الرقمي عن غيرها من الأدلة الجنائية الأخرى، لأن الدليل الرقمي في كثير من الحالات لا يمكن إتلافه أو تدميره أو التخلص منه بأي طريقة خاصة الرموز والأحرف والأرقام. الأدلة التقليدية التي يعرفها القانون تجد قوتها أمام القضاء في مسألة التشريع في كيفية الحصول عليها ومدى مشروعيتها، فبصمات الأصابع (finger print) مثلاً يمكن أن تكون محل إشكال خاصة إذا طالت المدة بين وقت إرتكاب الجريمة وبين الحصول عليها، وكذلك الشهادة إذا مضى عليها مدة من الزمن فإن مسألة الإستعانة بها تخضع لتحقيق متواصل بحيث يجب التعرف على مدى قدرة الشاهد على التذكر والعوامل المؤثرة في الذاكرة وما إذا كان يتمتع بمستوى ذاكرة مقبولة وفق نظرية ذاكرة الرجل العادي التي يعرفها القانون[1].

رغم إمكانية تعرض الدليل الرقمي لمحاولات الإتلاف، سواء بالحذف الكلي أو الجزئي، إلا أن هذه العمليات لا تؤدي بالضرورة إلى زواله بشكل نهائي. إذ يمكن في العديد من الحالات استرجاع البيانات المحذوفة باستخدام تقنيات متخصصة أو من خلال النسخ الاحتياطية المخزنة، وهو ما يعزز من قوة هذا الدليل ويحدّ من إمكانية التخلص منه بشكل تام.[2]

الفرع الثالث: الطبيعة القانونية للدليل الرقمي وحجيته في الإثبات الجنائي.

أولاً: الطبيعة القانونية للدليل الرقمي

1-اعتبار الدليل الرقمي دليلا حديثا في الاثبات الجنائي: يُعد الدليل الرقمي من الأدلة الحديثة في الإثبات الجنائي، إذ لم يكن معروفاً ضمن الوسائل التقليدية، وإنما أفرزه التطور التكنولوجي وظهور الجرائم المرتبطة بالأنظمة المعلوماتية. ويتميز بكونه غير مادي وقابلاً للنسخ والتعديل، مما يفرض إخضاعه لوسائل تقنية خاصة. ورغم

[1] حسن طاهر داؤد، جرائم نظم المعلومات، ط 1، الرياض، السعودية، 2000،ص29

[2] عيدة بالعابد، المرجع السابق، ص 138.

حداثته، فقد اعترف به المشرع الجزائري ضمنياً من خلال النصوص المتعلقة بمكافحة الجرائم المعلوماتية، وكذا مبدأ حرية الإثبات[1].

2- تكييف الدليل الرقمي بين الدليل المادي والدليل المعنوي

تنوع الأدلة الرقمية وطبيعتها لا تخرج على أن تكون ذات طبيعة مادية، أو طبيعة معنوية؛ فالأدلة المادية يقصد بها تلك الأدلة التي يمكن إدراكها بالحواس، وتتميز بطبيعة محسوسة كوجود الشيء المسروق في حيازة الجاني، بمعنى آخر أن الأدلة المادية هي التي تخرج من عناصر مادية معبرة عن نفسها، ولها تأثير في اقتناع القاضي بطريقة مباشرة.

أما الأدلة المعنوية فهي عكس الأدلة المادية، أي ليس لها وجود مادي ملموس يُعبّر عنها، سواء كان الأمر بالقول أو الإيحاء أو الكتابة، فهذه الأدلة يُطلق عليها تعبير الأدلة الناطقة، وهذا راجع إلى أن هذه الأدلة تصل للقاضي عن طريق لسان الغير كاعتراف المتهم وشهادة الشهود. وبقول آخر هي تلك الأدلة الصادرة من إرادة شخصية والمتجسدة في أقوال الغير، وتؤثر في اقتناع القاضي بطريقة غير مباشرة[2].

3-استقلالية الدليل الرقمي كوسيلة إثبات قائمة بذاتها

أثار موضوع استقلالية الدليل الرقمي نقاشاً فقهياً واسعاً، حيث ذهب اتجاه إلى اعتباره مجرد صورة حديثة للكتابة الإلكترونية، لا يخرج عن إطارها التقليدي. في المقابل، يرى اتجاه آخر أنه يتمتع باستقلالية تامة كوسيلة إثبات، بالنظر إلى طبيعته التقنية الخاصة والأساليب المميزة المعتمدة في استخراجه وتحليله. ويُرجّح هذا الرأي الأخير، على أساس أن الدليل

[1] عبد الفاتح بيومي حجازي، الدليل الرقمي وحجيته في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، 2010، ص25.

[2] هلال آمنة ، الإثبات الجنائي بالدليل الإلكتروني ، مذكرة ماستر في القانون الجنائي ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر بسكرة، 2014.2015 ،ص10.

الرقمي ينفرد بخصائص تقنية ووظيفية تجعله دليلاً قائماً بذاته، مع بقائه خاضعاً في تقديره لسلطة القاضي وفق مبدأ حرية الإثبات[1].

ثانياً: حجية الدليل الرقمي في الإثبات الجنائي

1-سلطة القاضي في تقدير الدليل الرقمي

1-1 سلطة القاضي الجنائي في تقدير الأدلة بذاتها

يتضح من خلال اجتهادات وأحكام محاكم النقض أن القاضي الجنائي يتمتع بسلطة واسعة في تقدير الأدلة المعروضة أمامه، إذ يملك الحرية الكاملة في تكوين قناعته الشخصية تجاه الدليل، دون أن يكون ملزمًا بالأخذ به متى لم يطمئن إلى صحته أو سلامته. وله كذلك أن يعتمد الدليل كاملاً إذا اقتنع بحجيته، أو أن يأخذ بجزء منه فقط ويطرح الجزء الآخر الذي لا ينسجم مع اقتناعه القضائي، وذلك في إطار مبدأ حرية الاقتناع القضائي الذي يحكم الإثبات الجنائي .

1-حرية القاضي الجنائي في استبعاد الأدلة:

يملك القاضي الجنائي سلطة استبعاد أي دليل يراه غير كافٍ أو غير مقنع، حتى وإن كان هذا الدليل قد تم الحصول عليه وفق الإجراءات القانونية، فالعبرة ليست بوجود الدليل فحسب وإنما بمدى اطمئنان القاضي إليه واقتناعه بقيمته الإثباتية. ولذلك يجوز له أثناء ممارسته لسلطته التقديرية في الدعوى أن يطرح الدليل جانبًا إذا رأى أنه يشوبه شك أو غموض أو لا يؤدي إلى الحقيقة بصورة مؤكدة[2].

---

[1] عبد الفاتح بيومي حجازي، مرجع سابق ، 110 .

انظر مادة 349 من قانون الاجراءات الجزائية، 25-14 .

[2] بن فردية محمد ، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة دكتورة في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر،2015، ص318 .

2-حرية القاضي الجنائي بالأخذ بالدليل:

كما يتمتع القاضي بحرية واسعة في الأخذ بالأدلة، إذ يمكنه الاعتماد على الدليل كاملاً دون تجزئة إذا اقتنع بصحته، كما يجوز له الأخذ بجزء منه فقط وطرح الجزء الآخر، باعتباره صاحب السلطة في تقدير القيمة الإثباتية لكل دليل. وله كذلك أن يهدر الدليل كليًا إذا لم يطمئن إليه، أو أن يأخذ به بالنسبة إلى متهم معين دون غيره من المتهمين في نفس الدعوى، متى رأى أن ظروف الدعوى وملابساتها تبرر ذلك.

2-1: سلطة القاضي الجنائي في تقدير الأدلة من حيث مصدرها

إن سيادة مبدأ الاقتناع القضائي في مجال الإثبات الجنائي أعطت للقاضي الجزائي الحرية في تقدير الأدلة بصرف النظر عن المصدر الذي استمدت منه مادام مشروعاً سواء كان هذا الدليل قد تحصل عليه في مرحلة من مراحل جمع الأدلة أو مرحلة التحقيق الابتدائي أو مرحلة المحاكمة[1].

2-3: سلطة القاضي الجنائي في تقدير الأدلة بمجموعها

إن الرأي السائد في مادة الإثبات الجنائي أن للقاضي الجنائي أن يقدر الأدلة بمجموعها ويستخلص منها قناعته، فالأدلة متساندة ومتآزرة يشد بعضها بعضا وأي خلل قد يحدث فيها قد يؤدي إلى إسقاط الأدلة كافة[2].

2-مساواة الدليل الرقمي بالأدلة التقليدية من حيث القوة القانونية

ترتب عن الاعتراف بالدليل الرقمي ضمن وسائل الإثبات الجزائي، اتجاه الفقه والتشريع الحديث إلى منحه نفس القوة القانونية التي تتمتع بها الأدلة التقليدية، وذلك متى تم الحصول عليه بطرق مشروعة وتوفرت فيه شروط السلامة الفنية والإجرائية. ويستند هذا التوجه إلى

[1] مرجع نفسه، ص322 .

[2] مرجع نفسه، ص 324 .

مبدأ حرية القاضي الجزائي في تكوين قناعته، بحيث لا يتقيد بنوع معين من الأدلة، بل يوازن بينها وفق ما تقتضيه ظروف كل قضية، غير أن هذه المساواة تبقى نسبية، بالنظر إلى الطبيعة التقنية الخاصة للدليل الرقمي، التي تجعله أكثر عرضة للتلاعب أو التغيير مقارنة بالأدلة المادية، الأمر الذي يفرض ضرورة إخضاعه لرقابة فنية وخبرة متخصصة لضمان مصداقيته. وعليه، فإن الدليل الرقمي أصبح يحتل مكانة موازية للأدلة التقليدية في الإثبات الجزائي، مع احتفاظه بخصوصيته التقنية التي تستوجب ضوابط إضافية عند التعامل معه[1].

المطلب الثاني: شروط قبول الدليل الرقمي

لا يمكن الاعتداد بالدليل الرقمي كأداة إثبات في الجريمة الالكترونية إلا إذا رافقته جملة من الشروط بمقتضاها يمكن قبوله كدليل إثبات في الجريمة الإلكترونية، وفيما يلي نبين جملة الشروط المطلوبة:

اذا سيتم التطرق في هذا المطلب الى مشروعية الدليل الرقمي في (الفرع الأول)، وأن يكون الدليل يقينيا في (الفرع الثاني).

الفرع الأول: مشروعية الدليل الرقمي

يقصد بالمشروعية أن يكون الدليل الرقمي مشروعاً من حيثً الوجود، وذلك بأن لا يكون مخالفاً للقانون في ذاته ومضمونه[2]، أي أن إجراءات جمع الأدلة الرقمية المستخرجة من الحاسب الآلي أو أي وسيلة إلكترونية أخرى، إذا تمت بطريقة مخالفة للقواعد القانونية والإجرائية التي تحدد كيفية الحصول عليها وضبطها، فإنها تفقد مشروعيتها وتصبح باطلة من الناحية القانونية.

[1] انظر المادة 349 ، قانون الإجراءات الجزائية .

[2] قنديل أشرف عبد القادر، مرجع سابق، ص207 .

وبالتالي لا يجوز للمحكمة الاعتماد عليها أو الاستناد إليها كدليل لإثبات الإدانة في المواد الجزائية، لأنها تكون قد شابها عيب في طريقة الحصول عليها يجعلها غير صالحة للإثبات [1].

أولا: سلامته التقنية وعدم التلاعب به

يشترط لقبول الأدلة المستمدة من الحاسب الآلي أن تتسم بدرجة عالية من الموثوقية واليقين، بحيث تعكس الحقيقة الواقعية قدر الإمكان وتبتعد عن كل ما هو قائم على الشك أو الافتراض. فلا يمكن الاعتماد عليها لإصدار حكم بالإدانة إلا إذا بلغت حدّ الإقناع الجازم لدى القاضي، إذ لا يُمكن المساس بقرينة البراءة أو العدول عنها إلا عندما يتكوّن لديه اقتناع مبني على اليقين لا على الاحتمال[2].

ثانياً: إمكانية مناقشة الدليل الرقمي

ويعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة فالقاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى، إذ لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضورياً أمامه[3]. وهذا يعني أن الأدلة المتحصلة من جرائم الحاسب الآلي سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب، أو كانت بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية ، كل هذه ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة

[1] نور الهدى محمود ، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث لدراسات الأكاديمية ، جامعة باتنة ، العدد 11 ، جوان 2017، ص919.

[2] بن الطيبي مبارك، مرجع سابق ص27.

[3] انظر المادة 212 ، قانون الاجراءات الجزائية.

تكنولوجيا المعلومات، يجب أن يعرض في الجلسة بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحواسيب[1].

ولا يختلف الدليل الرقمي عن باقي الأدلة الجنائية من حيث ضرورة مناقشته أمام القضاء، رغم طبيعته التقنية الخاصة، إذ قد يكون في شكل بيانات إلكترونية معروضة على أجهزة الحاسوب، أو ملفات رقمية مستخرجة منها، أو محفوظة على أقراص مدمجة أو وسائط إلكترونية مختلفة. لذلك يتعين على المحكمة عرض هذه الأدلة ومناقشتها بحضور طرفي الدعوى الجنائية، مع تمكينهما من إبداء ملاحظاتهما بشأن سلامة الدليل ومدى مشروعية الحصول عليه وصحته التقنية[2].

الفرع الثاني: أن يكون الدليل يقينيا

يشترط في الدليل أن يتسم باليقين، ويقصد بذلك أن يؤدي إلى تكوين قناعة ذهنية وعقلانية تؤكد حقيقة الواقعة محل الإثبات، ويتم التوصل إلى هذه القناعة من خلال مختلف وسائل الإدراك. كما يجب أن يكون الدليل واضحاً ومحدداً وخالياً من الشك والاحتمال، بحيث يسمح بالوصول إلى الحقيقة بصورة دقيقة وموضوعية.

ويكتسب هذا الشرط أهمية خاصة في مجال الدليل الرقمي، نظراً لما تتميز به البيانات الإلكترونية من قابلية للتخزين والمعالجة والنقل بوسائل تقنية متعددة، الأمر الذي يقتضي التأكد من سلامتها وصحتها قبل الاعتماد عليها في الإثبات. كما ينبغي أن يكون الدليل الرقمي قابلاً للتحقق والفحص الفني بما يضمن صحة محتواه وعدم تعرضه لأي تعديل أو تغيير من شأنه التأثير على قيمته الإثباتية.

[1] بن طيبي مبارك، مرجع سابق ، ص28.

[2] عبد الله هلالي، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، طبعة 1997،ص91

وعليه، فإن يقينية الدليل الرقمي تعد أساساً مهماً في تكوين اقتناع القاضي، إذ لا يمكن الاعتماد على دليل يشوبه الشك أو الغموض، بل يجب أن يكون كافياً لإقامة الدليل على الواقعة المراد إثباتها بصورة واضحة ومؤكدة.[1].

المبحث الثاني: ضمانات التحقيق في الدليل الرقمي بين الفعالية وحماية الحقوق

إن تحقيق التوازن بين فعالية التحقيق الجنائي وحماية الحقوق والحريات يظل رهانًا أساسيًا في مجال الدليل الرقمي، بما يضمن من جهة مكافحة الجريمة بكفاءة، ومن جهة أخرى صون حقوق الأفراد وعدم المساس بها إلا في إطار ما يقره القانون.

سيتم التطرق في هذا المبحث الضمانات الإجرائية في مرحلة جمع وتحرز الدليل الرقمي في (المطلب الأول)، و الضمانات الموضوعية لحماية الحقوق والحريات أثناء التحقيق الرقمي في (الفرع الثاني).

المطلب الأول: الضمانات الإجرائية في مرحلة جمع وتحرز الدليل الرقمي

تُعدّ مرحلة جمع وتحرير (أو تحرّز) الدليل الرقمي من المراحل الحساسة في مسار الإثبات الجنائي، نظراً لما تتطلبه من دقة تقنية عالية وإجراءات قانونية صارمة تضمن سلامة الدليل من جهة، وتحافظ على حقوق وحريات الأفراد من جهة أخرى.

اذا سيتم التطرق في هذا المطلب الى ضمانات المعاينة الرقمية في (الفرع الأول)، مشروعية إجراءات التفتيش الرقمي في (الفرع الثاني)، وضمانات الحجز والتحريز في (الفرع الثالث)، ضمانات الخبرة الرقمية في (الفرع الرابع) .

الفرع الأول: ضمانات المعاينة الرقمية

[1] عبد الله هلالي، مرجع سابق، ص126.

تتمثل أهم ضمانات المعاينة في مجال التحقيق الرقمي في ضرورة إجرائها من طرف جهة مختصة قانوناً ومؤهلة تقنياً، وذلك ضماناً لمصداقية العملية وسلامة نتائجها. كما يتعين أن يتم توثيق جميع مراحل المعاينة في محاضر رسمية دقيقة، تتضمن وصفاً مفصلاً للحالة التي وُجد عليها الدليل الرقمي، سواء تعلق الأمر بالأجهزة أو البيانات أو الأنظمة المعلوماتية محل الفحص.

كما تقتضي هذه الضمانات اتخاذ كافة الاحتياطات الفنية اللازمة أثناء المعاينة، بهدف تفادي أي تعديل أو حذف أو فقدان للبيانات الرقمية، وذلك من خلال استعمال وسائل وتقنيات متخصصة تضمن الحفاظ على سلامة المعطيات الإلكترونية وعدم المساس بها. إضافة إلى ذلك، يجب أن تتم المعاينة في حدود ما يسمح به التحقيق فقط، بحيث يقتصر الاطلاع على البيانات المرتبطة بالجريمة محل البحث دون غيرها، احتراماً لحق الأفراد في الخصوصية وحمايةً للحياة الخاصة من أي انتهاك غير مشروع.

وعليه، فإن الالتزام بهذه الضمانات الإجرائية والفنية يسهم بشكل مباشر في تعزيز موثوقية الدليل الرقمي، ويضمن سلامته القانونية، مما يجعله قابلاً للاعتماد عليه أمام الجهات القضائية في الإثبات الجزائي[1].

الفرع الثاني: مشروعية إجراءات التفتيش الرقمي

يشير الفقه الجنائي إلى أن إجراء التفتيش بالنظر إلى كونه يتمثل في البحث في مستودع السر، يمثل مساساً بحرمة الحياة الخاصة، وتقييداً للحرية الفردية، وهو ما يتطلب ضرورة توافر الضمانات القانونية اللازمة لصحته، وهي ضمانات الكتابة والتسبيب والاختصاص، أي أن يكون صدور الإذن بالتفتيش كتابة، وأن يكون مسبباً، وأن يكون بناءً على أمر قضائي صادر عن الجهة المختصة قانوناً بذلك، سواء كانت النيابة العامة أو

[1] انظر المادة 62 ، قانون الإجراءات الجزائية .

قاضي التحقيق، وأن يباشره الشخص أو الجهة المختصة قانوناً بذلك سواء كانت النيابة العامة أو مأمور الضبط القضائي في حالة ندبه، في غير حالات التلبس بالجريمة[1].

الفرع الثالث: ضمانات الحجز والتحرير

تتمثل هذه الضمانات في ضرورة توثيق عملية الحجز في محاضر رسمية، مع بيان طبيعة الأشياء أو البيانات المحجوزة، وكذا الحفاظ على سلامتها من أي تغيير أو تحريف، من خلال اتباع تقنيات التحريز الحديثة التي تضمن بقاء الدليل الرقمي في حالته الأصلية. كما يجب أن يتم الحجز في حدود ما تقتضيه ضرورة التحقيق، دون التوسع فيه بشكل يمس بحقوق الأفراد وعليه، فإن احترام هذه الضمانات من شأنه تعزيز مصداقية الدليل الرقمي وضمان قبوله أمام الجهات القضائية[2].

الفرع الرابع: ضمانات الخبرة الرقمية

وتتمثل ضمانات الخبرة في ضرورة تعيين خبير مختص يتمتع بالكفاءة والخبرة في المجال المعلوماتي، مع التزامه بالحياد والموضوعية أثناء أداء مهمته. كما يجب أن تُوثّق أعمال الخبرة في تقرير مكتوب يتضمن الإجراءات التي قام بها والنتائج التي توصل إليها، حتى يتسنى للقاضي والأطراف مناقشتها.

ومن جهة أخرى، تقتضي ضمانات الخبرة تمكين الأطراف من مناقشة تقرير الخبير والطعن فيه عند الاقتضاء، بما يكرّس حقوق الدفاع ويضمن تحقيق مبدأ المواجهة. كما يمكن للقاضي أن يأمر بإجراء خبرة مضادة إذا تبين له وجود نقص أو غموض في التقرير.

[1] رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الإتفاقات والمواثيق الدولية ، دار النهضة العربية ،الطبعة الأولي،2012، ص 95 .

[2] انظر المادة 51 ،قانون الإجراءات الجزائية .

وعليه، فإن الخبرة الرقمية تشكّل أداة حاسمة في تفسير الأدلة التقنية، غير أنها تظل مقيدة بضرورة احترام الضوابط القانونية التي تضمن نزاهتها ومصداقيتها[1].

المطلب الثاني: الضمانات الموضوعية لحماية الحقوق والحريات أثناء التحقيق الرقمي

نظراً لما قد تمسّه إجراءات التحقيق الرقمي من حقوق وحريات الأفراد، أقرّ المشرّع جملة من الضمانات الموضوعية لضبطها ومنع التعسف في استعمالها، بما يحقق التوازن بين فعالية البحث الجنائي وحماية الحقوق الأساسية. وعليه، نتناول في هذا المطلب أبرز هذه الضمانات.

اذا سيتم التطرق في هذا المطلب حماية الحق في الخصوصية وسرية المراسلات الإلكترونية في (الفرع الأول)، في مبدأ التناسب بين خطورة الجريمة والإجراءات الرقمية المتخذة (الفرع الثاني)، وبطلان إجراءات التحقيق الرقمي كجزاء للإخلال بالضمانات القانونية في (الفرع الثالث).

الفرع الأول : حماية الحق في الخصوصية وسرية المراسلات الإلكترونية

قد كرس المشرّع الجزائري هذه الحماية في النصوص الدستورية، حيث نص الدستور على ضمان حماية الحياة الخاصة وحرمة المراسلات والاتصالات، مما يجعلها من الحقوق الأساسية التي لا يجوز المساس بها إلا في إطار القانون[1].

[1] سبق الاشارة اليه في الفصل الأول.

كما جرم قانون العقوبات كل اعتداء على حرمة الحياة الخاصة، لاسيما من خلال التقاط أو تسجيل أو نقل مكالمات أو صور دون إذن صاحبها[2].

و كما جاء قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ليؤكد على ضرورة التوفيق بين فعالية التحقيق الرقمي وحماية الحقوق والحريات الأساسية[3].

ولا تقتصر الحماية القانونية على سرية المراسلات الإلكترونية فقط، بل تمتد لتشمل سرية إجراءات التحقيق في حد ذاتها، باعتبارها إطاراً أساسياً لضمان حماية المعطيات والمعلومات المتداولة أثناء البحث والتحري، والتي يقصد بها عدم السماح للجمهور بحضور إجراءات التحقيق، بل القيام به في سرية تامة بعيدا عن أنظار الجمهور، ويجب أن لا تمس هذه السرية حقوق الدفاع، أي أنه لا يجوز استخدامها كذريعة لحرمان المتهم أو محاميه من الاطلاع على الملف، أول الضمانات المحاكمة العادلة[4].

الفرع الثاني: مبدأ التناسب بين خطورة الجريمة والإجراءات الرقمية المتخذة.

يُعد مبدأ التناسب حجر الزاوية في الموازنة بين فاعلية التحقيق الرقمي وحماية الحريات الأساسية للمشتبه فيهم، وقد كرس المشرع الجزائري هذا المبدأ من خلال إخضاع الإجراءات الرقمية لشرطي الضرورة والملائمة. ويتجلى ذلك بوضوح في القانون 09-04 ، حيث قيد اللجوء إلى إجراءات التحقيق الخاصة -كاعتراض المراسلات أو التفتيش الإلكتروني- بوجود مبررات قوية ترتبط بجسامة الجريمة، لاسيما في جرائم الإرهاب والمساس بأمن الدولة والجرائم المنظمة[5]. كما عزز المشرع هذه الضمانة الموضوعية من خلال القانون 18-07

---

[1] المادة 47و48 من الدستور الجزائري ، الصادر بموجب المرسوم الرئاسي 20-442 في 30-12-2020 ج ر 82 لسنة 2020 .

[2] انظر المادة 303 ،قانون العقوبات الجزائري.

[3] قانون رقم 09-04 .

[4] باغي صبرينة ، قريقة غادة ،مرجع سابق، ص55 .

[5] انظر مواد 4،5،6 من قانون 09-04 .

المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، والذي نص صراحة في مادته السابعة على وجوب أن تكون المعطيات المجموعة في إطار المعالجة "كافية وصلبة وغير مفرطة"[1].

وهو ما يمنع سلطات التحقيق من التوسع في سحب البيانات الرقمية أو اختراق الخصوصية بشكل لا يتناسب مع خطورة الفعل المجرم محل البحث. إن هذا التلازم بين "خطورة الجرم" و"جسارة الإجراء الرقمي" يهدف إلى منع أي انحراف بالسلطة قد يؤدي إلى إهدار الحق في الخصوصية المكفول دستورياً.[2]

الفرع الثالث: بطلان إجراءات التحقيق الرقمي كجزاء للإخلال بالضمانات القانونية

لا تكتمل الحماية القانونية للحقوق والحريات في الفضاء الرقمي إلا بوجود جزاء قانوني يضمن احترام الضمانات الإجرائية ويمنع تعسف جهات التحقيق أو تجاوزها للسلطات المخولة لها، ويُعد هذا الجزاء هو البطلان.

ويُقصد بالبطلان في هذا السياق عدم الاعتداد بالإجراء الرقمي وما ترتب عنه من آثار قانونية، كلما تم إنجازه في مخالفة للقواعد القانونية المنظمة له. فكل إجراء من إجراءات التحقيق الرقمي، مثل تفتيش الحواسيب أو الولوج إلى الأنظمة المعلوماتية أو اعتراض المراسلات الإلكترونية، يجب أن يتم وفق ضوابط دقيقة أهمها احترام مبدأ المشروعية ومبدأ التناسب والحصول على إذن قضائي مسبق كلما كان ذلك واجباً.

وعليه، فإن أي إخلال بهذه الشروط، سواء تمثل في تنفيذ الإجراء دون إذن قضائي، أو تجاوز نطاق الإذن، أو عدم احترام الضوابط القانونية الخاصة بجمع الدليل الرقمي، يؤدي

[1] قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] انظر المادة 47 الدستوري الجزائري.

إلى ترتيب أثر البطلان على الإجراء. ولا يقتصر هذا البطلان على الإجراء في حد ذاته، بل يمتد ليشمل جميع الأدلة والنتائج المتحصلة عنه باعتبارها أدلة غير مشروعة وغير قابلة للاعتماد عليها في الإثبات الجزائي[1].

كما يمتد هذا البطلان ليشمل المعالجة غير المشروعة للمعطيات الشخصية التي تتم أثناء التحقيق إذا لم تراعِ الشروط المنصوص عليها في القانون 18-07[2].

خلاصة الفصل الثاني

في ختام هذا الفصل يتبين الدليل الرقمي أصبح يحتل مكانة محورية في منظومة الإثبات الجزائي، خاصة في ظل التطور المتسارع لجرائم تكنولوجيات الإعلام والاتصال. وقد تبيّن أن هذا الدليل يتميز بخصائص تقنية وقانونية تجعله مختلفًا عن الأدلة التقليدية،

[1] انظر المادة253 ، قانون الإجراءات الجزائية .

[2] انظر المادة 18 من قانون 18-07 .

من حيث طبيعته اللامادية، وقابليته للاستنساخ والتعديل، وحاجته إلى خبرة فنية متخصصة لاستخراجه وتحليله.

كما اتضح أن المشرّع الجزائري، من خلال تعديل أحكام قانون الإجراءات الجزائية، قد حاول مواكبة هذه التحولات عبر إدراج آليات إجرائية تسمح بالتفتيش والمعاينة والحجز في المجال الرقمي، إلى جانب إصدار القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والقانون 18-07 المتعلق بحماية المعطيات الشخصية، مما وضع إطارًا قانونيًا خاصًا للتحري وجمع الأدلة الإلكترونية.

غير أن فعالية هذه الآليات تظل مرتبطة بمدى احترام الضمانات الإجرائية والموضوعية التي تحكم التحقيق الرقمي، وعلى رأسها مبدأ الشرعية، واحترام حرمة الحياة الخاصة، ومبدأ التناسب. وقد استقر لدينا أن أي تجاوز لهذه الضمانات يرتب جزاءً إجرائياً صارماً وهو بطلان إجراءات التحقيق وما يسفر عنها من أدلة؛ فالبطلان في البيئة الرقمية هو الحارس الأمين لحرمة الحياة الخاصة، وبدونه تفرغ الضمانات الدستورية من محتواها.

وعليه، يتضح أن التحدي الحقيقي لا يكمن فقط في إضفاء المشروعية على الدليل الرقمي، بل في تحقيق توازن دقيق بين ضرورات الكشف عن الحقيقة الجنائية ومتطلبات حماية الحقوق الفردية، مع تكريس نظام رقابة قضائية قادر على استبعاد كل دليل استُخلص بالمخالفة للقانون. وهو توازن يظل رهين التطوير المستمر للنصوص القانونية، وتعزيز التكوين التقني للقضاة وأعوان الضبطية القضائية لضمان سلامة الإجراءات من أي عيوب قد تؤدي لبطلانها.

الخاتمة

في ختام هذه الدراسة، يتبين أن جرائم الفضاء الإلكتروني أصبحت من أخطر التحديات التي تواجه العدالة الجنائية، نظرا لخصوصيتها التقنية وطابعها العابر للحدود، الأمر الذي جعل وسائل التحقيق التقليدية غير كافية لمواجهتها، وفرض ضرورة اعتماد تحقيق رقمي قائم على وسائل تقنية وإجرائية حديثة.

وقد أظهرت الدراسة أن فعالية التحقيق الرقمي تقوم على تكامل الإجراءات التقليدية مع الإجراءات المستحدثة، إلى جانب الاعتماد على التعاون الدولي لمواجهة الصعوبات المرتبطة بتتبع الجناة وجمع الأدلة الرقمية. كما تبين أن الدليل الرقمي أصبح وسيلة إثبات أساسية في الجرائم الإلكترونية، غير أن خصوصيته تقتضي توفير ضمانات قانونية وتقنية تكفل سلامته وتحافظ على حجيته.

ويمكن القول إن التحقيق الرقمي يعد آلية فعالة في مواجهة جرائم الفضاء الإلكتروني، غير أن فعاليته تبقى مرتبطة بمدى تطوير التشريعات، وتعزيز التأهيل التقني للمحققين، وتدعيم التعاون الدولي، بما يحقق التوازن بين مكافحة الجريمة الإلكترونية وحماية الحقوق والحريات الأساسية.

ولقد أفرز التكور التكنولوجي المتسارع واقعا جديدا فرض على الأنظمة القانونية والقضائية تحديات غير مسبوقة، خاصة في ظل تنامي جرائم الفضاء الالكتروني التي أصبحت تمس مختلف جوانب الحياة الاقتصادية والاجتماعية والأمنية. فهذه الجرائم لم تعد تقتصر على الاعتداء على الأنظمة المعلوماتية او سرقة البيانات فحسب، بل امتدت لتشمل صورا أكثر تعقيدا وخطورة، مستفيدة من التطور المستمر لوسائل الاتصال الحديثة والتقنيات الرقمية.

وفي هذا السياق، برز التحقيق الرقمي كأحد أهم الآليات الحديثة التي اعتمدتها السلطات المختصة لمواجهة هذا النوع من الجرائم، وذلك لما يوفره من وسائل تقنية متطورة تساعد على كشف الحقيقة وتتبع الجناة وجمع الأدلة الرقمية لا ترتبط فقط بمدى توفر الوسائل

التقنية الحديثة، وإنما كذلك بوجود إطار قانوني متكامل يحدد إجراءات التعامل مع الأدلة الرقمية ويضمن مشروعيتها وحجيتها أمام الجهات القضائية.

كما تبين أن المشرع الجزائري قد سعى الى مواكبة التحولات التي فرضها العصر الرقمي من خلال سن العديد من النصوص القانونية ذات الصلة بمكافحة الجرائم الالكترونية وتنظيم إجراءات البحث والتحري بشأنها، غير أن التطور السريع للتقنيات الحديثة يجعل من الضروري مواصلة مراجعة وتحيين هذه النصوص بصورة مستمرة حتى تظل قادرة على الاستجابة للتحديات المستجدة.

ومن جهة أخرى، فإن نجاح التحقيق الرقمي يظل رهينا بتوفير العنصر البشري المؤهل والقادر على التعامل مع الوسائل التقنية الحديثة، إذ ان الخبرة الفنية والكفاءة المهنية للمحققين والخبراء تعلب دورا أساسيا في ضمان سلامة الإجراءات والحفاظ على الأدلة الرقمية من العبث أو التلف أو الفقدان. كما أن تعزيز التعاون بين مختلف الجهات الوطنية والدولية أصبح ضرورة حتمية بالنظر الى الطبيعة العابرة للحدود التي تتميز بها الجرائم الالكترونية.

وعليه، فإن مواجهة جرائم الفضاء الالكتروني لا يمكن ان تعتمد على الجانب القانوني أو التقني بصورة منفردة، بل تتطلب تبني مقاربة شاملة تقوم على التكامل بين التشريع والتكنولوجيا والتكوين المتخصص والتعاون الدولي، بما يسمح بتحقيق التوازن بين متطلبات مكافحة الجريمة من جهة وضمان احترام الحقوق والحريات الفردية من جهة أخرى.

وفي الأخير، يمكن التأكيد على أن التحقيق الرقمي أصبح اليوم ركيزة أساسية في السياسة الجنائية الحديثة، ووسيلة لا غنى عنها في كشف الجرائم الالكترونية إثباتها، الامر الذي يفرض مواصلة تطوير آلياته وتعزيز فعاليته بما يتلاءم مع طبيعة البيئة الرقمية المتجددة والتحديات المستقبلية التي قد تفرضها الثورة التكنولوجية المتسارعة.

وفي ضوء ما تم التوصل إليه من خلال هذه الدراسة، وبعد استعراض مختلف الجوانب المتعلقة بالتحقيق الرقمي في مواجهة جرائم الفضاء الالكتروني، يمكن استخلاص جملة من النتائج الأساسية التي اسفرت عنها الدراسة، وذلك على النحو التالي:

النتائج

1. لم تعد الإجراءات التقليدية للتحقيق الرقمي كافية لوحدها لمواجهة الجرائم الإلكترونية، مما استوجب استحداث إجراءات حديثة أكثر فعالية.

2. أصبح الدليل الرقمي وسيلة أساسية في الإثبات الجنائي، لما له من دور في كشف الحقيقة وإثبات الجريمة.

3. ترتبط حجية الدليل الرقمي بضرورة احترام القواعد القانونية والتقنية أثناء جمعه وتحليله وحفظه.

4. يعد التعاون الدولي الأمني والقضائي ضرورة أساسية لضمان فعالية التحقيق في الجرائم الإلكترونية.

5. حاول المشرع الجزائري مواكبة التطور التكنولوجي من خلال تنظيم إجراءات التحقيق الرقمي، غير أن هذه النصوص ما تزال بحاجة إلى تطوير مستمر.

واستنادا الى النتائج المتوصل إليها من خلال هذه الدراسة، وحرصا على تعزيز فعالية التحقيق الرقمي في مواجهة جرائم الفضاء الالكتروني، يمكن تقديم جملة من الاقتراحات نوجزها فيما يأتي:

الاقتراحات

1.استحداث تنظيم قانوني مستقل للتحقيق الرقمي ضمن قانون الإجراءات الجزائية.

2.تمكين جهات التحقيق من وسائل قانونية وتقنية تسمح بالتدخل السريع لتجميد وحفظ البيانات الرقمية المعرضة للمحو أو التغيير، نظرا لطبيعة الأدلة الرقمية.

3. تدعيم التعاون الدولي الأمني والقضائي وتسهيل تبادل المعلومات والخبرات المتعلقة بالجرائم الإلكترونية.

4. تعزيز التعاون بين السلطات القضائية ومزودي خدمات الإنترنت والاتصالات بما يساهم في سرعة الوصول إلى الأدلة الرقمية.

5. تحقيق التوازن بين فعالية إجراءات التحقيق الرقمي واحترام الحقوق والحريات الأساسية، خاصة الحق في الخصوصية وسرية المعطيات الشخصية.

قائمة المصادر

والمـــــــــراجع

Les références

قائمة المصادر والمـــــــــراجع:

أولًا: النصوص القانونية

- الدستور الجزائري، الصادر بموجب المرسوم الرئاسي 20-442 المؤرخ في 30 ديسمبر 2020، الجريدة الرسمية للجمهورية الجزائرية، العدد 82، سنة 2020.
- القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- القانون رقم 18-07 المؤرخ في 25 رمضان 1439 الموافق 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، سنة 2018.
- القانون رقم 25-14 المؤرخ في 09 صفر 1447 الموافق 03 غشت 2025، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 54، سنة 2025.
- اتفاقية بودابست لمكافحة الجرائم المعلوماتية، الموقعة في 23 نوفمبر 2001.

ثانيا: الكتب

- أبو عامر، محمد زكي، الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، الطبعة السابعة، 2002.
- أبو بكر بن يونس، عمر محمد، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، 2004.

- إبراهيم، خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2009.
- حجازي، عبد الفاتح بيومي، الدليل الرقمي وحجيته في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، 2010.
- حسن طاهر داؤد، جرائم نظم المعلومات، ط 1، الرياض، السعودية، 2000م.
- رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي ، جامعة الإسكندرية، العدد 24، مصر، 1992.
- عبد المطلب، ممدوح عبد الحميد، البحث والتحقيق الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006.
- فاضل، سليمان أحمد، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، 2007.
- قنديل، أشرف عبد القادر، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015.
- مصطفى، عائشة بن قارة، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، سنة 2025.
- هروال، نبيلة هبه، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2013.

- هلالي عبد الله ، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، طبعة 1997.

- يس حسن محمد عثمان ، الدليل الرقمي وأثره على الدعوى الجنائية ، مجلة العلوم القانونية والاجتماعية،جامعة زيان عاشور بالجلفة ، الجزائر، العدد 3 المجلد 5 ، سبتمبر 2020.

ثالثا: الأطروحات والمذكرات الجامعية

أطروحات الدكتوراه

- بوعناد، فاطمة الزهراء، مشروعية الدليل الإلكتروني في مجال الإثبات الجنائي، أطروحة دكتوراه، جامعة سيدي بلعباس، 2013-2014.

- بن فردية، محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة دكتوراه في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2015.

- بن يونس، عمر أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة عين شمس، 2004.

مذكرات الماستر

- باغي، صبرينة، وقريقة، غادة، مرحلة التحقيق في الجرائم المعلوماتية في ظل التشريع الجنائي الجزائري، مذكرة ماستر في القانون، المركز الجامعي عبد الحفيظ بوالصوف، ميلة، 2024-2025.

- بن عنطر، سهام، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة ماستر، جامعة مولود معمري، تيزي وزو، 2023.

- بلعلمي، جليلة، ومزري، صالح، الدليل الرقمي والإثبات الجنائي، مذكرة ماستر في الحقوق، جامعة قاصدي مرباح ورقلة، 2021-2022.
- زياده، هادي، آليات التعاون الدولي في مكافحة الجريمة السيبرانية، مذكرة ماستر، جامعة مستغانم، 2023.
- صون، آسيا، التعاون الدولي في مكافحة الجرائم الإلكترونية، مذكرة ماستر، جامعة مستغانم، 2022.
- معتوق، محمد أكلي، وعاشور، سهام، التعاون الدولي في مكافحة الجريمة الإلكترونية، مذكرة ماستر، جامعة برج بوعريريج، 2023.
- هلال، آمنة، الإثبات الجنائي بالدليل الإلكتروني، مذكرة ماستر في القانون الجنائي، جامعة محمد خيضر بسكرة، 2014-2015.

رابعا: المقالات العلمية

- بالعابد، عيدة، "الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية"، مجلة آفاق علمية،جامعة سعيدة، الجزائر، المجلد 11، العدد 01، 2019.
- بن الطيبي، مبارك، "شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية"، مجلة القانون والعلوم السياسية،جامعة احمد دراية، أدرار، المجلد 05، العدد 02، 2019.
- بوقصة، إيمان، وبدايرية، يحي، "أثر خصوصية إجراءات التحقيق في الجرائم المعلوماتية على حجية الدليل الرقمي في الإثبات"، مجلة الحقوق والحريات، جامعة محمد خيضر بسكرة، المجلد 13، العدد 02، جوان 2025.

- حليم، رامي، "إجراءات استخلاص الدليل في الجرائم المعلوماتية"، مجلة دفاتر البحوث العلمية، جامعة البليدة 2، المجلد 09، العدد 01، 2021.
- رضا، هميسي، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، جامعة الوادي، العدد 05، جوان 2012.
- محمود، نور الهدى، "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية"، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة، العدد 11، جوان 2017.

خامسا: المداخلات العلمية

- غدامسي، موسى، "السياسة التشريعية الجزائرية لحماية النظام العام والآداب العامة في البيئة الرقمية"، مداخلة مقدمة ضمن المحور الثاني: الآليات القانونية لحماية النظام العام والآداب العامة في البيئة الرقمية، كلية الحقوق والعلوم السياسية، جامعة أحمد بوقرة بومرداس.

الفهرس

العنوان	الصفحة
مقدمة	أ
الفصل الأول: الاجراءات والاساليب الدولية للتحقيق الرقمي	6
المبحث الأول : إجراءات التحقيق الرقمي	7
المطلب الأول : الإجراءات التقليدية للتحقيق الرقمي	7
الفرع الأول: المعاينة في الوسط الرقمي	7
الفرع الثاني: التفتيش الرقمي	9
الفرع الثالث: الضبط الرقمي	12
الفرع الرابع : الخبرة الرقمية	14
المطلب الثاني : الإجراءات المستحدثة للتحقيق الرقمي	15
الفرع الاول : التسرب الالكتروني	16
الفرع الثاني : اعتراض المراسلات	18
الفرع الثالث : المراقبة الالكترونية	19
الفرع الرابع: الحفظ والافشاء العاجلان للمعطيات الالكترونية	20
المبحث الثاني : الأساليب الدولية للتحقيق في الجرائم الالكترونية	21
المطلب الأول : التعاون الأمني الدولي للتحقيق في الجرائم الالكترونية	22
الفرع الاول : تعريف التعاون الامني الدولي و أساسه	23
الفرع الثاني: صور التعاون الأمني الدولي في مجال التحقيق الرقمي والجهود المنظمة الدولية للشرطة الجنائية	24

المطلب الثاني : التعاون القضائي الدولي في الجرائم الالكترونية	25
الفرع الأول: المساعدة القضائية والتحقيقات المشتركة في مجال الجريمة الالكترونية	25
الفرع الثاني : الانابة القضائية الدولية	27
خلاصة الفصل الاول	27
الفصل الثاني : الآثار القانونية للتحقيق الرقمي والضمانات الإجرائية المقررة له	30
المبحث الأول : الإطار القانوني للدليل الرقمي	31
المطلب الأول : مفهوم الدليل الرقمي	32
الفرع الاول: تعريف الدليل الرقمي وتمييزه عن الأدلة التقليدية	34
الفرع الثاني : خصائص الدليل الرقمي	33
الفرع الثالث: الطبيعة القانونية للدليل الرقمي وحجيته في الإثبات الجنائي.	34
المطلب الثاني : شروط قبول الدليل الرقمي	36
الفرع الاول : مشروعية الدليل الرقمي	36
الفرع الثاني : أن يكون الدليل يقينيا	38
المبحث الثاني : ضمانات التحقيق في الدليل الرقمي بين الفعالية وحماية الحقوق	38
المطلب الأول : الضمانات الإجرائية في مرحلة جمع وتحرز الدليل الرقمي	38
الفرع الأول: ضمانات المعاينة الرقمية	39
الفرع الثاني: مشروعية إجراءات التفتيش الرقمي	39
الفرع الثالث: ضمانات الحجز والتحرير	39
الفرع الرابع : ضمانات الخبرة الرقمية	39
المطلب الثاني : الضمانات الموضوعية لحماية الحقوق والحريات أثناء التحقيق	40

الرقمي	
الفرع الأول : حماية الحق في الخصوصية وسرية المراسلات الإلكترونية	40
الفرع الثاني: مبدأ التناسب بين خطورة الجريمة والإجراءات الرقمية المتخذة.	41
الفرع الثالث: بطلان إجراءات التحقيق الرقمي كجزاء للإخلال بالضمانات القانونية	41
خلاصة الفصل	42
الخاتمة	45
قائمة المراجع	47

الملخص

الملخص

ملخص:

تناولت هذه الدراسة موضوع التحقيق الرقمي في مواجهة جرائم الفضاء الإلكتروني، باعتباره من أهم الآليات الحديثة التي فرضها التطور التكنولوجي وتزايد الجرائم الإلكترونية، خاصة جريمة الدخول أو البقاء غير المشروع داخل الأنظمة المعلوماتية. وهدفت الدراسة إلى بيان مدى فعالية إجراءات التحقيق الرقمي والأساليب التقنية الحديثة في كشف الجرائم الإلكترونية والوصول إلى مرتكبيها، مع التركيز على الدليل الرقمي وحجيته القانونية والضمانات المقررة لحمايته. كما عالجت الدراسة أهم الإشكالات القانونية والعملية التي يثيرها التحقيق الرقمي، من خلال الاعتماد على المنهجين الوصفي والتحليلي وتحليل النصوص القانونية المتعلقة بالموضوع.

الكلمات المفتاحية: التحقيق الرقمي، جرائم الفضاء الإلكتروني، الجريمة الإلكترونية، الدخول غير المشروع، الدليل الرقمي.

Résumé :

Cette étude a porté sur le thème de l'enquête numérique face à la cybercriminalité, considérée comme l'un des mécanismes modernes les plus importants imposés par l'évolution technologique et la recrudescence des crimes électroniques, notamment l'infraction d'accès ou de maintien frauduleux dans des systèmes informatiques. L'étude visait à démontrer l'efficacité des procédures d'enquête numérique et des techniques modernes pour détecter les crimes électroniques et identifier leurs auteurs, tout en mettant l'accent sur la preuve numérique, sa force probante juridique et les garanties instaurées pour sa protection. Elle a également traité les principales problématiques juridiques et pratiques soulevées par l'enquête numérique, en s'appuyant sur les approches descriptive, analytique et l'analyse des textes juridiques relatifs au sujet.

Mots-clés : Enquête numérique, cybercriminalité, crime électronique, accès non autorisé, preuve numérique

Abstract*:*

This study addressed the topic of digital investigation in confronting cybercrimes, as one of the most important modern mechanisms imposed by technological development and the increasing spread of electronic crimes, especially the crime of illegal access to or unauthorized presence within information systems. The study aimed to show the effectiveness of digital investigation procedures and modern technical methods in detecting cybercrimes and identifying their perpetrators, with a focus on digital evidence, its legal probative value, and the safeguards established for its protection. The study also examined the main legal and practical issues raised by digital investigation, relying on the descriptive .and analytical approaches and the analysis of **l**egal texts related to the subject

Keywords: Digital investigation, cybercrimes, electronic crime, illegal access, digital evidence, electronic evidenc**.**