الجمهورية الجزائرية الديموقراطية الشعبية
وزارة التعليـــم العـــالـــي والبحث العلمـــي
جامعة "بلحاج بوشعيب "-عين تموشنت-
كلية الحقوق
قسم: الحقوق

تحديات التحقيق الإلكتروني في ظل الفضاء الرقمي

مذكرة مكملة لنيل شهادة الماستر في الحقوق -تخصص: قانون خاص معمق

من إعـداد الطالـــــب:
بشير بـن داوود فـهد

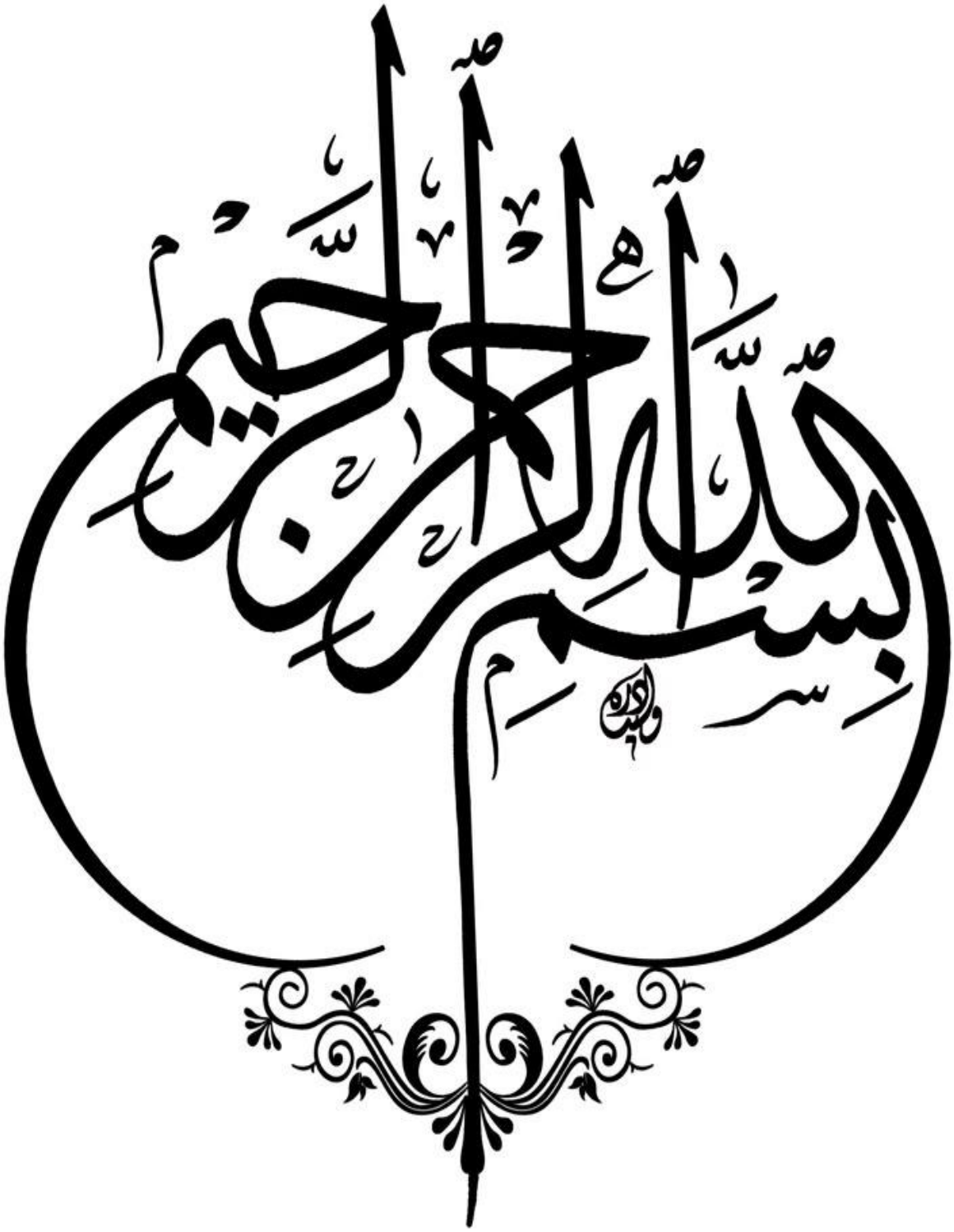
تحت إشـراف الأستـاذة:
د. زعزوعـــــة نجاة

لجنـــــة المناقشـــــة

الرئيس	أ.د صديق سهـــــام	أستاذة محاضرة أ	جامعة عين تموشنت
الممتحن	د. سي بوعزة إيمان	أستاذة محاضرة أ	جامعة عين تموشنت
المشرف	د.زعزوعـــــة نجاة	أستاذة محاضرة ب	جامعة عين تموشنت

السنة الجامعية

2026/2025


بسم الله الرحمن الرحيم

إهداء

إلى والدتي الحبيبة التي رافقتني بروحها وإن فارقتني بجسدها.

إلى والدي العزيز الذي وضع أسس بنياني المعرفي.

إليكم يا أعز الأحباب أهدي هذه الرسالة.

شكر والتقدير

إلى السادة المشرفين الأفاضل الذين مدوا لي يد العون، وذللوا لي كل عسير، وأخذوا بيدي بينما أخطوا خطواتي الأولى في هذا الميدان الصعب.

والله العظيم أسأل أن يجزيهم بإحسانهم إحساناً وأن ينفع ببحثي هذا البلاد والعباد.

أتوجه بالشكر إلى الأساتذة الكرام الذين لم يبخلوا علينا بعلمهم، ولم يألوا جهداً في سبيل المعرفة والعلم.

والشكر موصول إلى إدارة الجامعة التي ذللت الصعوبات من أجل إنجاز هذه الرسالة بجودة وكفاءة

المقدمة

مقدمة:

يشهد العالم في العصر الراهن ثورة تكنولوجية ومعلوماتية متسارعة، أحدثت تحولات جذرية في مختلف مناحي الحياة الإنسانية. فقد أدى الانتشار الواسع لشبكة الإنترنت وتطور أنظمة الاتصالات وتكنولوجيا المعلومات إلى ظهور بيئة جديدة موازية للبيئة المادية، وهي ما يُصطلح عليه بـ "الفضاء الرقمي" أو "البيئة السيبرانية". هذا الفضاء، بخصائصه المتمثلة في السرعة، اللامركزية، وإلغاء الحدود الجغرافية، قدم للبشرية تسهيلات لا حصر لها في مجالات الاقتصاد، التعليم، والإدارة. إلا أنه، وكضريبة حتمية لهذا التقدم، أفرز ظواهر سلبية خطيرة، تجلت أبرزها في ظهور أنماط إجرامية مستحدثة تُعرف بـ "الجرائم المعلوماتية" أو "الجرائم الإلكترونية".

إن الجريمة الإلكترونية تختلف اختلافاً جوهرياً عن الجريمة التقليدية؛ فهي لا تعترف بالحدود الوطنية، وتُرتكب في بيئة افتراضية لا مادية، باستخدام وسائل تقنية معقدة، ومن قِبل مجرمين يتمتعون بذكاء وخبرة فنية عالية. هذا التطور النوعي في السلوك الإجرامي أدى إلى انتقال "مسرح الجريمة" من مسرح مادي ملموس يترك فيه الجاني آثاراً بيولوجية أو مادية (كبصمات الأصابع أو الأسلحة)، إلى "مسرح جريمة افتراضي" يترك فيه الجاني آثاراً رقمية (كعناوين IP، وسجلات الدخول، والبيانات المشفرة)، وهو ما يُعرف بـ "الدليل الرقمي أو الإلكتروني".

أمام هذا الواقع الجديد، وجدت الأجهزة المكلفة بإنفاذ القانون (الضبطية القضائية وجهات التحقيق) نفسها أمام تحدٍ حقيقي. فالقواعد والإجراءات الجنائية التقليدية، التي صُممت في الأصل للتعامل مع الجرائم المادية، أثبتت قصورها في استيعاب الطبيعة الخاصة للجريمة الإلكترونية. ومن هنا، برزت الحاجة الملحة إلى تطوير منظومة إجرائية جديدة تتلاءم مع طبيعة الفضاء الرقمي، وهو ما أدى إلى ميلاد مفهوم "التحقيق الإلكتروني".

يُقصد بالتحقيق الإلكتروني مجموعة الإجراءات والتدابير الفنية والقانونية التي تتخذها السلطات المختصة لجمع الأدلة الرقمية، تحليلها، وحفظها، بهدف كشف الحقيقة ونسبتها إلى مرتكبيها. غير أن هذه العملية ليست باليسيرة، إذ تواجه جهات التحقيق جملة من التحديات المعقدة؛ فمن الناحية التقنية، يتميز الدليل الرقمي بقابليته السريعة للمحو، التعديل، والتدمير، ناهيك عن تعقيدات التشفير والتخزين السحابي. ومن الناحية القانونية، تبرز إشكاليات عميقة تتعلق بتنازع الاختصاص القضائي الدولي، وغياب التشريعات الإجرائية المتخصصة، فضلاً عن التحدي الأكبر المتمثل في الموازنة بين مقتضيات مكافحة الجريمة وكشف الحقيقة، وبين احترام حقوق الإنسان وضمانات الخصوصية الفردية التي كفلتها الدساتير والمواثيق الدولية.

تكتسي هذه الدراسة أهمية بالغة يمكن تقسيمها إلى شقين:

الأهمية النظرية (العلمية): تتجلى في إثراء المكتبة القانونية ببحث متخصص يسلط الضوء على موضوع حديث ومتجدد يجمع بين تقنية المعلومات والقانون الجنائي الإجرائي. كما تسهم الدراسة في توضيح المفاهيم المتعلقة بالتحقيق الإلكتروني والدليل الرقمي، وبيان مدى استيعاب القواعد العامة في قانون الإجراءات الجزائية لمعطيات الفضاء الرقمي، مما يشكل مرجعاً للباحثين والمهتمين بالسياسة الجنائية الحديثة.

الأهمية العملية (التطبيقية): تنبع من الواقع العملي الذي تعيشه أجهزة العدالة (قضاة تحقيق، وكلاء جمهورية، وضباط شرطة قضائية) الذين يواجهون يومياً عقبات تقنية وقانونية في تتبع الجرائم الإلكترونية. تسعى هذه الدراسة إلى تشخيص هذه التحديات بدقة، وتقديم مقاربات وحلول تساعد الممارسين في تذليل العقبات، كما تضع بين يدي المشرع (لا سيما المشرع الجزائري) مقترحات لسد الفراغ التشريعي وتطوير النصوص الإجرائية بما يتوافق مع الاتفاقيات الدولية (كاتفاقية بودابست).

كمايهدف هذا البحث إلى تحقيق الغايات الآتية:

التعريف الدقيق للتحقيق الإلكتروني وبيان طبيعته وخصائصه التي تميزه عن التحقيق الجنائي التقليدي.

تحديد الإطار القانوني والتقني لجمع وضبط الأدلة الرقمية في الفضاء الافتراضي.

حصر وتحليل التحديات التقنية (الفنية) التي تعيق عمل المحققين في الفضاء الرقمي، مثل تقنيات التشفير، إخفاء الهوية، والحوسبة السحابية.

تسليط الضوء على الإشكاليات القانونية، وفي مقدمتها إشكالية الاختصاص القضائي، ومشروعية الدليل الرقمي، وحماية الحق في الخصوصية أثناء التفتيش والمراقبة الإلكترونية.

تقييم مدى فعالية التعاون الدولي في مجال التحقيقات الإلكترونية، بالنظر إلى الطبيعة العابرة للحدود للجرائم السيبرانية.

الخروج بجملة من التوصيات القانونية والتقنية التي من شأنها تعزيز كفاءة أجهزة التحقيق في مواجهة الإجرام الرقمي.

جاء اختيارنا لموضوع "تحديات التحقيق الإلكتروني في ظل الفضاء الرقمي" بناءً على عدة مبررات، منها:

مبررات ذاتية:

الرغبة الشخصية والميل إلى دراسة المواضيع التي تتقاطع فيها العلوم القانونية مع التطورات التكنولوجية الحديثة، فضلاً عن السعي لاكتساب خبرة معرفية حول آليات مكافحة الجريمة السيبرانية.

مبررات موضوعية:

التزايد المخيف في معدلات الجرائم الإلكترونية وتنوع أساليبها، مما يهدد الأمن القومي والاقتصادي للدول.

القصور الملاحظ في بعض التشريعات الإجرائية الحالية التي لا تزال تتعامل مع الجريمة الإلكترونية بمنطق الجريمة الكلاسيكية.

التعقيد البالغ الذي يتسم به الدليل الرقمي، والذي يجعله عرضة للبطلان أمام القضاء إذا لم تُتخذ إجراءات جمعه وتحليله وفق ضوابط صارمة جداً.

بناءً على ما تقدم من معطيات، ومحاولةً للإحاطة بمختلف جوانب الموضوع، تتبلور الإشكالية الرئيسية لهذه الدراسة في التساؤل الجوهري الآتي:

"إلى أي مدى تؤثر التحديات التقنية والقانونية التي تعترض جهات التحقيق الالكتروني في سعيها للموازنة بين فعالية مكافحة الجريمة السيبرانية وحماية الحقوق والحريات الأساسية؟"

لضمان الإلمام بكافة جوانب الموضوع والإجابة على الإشكالية المطروحة بشكل علمي دقيق، اعتمدنا على تكامل منهجي يرتكز على:

المنهج الوصفي التحليلي: من خلال وصف الظاهرة الإجرامية في الفضاء الرقمي، وتحديد مفاهيم التحقيق والدليل الإلكتروني، ثم القيام بتحليل النصوص القانونية الإجرائية (في التشريع الجزائري والاتفاقيات الدولية) لاستخلاص الأحكام وبيان مدى ملاءمتها لمكافحة هذه الجرائم.

المنهج المقارن وذلك من خلال الاستئناس ببعض التشريعات المقارنة (كالتشريع الفرنسي أو المصري) أو الاتفاقيات الدولية (اتفاقية بودابست المتعلقة بجرائم الفضاء الإلكتروني لسنة 2001) لتوضيح أوجه النقص والقصور في التشريع الوطني واقتراح الحلول المناسبة.

فلا يخلو أي عمل بحثي من صعوبات وعراقيل، وقد واجهنا أثناء إنجاز هذه المذكرة بعض التحديات، لعل أبرزها:

تشعب الموضوع وحداثته: حيث يجمع البحث بين مصطلحات فنية معلوماتية دقيقة (تشفير، حوسبة سحابية، IP) وبين نصوص قانونية، مما استلزم جهداً مضاعفاً لفهم الجانب التقني لإسقاطه على الجانب القانوني.

التطور التكنولوجي المتسارع: إن الوتيرة السريعة لتطور التقنيات الرقمية تجعل بعض الحلول أو النصوص القانونية تبدو متقادمة بمجرد صدورها، مما صعّب من عملية تتبع أحدث المستجدات في مجال الجريمة والتحقيق.

ندرة المراجع المتخصصة المحدثة: خاصة تلك التي تتناول الشق "الإجرائي والعملي" للتحقيق الإلكتروني في التشريع الجزائري، مقارنة بالمراجع التي تتناول الشق "الموضوعي" (أركان الجريمة وعقوباتها).

استناداً إلى طبيعة الموضوع، وبغية الإجابة على الإشكالية المطروحة بشكل منهجي ومتسلسل، ارتأينا تقسيم هذه المذكرة إلى فصلين رئيسيين، يسبقهما مقدمة (هذه) وتليهما خاتمة تتضمن أهم النتائج والتوصيات.

الفصل الأول: الإطار المفاهيمي والقانوني للتحقيق الإلكتروني

الفصل الثاني: المعوقات التقنية والقانونية في التحقيق الإلكتروني

الفصل الأول:

ماهية التحقيق الالكتروني

1.المبحث الأول: مفهوم التحقيق الإلكتروني

يعد التحقيق الجنائي في مجال الجرائم الإلكترونية من ادق وأعقد مراحل الدعوى العمومية، إذ يقوم على مواجهة غير متكافئة بين المحقق والجاني، حيث يسعى الأول إلى كشف الحقيقة وإثبات الوقائع اعتمادا على الأدلة، في حين يعمل الثاني على طمسها واستعمال وسائل تقنية متطورة للإفلات من مساءلة.

ومن ثم، فإن نجاح هذا التحقيق يظل زهيدا بمدى كفاءة المحقق، وخبرته الفنية، وإلمامه بمختلف العلوم ذات الصلة، لا سيما المعلوماتية والعلوم الجنائية.

ويتميز التحقيق في الجرائم الإلكترونية بخصوصية تميز عن نضيره التقليدي، بالنظر إلى الطبيعة غير المادية لمسرح الجريمة، وارتباطها بالبيئة الرقمية، الأمر الذي يفرض اعتماد آليات وأساليب حديثة تتلاءم مع هذا التطور التكنلوجي المتسارع، بما يمكن جهات التحقيق من فك غموض الجريمة، وتحديد هوية الفاعل، وإقامة الدليل على نسبة الفعل الإجرامي إليه.

كما لا يقتصر هذا النوع من التحقيق على جمع الأدلة المادية، بل يمتد ليشمل تحليل البيانات الرقمية وتتبع الآثار الإلكترونية التي يخلفها النشاط الإجرامي، سواء أثناء ارتكابه أو بعده، من خلال فحص الأنظمة المعلوماتية، واسترجاع البيانات، وتحليل سجلات التشغيل، بما يتيح إعادة بناء وقائع الجريمة بصورة دقيقة.

وعليه، يقتضي التحقيق في الجرائم الإلكترونية توفر كفاءات بشرية مؤهلة تقنيا وقانونيا، مدعومة بوسائل مادية وتقنية متطورة، ويسهم في تحقيق العدالة الجنائية في ظل البيئة الرقمية.

وتأسيسا على ما سبق، يقتضي الفصل تقسيم هذا المبحث إلى ثلاث مطالب، فسوف يعالج المطلب الأول تعريف التحقيق الإلكتروني وشروطه، ويخصص المبحث الثاني عناصر التحقيق الإلكتروني وخصائصه، على أن ينفرد المطلب الثالث لعرض الهيئات ووسائل التحقيق الإلكتروني.

المطلب الأول: تعريف التحقيق الإلكتروني وشروطه

يعد التحقيق الإلكتروني من المفاهيم الحديثة التي فرضها التطور التكنلوجي المتسارع، حيث أصبح من الضروري تأطيره علميا وقانونيا لفهم طبيعته وحدوده. ولتحديد هذا التعريف بدقة، لا بد من الانطلاق من جذوره الأساسية عبر التطرق إلى تعريفه من مختلف الزوايا (الفرع الأول)، ثم تحديد شروطه (الفرع الثاني).

الفرع الأول: تعريف التحقيق الإلكتروني:

أولا-التعريف اللغوي:

التحقيق هو التصديق أو التأكيد والتثبيت، نقول حقق الظن، بمعنى صدقه وحقق الأمر أي أكه وأثبته وجاء في معجم الوسيط الفعل حقق الأمر وأثبته وصدقه، يقال حق تاغني وحقق القول والقضية، وحقق الشيء والأمر: أحكمه.

ويقال حقق الثوب أحكم نسجه، وصبغ الثوب صبغا تحقيقا مشبعا وكلام محقق، محكم الصنعة رصين وحقق الثوب وغيره: وشاه يوشي على صورة الأحقاق، وحقق مع فلان في قضية آخذ أقوال فيها، تحقق الأمر[1].

ثانيا- التعريف الاصطلاحي:

هو مجموعة من الإجراءات التي تقوم بها الجهات القضائية المختصة، بهدف التأكد من صحة الوقائع المعروضة عليها، ولكشف عن حقيقة الأفعال المرتكبة، ومعرفة الأشخاص الذين يساهموا في ارتكابها، ثم إحالة المتورطين إلى جهة الحكم من أجل توقيع الجزاء المناسب عليهم عند الاقتضاء[2] .

وناك من عرفه على انه، مجموعة من الإجراءات التي تقوم بها السلطة المختصة بالتحقيق وفق الشروط والأوضاع التي يحددها القانون، بهدف التنقيب عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة أرتكبت وذلك لتحديد ما إذا كان ينبغي محاكمة الشخص المدعى عليه أو عدم لزوم ذلك[3].

ونستنتج من التعاريف أن التحقيق هو إجراءات قانونية تقوم بها السلطة المختصة لكشف الحقيقة وجمع الأدلة وتحديد المسؤول عن الجريمة تمهيدا لإحالتهم على القضاء.

على الرغم تعدد التعريف الفقهية للتحقيق الجنائي فإنها تتفق في جوهرها على اعتباره مجموعة من الإجراءات القضائية التي تمارسها سلطة التحقيق في إطار قانوني محدد بقصد البحث عن الأدلة لمتعلقة بالجريمة وجمها وتقدير كفاية، لاتخاذ القرار المناسب سواء بإحالة المتهم إلى المحكمة أو بحفظ الدعوى وبهدف التحقيق أساسا إلى كشف الحقيقة مع ضمان حقوق الأفراد في مرحلة ما قبل

[1]- جيلالي بغدادي، التحقيق دراسة مقرانة نظرية وتطبيقية، الديوان الوطني للأشغال التربوية، الجزائر ط1، 1950، ص 7.
[2]- دليلة جلول، الأسس النفسية للتحقيق الجنائي، دار الهدى للطباعة والنشر الجزائر، ط2، 2015، ص 11.
[3]- حسن جوفندار، التحقيق الإبتدائي في قانون الأصول المحاكمات الجزائية، دار الثقافة، عمان، ط1، 2008، ص 11.

المحاكمة، مما يبرر صلته الوثيقة بمرحلة جمع الاستدلالات في إطار السعي المشترك نحو تحقيق العدالة[1].

ويتضح من ذلك أن الدعوى الجنائية تمر قبل أن توضع أمام القضاء للفصل فيها وذلك بمرحلة تحقيق الابتدائي هي مرحلة جمع الاستدلالات فلا تعد من إجراءات التحقيق القضائي وإن كانت الجريمة في حالة تلبس[2].

فالتحقيق الجنائي ل معنيان:

"معنى يقصد به إجراءات التحقيق التي تقوم بمباشرتها سلطة التحقيق مطابقا إليها إجراءات جمع الإستدلالات التي يقوم به مأموري الضبط القضائي بما فيهم النيابة العامة في الأحوال التي يباشر فيها التحقيق"

والمعنى الآخر " يقصد بع ما يقوم به قاضي التحقيق والنيابة العامة في الأحوال التي يباشر فيها التحقيق"

ثالثا-التعريف الفقهي:

تشير النصوص إلى أن أغلب التشريعات الجنائية لا تضع تعريفا محددا للتحقيق لأن صياغة التعاريف من اختصاص الفقه أكثر من لكونها من عمل المشرع الذي يهدف عادة إلى ترتيب آثار قانونية لا تضع تعريفات علمية مجردة، لذلك تصدرت التعريفات الفقهية للتحقيق الجنائي.[3]

فقد عرفه الفقاء المصريين على انه: "إتخاذ جميع الإجراءات والتدابير المشروعة التي تهدف إلى الوصول إلى الحقيقة وغرضا، فمن البديهي أن الطبيعة البشرية دائما تدفع الإنسان إلى البحث عن الأسباب التي أدت إلى ارتكاب الحادث وكيف وقع ومن ارتكبه وهكذا إلى حين وصوله في الأخير إلى نتيجة يراها صواب في نظره[4].

---

[1]- حمد أبو الروس، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، المكتب الجامعي الحديث، الإسكندرية،د ط، سنة1998، ص 3.

[2]-محمد سعيد نمور، أصول الإجراءات الجزئية، شرح قانون أصول المحاكمات الجزائية، دار الثقافة للنشر و التوزيع ، ط 2، سنة 2012، ص326.

[3]- المرجع نفسه، ص 326.

[4]- محمد أنور عاشور، المبادئ الأساسية في التحقيق الجنائي العملي، عالم الكتب القاهرة، ط ، سنة 1987، ص 8.

وعرفه الفقيه عد الواحد إمام أنه "مجموعة إجراءات والوسائل المشروعة قانونا التي يقدم بها المحقق لكشف إستجلاء غموض الحادث والتوصل إلى فاعله وإسناد الإتهام إليه[1] .

الفرع الثاني: شروط التحقيق الإلكتروني:

أولا- أن يكون التحقيق بصدد جريمة (جناية او جنحة):

يشترط لبدء إجراءات التحقيق أن يكون الفعل محل البحث يشكل جريمة معاقب عليها قانونا سواءا كانت جنحة أو جناية إذ لا يكفي مجرد وقوع الواقعة بل يجب التأكد من وجود نص قانوني يجرمها ويحدد طبيعتها، وفي حال عدم وجود تجريم قانوني للفعل فلا مجال لتحريك الدعوى أو إتخاذ أي إجراء بشأنه، تطبيقا لمبدأ الشرعية الجنائية القائم على قاعدة "لاجريمة ولا عقوبة إلا بنص" كون يعد التحقيق ضمانة أساسية للمتهم ولا يجوز إحالته إلى جهة الحكم دون المرور به

يعد فتح تحقيق في المواد الجنايات قاعدة أساسية يترتب على مخالفتها البطلان مما يوجب على القاضي التحقيق مباشرة الإجراء حتى وإن كانت بسيطة، لأن تقدير جسامة الجريمة وتحديد المسؤولية عنها يجب أن يتم بصورة واضحة، أما في مواد الجنح فإن اللجوء إلى التحقيق يكون حسب طبيعة القضية إذ أصبح إلزاميا كلما كانت الوقائع معقدة أو خطيرة أو استلزمت إتخاذ كل تدابير تحقيقية تدخل ضمن الاختصاص الحصري لقاضي التحقيق كإصدار أوامر بالحبس المؤقت أو إجراء إنابة قضائية خارج الاختصاص المحلي.

يصبح فتح التحقيق أمرا لازما كذل إذا كان مرتكب الجريمة مجهولا في حالة فرار أو تعذر الوصول إلى لأي سبب كما يقتضيه ذلك من إجراءات بحث وتحري كما يكون التحقيق ضروريا في بعض المخالفات التي تسير بخطورة خاصة، وكذلك في الحالات التي تستدعي تدابير حقيقية تتجاوز الرسائل العادية كوجود غموض في الوقائع أو حاجة إلى جمع أدلة أو إنشاء مراكز قانونية محتملة.[2]

[1]- مصطفى محمود موسى، التحقيق الجنائي في الجريمة الإلكترونية، بدون دار النشر، ط 1، القاهرة، ص 165، 166.

[2]- عمارة فوزي، قاضي التحقيق، أطوحة دكتوراه العلوم، كلية الحقوق، جامعة الأخوة منثوري قسنطينة، 2009، 2010، ص 39.

ثانيا – أن تكون الجريمة قد وقعت فعلا أو ترجح وقوعها:

يشترط اتخاذ الإجراءات في الجرائم الإلكترونية أن تكن الجريمة قد وقعت فعلا أو توجد مؤشرات على وقوعها، إذ لا يجوز مباشرة التحقيق في الجرائم محتملة فقط، وإلا عد الإجراء غير صحيح.

كما يثار في هذا السياق التمييز بين نوعين من التدخل:

1- الإجراءات السابقة على مباشرة التحقيق والتي تجري لكشف جريمة ثم الإعداد والتخطيط لإرتكابها .

2- إجراءات الضبط الإداري التي تستخدم للعمل على منع وقوع الجريمة يجيز القانون لمأمور الضبط الإداري الفضائي مباشرة إجراءات الاستدلال وجمع التحريات متى توافرت الدلائل الكافية على وقوع الجريمة، دون اشتراط ضبطها حال ارتكابها، إذ يعد ذلك من صميم وظيفته سواء تعلق الأمر بجرائم تقليدية أو الكترونية، ولا يعد تدخله في هذه الحالة تحريضا على الجريمة، كما يثار إشكال في الجرائم المعلوماتية بشأن تحقق حالة التلبس، حيث قد تتم مشاهدة الجريمة عن بعد عبر الوسائط الإلكترونية، وهو ما يوسع من مفهوم المشاهدة مقارنة بالجريمة التقليدية وتظهر التطبيقات العلمية، مثل تعاون مرودي الإنرنت مع السلطات، إمكانية الكشف عن الجرائم وتعقب مرتكبيها اعتمادا على المراقبة التقنية وكذلك قد تنشأ حالة تلبس في بيئات مثل المقاهي الأنترنت عند اكتشاف محتوى غير مشروع أثناء الاستخدام، مع التزام القائمين عليها بإبلاغ الجهات المختصة، و إلا تعرضوا للمساءلة، و مع ذلك يظل مفهوم التلبس في الجرائم الإلكترونية محل نقاش نظرا لاختلاف طبيعة عن الجريمة التقليدية و إمكانية تحققه بوسائل غير مباشرة.[1]

ثالثا-أن يجرى التحقيق في مواجهة متهم معني بارتكاب جريمة أو البحث عنه:

يتطلب ذلك معرفة من هو المتهم بارتكاب جريمة سواء كانت إلكترونية أم تقليدية، وينصرف إصلاح المتهم إلى شخص الذي يوجه إليه الاتهام بارتكاب أحد بالجرائم المنصوص عليها فيق.ع أو في إحدى التشريعات الجنائية الخاصة كقانون مكافحة تقنية المعلومات سواءا بوصفه فاعلا أو شريكا فيها[2].

فيظهر المتهم في إطار الدعوى الجنائية هو على أنه الشخص الذي نسب إليه واقعة إرتكاب جريمة سواء كان فاعلا اصليا أم شريكا فيها وذلك إسنادا إلى نصوص ق.ع أو التشريعات الخاصة ذات

---

[1]- بوحزمة نصيرة، التحقيق الجنائي في الجرائم الإلكترونية، دراسة مقارنة، رسالة دكتوراه، جامعة جيلالي اليابس سيدي بلعباس، كلية الحقوق والعلوم السياسية، ص 102، 103.

[2]- هدى أحمد العوضي، استجواب المتهم في مرحلة التحقيق الابتدائي ، مذكرة ماجستر في الحقوق، تخصص قانون عام، جامعة مملكة البحرين، 2009، ص 18.

صلة، وتحرك الإجراءات الجنائية ضده بإعتباره الطرف الذي يسعى السلطة القضائية إلى مساءلته والتحقق من مسؤوليته الجنائية بناءا على ما يتوفر من أدلة وقرائن.

كما ينظر إلى صفة المتهم من زاويتين :

الأولى تعتبره كل شخص قامت ضده دعوى جنائية لمجرد الإشتباه في إرتكاب الجريمة أو المساهمة فيها.

أما الثانية فتشترط قيام أدلة أو قرائن قوية تبرر توجيه الإتهام وتحريك الدعوى وهو الإتجاه التوجيهي الذي يخص بقبول أوسع من الناحية القانونية وتظل صفة المتهم ملازمة للشخص منذ توجيه الإتهام إليه إلى حتى الفصل النهائي في الدعوى، حيث قد تنتهي بصدور حكم بالبراءة او الإدانة وفي الحالة الأخيرة تتحول صفته إلى المحكوم عليه، كما أن هذه الصفة تقتضي خضوع شخص للإجراءات القانونية المقررة بدف تشخيص الأدلة وتقديرها وصولا إلى تحقيق العدالة الجنائية.

المطلب الثاني: عناصر التحقيق الإلكتروني وخصائصه

بعد تحديد مفهوم التحقيق الإلكتروني وبيان أهميته، يقتضي الأمر الوقوف على العناصر التي يقوم عليها هذا النوع من التحقيق، باعتبارها الأساس الذي تستند إليه إجراءات البحث والتحري في الجرائم الإلكترونية، والتي لا تختلف في أركانها القانونية عن الجرائم التقليدية، وإن كانت تتميز بخصوصيات تقنية تفرض آليات خاصة في الإثبات وجمع الأدلة الرقمية. كما يتميز التحقيق الإلكتروني بجملة من الخصائص التي تفرضها طبيعة البيئة الرقمية، سواء من حيث سرعة ارتكاب الجريمة، أو سهولة إخفاء آثارها وإتلاف أدلتها، أو ما تتطلبه من سرية ودقة في مباشرة إجراءات التحقيق. وعليه، سيتم تناول هذا المطلب من خلال بيان عناصر التحقيق الإلكتروني أولًا، ثم إبراز أهم خصائصه ثانيًا، في فرعين.

الفرع الأول: عناصر التحقيق الإلكتروني:

أولا–تبيان الركن الشرعي للجرائم الإلكترونية:

لقد نصت عليه المادة الأولى من ق.ع.ج: "لاجريمة ولا عقوبة إلا تدابير أمن بغير قانون" فالمقصود هنا وجود نص يجرم الفعل ويوضح العقاب المترتب عليه وقت وقوع هذا الفعل.[1]

ولقد خصص المشرع الجزائري منذ تعديلات 2004 و2006 وتبعته تعديلات 2024 من القسم السابع مكرر من ق.ع تحت عنوان المساس بالأنظمة المعالجة الآلية للمعطيات والذي يندرج ضمن الباب

[1]–الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 يتضمن قانون العقوبات المعدل والمتمم.

الثاني الجنايات والجنح ضد الأفراد الفصل الثالث الجنايات والجنح ضد الأموال المواد 344 مكرر إلى 394 مكرر 8 منق.ع.ج.

وهناك إلى جانبه القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال ومكافحتها كجانب وقائي من وقوع الجرائم المعلوماتية وذلك بالقيام بإجراءات وقائية تقنية تتمثل في مراقبة الاتصالات الإلكترونية، التسجيل والتجميع محتواها، القيام إجراءات التفتيش داخل المنظومة المعلوماتية.[1]

ثانيا-الركن المادي:

يتطلب السلوك المادي في الجرائم الإلكترونية وجود بينة رقمية واتصال بالأنترنت وكذلك توقيت بداية النشاط الإجرامي والشروع فيه وتحقق النتيجة.

فمثلا: يقوم المجرم بتحضير الحاسوب كي يحقق له حدوث جريمة فيقوم بتحميل برامج إختراق أو بعدها بنفسه أو يقوم بإعداد برامج فيروسات ليتم بثها ولكن ليست كل الجرائم تستلزم وجود أعمال تحضيرية هناك جرائم إلكترونية متعدية يعني جرائم سلوك فبمجرد القيام بالسلوك الإجرامي تتحقق الجريمة دون الحاجة إلى نتيجة [2] .

يتكون الركن المادي للجريمة من سلوك إجرامي والنتيجة والعلاقة السببية علما أنه يمكن تحقيق الركن المادي دون تحقيق النتيجة.

الركن المادي هو سلوك إجرامي يقوم به الإنسان ذو أهلية يكون السلوك إيجابيا كالقيام بفعل أو سلبيا كالإمتناع عن القيام بفعل يؤدي هذا السلوك تمس الحقوق التي يحميها القانون[3].

1- السلوك الإجرامي: في الجريمة الإلكترونية يكون بصورتين إما بفعل إيجابي أو بفعل سلبي ويمكن أن يجتمعا السلوكان في جريمة واحدة.

2- النتيجة الإجرامية: هو الأثر المادي الذي يحدثه السلوك الإجرامي.

---

[1]- أجعود فطيمة، خصوصية التحقيف في الجريمة الإلكترونية، مذكرة نيل شهادة ماستر في الحقوق، تخصص قانون إعلام آلي و أنترنت، جامعة محمد البشير الإبراهيمي، 2021، 2022، ص 11.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ط 1، الإسكندرية، 2018، ص 13.

[3]- أجعود فطيمة، المرجع السابق، ص 22

3- العلاقة السببية: هي العلاقة التي تربط الفعل بالنتيجة وذلك بإثبات أن الفعل الذي وقع هو سبب حدوث النتيجة وبذلك بمجرد إسناد الفعل إلى النتيجة شرط أساسي لتقرير المسؤولية.

من المقرر في القواعد العامة للقانون الجنائي أن الأعمال التحضيرية لا تستوجب العقاب ما لم تتجاوز مرحلة الإعداد إلى مرحلة البدء في التنفيذ غير أن هذا الأصل، يواجهه استنادا في نطاق الجرائم الإلكترونية نقل خصوصياتها التقنية و خطورة آثارها إذ قد يرى المشرع تجريم بعض الأفعال التحضيرية بذاتها متى كانت تنطوي على خطر حقيقي على المصالح المحمية قانونا كما هو الشأن في إقتناء برامج الإختاق أو أدوات فك التشفير وكلمات المرور أو حيازة مواد الإستغلال الجنسي للأطفال حيث يعد مجرد الحيازة أو الإقتناء سلوكا مجرما مستقلا عن الجريمة اللاحقة[1] .

ثالثا-الركن المعنوي:

الركن المعنوي للجريمة هو أحد أركان الأساسية للمسؤولية الجنائية إلى جانب الركن المادي ويتمثل هذا الركن في الحالة النفسية التي تربط الجاني بالفعل الإجرامي ويقوم على عنصرين جوهريين هوما العلم والإرادة إذ يشترط أن يكون الفاعل عالما بعناصر الجريمة ومدركا لعدم مشروعية فعل وأن تتجه إرادته إلى تحقيق النتيجة الإجرامية.

اما بالنسبة للجرائم الإلكترونية فلا تخرج عن إطار العام في مفهوم الركن المعنوي.[2]

رابعا-تحديد وقت ومكان ارتكاب الجريمة:

تطرح الجريمة الإلكترونية إشكالية حقيقية على المستوى تحديد الزمان ومكان إرتكابها نظرا لإرتباطها ببيئة رقمية لا تعترف بالحدود الجغرافية التقليدية، فقد تتنوع عناصر الجريمة بين عدة دول سواءا من حيث تواجد الفاعل أو موقع الخادم المعلوماتي أو محل تحقق النتيجة الإجرامية الأمر الذي يؤدي إلى تعقيد مسألة الإختصاص القضائي وتحديد القانون الواجب التطبيق.

فعلى سبيل المثال: لو قام أحد المجرمين في أوروبا بإختراق جهاز خادم أحد البنوك في سوريا وهذا الخادم موجود في فنزويلا، هنا تثير مشكلة ما مكان إرتكاب الجريمة وأيضا ما هو القانون الواجب التطبيق[3].

---

[1]-خالد ممدوح إبراهيم، المرجع السابق، ص 52، 53.

[2]- المرجع نفسه، ص 52، 53.

[3]- بوحزمة نصيرة، المرجع السابق، ص 134، 135.

خامسا-علانية التحقيق:

تعد علانية التحقيق من الضمانات الأساسية التي تكفل تحقيق العدالة وتعزز الثقة في إجراءات الجنائية إذ لا يقتصر دورها على طمأنة المتهم فحسب بل تمتد إلى حماية القاضي من أي تأثير محتمل كما تمنح الجمهور الإطمئنان إلى مسار العدالة يتم وفق القواعد القانونية السلبمة[1].

تختلف طبيعة العلانية في الإجراءات الجنائية بإختلاف المرحلة التي تمر بها الدعوى، حيث تكون في مرحلة التحقيق الإبتدائي علانية نسبية تقتصر على الأطراف الدعوى في حين تتم جلسات المحاكمة بالعلانية كأصل عام بما يسمح للجمهور بحضورها، ومع ذلك يمكن في بعض الحالات الإستثنائية تقرير سرية بعض إجراءات التحقيق إذا اقتضت المصلحة ذلك بإعتبار أن العلنية ليست مبدأ مطلقا.

فلا بد من أن يتم تحديد الأحوال التي يجوز فيها التحقيق سريا وهذه على كل حال رخصة لا يحسن الإلتجاء إليها إلا عند الضرورة[2].

إن إجراء التحقيق في إطار السرية قد يثير الشك ويزعزع الإطمئنان سواءا لدى المتهم أو الشاهد خاصة إذا تعلق الأمر بأدلة جنائية ذات أهمية، فغياب العلانية قد ينعكس سلبا على الحالة النفسية للشاهد فيظهر ذلك في صورة إضطراب أو تردد أثناء الإدلاء بأقواله بل وقد يصل الأمر إلى إنكار بعض المعلومات المرتبطة بالواقعة موضوع التحقيق [3]

تقتضي خصوصية بعض التحقيقات ضرورة التعامل بحذر عند الإستناد إلى أقوال الشهود، مع مراعاة أن العلانية في مرحلة التحقيق الإبتدائي تظل العلانية نسبية تقتصر على أطراف الدعوى.

ومع ذلك فإن لطبيعة حضور هؤلاء الأطراف أثرا نفسيا قد يؤثر في الشاهد مما يستدعي حملة من الإعتبارات العملية المرتبطة بعلانية التحقيق من قبيل إختيار مكان مناسب لإجراءه وتنظيم حضور الخصوم، وإحترام الضوابط الواجب إتباعها أثناء سير الإجراءات[4].

الفرع الثاني: خصائص التحقيق الإلكتروني:

أولا-الخفاء وصعوبة إكتشاف الجريمة:

---

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص 54.

[2]-بوحزمة نصيرة، المرجع السابق، ص 135، 136.

[3]- خالد ممدوح إبراهيم، المرجع السابق، ص 55.

[4]- بوحزمة نصيرة، المرجع السابق، ص 136.

تشير الدراسات إلى أن الجرائم المعلوماتية تتم غالبا في الخفاء بإستخدام الحاسوب، حيث تستهدف البيانات المخزنة أو المتداولة عبر الشبكات، ولذلك يتطلب التحقيق فيها أساليب خاصة للحفاظ على الأدلة الرقمية والتعامل مع مسرح الجريمة الإلكترونية بحذر[1] .

ثانيا-السرعة في إجراءات التحقيق:

تعد السرعة في مباشرة إجراء التحقيق من العوامل الأساسية لكسب الحقيقة، إذ يساعد على المحافظة على الأدلة ومنع ضياعا أو العبث بها، غير أن هذه السرعة ينبغي أن تتم في إطار إحترام القانون وضمان حقوق الأفراد حتى لا تتحول إلى تعسف يمس ضمانات العدالة.[2]

ثالثا-السرية في التحقيق:

يتميز التحقيق الإلكتروني فال جرائم الإلكترونية بالسرية حفاظا على مجريات التحقيق وعدم إفشاء معلوماته وذلك حسب المادة 01/19 ق.إ.ج الجديد 25-14 (مادة 11 سابقا).

البند الرابع-سهولة إتلاف الدليل:

يختلف التحقيق في الجرائم الإلكترونية عن التحقيق في الجرائم التقليدية على أنه مرتكبو الجرائم الإلكترونية يتمتعون بمهارات عالية تمكنهم من إتلاف الأدلة الرقمية أو تشويهها بصورة كبيرة كما ان هاته الجرائم في أغلب الأحيان لا تترك آثار مادية واضحة في مسرح الجريمة مما يجعل علنية الكشف عنها معقدا.[3]

البند الخامس-التدوين والكتابة:

"يحرر نسخة عن هذه الإجراءات وكذلك على جميع الأوراق ويؤشر أمين الضبط التحقيق أوضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل وذلك مع مراعاة ما أشير إليه في الفقرة الخامسة من هاته المادة" المادة 141 من ق.إ.ج حسب التعديل الأخير 25-14.

---

[1]- خالد عياد حلبي، إجراءات التحري والتحقيق في الجرائم الحاسوب والأنترنيت، دار الثقافة، الأردن، ط1، 2011، ص 123.

[2]- خالد علي نزال الشعار، التحقيق الجنائي في الجرائمم الإلكترونية، رسلة دكتوراه، كلية الحقوق، جامعة المنصورة، ص16.

[3]- خالد ممدوح إبراهيم، المرجع السابق، ص 17.

ومن هذا النص نستنتج أن التدوين من إجراءات التحقيق من المبادئ الأساسية في الإجراءات الجزائية حيث يتم إثبات ما يقوم به المحقق من إجراءات في محاضر مكتوبة تعد حجة في الإثبات متى استوفت الشروط القانونية، ويهدف هذا التدوين إلى توثيق مجريات التحقيق وضمان الرجوع إليها لاحقا.[1]

البند السادس-الإستقلالية:

كون هاته الميزة تنتمي إلى البيئة الإلكترونية مما يجعل التحقيق يرتبط بمواقع التواصل الاجتماعي وشبكة الأنترنت.[2]

المطلب الثالث: هيئات ووسائل التحقيق الإلكتروني:

يمكن تعريف المحقق بأنه شخص الذي يتولى مهمة التحقيق، سواء كان من رجال الضبطية القضائية أو من أعضاء النيابة العامة أو قضاة التحقيق.

ويعد الباحث الجنائي جزءا من جهاز الشرطة القضائية، حيث يخول له القانون القيام بجمع الأدلة والاستدلالات المتعلقة بالمشتبه بهم[3].

وخلال هذا المطلب، سيتم التطرق إلى أبرز الجهات المختصة بمكافحة الجرائم الإلكترونية في الفروع التالية.

الفرع الأول: هيئات التحقيق القضائي

أولا-الهيئات الغير قضائية:

تتمثل الهيئات الغير القضائية المكلفة في التحقيق في الجرائم المعلوماتية في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الإتصال، و السلطة الوطنية للمعالجة المعطيات ذات طابع شخصي، ووكالة أمن للأنظمة المعلوماتية.

1-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال:

أ-مفهومها:

---

[1]- بوحزمة نصيرة، المرجع السابق، ص 122.

[2]-خالد ممدوح إبراهيم، المرجع السابق، ص 55.

[3]- بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة أستاذ الباحث للدراسات القانونية جامعة بوضياف المسيلة العدد 11، سنة 2018، ص 366.

لقد نشأت سنة 2009 بموجب المادة 13 من قانون 09-04 وترك تشكيلتها وتنظيمها وكيفية سيرها عن طريق التنظيم، حيث خضعت وفقا لعدة مراسيم بداية بمرسوم الرئاسي 15-261 المؤرخ في 8 أكتوبر 2015[1]، الذي عرف بالهيئة بموجب المادة 2 على أنها: "سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي توضع لدى الوزير المكلف بالعمل"، كما جاء مرسوم رئاسي 19-172 المؤرخ في 6 يونيو 2019[2] وأعاد التعريف الهيئة بموجب المادة 02 على أنها:

"مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والإستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني"وأعيد تنظيم الهيئة من جديد بموجب المرسوم الرئاسي 800-183 المؤرخ في 13 يوليو 2020[3] حيث عرفت "الهيئة بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الإستقلالية المالية توضع تحت سلطة ريس الجمهورية".

ب-مهام الهيئة:

أبقى المرسوم الرئاسي في سنة 2020 على مهام الهيئة تحت رقابة السلطة القضائية المتمثلة في:

1.1 إقتراح عناصر الاستراتيجية الوطنية من الجرائم المتصلة بالتكنلوجيا الإعلام و الإتصال ومكافحتها.

2.1تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بالتكنلوجيا والإعلام و الإتصال ومكافحتها.

3.1مساعدة السلطة القضائية المختصة والمصالح الشرطة القضائية في الجرائم المتصلة بتكنلوجيا الإعلام والإتصال لا سيما من خلال دمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

4.1ضمان المراقبة وقائية للإتصالات الإلكترونية قصد الكشف عند الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

5.1تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصيرها ومسارها من أجل استعمالا في الإجراءات القضائية.

6.1السهر على تنفيذ الطلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على مستوى الدولي في مجال اختصاصاتها.

---

[1] سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الاعلام و الاتصال ، بين سرية المعطيات الشخصية ومكا فحة الجراءم الالكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد 02 ،2022، ص502 .

[2] المادة 13 من القانون09-04، المؤرخ في 2009/08/05 ،ج ر 47 ، الصادرة في 08/16 /2009 .

[3] المادة الاولى من المرسوم الرئاسي رقم 19-172، المؤرخ في 06/06 /2019، الجريدة الرسمية، العدد37 ،2019.

7.1تطوير التعاون بين المؤسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنلوجيات الإعلام والإتصال.

8.1المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنلوجيات الإعلام الإتصال .

9.1المساهمة في تحسين المعايير القانونية في مجال إختصاص الهيئة.

ج-تنظيم الهيئة:

وضع مرسوم رئاسي لسنة 2020 كل من مجل التوجيه ومديرية عامة، تحت السلطة المباشرة لرئيس الجمهورية ويقدمان له عرفا عن نشاطتها.[1]

د-مجلس التوجيه:

أبقى المرسوم الرئاسي الجديد على نفس الصلاحيات الممنوحة لمجلس التوجيه بموجب مرسوم الرئاسي لسنة 2019 غير أنه عدل التشكيلة برئاسة رئيس الجمهورية حيث يتشكل من الوزير المكلف بالعدل، والمكلف بالداخلية، والمدير العام للأمن الداخلي، قائد الدرك الوطني، المدير العام للأمن الوطني ممثل عن رئاسة الجمهورية فممثل عن وزارة الدفاع الوطني.

المجلس يجتمع في دوة عاجية مرتين في السنة بدعوى من رئيسه ويمكن أن يجتمع في دورات غير عادية إذا دعت الضرورة طلب من رئيسه.

هـ-المديرية العامة:

يترأسها مدير عام تعيينه وإنهاء بموجب مرسوم رئاسي.

أسندت للمديرية العامة نفس الصلاحيات المنصوص عليها في المرسوم 2019 كذلك تضمن المديرية مديريات ومصالح تابعة لها.

- مديرية للمراقبة والوقاية و اليقضة الإلكترونية.
- مديرية للإدارة والوسائل.
- مصلحة الدراسات والتلخيص.
- مصلحة التعاون واليقضة الإلكترونية.

ثانيا: الهيئـــــات القضائيـــــة

1-على مستوى جهاز الشرطة:

[1]المادة الثانية من نفس المرسوم.

عملت المديرية العامة للأمن الوطني على إنشاء مخبر مركزي متخصص تابع للمركز الشرطة بشاطوناف في الجزائر العاصمة إلى جانب مخبريين بكل من قسنطينة ووهران وتضم هذا هياكل فروعا تقنية من بينها خلية إعلام الآلي وفرق متخصصة في التحقيق في الجرائم الإلكترونية وكشفها[1].

كما تم إنشاء مخابر إضافية إلى مستوى بعض الولايات على غرار بشار و ورقلة وتمنراست في إطار توسيع إنتشار هذا النوع من الهياكل عبر مختلف أنحاء الوطن وفي نفس السياق أنشئ مخبر الأدلة الرقمية والآثار التكنلوجية ضمن مصالح الشرطة العلمية يغطي ولايات الجزائر، وهران، قسنطينة ويعني هذا المخبر بالتحقيق في الجرائم الإلكترونية حيث يتولى جمع الأدلة الرقمية وتحليلها للكشف عن التهديدات الأمنية ذات الطابع التكنلوجي ومكافحتها وينقسم إلى عدة أقسام من بينها:

قسم الأدلة الرقمية والحواسيب والشبكات.

قسم إستغلال الأدلة المستمدة من الهواتف النقالة.

قسم تحليل الأصوات بإستخدام تجهيزات تقنية متطورة للكشف عن الجرائم الإلكترونية[2].

ويعتمد نجاح الضطية القضائية في هذا المجال على مدى التنسيق و التعاون بين جهاز الشرطة والجهاز القضائية، إضافة إلى تكريس الموارد البشرية و تأهيلها مع الإعتماد على أحدث الوسائل والتقنيات في جمع الأدلة الرقمية كما توفر على مستوى أمن الولايات فرق متخصصة في الجرائم الإلكترونية تعمل تحت شراف مصالح الشرطة القضائية وتتكون من خبراء وتقنيين مختصين في مجالات الإعلام الآلي.

أمن المعلومات والتحقيق الرقمي على جانب تخصصات أخرى ذات صلة.

2-على مستوى جهاز الدرك الوطني:

يعد جهاز الدرك الوطني من بين الهيئات الأمنية الفعالة في مجال مكافحة الجرائم الإلكترونية حيث يضطلع بهذه المهمة من خلال المعهد الوطني للأدلة الجنائية وعلم الإجرام الكائن بمقر بوشاوي التابع لقيادة الدرك الوطني لاسيما عبر قسم الإعلام والإتصال الإلكتروني المختص بالتحقيق والكشف عن هذا النوع من الجرائم [3].

---

[1]- طلاح عبد القادر، آيت عبد المالك ، التحقيق الجنائي للجرائم الإلكترونية في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019، ص 1695.

[2]-طلاح عبد القادر، آيت عبد المالك ، المرجع السابق، ص1696.

[3]- المرجع نفسه، ص 1696.

ويضيف هذا المعهد كمؤسسة عمومية ذات طابع إداري أنشأت بموجبه مرسوم رئاسي رقم 04-183 المؤرخ في 26 جوان 2004 ويعتبر أداة متخصصة تستند إلى الخبرات التطبيقية والتحاليل العلمية الحديثة المدعومة بالتكنلوجيا المتطورة بما يساهم في توجيه التحقيقات وكشف الحقيقة إعتمادا على الأدلة العلمية والتحليلية كما يوفر دعما تقنيا لوحدات التحقيق والجهات القضائية، الأمر الذي يعزز فعالية ودقة العمل القضائي.

تمارس مهام الضبطية الفضائية تحت إشراف وكيل الجمهورية المختص إقليميا بإعتباره ممثل النيابة العامة، حيث يتولى الإشراف على يسر التحقيقات وإتخاذ القرارات القانونية المناسبة إسنادا إلى الأدلة المقدمة إضافة إلأى منحه صلاحية مباشرة إجراءات التحقيق لمصالح الأمن.

كما يتوفر الدرك الوطني على مستوى القيادة العامة من وحدات وهياكل تسهم في تنفيذ مهامه في مجال المكافحة الجرائم الإلكترونية من بينها:

- المصالح المركزية للتحريات الجنائية.
- المصالح والمراكز العلمية والتقنية.
- هياكل التكوين.
- المعهد الوطني لعلم الإجرام.

أ-صلاحية الضبطية القضائية:

يقصد بالإختصاص النوعي في النظام القضائي تحديد قضية معينة من الجرائم التي تقارن الضبطية القضائية التحقيق فيها، مثل الجرائم الإلكترونية وهو ما يساهم في توجيه الجهود القضائية وتركيزها في المجال المعلوماتي، يفهم من ذلك أن المشرع يعتمد على تخصيص أجهزة وتحقيقا متخصصة بكل نوع من الجرائم، بهدف تحقيق نتائج دقيقة وحريصة لتفادي الخطأ بين مختلف القضايا

ويقصد بالإختصاص المحلي هو تحديد النطاق الإقليمي الذي يمارس فيه ضابط الشرطة القضائية مهامه في التحري والتحقيق خاصة في مجال الجرائم الإلكترونية حيث يحدد هذا الاختصاص حدود تدخل جهات المكلفة بالبحث وفقا للمجال الجغرافي للمعني.

وتشمل صلاحية الضبطية القضائية في:

- لها صلاحية مراقبة الأنترنت والبحث عن الأنشطة الغير قانونية والغير مشروعة التي تهدد سلامة الأمن والوطن.

– لها صلاحية التعاون مع وكلات أجنبية دولية لقمع جرائم الإلكترونية التي تتجاوز حدود الوطنية.

– إصدار أوامر إعتقال وتقديم الدعم الفني للتحقيقات فهي تجمع الأدلة الرقمية وتحليلها إلى جانب إصدار أوامر الإعتقال تحت إشراف وكيل الجمهورية المختص

– التعاون مع الشركات التقنية والمعلوماتية للحصول على معلومات تساعدها على حل القضايا.

– إعتراض المراسلات وتسجيل الأصوات والتقاط الصور وذلك حسب المواد من 114 إلى 119 ق.إ.ج حسب تعديل 25–14 في الجرائم المعلوماتية مع الحصول على إذن من وكيل الجمهورية.[1]

ب –**تمديد الإختصاص المحلي:**

وفقا للمادة 03/78 من القانون 25–14 الجدد حيث إذا تعلق الأمر بالجرائم المنصوص عليها على سبيل الحصر في المادة نفسها الفقرة 3 والتي من بينها الجرائم المتصلة بتكنلوجيا الإعلام و الإتصال.حيث ورد في المادة من نفس المادة على انه يمنح المشرع قاضي التحقيق عندما يتعلق الأمر ببعض الجرائم ذات الخطورة، صلاحيات واسعة تخوله القيام بعمليات التفتيش والحجز في أي وقت ليلا أو نهارا وعلى كامل التراب الوطني كما يمكن تكليف ضباط الشرطة القضائية المختصين بتنفيذ هذا الإجراءات بطلب منهم أو بأمر من النيابة أو قاضي التحقيق المختص[2] .

الفرع الثاني: الوسائل والأدوات التحقيق في الجرائم الإلكترونية

أولا–وسائل التحقيق:

يتعين على المحقق عند مباشرته التحقيق في أي جريمة أن يلتزم بالقوانين والتشريعات واللوائح المعمول بها، إضافة إلى إتباع القواعد الفنية التي تتضمن مشروعية الإجراءات وسهولة الوصول إلى الجاني، ونظرا للطبيعة الخاصة للجرائم الإلكترونية، فإن التحقيق فيها يتطلب فهما دقيقا لوسائل إرتكابها والإلمام بكيفية تحليلها للوصول إلى الفاعل، ولهذا الغرض توجد مجموعة من الوسائل التي تساعد المحقق، وتنقسم إلأى وسائل مادية (أولا)، ووسائل إجرائية (ثانيا).

1– الوسائل المادية:

[1]–جباري عبد المجيد، دراسات قانونية عن المادة الجزائية، على ضوء أهم تعديلات الجديدة دار الهومة، 2012، ص 29.

[2]– المادة 78 من ق إ ج، 25–14 الجديد.

تشمل الوسائل المادية الأدوات التقنية التي تستخدم غالبا ضمن أنمة المعلومات والتي تساعد في إثبات وقوع الجريمة وتحديد هوية مرتكبها ومن أبرز هذه الوسائل عناوين الأنترنت(IP) والبريد الإلكتروني، وبرامج المحادثة.

فعنوان الأنترنت (IP) يعد المسؤول عن إرسال وإستقبال حزم البيانات عبر الشبكة، حيث يقوم بتوجيهها إلى وجهتها الصحيحة، ويشبه في وظيفته عنوان البريد التقليدي، إذ يتيح للشبكات نقل البيانات بدقة، ويوجد هذا العنوان في كل جهاز متصل بالأنترنت، ويتكون من أربعة أجزاء، يحتوي كل جزء على أرقام محددة، ويصل مجموعها إلى إثنتي عشر خاصية كحد أقصى، ويشير الجزء الأول، إلى الموقع الجغرافي، والثاني إلى مزود الخدمة والثالث إلى مجموعة الأجهزة المرتبطة بينما يحدد الجزء الرابع المستخدم للإتصال[1].

وفي حالة وقوع أي مشكلة أو عمل تخريبي، فإن أول خطوة يجب على المحقق القيام بها هي البحث عن رقم الجهاز وتحديد موقعه لمعرفة الشخص الذي قام بالفعل الغير المشروع، ويمكن لمزود الخدمة الأنترنت مراقبة المستخدم، كما تستطيع شبكات الاتصالات الهاتفية تتبع أيضا إذا توافرت لديها الأجهزة والبرامج اللازمة لذلك.

وتوجد عدة طرق لمعرفة عنوان الجهاز الإلكتروني خاصة في حالة الإتصال المباشر فعلى سبيل المثال، نظام التشغيل Windows يمكن إدخال الأمر WINPCFG في نافذة التشغيل ليظهر مربع يحتوي على عنوان الأنترنت (IP)، ويلاحظ أن هذا العنوان قد يتغير مع كل إتصال جديد بالشبكة[2].

فيشترط الإعتماد على بيانات البريد الإلكتروني أن تكون المعلومات التي أدخلها المستخدم أثناء إعداد حسابه صحيحة، حتى يمكن الإستفادة منها في تحديد هويته بشكل دقيق[3].

والسؤال الذي يمكن طرحه في هذا السياق ماذا يكشف رقم (IP) ويمك ذلك الإستفادة منه في التحقيق الجنائي؟

---

[1]–حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، د ط 2009، ص 511.

[2]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دار الكتب والوثائق القومية، القاهرة، مصر، د ط، 2012، ص 70.

[3]– حسين بن سيعد غافري، المرجع السابق، ص 512.

يمكن توضيح أنه عند دخول أي شخص إلى موقع إلكتروني يقوم هذا الموقع بتسجيل عنوان الـ (IP) الخاص بلجهاز المستخدم في الإتصال، كذلك عند إرسال بريد إلكتروني، المسلم التعرف على عنوان الـ (IP) اخاص بجهاز المرسل، فعلى سبيل المثال: إذا كان المرسل يستخدم برنامج (OUTLOOX) يمكن ببساطة فتح الرسالة كم إختيار (option) للإطلاع على هذا العنوان الـ(IP) ، ولكن يبقى التساؤل هل يحدد عنوان الـ (IP) هوية هوية جهاز المتصل بدقة كاملة؟

إذا كان الحاسوب المتصل تابعا لشبكة مرتبط بخط خاص مؤجر، كما هو الحال في العديد من المؤسسات المتوسطة والكبيرة، فإن عنوان الـ(IP) قد يكشف إسم المؤسسة ورقم جهاز المستخدم، أما في حال كان الإتصال يتم عبر خط هاتف عادي، فإن عنوان الـ (IP)وحده لا يكفي لتحديد الجهة المتصلة أو مرسل الرسالة بدقة، إذ يمكن من خلال أجزاءه الأولى التعرف على مزود الخدمة الأنترنت، بينما تشير الأجزاء المتبقية إلى مجموعة من الأجهزة المرتبة به.

لكن يظل التساؤل قائما: كيف يمكن تحديد هوية المستخدم إذا كان نفس الجهاز يستخدم عناوين متشابهة في أوقات مختلفة؟

في هذه الحالة يمكن اللجوء إلى مزود خدمة الأنترنت (isp)، الذي يحتفظ بتسجيلات تفصيلية لجميع الاتصالات، تتضمن تاريخ ووقت الاتصال، بالإضافة إلى بيانات المشترك، ومن خلال هذه المعلومات، يمكن التعرف على المستخدم خاصة إذا تم تزويد الجهة المختصة بالبيانات اللازمة، كما يمكن التعاون مع شركة الاتصالات، تتبع الرقم الذي ثم الاتصال من خلاله، إلا أن هذه الإجراءات تتطلب تدخل الجهات الرسمية المختصة بتطبيق القانون[1].

تعتمد معظم المواقع الإلكترونية على نظام أو ما يعرف بملفات تعريف الارتباط (cookies) والتي تتسم تسريع عملية الدخول إلى المواقع، ويعود استخدامها بشكل أساسي إلى أهداف تجارية، حيث تمكن هذه التقنية المواقع من جمع بعض المعلومات الخاصة بالمستخدم، مثل عدد مرات الزيارات ونوع الجهاز المستخدم، كما يمكن لبعض البرامج الموجودة على الحاسوب تمرير هذه البيانات، وقد تقوم المواقع أيضا بإرسال ملفات صغيرة إلى القرص الصلب (الهارد ديسك) عبر هذه التقنية.

ومن جهة أخرى توجد على الشبكة الأنترنت، مواقع تهدف إلى حماية خصوصية المستخدم و تأمين تحركاته مثل موقع (anonymizer.com) الذي يتبع إخفاء عنوان الـ (IP) عند زيارة المواقع

[1]– ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في الجرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مص، دط، 2006، ص 71.

بحيث لا يتمكن الموقع المقصود من تسجيل معلومات حقيقية عن المستخدم، بل يظهر له و كأن الزيارة تمت من عنوان مختلف وتقدم هذه الخدمة إما بشكل مجاني بسرعة محدودة أو مدفوعة بسرعة أفضل ومزايا إضافية.

كما تتيح هاته الخدمات إخفاء هوية المستخدم عن مزود خدمة الأنترنت نفسه وذلك عبر تمرير نشاطه من خلال مزود آخر بإستخدام تقنيات التشفير متقدمة (128بت) ومع ذلك، لا تكون هذه الحماية مطلقة، إذ قد يتمكن بعض مزودي الخدمة من معرفة المواقع التي يزورها المستخدم او الكلمات التي التي يبحث عنها، لذلك ظهرت من معرفة المواقع التي يزورها المستخدم أو الكلمات التي يبحث عنها، لذلك ظهرت وسائلأخرى لتعزيز الخصوصية مثل الأنترنت، وتوفير برامج مجانية مثل(MAIL لإرسال رسائل بشكل مجهول.

ولكن هل يضمن الإشتراك في هذه الخدمات إخفاءا لهوية بشكل كامل أثناء استخدام الأنترنت؟ في الواقع لا يمكن إخفاء تام للهوية، إذ أن الجهات الوسيطة التي تقدم هذه الخدمات تحتفظ بسجلات تتضمن مختلف تحركات المستخدم، ومع ذلك لا تتم الكشف عن هذه البيانات إلا في حالات محددة، مثل وقوع إعتداء وارتكاب أفعال غير قانونية كإرسال رسائل تهديد أو فيروسات، أو القيام بأي نشاط يخالف القوانين و التشريعات العمول بها[1].

أ- البروكسي (PROXY):

يعد البروكسي حلقة وصل بين المستخدم وشبكة الأنترنت، رغم أن البعض يرى أن استخدامه قد يسبب بعض المشكلات، إلا أن منافعه تفوق تلك المشكلات بكثير.

يعمل البروكسي كوسيط بين الشبكة ومستخدميها حيث تعتمد عليه الشركات الكبرى المزودة لخدمة الأنترنت لما يوفره من إمكانيات لإدارة الشبكة وتعزيز الأمن، إضافة إلى تقديم خدمات الذاكرة المؤقتة (cache memory) وتقوم فكرته على استقبال طلبات المستخدمين للبحث عن صفحات معينة تم التحقق مما إذا كانت هذه الصفحات مخزنة مسبقا في الذاكرة المؤقتة (cache) فإذا وجدت يتم إرسالها

[1]- ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 72.

مباشرة دون الحاجة للإتصال بالأنترنت، أما إذا لم تكن متوفرة فيتم جلبها من الشبكة العالمية باستخدام عنوان (IP)، ومن أبرز مزاياه قدرته على الإحتفاظ بسجل العمليات التي تتم عبره[1].

وهذا ما يمنحه دورا مهما في عملية التتبع، من خلال مراجعة تلك العلميات المخزنة والتي تكون مرتبطة بالمستخدمين الموجودين لدى مزود الخدمة تتمثل المهمة الأساسية لمزودات البروكسي في تسريع الوصول إلى المعلومات حيث يستطيع البروكسي جلب البيانات من المواقع بسرعة أكبر مقارنة بإتصال المستخدم المباشر، وقد أشار أحد مديري شركات الأنترنت في البيانات إلى أن 60% من المواقع التي يزورها المستخدمون تتكرر زيارتها وأن إستخدام البروكسي يمكن أن يوفر ما يقارب 50% من الوقت.[2]

لم تقتصر تقنية البروكسي على غرض واحد، بل تطورت لتشمل أدوارا متعددة تتجاوز وظيفتها الأساسية، وفيما يلي إستعراض بأبرز مهامها وآليات عملها:

1.1 البروكسي كآلية جدار(five wall): استخدمت تقنية البروكسي في بدايتها كأداة أساسية لإنشاء جدران الحماية تعمل هذا النظام كحارسي أمني صارم، حيث يفرض مرور كافة البيانات (الحزم) الصادرة من الشبكة الداخلية لمؤسسة أو الواردة إليها عبز جهاز وسيط واحد فقط.

-**آلية العمل:** عندما يرغب المستخدم في جلب مستند أو بيانات من شبكة الأنترنت، لا يتم الإتصال بالوجهة مباشرة، بل يرسل الطلب إلى مزود بروكسي الذي يتولى تنفيذ المهمة وتمرير البانيات للمستخدم يعد توجيها، مما يعزز من الشبكة.

- **تحسين جودة الخدمة عبر الذاكرة المخبأة: تتميز** البروكسي بقدرتها على رفع كفاءة الإتصال من خلال تقنية الذاكرة المخبئة، وذلك عبر وسيلتين رئيسيتين:
- **تحسين النسخة الترددية:** تساهم الذاكرة المختبئة في توفير مساحة أكبر لنقل البيانات المتاحة عبر الشبكة مما يشكل من الإزدحام.
- **تسريع التصفح:** تعمل هذه الذاكرة على تقليص من الزمن المستغرق لتحميل خدمات الأنترنت، حيث يتم استرجاع البيانات المخزنة مسبقا بسرعة فائقة وعرضها على أجهزة الكمبيوتر الخاصة بالمشتركين. [3]

2.1- برمجيات التتبع

---

[1]-اشرف صلاح الدين، طرق الحماية التكنلوجيا بانواعها واشكالها المختلفة، اعمال مؤتمرات حول مكافحة الجريمة عبر الانتر نت، المنظمة العربية للتنمية الادارية، القاهرة، 2010 ، ص203 .

[2]- ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 84.

[3]-ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 85.

تختص هذه البرمجيات بالكشف عن محاولات الإختراق السيبراني التي تستهدف النظام، حيث تعمل على تزويد لمستخدم بتقرير تحليلي شامل يتضمن تفاصيل الهجوم، يشمل هذا التقرير مسمى الحادثة الأمنية التوقيت الدقيق لحدوثها (التاريخ والوقت) بالإضافة إلى تحديد العنوان البروتوكولي (IP ADRESSE) الذي نفذت من خلاله عملية الإختراق كما يمتد التحليل ليشمل تحديد الهوية المؤسسة بمزود خدمة الإنترنت (ISP) الخاصة بالمخترق، وتعيين أرقام المنافذ والوجهات الشبكية المستخدمة في الإتصال، إلى جانب بيانات قضية أخرى ذات صلة[1].

ومن أبرز النماذج التطبيقية لهذه البرمجيات برنامج (HACK TRACPI) والذي يتميز بمواجهة رئيسية تمنح المستخدم بيانا استقصائيا مفصلا حول محاولة النفاذ غير المصرح بها يتضمن هذا البيان بيانات جوهرية تشمل: طبيعة الواقعة، وتاريخها، العنوان البرتكولي(IP) المصدر والنطاق الجغرافي (الدولة) الذي انطلقت منها المحاولة علاةو على ذلك، يستعرض البرنامج المعلومات التفصيلية عن الشركة المزودة للخدمة للمهاجم بما في ذلك أرقام المنافذ والبوابات الخاصة والبيانات الشبكية التابعة لها، وصولا إلى قنوات التواصل الخاصة بالشركة (كالهاتف والفاكس) وآخر تحديات التقنية التي طرآت على أجهزة الخدمة المعينة، وغيرها من البيانات المعلوماتية المهمة[2] .

3.1-نظام كشف الإختراق:

يعرف نظام كشف الإختراق المشار إليه إختصارا بـ (IDS) بانه فئة متخصصة من البرمجيات المصممة لمراقبة العمليات والأنشطة إلى تجري ضمن بيئة الحاسب الآلي أو الشبكة المعلوماتية، وتتمثل الوظيفة الجوهرية لهذا النظام في تحليل هذه العمليات بصفة مستمرة للكشف عن أي دلالات أو مؤشرات.

قد تشكل تهديدا أمنيا لسلامة النظام أو استقرار الشبكة[3].

تتحقق هذه الرقابة من خلال فحص وتحليل حزم البيانات (DATA PACKETS) أثناء تدفقها عبر الشبكة، ومتابعة ملفات نظام التشغيل الحساسة.

حيث يعمل النظام على تسجيل الأحداث فور وقوعها في الحاسب أو الشبكة ومن ثم إخضاع نتائج هذا التحليل لعملية مقارنة مع قاعدة بيانات تحتوي على "توقيعات" (SINGNATURE) تمثل الأنماط والخصائص المشتركة للإعتداءات الرقمية المعروفة لدى المختصين، وفي حال رصد أي تطابق مع هذه

---

[1]– حسين بن سعيد الغافري، ص513.

[2]– علي عدنان الفيل، المرجع السابق، ص 71.

[3]– حسين بن سعيد الغافري، المرجع السابق، ص 513، 519.

التوقيعات يقوم النظام بإخطار مدير النظام فورا عبر إنذار تقني، مع توثيق كافة البايان المتعلقة بالواقعة بفي السجلات حاسوبية متخصصة، لما يوفر مادة معلومات قيمة لفرق التحقيق الجنائي الرقمي تساعدهم في استنباط منهجية الجريمة، أسلوب تنفيذها، وتحديد مصدرها المحتمل.[1]

4.1-نظام مصيدة المخترقين (HONEYPOT):

يعرف نظام مصيدة المخترقين بأنه بيئة حاسوبية افتراضية أو فيزيائية، يتم تصميمها وتكوينها بشكل متعمد لتكون هدفا محتملا للهجمات السيبرانية عبر الشبكة، يرتكز المبدأ التشغيلي لهذا النظام على عنصر التضليل، حيث يفتقر النظام في حقيقته إلى أي بيانات ذات قيمة إنتاجية أو حساسة، إلا أنه يظهر للمهاجم واجهة توحي بسهولة الإختراق والوصول إلى موارد الشبكة الأخرى

- **الأهداف الاستراتيجية للنظام:**

✓ **الاستطلاع وجمع البيانات:** يتيح النظام مراقبة سلوك المهاجمين في بيئة معزولة، مما يساعد في رصد التقنيات والأساليب والبروتوكولات التي يستخدمونها أثناء محاولة الاختراق.

✓ **التحليل والوقاية الاستباقية:** تساهم المعلومات المستخلصة في فهم الثغرات الأمنية وتطوير بليات دفاعية وقائية فعالة، مما يعزز من مناعة الشبكة الحقيقية ضد الهجمات المستقبلية.

✓ **الدعم الجنائي الرقمي:** توفر البيانات التي يتم تحصيلها مرجعيا تحليليا هاما لفرق التحقيق الجنائي الرقمي، حيث تساعد في تحديد أبعاد الهجوم وتتبع الآثار الرقمية التي تشكل معالم الجريمة المعلوماتية.

ثانيا: أدوات التحقيق في الجريمة الإلكترونية:

تعد أدوات التدقيق والمراجعة برمجيات متخصصة تهدف إلى مراقبة وتحليل الأنشطة والعمليات المختلفة التي تنفذ على ملفات النظام ونظام التشغيل في بيئة حاسوبية محددة، وتعمل هذه الأدوات على أتمة عملية التوثيق من خلال تسجيل كافة الأحداث في ملفات سجلات مرجعية تعرف بـ (LOGS).

1-خصائص وآلية العمل:

أ-التوافر المدمج: تتوفر العديد من هذه الأدوات كخصائص قياسية مدمجة ضمن نظم التشغيل الحديثة، وتتطلب فقط تهيئة وإعدادات أولية لتصبح قادرة على رصد العمليات.

[1]- علي عدنان الفيل، المرجع السابق، ص 71، 72.

ب-الإستباقية: يستلزم تفعيل هذه الأدوات وتجهيزات من قبل مدير الشبكة أو النظام في وقت مبكر وقبل وقوع أي خروقات أمنية، لضمان التسجيل المستمر للبيانات التي قد تكون ذات صلة بأي حادثة مستقبلية.

ج-الأهمية الجنائية: تكمن القيمة الجوهرية لهذه السجلات في قدرتها على المساعدة في كشف الأنماط الإجرامية (MONDUS OPERANDI) وتحديد هوية الأفراد المسؤولين عن الإنتهاكات الأمنية [1].

2-نماذج تطبيقية:

تتنوع أدوات التدقيق باختلاف بيئات العمل، ومن أبرز الأمثلة الشائعة عليها:

أ-**Event Viewer:** الأداة القياسية لمراقبة الأحداث في بيئة نظام التشغيل ويندوز "Windows".

ب-**Syslogd:** الأداة المسؤولة عن إدارة سجلات والأنظمة (Unix) "النظام في بيئات" يونكس الشبيهة بها.

3-أدوات الضبط الجنائي الرقمي:

تتطلب عمليات التحقيق وجمع الاستدلالات جهودا حثيثة لضبط الجرائم وإثبات وقوعها، مع ضرورة الحفاظ على سلامة الأدلة وضمان عدم العبث بها لضمان نسبتها إلى الجاني. وتقدم هذه الأدلة إلى النيابة العامة لتعزيز ملف الدعوى واستحصال الاعتراف، ومن ثم تحال إلى القضاء للمحاكمة.

وتعد أدوات الضبط من أهم الوسائل المادية والتقنية التي تساهم في كشف الجرائم الإلكترونية، ومن أبرز هذه الأدوات:

أ-**أنظمة الحماية والمراجعة:** وتشمل البرمجيات المسؤولة عن أمن الشبكات.

ب-**أدوات الرقابة والتحليل:** مثل برامج التنصت **(sniffers)** والتقارير الصادرة عن أنظمة أمن البيانات ومراجعة قواعد البيانات.

ج-**برمجيات النسخ الإحتياطي الجنائي:** وهي الأدوات المستخدمة لاستخراج نسخة طبق الأصل (Bit Stream Backup) للأقراص الصلبة في الحسابات الإلكترونية الخاضعة للتحقيق، تكمن أهمية هذه النسخ في تمكين المحققين من إجراء الفحوصات الجنائية دون المساس بالأقراص الأصلية أو ‘حدات أي تغيير في البيانات المخزنة عليها.

[1]- خالد عياد الحلبي، المرجع السابق، ص 210.

د-البرمجيات المساعدة في جمع البيانات: مثل برمجيات (Java Applets) أو لغة (Java)، والتي يمكن توظيفها كأدوات لجمع المعلومات التقنية عن زوار المواقع الإلكترونية المتورطة في أنشطة جرمية.[1]

المبحث الثاني: الدليل الرقمي:

"بعدأن تم تفكيك الإطار المفاهيمي للتحقيق الإلكتروني في المبحث الأول، والوقوف على تعريفه، خصائصه، مصادره، والشروط القانونية والتقنية المحيطة به، يستلزم الأمر الانتقال إلى دراسة النتيجة الجوهرية والغاية المستهدفة من هذا التحقيق، والمتمثلة في" الدليل الرقمي ."فإذا كان التحقيق الإلكتروني هو البيئة الإجرائية المستحدثة، فإن الدليل الرقمي هو المحور الموضوعي والكيان المعلوماتي الذي تتولد عنه القناعة القضائية في الجريمة الإلكترونية .ونظراً للطبيعة الافتراضية لهذا الدليل، فإنه لا يتخذ شكلاً واحداً، بل تتعدد وتتنوع صوره تبعاً للوسائط والأنظمة التقنية التي يُستمد منها .وتأسيساً على ذلك، سنخصص هذا المبحث للغوص في أعماق هذا المفهوم المستحدث، حيث سنعمل على تحديد ماهية الدليل الرقمي أولاً، ثم ننتقل لتفصيل أنواعه المختلفة وأشكاله المتعددة في الفضاء السيبراني، وذلك وفق خطة التقسيم التالية :المطلب الأول :ماهية الدليل الرقمي مفهومه وطبيعته اما في المطلب الثاني أنواع وأشكال الدليل الرقمي واخيرا المطلب الثالث حجية الدليل الرقمي.

المطلب الأول: الإطار المفاهيمي

بعد أن أصبح الدليل الرقمي يشكل الركيزة الأساسية في إثبات الجرائم الإلكترونية، برزت الحاجة إلى تحديد مفهومه وضبط إطاره القانوني والفقهي، بالنظر إلى خصوصيته واختلافه عن الأدلة التقليدية من حيث طبيعته ووسائل استخراجه وحفظه وتقديمه أمام القضاء. كما أن التطور المتسارع لتكنولوجيا المعلومات فرض على التشريعات الوطنية والدولية مواكبة هذا النوع من الأدلة وتنظيم أحكامه بما يضمن حجيته في الإثبات ويحافظ على سلامته من أي تلاعب. وعليه، يقتضي هذا المطلب التطرق إلى مفهوم الدليل الرقمي وعناصره الأساسية، ثم بيان خصائصه وطبيعته القانونية وأوجه تميزه عن الدليل التقليدي، وذلك من خلال فرعين متكاملين.

الفرع الأول: مفهوم الدليل الرقمي:

تعد الأدلة الرقمية من أهم وسائل الإثبات في العصر الحديث خاصة مع تطور التكنلوجي و انتشار الأجهزة الإلكترونية في مختلف مجلات الحياة، ويقصد بها كل البيانات المخزنة أو المنقولة عبر الوسائط الإلكترونية التي يمكن توظيفها لإثبات واقعة معينة أمام الجهات القضائية كما تشمل هذه الأدلة أنواعا

[1]- خالد عيادي الحلبي، المرجع السابق، ص 210.

متعددة، منها ما هو مادي ومنها ما هو الكتروني وتمتاز بخصائص خاصة تميزها عن الأدلة التقليدية، كقابليتها للتلاعب مما يستوجب تأمينها وحمايتها لذلك يوليها المشرع عناية خاصة من خلال تنظيم طرق معالجتها وتقييمها ضمن الإطار القانوني المعتمد[1].

أولا-التعريف اللغوي:

يعرف على أنه "المرشد" هو ما يستدل به ويقال أدل بأمل والاسم الدالة بتشديد اللام وفلان يدل بفلان أي يثق به[2]، دل دال على الشيء، وإليه دلالة، أرشد فهو دال والشيء مدلول عليه وإليه[3] .

كما يعرف أنه: المرشد وما يتم به الإرشاد وهو ما يستدل به والدليل هو دال أيضا والجمع: أدلة أو دلالات[4].

"ذل – دله "– دلالة و دلولة و دليلي أي الشيء وعليه إرشده وهداه "أدل، دلالا"": وثق بحجة. فأفرد عليه، وكذا البازي على هديه "أدل" بالطريق "عرفة".[5]

ثانيا-تعريف الدليل الرقمي الفقهي:

أدى التطور المتسارع في مجال التكنلوجيا المعلومات إلى إضفاء طابع متغير ومعقد على مفهوم الدليل الرقمي مما جعل من الصعب وضع تعريف ثابت له يواكب هذا التطور المستمر، وقد ساهمت الخلافات الفقهية حول مضمونه في تعميق هذا الإشكال حيث سعى الفقهاء إلى تقديمهم تعريفات تائم مع طبيعة المتعددة، مما أفرز إتجاهين رئيسيين أحدهما تبني مفهوما ضيقا يربط الدليل الرقمي بالحاسوب فقط والثاني يدعوا إلى توسيع نطاقه ليشمل مختلف الوسائط والتقنيات التي يمكن أن تنتج أدلة رقمية[6] .

1-الإتجاه الضيق:

يرى االإتجاه الضيق أن الدليل الرقمي يقتصر على كونه مجموعة من الإشارات أو النبضات الإلكترونية ليتم تحويلها إلى صور أو نصوص أو رموز أو أصوات قابلة للهم والتحليل.

---

[1]– حسين علي محمد علي الشاعور نقبي، سلطة القاضي الجنائي في تقدير الأدلة، دراسة مقارنة، دار النهضة العربية، مصر،د ط، 2007، ص 153.

[2]– ابن المنظور، لسان العرب، المجلد 11، ط3، دار الصادر بيروت، 1994، ص 248، 249.

[3]– إبراهيم مكبور، المعجم الوجيز، ط1، مجمع اللغة العربية، مصر، 1973، ص232.

[4]– جميل صليبا، المعجم فلسفي، ط1، دار الكتاب اللبناني، بيرقت، 1970، ص 23.

[5]–فؤاد الأفرام البستاني، منجد الطلاب، الطبعة 45، دار المشرق بيروت، 1997، ص 204.

[6]– محمد زهير، الحجية القانونية للدليل الرقمي في الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، 2021، ط1، ص 25، ص 33.

وتعد هذه المعطيات نتيجة لتفاعل الأنظمة لتكنلوجية مع البيانات حيث يمكن تقديمها لاحقا أمام القضاء كدليل يسهم في كشف الحقيقة في إطار التحقيقات والإثباتات الجنائية.[1]

كما عرفه أيضا أنه كل المعلومات والبيانات التي يمكن معالجتها أو تخزينها في شكل رقمي بحيث تسمح للأجهزة الإلكترونية والتقنيات الحديثة بالتعامل معها لأغراض محدودة وقد تبنت بعض الهيئات الدولية هذا المفهوم، حيث اعتبر الدليل الرقمي كل المعلومات المخزنة أو المنقولة بطريقة تتيح استخدامها في الإثبات أمام الجهات القضائية [2].

2-الإتجاه الموسع:

يتجه الرأي الموسع إلى توسيع مفهوم الدليل الرقمي ليشمل مختلف الوسائل الرقمية الناتجة عن تطور تكنولوجيا المعلومات والاتصالات، حيث يعد هذا النوع من الأدلة الأداة الأساسية لإثبات الجرائم المرتبطة بهذه التقنيات.

ويرى أنصاره أن الدليل الرقمي لا يقتصر على شكل معدد، بل يشمل كافة البيانات والمعلومات الرقمية المرتبطة بعملية الإثبات، سواءا كانت منقولة أو مخزنة عبر الحاسوب، متى كان من شأنها تأكيد أو نفي الوقائع المرتبطة بالجريمة[3].

ويرى بعض أنصار الإتجاه الموضع أن الدليل الرقمي يشمل البرامج الحاسوبية والبيانات المرتبطة بها، والتي تستخدم بالإجابة عن المسائل الجوهرية المتعلقة بالوقائع الإجرامية، ويبرز هذا التطور الدور الأساسي للتكنلوجيا الرقمية في تحليل المعطيات وتقديم نتائج دقيقة حول الحوادث الأمنية، من خلال إستقلال البيانات المستخرجة من الأجهزة الإلكترونية، كما يستند هذا الإتجاه إلى إجتهادات فقهية ودراسات علمية في مجال القانون وتقنية المعلومات، أكدت أهمية الأدلة الرقمية في الإثبات الجنائي.[4]

3-تعريف المشرع الجزائري للدليل الرقمي:

---

[1]- طارق محمد الجميلي، الدليل الرقمي في مجال الإثبات الرقمي، ورشة عمل مقدمة للمؤتمر المغاربي الأول، حول المعلوماتية والقانون المنعقد في 2009، ص 2.

[2]- درابلة العمري سليم، حجية الدليل الرقمي في الإثبات الجنائي، تخصص قانون جنائي والعلوم الجنائية، 2024-2025، ص 27.

[3]- المرجع نفسه، ص 27.

[4]- درابلة العمري سليم، المرجع السابق، ص 28

لم يقدم المشرع الجزائري تعريفا صريحا للدليل الإلكتروني وإنما أشار بشكل غير مباشر من خلال أحكام ق.م.ج ، خاصة المادة 323 مكرر 1: التي اعتبرت الكتابة في الشكل الإلكتروني من أمكن من أمكن من التحقق من هوة صاحبه وضمان سلامته.[1]

وفي سياق مقارن إتجه المشرع الفرنسي إلى توضيح هذا المفهوم بشكل أذق، حيث أقر بإمكانية قبول الوثائق والبيانات الإلكترونية كأدلة قانونية، شريطة إمكانية تحديد مصدرها والتأكد من عدم تعرضها للتلاعب وذلك حسب م 1366.

ثالثا-التعريف العلمي للدليل الرقمي:

حسب قاموس كمبريدج، فإن التخزين الرئيسي هو عملية تحويل وتسجيل المعلومات على شكل أرقام ثنائية (1/0) وتسمى هذه الأرقام "البيت (BIT)، يمثل الرقم (0) حالة إغلاق off ويمثل الرقم (1) التشغيل "(01)" وتستعمل هذه الصيغة الثنائية لتمثيل كافة البيانات المخزنة في أجهزة الحاسوب ويعتبر النظام الثنائي الطريقة الأساسية لتخزين البيانات في الأجهزة الرقمية، بحيث يتم تحويل كافة المعلومات (سواءا كانت حروفا، أرقاما، رموزا أو أشكالا) إلى سلسلة من الأرقام الثنائية على سبيل المثال[2]:

الرقم 65 نظام عشري يتم تمثيله (0100001) وهذا الرقم يشير إلى الحرف (A) في جدول ascii.

الرقم 66 في النظام العشري يتم تمثيله (01000010) وهو يرمز إلى حرف (B) على نفس المنوال، يتم تمثيل مسافة بين كلمتين بالرقم 32 الذي يكتب في النظام الثنائي ك(00100000)[3].

تعرف المعلومات على أنها بيانات تم جمعها ومعالجتها بحيث أصبحت ذات معنى وقيمة، حيث تسهم في الوصول إلى نتائج معينة وتساعد على تنفيذ المعرفة، وتطويرها، كما تستخدم لشرح خصائص الأشياء، ووظائفها، ولكي تكون مفيدة يجب تنظيمها وتصنيفها بشكل مناسب.[4]

---

[1]- أنظر المادة 323 مكرر 1 من ق م ج بموجب قانون رقم 05-10 المؤرخ في 20 يونيو 2005 والذي نشر فيج ر الجمهورية الجزائرية الديمقراطية الشعبية العدد 54 بتاريخ 26 يونيو 2005.

[2]- حرف (A) يمثل الرقم العشري: 65 التمثيل الثنائي: 01000001 يعبر عن "A" في جدول

[3]- قاموسكامبردج معنى الدليل الرقمي تاريخ الدخول 2026/04/15 انظر الموقع الالكتروني التالي : https://dictionry.combridge/english/digital.

[4]-انظر احمد إبراهيم مصطفى سليمان، الارهاب والجريمة المنظمة، مطبعة العشري القاهرة، الطبعة 2006، ص 31.

ويشير مصطلح المعلوماتية الذي يعرف باللغة الإنجليزية (informatique) الذي يعالج المعلومات باستخدام الأنظمة الرقمية والبرمجيات المتقدمة

رابعا-التعريف التشريعي للدليل الرقمي:

لقد عرفه المشرع المصري في المادة الأولى من القانون رقم 175 سنة 2018 يتضمن مكافحة جرائم تقنية المعلومات بأنه:

"كل معلومات رقمية تتمتع بقوة أو قيمة ثبتية، سواءا كانت المخرجة أو المنقولة أو مستخرجة من أجهزة الحاسب الآلي أو الشبكات المعلوماتية وما في حكمها، بحيث يمكن تجميعها و تحليلها بإستخدام تقنيات متخصصة مثل برامج أو تطبيقات الرقمية"[1].

بحيث يتكون الدليل الرقمي من عنصرين هما:

المحتوى الرسمي الذي يحمل القيمة القانونية: المصدر التقني الذي ينتج هذا المحتوى سواء كان عن طريق الأجهزة الرقمية أو عن طريق وسائل الاتصالات المعلوماتية أو الوسائل التكنلوجية.

وقد أعطاه المشرع المصري طابعا من المرونة والشمولية حيث لم يقتصر على المخرجات التي يتم الحصول عليها من الحاسب الآلي وإنما يشمل حتى النواتج التي ترتبط بتقنيات المعلومات والإتصالات.

أما بالنسبة للتتشريع الفرنسي لم يقدم تعريفا محدادا للدليل الرقمي فقد نظم التعامل مع الأدلة الرقمية من خلال نصوص قانونية 323-1 ق.ع.ف التي تضمنت العقوبات المتعلقة بالمساس بالأنظمة المعلوماتية وهذا يعد تعريفا ضمنيا للدليل الرقمي.[2]

أما بالنسبة للتعريف الدولي في مجال الطب الشرعي فإن الدليل الرقمي فعرفته "أي معلومات يتم إنشاءها أو معالجتها أو تخزينها أو نقلها في شكل رقمي يمكن أن تقبلها المحكمة كدليل موثوق به بالإضافة إلى نسخ أخرى محتملة من المعلومات الرقمية الأصلية التي لها قيمة إثباتية يمكن للمحكمة الإعتماد عليها.

خامسا-مقارنة بين التشريع الجزائري والتشريعات الأخرى:

إن المشرع الجزائري لم يضع تعريفا دقيقا وشاملا، للدليل الرقمي رغم إعترافه بإمكانية إستخدامه في القضايا الإلكترونية، وهو ما يعكس تأثره النسبي بالمعايير الدولية مثل: إتفاقية بودابست، غير أن هذا

[1] المادة الأولى منق م رقم 175 سنة 2018 يتضمن مكافحة جرائم تقنية المعلومات، ج.ر.ج، العدد 31، الصادرة بتاريخ 14 /2018/08 .

[2] Article 323-1 – c p (version en vigueur depuis le 26 janvier 2023)

التنظيم لا يزال يفتقر إلى التفصيل، خاصة في ما يتعلق بأليات جمع وتحليل الأدلة الرقمية، مقارنة بالتشريعات الأروبية ففي المقابل يتميز التشريع الفرنسي بوضوح أكبر وإجراءات أكثر دقة في التعامل مع هذا النوع من الأدلة، مما يضمن حماية حقوق الأفراد ضمن إطار العدالة الجنائية، كما تؤكد الإتفاقية الدولية على أهمية التعاون بين الدول في مكافحة لجرائم الإلكترونية وضرورة توحيد الأطر القانونية المنظمة لإستخدام الأدلة الرقمية وبناءا على ذلك لا يزال في طور التطور ويحتاج المزيد من التوضيح والتفصيل لمواكبة التطورات الحديثة في هذا المجال.[1]

الفرع الثاني: خصائص الدليل الإلكتروني وطبيعته:

أولا – خصائص الدليل الرقمي:

1- الدليل الجنائي الرقمي هو دليل علمي وتقني ذو طبيعة مزدوجة:

يعد الدليل الجنائي الرقمي دليلا ذا طبيعة مزدوجة تجمع بين البعد العلمي و التقني، بإعتباره نتاجا لتكنولوجيا المعلومات، مما يجعله مختلفا جوهريات عن الأدلة المادية التقليدية التي تتسم بكونا مرتبة وملموسة ويستلزم التعامل مع هذا النوع من الأدلة اتباع أساليب غير تقليدية تقوم على إجراءات علمية وتقنية دقيقة لإستخراجه وتحليله وتقديمه أمام القضاء، كما يتطلب ذلك توفر خبرات متخصصة في مجال تكنولوجيا المعلومات، نظرا لصعوبة الوصول إلى محتواه أو تفسيره دون الإعتماد على الوسائل تقنية حديثة، وبذلك فغن الدليل الرقمي يتكون من بيانات ذات طبيعة الإلكترونية غير ملموسة ولا يمكن إدراكها أو الإستفادة منها إلا من خلال إستخدام أنظمة وأدوات متطورة، سواءا على الأجهزة (hardware) أو برمجيات (soft wark) مما يجعله قابلا للفهم فقط من قبل المختصين.[2]

2-الدليل الرقمي صعب محواه أو التخلص منه

يعد الدليل الجنائي الرقمي من الأدلة التي يصعب التخلص منها أو محوها بشكل كامل، بخلاف الأدلة المادية التقليدية التي يمكن إتلافها أو إخفائها بوسائل مختلفة، ويرجع ذلك إلى طبيعة الغير ملموسة للأدلة الرقمية، حيث تترك الجرائم الإلكترونية آثارا رقمية على الأجهزة والأنظمة المعلوماتية، ولا تزول بسهولة حتر مع محاولة حذفها.

---

[1] درابلة العمري سليم، المرجع السابق، ص43-44 .

[2] – مراد بن عيسى، حجية الدليل الرقمي في المادة الجزائية، أطروحة الدكتوراه، كلية الحقوق، جامعة الجزائر1، 2019، ص 38.

إذ يمكن استرجاعها باستخدام تقنيات حديثة، مما يجعل عملية إخفاءها أو القضاء عليها أمرا معقدا.

كما أن النشاط الرقمي الذي يقوم به الأفراد عبر الأنترنت أو من خلال الأجهزة الإلكترونية يظل غالبا مستجدا داخل أنظمة الحوسبية او الشبكات ويمكن تتبعه لاحقا، حتى بعد محاولات محوه، وقد تخزن هذه الأدلة في خوادم أو أنظمة ــ لفترات طويلة، الأمر الذي يزيد من صعوبة التخلص منها نهائيا، ويعزز من قيمتها كوسيلة إثبات في المجال الجنائي.

3-الدليل الجنائي الرقمي متنوع ومتطور باستمرار:

يتميز الدليل الرقمي الجنائي الرقمي بكونه دليلا متنوعا ومتطورا باستمرار، إذ لا يقتصر على شكل واحد رغم اعتماده على لغة الرقمية موحدة، بل يشمل مختلف أنواع البيانات والمعلومات التي يمكن تداولها إلكترونيا عبر الرسائل النصية والبريد الإلكتروني والمحادثات عبر الإنترنت إضافة إلى البيانات المستخرجة من الحواسيب وكمرات المراقبة والسجلات الرقمية والتي تربط بالجريمة بشكل مباشر وغير مباشر مما يجعلها ذات قيمة إثباتية في القضايا الجنائية[1].

كما هذا التنوع يقترن بتطور مستمر نتيجة التقدم التكنلوجي، حيث يظهر تقنيات حديثة تهدف إلى حماية البيانات مثل التشفير، في المقابل تطوير وسائل أخرى لفكها وتميز الأدلة الحقيقية من المزيفة، ويدي هذا التطور المتسارع إلى زيادة تقييد عملية فحص الأدلة الرقمية والتحقق من مصداقيتها الأمر الذي يطرح تحديات أمام الجهات القضائية في تقدير قوتها الإثباتية ومدى موثوقيتها[2].

4-الدليل الجنائي الرقمي عابر للحدود:

يتميز الدليل الجنائي الرقمي بقدرته على تجاوز الحدود الجغرافية إذ يمكن أن يوجد في أكثر من ولاية قضائية في الوقت ذاته مما يجعله غير ميد، بإقليم محدد على خلاف الأدلة المادية التقليدية، ويرتبط ذلك بطبيعته الديناميكية وسرعة انتقاله عبر شبكة الأنترنت حيث يمكن تخزين البيانات والمعلومات في خوادم موزعة عبر عدة دول وهو ما يزيد من صعوبة تحديد مكان وجود بدقة.

---

[1]–سعيد ،بن نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستر في العلوم القانونية تخصص العلوم الجنائية، جامعة مولود معمري، تيزي وزو، السنة 2012–2013، ص 129.

[2]– محمد بن يونس، مرجع السابق، ص 345.

ويؤدي هذا الامتداد العابر للحدود إلى تقييد إجراءات البحث عن الأدلة الرقمية وضبطها، خاصة في ظل الاعتماد المتزايد على تقنيات الحوسبة السحابتية، التي تسمح بخزين البيانات والوصول إليها عن بعد بدلا من حفظها محليا كما يطرح هذا الواقع تحديات قانونية تتعلق بتداخل الاختصاصات القضائية ين الدول، مما يستلزم اتخاذ إجراءات قانونية دولية مثل الحصول على أذونات من السلطات المختصة في الدول المعنية.

وبناءا على ذلك فإن فعالية ملائمة الجرائم الإلكترونية على المستوى الدولي تقتضي تنسيقا وتعاونا قضائيا بين الدول، بما يحقق التوازن بين احترام سيادة الدول وضمان نجاعة الإجراءات الجنائية في مواجهة هذا النوع من الجرائم[1].

ثانيا-الطبيعة القانونية للدليل الإلكتروني:

تثير مسألة تحديد الطبيعة القانونية للدليل الجنائي الرقمي لإشكاليات جوهرية، خاصة عند محاولة تصنيفه ضمن التقسيمات التقليدية للأدلة الجنائية، إذ يطرح التساؤل حول ما إذا كان يعد دليلا ماديا بحكم استخراجه من الوسائط الملموسة، كالأجهزة الإلكترونية، أم أنه أقرب إلى الأدلة الغير المادية نظر الطبيعة القائمة على البيانات والمعلومات الرقمية الغير مرئية وفي هذا السياق، يختلف الدليل ارقمي عن الأدلة التقليدية التي تقوم على عناصر محسوسة، حيث يظل محصورا في نطاق الأنظمة المعلوماتية والبيانات المخزنة داخلها، وهو ما يؤثر في طرق التعامل معه إجرائيا وقانونيا كما يبرز التساؤل آخر يتعلق بحجيته، وما إذا كان يعد دليلا فنيا يعتمد على خبرة المختصين، على غرار تقارير الطب الشرعي، نظرا لما يتطلبه من تقنيات دقيقة في الفحص والتحليل وضمان سلامة البيانات من التلاعب وبناءا على ذلكن يمكن إعتبار الدليل الرقمي فئة خاصة من الأدلة تستوجب تنظيما قانونيا متميزا، يجمع بين طبيعة التقنية وخصوصيتها الإثباتية بما يبرر الحاجة إلى تصنيف مستقل يراعي خصائصه الفريدة[2].

1-إعتبار الدليل الرقمي دليلا ماديا:

يرى هذا الإتجاه الفقهي أن الدليل الجنائي الرقمي يمكن إعتباره إمتدادا متطورا للأدلة المادية التقليدية، على أساس أن مخرجاته، مهما إختلفت أشكالها بين نصوص أو صور أو ملفات صوتية أو رموز رقمية، تظل قابلة للإدراك والمعالجة عبر الوسائل تقنية محددة، فحتى وإن إتخذ هذا الدليل طابعا

[1]-جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنلوجيا الحديثة، دار النهضة العربية، القاهرة ، د ط، ، ص116 .
[2]- درابلة العمري سليم، مرجع سابق، ص55-56.

غير ملموسة في صورته الأصلية، فإنه قد يتجمد في مخرجات مادية أو يرتبط ـــ مادية تتيح تخزينه وإسترجاعه.

كما يستند هذا الرأي إلى الإرتباط الوثيق بين الأدلة الرقمية والأنظمة المعلوماتية، حيث تعد هذه الأدلة إمتدادا للوسائط التخزينية والأجهزة الإلكترونية مثل الأقراص الصلبة ووسائط التخزين المحمولة والخوادم وينظر إلى الدليل الرقمي في هذا السياق، بوصفه كيانا مستقلا يتمثل في البيانات المخزنة، أو المنقولة إلكترونيا، مع تمييزه عن المكونات الفزيائية التي تحتويه.

وعليه فإن الطبيعة المادية للدليل الرقمي لا تنفصل عن البيئة التقنية التي يوجد فيها، إذا يشكل العتاد المعلوماتي عنصرا أساسيا في إستخراجه وتحليله، ضمن إطار متكامل لتكنلوجيا المعلومات يضمن إنتاج هذا الدليل وتفسيره في السياق الجنائي.[1]

2-إعتبار الدليل الرقمي دليلا معنويا:

يرى هذا الإتجاه الفقهي أن الدليل الرقمي يعد دليلا ذا طبيعة متميزة تختلف عن سائر الأدلة الجنائية، لما يتسم من خصائص تقنية ومعنوية تجعله أقرب إلى فئة مستقلة تضاف إلى التصنيفات التقليدية للأدلة ويستند هذا الرأي أن الدليل الإلكتروني يجمع بين أبعاد متعددة ولا يمكن إدراجه بشكل كامل ضمن الأدلة المادي أو القولية أو حتى فنية بشكل منفصل لكل الخصوصية التقنية وفي المقابل يذهب الرأي آخر إلى أن الأدلة الرقمية ل

تمثل فئة جديدة مستقلة، بل تعد إمتداد وتطور للأدلة المادية

التقليدية بحيث تعكس حالة تكامل بين الجوانب المادية والتقنية، مع بروز بعدها القانوني كوسيلة للإثبات، وفي هذا الإطار تظهر الأدلة الإلكترونية قدرة على الإستفادة من التطور التكنلوجي مما يسهم في تسهيل تتبع الجناة وتحليل الأنشطة الإجرامية ويعزز من فعالية الإجراءات التحقيق بإستخدام الوسائل التقنية الحديثة.[2]

ثالثا-التمييز بين الدليل الرقمي والدليل التقليدي:

---

[1]- المرجع نفسه، ص60 .

2- أحمد أبو القاسم، المفهوم العلمي والتطبيقي للدليل الجنائي المائي، مجلة مركز البحوث الشرطة، العدد 27 يناير 2005، ص17.

يتواجد الدليل الرقمي بنية إفتراضية تحتوي على بيانات رقمية متعددة الأنواع، أضفت عليه عدة مميزات جعلته يختلف فيها عن الأدلة التقليدية إلا أنه هناك أوجه تشابه عديدة من حيث الوظيفة القانونية والهدف مما يستدعي دراستها في إطار واحد لفهم دور كل منهما لتحقيق العدالة.

1-أوجه التشابه: يتشابه الدليل الرقمي مع الدليل التقليدي في كونهما يخضعان لإجراءات قانونية متقاربة تهدف إلى الكشف عن الجرائم لمختلف صورها، حيث يستندان إلى وسائل معتمدة في الإثبات الجنائي، فكلاهما قد يعتمد على أدلة مادية ناتجة عن وقائع ملموسة، سواءا تعلق الأمر بالجرائم الإلكترونية التي يتم فيها فحص الأجهزة ومحتوياتها من البيانات الرقمية كالصورة والرسائل.

كما تشابه إجراءات الضبط والتفتيش في كلا النوعين إذ يلجأ في الدليل التقليدي إلى ضبط الأدوات أو الأشياء المرتبطة بالجريمة في حين يقابل ذلك في المجال الرقمي تفتيش الأجهزة الإلكترونية لإستخراج الملفات والبيانات ذات صلة.

2-أوجه الإختلاف: يعد الإختلاف بين الدليل الرقمي والدليل التقليدي إختلافا ـــ يمس جوهر كل منهما، وليس مجرد تباين شكلي، فالدليل التقليدي يرتبط أساس بواقع مادي محسوس إذ ينشأ في بيئة ملموسة يمكت إدراكها بالحواس مباشرة، مثل الأدوات المستعملة في الجريمة والآثار المادية كالبصمات والوثائق الورقية، وهذا الطابع المادي يمنحه نوعا من الاستقرار والثبات، حيث يكون وجوده مستقلا عن الوسائط التقنية ويمكن الإطلاع عليه وفحصه دون الحاجة إلى وسائل معقدة.[1]

في المقابل يتميز الدليل الرقمي بطبيعته المادية، إذ يتكون من بيانات ومعلومات مخزنة داخل أنظمة إ لكترونية منقولة عبر شبكات الإتصال، وهذا يعني أنه لا يدرك بذاته بل يتطلب وسائط تقنية (كالحواسيب والب رمجيات) لقراءته تحليله، ومن هنا تظهر أولى الإشكاليات، وهي فهم الدليل الرقمي لا يكون مباشرة، بل يمر عبر عمليات تقنية قد تؤثر على طريقة تفسيره وقيمته الإثباتية.

ومن حيث النشأة، فإن الدليل التقليدي غالبا ما يكون نتيجة فعل مادي مباشر مرتبط بمسح الجريمة، بينما الدليل الرقمي هو نتاج تفاعل تكنلوجي معقد، قد يتم داخل بيانات إفتراضية عابرة للحدود مثل الأنترنت أو الحوسبة السحابية، وهذا ما يجعل تحديد مصدره ومكان وجوده أمرا أكثر تعقيدا ويطرح إشكالات قانونية تتعلق بالإختصاص القضائي والسيادة.

[1] المرجع نفسه، ص62.

أما من حيث القابلية للتغيير، فالدليل الرقمي يتميز بإمكانية تعديل أو التسخ أو الحذف بسهولة كبيرة، أحيانا دون ترك آثار واضحة، وهو ما يثير مخاوف بشأن سلامته ومصداقيته، غير أن هذه الخاصية يقابلها عنصر قوة يتشكل في إمكانية إكتشاف التلاعب عبر أدوات تحليل متقدمة وكذلك إمكانية إسترجاع البيانات حتى بعد حذفها في المقابل، فإن الدليل التقليدي أقل عرضه للتعديل الخفي، لكنه إذ تعرض للتلف أو الإتلاف فإن إسترجاعه يكون شبه مستحيلا.

ومن زاوية الدعامة يعتمد الدليل التقليدي على حامل مادي مستقل (كالورق والأشياء المادية) بينما يرتبط الدليل الرقمي بدعامة تقنية مزدوجة تتمثل في العتاد (HARDWARE) وبرمجيات (SOFT WARE) من جهة أخرى يلتقي النوعان في الإعتماد على الخبرة الفنية حيث يستعين القاضي بخبراء مختصين لتحليل الأدلة وتفسيرها متى كانت ذات طبيعة تقنية متعددة، ويقدر أي خبير في هاته الحالة عنصرا مساعدا في تكوين قناعة القضاء دون أن يشكل دليلا مستقلا بذاته.

كذلك تشترك الأدلة القولية في كلا المجالين بوصفها وسيلة إثبات قائمة على الأقوال، سواءا أصدرت عن شهود في صورة تلقائية أو خلال إجراءات الإستجواب والمواجهة.

وهذا الإرتباط يجعل وجوده وإستعماله مرهونين بسلامة هذه البيئة التقنية وهو يفرض ضرورة الحفاظ على سلسلة الحيازة الرقمية لضمان عدم العبث به.

كذلك يتميز الدليل الرقمي بسعة تخزينية هائلة وإمكانية نقل سريعة جدا مما يسمح بتجميع كميات كبيرة من المعلومات في وقت قصير وهو ما يعزز فعالية التحقيقات الجنائية، خاصة في الجرائم المعقدة في المقابل يظل الدليل التقليدي محدودا من حيث الحجم والإنتشار.

ومن الناحية القانونية يعتبر الدليل الرقمي حديثا نسبيا لذلك لا تزال التشريعات تختلف في تنظيمه ووـــ قبوله، خاصة في مايتعلق بمشروعية الحصول عليه و إحترام الخصوصية، أما الدليل التقليدي فقد إستقر تنظيمه منذ زمن طويل.

وتعددت قواعده بشكل واضح في مختلف الأنظمة القانونية، فقد يتطلب التعامل مع الدليل الرقمي خبرة تقنية متخصصة سواءا في جمعه أو تحليله او تقديمه أمام القضاء، وهو ما يفرض دول أكبر للخبراء النيين مقارنة بالدليل التقليدي الذي يمكن في كثير من الحالات التعامل معه بوسائل أبسط.

فالدليل الرقمي لا يمثل إمتداد للدليل التقليدي بل يعد نمطا جديدا من الأدلة بفرض إعادة النظر في المفاهيم الإجرتئية والقانونية التقليدية بما يتلائم مع خصوصيات البيئة الرقمية.[1]

المطلب الثاني: ماهية الأدلة الرقمية وتصنيفاتها المعرفية

تتسم الأدلة الرقمية بتنوع بنيوي تَبَعًا لتعدد صور الجرائم الإلكترونية ونمطيتها؛ وبناءً عليه، فإنها تنشأ وتتحقق في بيئة افتراضية (غير مادية) عبر أنظمة الحاسب الآلي أو من خلال الفضاء السيبراني (شبكة الإنترنت). ويتم تمثيل هذه الأدلة وإرسالها بواسطة نبضات إلكترونية رقمية غير مرئية، يملك الجاني القدرة على بثها وتوجيهها صوب البيانات أو البرمجيات الحاسوبية في أي وقت ومن أي مكان، وهو ما يفسر الصعوبة البالغة الكامنة في ضبط دليل مادي ملموس في هذا النمط من الجرائم.

وعليه، يمكن مقاربة أنواع الدليل الرقمي وتصنيفاته وفقًا للمحددات الفقهية (المطلب الأول) والتشريعية (المطلب الثاني).

يُلاحظ أن فقه القانون الجنائي لم يتناول صور الدليل الرقمي من حيث مصدره ومُنطلقاته بإسهاب وتفصيل موسع؛ ويُعزى ذلك بالدرجة الأولى إلى الحداثة النسبية لهذا الدليل، متأثرًا بالطفرة التكنولوجية المتلاحقة والمتسارعة. ورغم ذلك، تبلورت جهود ومحاولات فقهية رائدة استقرت على تقسيم الدليل الرقمي إلى أربعة أقسام جوهرية، بيانها كالتالي:

الفرع الأول: التقسيمات الفقهية للدليل الرقمي

أولا-الأدلة الرقمية المرتبطة بجهاز الكمبيوتر وشبكاته:

يختص هذا النوع بالأنشطة الإجرامية الواقعة مباشرة على الحواسب الآلية بطرق غير مشروعة، وتتفرع بدورها إلى:

1-المكونات المادية (Hardware):

ويُقصد بها الأجزاء العينية الملموسة التي يتألف منها النظام الحاسوبي، وتشمل الوحدات المستقلة بذاتها مثل الشاشة، لوحة المفاتيح، وغيرها. ومن أبرز وسائط التخزين المادية الملحقة بها:

[1] مايدي شهرة مسعودي أمال ،الدليل الرقمي و دوره في الإثبات الجنائي، أطروحة ماستر ، قانون إعلام الالي و الأنترنت، كلية الحقوق والعلوم
السياسية، جامعة محمد البشير الابراهيمي ، برج بوعريريج ، 2004-2025 ، 2025/06/04، ص19 .

أ-**الأشرطة المغناطيسية:** تُوظف هذه الأشرطة في عمليات الحفظ المتتابع للبرامج والملفات الضرورية لقراءة البيانات؛ حيث تبدأ قراءتها تتابعيًا من نقطة انطلاق الشريط، وتتنظم المعلومات داخلها ضمن وحدات مستقلة ومخصصة. وتُعرف كل وحدة تخزينية بـ "الحزمة"، ويتحكم مستخدم الجهاز في تحديد حجمها وسعتها التخزينية. وبناءً عليه، يُتعامل مع الحزمة ككيان ووحدة متكاملة ومترابطة عند الحفظ أو الاستخراج من الشريط، كما يعمد البعض إلى إيداعها وحفظها في الخزائن البنكية أو مراكز التوثيق الحكومية الأمنية.[1]

الأقراص المغناطيسية: تتمتع هذه الأقراص بخصائص استيعابية وقدرات تخزينية فائقة؛ مما جعلها في صدارة الوسائط التخزينية المفضلة، وتنقسم إلى:

- **القرص المرن:** يُستعمل بصفة رئيسية في الحواسب الشخصية والمتوسطة، نظرًا لمرونة تداوله وسهولة استخدامه في نقل البيانات.
- **القرص الصلب:** عبارة عن قرص معدني رقيق، مُغلف بطبقة من مادة قابلة للمغنطة، ويُطلق عليه "القرص الثابت" لكونه مُستقرًا داخل البنية الداخلية للحاسب الآلي، ويمتاز بسعة تخزينية ضخمة وسرعة فائقة في تسجيل البيانات واسترجاع المعلومات.
- **الأقراص المدمجة:** تُمثل وحدات تخزينية رقمية متنقلة ومدمجة، تحتوي على ثروة معلوماتية وتتيح إمكانية تخزين البيانات وإعادة تسجيلها ومعالجتها.

-**المصغرات الفيلمية:** هي عبارة عن أفلام فوتوغرافية تُستغل في توثيق وتصوير صفحات البيانات، وتتميز بقدرتها العالية على تصغير المواد التوثيقية لدرجات متناهية، ويتم ذلك عبر تحويل البيانات المُسجلة على الأشرطة والأقراص الممغنطة.[2]

2-المكونات المعنوية (Software):

وتتمثل في العناصر غير الملموسة أو غير المحسوسة في النظام الحاسوبي، كالبرمجيات التطبيقية، ونظم التشغيل، وقواعد البيانات الرئيسية.

أ-الأدلة الرقمية المتعلقة بالإنترنت:

---

[1] أسامة محي الدين عبد العال، حجية الدليل الرقمي في الإثبات الجنائي مجلة البحوث القانونية والاقتصادية، العدد 76، منصورة، للجرائم المعلوماتية، دراسة تحليلية مقارنة، ص660.

[2] وهيبة لعوارم، الدليل الرقمي في مجال الإثبات الجنائي وفقا للتشريع الجزائري، المجلة الجنائية القومية، المجلد57، العدد الثاني، القاهرة، يوليو، 2014، ص72.

ينطبق هذا النمط على الجرائم المرتكبة عبر الفضاء الافتراضي (الإنترنت)، والتي تقوم بنيتها على فكرة نقل وتداول المعلومات بين مستخدمي الشبكة العالمية بوسائل غير مشروعة، ومن أمثلتها: الولوج غير المصرح به للمواقع الإلكترونية، واستخدام عناوين بروتوكولية زائفة أو وهمية لتسهيل اختراق الشبكة.[2]

ب-الأدلة الرقمية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات:

تتمحور هذه الأدلة حول الجرائم التي تُرتكب بواسطة الكمبيوتر أو شبكة الإنترنت كأداة ومسهل رئيسي لتنفيذ السلوك الإجرامي، مثل جرائم نقل وتجارة المخدرات، أو عمليات غسيل الأموال؛ وفي هذه الحالات، يُمثل الجهاز الحاسوبي المستودع الأساسي للاحتفاظ بالبيانات والمعلومات التي تُرشد إلى هوية الجاني وتثبت إدانته.[1]

ج-الأدلة الرقمية المتعلقة بالشبكة العالمية للمعلومات:

يتوافق هذا الصنف مع الجرائم المتصلة اتصالًا مباشرًا بشبكة الإنترنت، بحيث يشكل السلوك الإجرامي اعتداءً غير مشروع يقع على النصوص، أو الوثائق، أو المحتويات الرقمية المتاحة على الشبكة، ومثال ذلك جريمة سرقة بطاقات الائتمان، والاعتداء على حقوق الملكية الفكرية للبرمجيات، وغيرها من الجرائم التي يستلزم قيامها الاتصال بالشبكة.

الفرع الثاني: التقسيمات التشريعية والقضائية للدليل الرقمي

شهدت الساحة القانونية بروز عدة تشريعات تهدف إلى تأطير الدليل الرقمي وتحديد ماهيته؛ وحظي هذا الموضوع باهتمام بالغ من قبل الهيئات القضائية. وفي هذا الصدد، سنرتكز على التقسيم المعتمد من قِبل وزارة العدل الأمريكية عام 2002، والتي صنفت الدليل الرقمي إلى ثلاثة أنواع رئيسية.

أولا-السجلات المحفوظة في الحاسوب الآلي:

وهي عبارة عن وثائق ومستندات مكتوبة تأخذ شكل حروف، أو أرقام، أو رموز، أو أي إشارات دلالية أخرى، وتكون مخزنة ومثبتة على دعامة رقمية، أو إلكترونية، أو صوتية، أو أي وسيلة مشابهة

[1] ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص95 .

يحج بها العمل القانوني؛ ومن أبرز نماذجها رسائل البريد الإلكتروني (E-mail)، والتي تُحفظ في صندوق الوارد التابع لصاحب الحساب وتشمل الرسائل المرسلة إليه وكافة الملفات المرفقة بها.[1]

ثانيا-السجلات المحفوظة جزئيًا في الحاسوب الآلي:

يتم توليد وإنشاء هذا النوع من السجلات آليًا بموجب البرمجيات والأنظمة التشغيلية للحاسب، وتُصنف على أنها مخرجات برامج الكمبيوتر التي لم تتدخل الإرادة البشرية في صياغتها بشكل مباشر، ومن الأمثلة الشائعة عليها: الفواتير الصادرة عن أجهزة السحب الآلي (ATM)، وسجلات وتفاصيل المكالمات الهاتفية.[2]

ثالثا-السجلات المحفوظة للإدخال والمنشأة بواسطة الحاسوب الآلي:

يُعد هذا التصنيف من الأدلة محل اتفاق وتطبيق في القضاء الأمريكي؛ ويكمن التمييز الأساسي فيه بين السجلات المتولدة تلقائيًا بواسطة الحاسوب والسجلات المخزنة فيه، في تحديد "المنشئ" الحقيقي لمحتوى السجل أو الوثيقة؛ فهل الآلة هي التي أنشأت المحتوى أم أن الدور اقتصر على تخزين وثائق تتضمن كتابات ورسائل صادرة عن أشخاص (كما هو الحال في رسائل البريد الإلكتروني)؟ أما بالنسبة للسجلات المتولدة آليًا، فالكمبيوتر هو الذي يصدرها دون تدخل بشري، ومثال ذلك سجلات الدخول إلى شبكة الإنترنت الصادرة عن مزود الخدمة (ISP).

بالإضافة إلى ذلك، يوجد نوع ثالث يدمج بين التدخل الإنساني والتوليد الآلي؛ ويتحقق ذلك عندما يقوم شخص بإدخال بيانات محددة ويطلب من الحاسوب معالجتها والوصول بها إلى نتائج رقمية معينة يتيحها البرنامج المستخدم؛ ومثال ذلك: قيام شخص يتهرب من

الضرائب بتسجيل بيانات مالية غير حقيقية عن دخله وأرباحه عبر برنامج حاسوبي لحساب الضريبة المستحقة عليه. وهنا يمكن القول إن هذه التقسيمات لا تستغرق كافة صور الدليل الرقمي، بل اقتصرت على نوع واحد وهو سجلات الحاسوب الآلي .[1]

إن التنوع البنيوي للدليل الرقمي يؤكد عدم وجود وسيلة أحادية للحصول عليه، بل يتخذ صورًا متعددة في شتى الأحوال، ويظل متمتعًا بالطبيعة الإلكترونية حتى وإن تغيرت الهيئات والأشكال

---

[1] فراح مناني، أدلة الإثبات الحديثة في القانون، دار العمري للطباعة والنشر والتوزيع، الجزائر، د ط، 2013، الجزائر، ص59.

[2] أسامة محي الدين عبد العال، المرجع السابق، ص 658.

التكنولوجية؛ وتبعًا لذلك، فإن القوانين والتشريعات الحديثة باتت تعترف بهذا النوع من الأدلة ذات الطابع الافتراضي، وتتعامل معها كأدلة إثبات أصلية في المسائل الجنائية.[1]

الفرع الثالث: الدليل الرقمي من حيث إثباته

يتفرع الدليل الرقمي بالنظر إلى معيار وسيلة الإثبات ومدى إعداد الدليل مسبقًا إلى طائفتين رئيستين؛ تتمثل الأولى في الأدلة التي جرى إعدادها وتجهيزها لتكون وسيلة من وسائل الإثبات القانوني، في حين تنصرف الطائفة الثانية إلى الأدلة التي لم تُعد ابتداءً لتشكل وسيلة إثبات.

أولا-الأدلة المُعدّة لتكون وسيلة إثبات:

تتميز هذه الطائفة من الأدلة بتصنيفها الثنائي المستند إلى كيفية التكوين؛ حيث تنقسم الأدلة الرقمية هنا إلى قسمين؛ يضم القسم الأول البيانات والمعلومات التي تنشأ بصورة تلقائية وعبر المعالجة الذاتية للحاسب الآلي، بينما يشتمل القسم الثاني على البيانات والمعلومات ذات الطبيعة المزدوجة أو المختلطة.

1- البيانات والمعلومات الناشئة تلقائيًا من الحاسوب الآلي:

وهي تُمثل جملة المعطيات والمعلومات الرقمية التي تتولد ذاتيًا عبر الأنظمة البرمجية للحاسب الآلي، دون أن يكون للمستخدم أو العنصر البشري أي تدخل مباشر أو إرادي في عملية إنشائها أو صياغتها؛ إذ تُعد من قبيل المخرجات الخالصة للآلة، ومن أبرز أمثلتها

التوضيحية: الفواتير الصادرة آليًا عن الأنظمة والبطاقات البنكية.[2]

2-البيانات والمعلومات ذات الطبيعة المختلطة:

ويُقصد بها تلك البيانات الرقمية التي يتداخل في تكوينها عنصران؛ حيث يُنشأ جزء منها بطريقة آلية ومستقلة بواسطة الحاسب الآلي، في حين يقوم الجزء الآخر منها على عملية الإدخال البشري للبيانات أو المعلومات؛ وتتصف هذه الأدلة ذات الطبيعة المركبة بأنها تُحفظ عادة في الأنظمة الرقمية لغرض الاحتجاج والاستدلال بها عند الحاجة مستقبَلًا.

ثانيا-الأدلة غير المُعدّة لتكون وسيلة إثبات:

---

[1] المرجع نفسه، ص659-660.

[2] المرجع نفسه، نفس الصفحة.

يُصطلح على تسمية هذا النمط من الأدلة بـ "البصمة الرقمية"، وهي الأدلة التي تتولد وتتحقق في البيئة الافتراضية بمعزل عن إرادة الشخص ورغبته الوعية؛ إذ لا تعدو كونها أثرًا تكنولوجيًا يخلّفه المستخدم وراءه أثناء القيام بعمليات إرسال أو استقبال الرسائل الإلكترونية، أو نتيجة للاتصالات والأنشطة الرقمية التي تم تنفيذها عبر النظام المعلوماتي.[1]

ومن النماذج الشائعة على هذا النوع: البيانات والمعلومات الحيوية المتضمنة في ملفات سجلات الولوج والنشاط والمعروفة بـ (Log\ files)، والتي تشتمل على تفاصيل تقنية دقيقة؛ مثل تاريخ وتوقيت عمليات التحميل، أو سجلات إرسال واستقبال ملفات المستخدم. وتكمن الأهمية الجنائية البالغة لهذه الأدلة في قدرتها الفعالة على معاونة جهات التحقيق في الكشف عن الهوية الحقيقية لمرتكب السلوك الإجرامي، والتوصل إليه عبر تقنيات تكنولوجية[2]

المطلب الثالث: حجية الدليل الرقمي في النظم الإجرائية للإثبات الجنائي

شهد الفقه القانوني والقضائي تبايناً ملحوظاً في الآراء والتوجهات حول مسألة مشروعية الدليل الرقمي المستمد من الوسائل التكنولوجية الحديثة، وتمحور هذا الخلاف الجوهري حول مدى إمكانية وسلطة القاضي الجنائي في الاستناد إليه والأخذ به؛ وثمة اتجاهان رئيسيان في هذا الصدد :هل يتمتع القاضي بحرية مطلقة) أو نسبية (في قبول واستنباط الأحكام من الأدلة الرقمية كغيرها من الأدلة التقليدية؟ أم أن سلطته في هذا السياق تظل مقيدة ومحكومة بالضوابط والمسارات الإجرائية التي يقرها المشرع صراحة في النصوص القانونية؟[3]

الفرع الأول: حجية الدليل الرقمي في نظام الإثبات المقيد

تأسس هذا النظام القانوني على قاعدة مبدئية مفادها أن المشرع الجنائي هو الجهة الحصرية والوحيدة المنوط بها تحديد وتعيين وسائل وطرق الإثبات بصورة مسبقة وحصرية .وبناءً على ذلك، يجد القاضي الجنائي نفسه مقيداً وملزماً بما يمليه القانون صراحة، فلا يجوز له اللجوء إلى أي دليل خارج هذه

---

[1] خلود فراحتية، دور الدليل الرقمي في الأثبات في الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر تخصص قانون الإعلام آلي وانترنت، كلية الحقوق والعلوم السياسية، جامعة محد البشير الإبراهيمي برج بوعريريج، 2021-2022، ص14.

[2] عبد الناصر محمد محمود الفرغلي، محمد عبيد سيف سعيد المسماري، الأثبات الجنائي للأدلة الرقمية من الناحيتين، القانونية والفنية "دراسة مقارنة"، جامعة نايف العربية للعلوم الامنية، السعودية، 2007، ص14 .

[3] خالد ممدوح إبراهيم، أمن الجرائم الإلكترونية، الدار الجامعية للطباعة والنشر والتوزيع، مصر، د ط، 2000 ، ص2 .

القائمة التشريعية المحددة، كما تقتصر سلطته التقديرية على تقييم القيمة الإقناعية للدليل في حدود ما سمح به المشرع.[2] وتأسيساً على هذا النظام، فإن الدور المنوط بالقاضي لا يتجاوز فحص الدليل المادي والتحقق من مدى استيفائه[1]للشروط والشبهات القانونية والتقنية المقررة سلفاً .وينتمي هذا النظام الإجرائي تاريخياً وتشريعياً إلى النظم القانونية ذات الثقافة الأنجلوسكسونية، وفي مقدمتها (بريطانيا لمملكة المتحدة والولايات المتحدة الأمريكية) بناءً على ما تقدم، فإن النظم التي تبنت هذا الاتجاه لا يمكنها الاعتراف بأي قيمة إثباتية أو حجية قانونية للدليل الرقمي ما لم ينص المشرع على ذلك صراحة وبشكل قاطع ضمن قائمة أدلة الإثبات المعتمدة، شريطة توافر شروط اليقين الكاملة فيه[2].

وتُعد بريطانيا الدولة الرائدة والأولى عالمياً التي بادرت بإصدار تشريع خاص ومستقل ينظم الحاسب الآلي، وهو" قانون إساءة استخدام الحاسب الآلي "الصادر في 29 يونيو Computer) 1990 Misuse Act 1990).ومع ذلك، يُعاب على هذا القانون أنه لم يتضمن قواعد صريحة ومباشرة تحكم قبول الأدلة الناتجة عن الأجهزة والأنظمة الرقمية؛ وذلك نظراً لأن هذه المسألة كانت منظمة ومحددة سابقاً بموجب نصوص معينة في" قانون البوليس والإثبات الجنائي "الصادر سنة Police and) 1984 Criminal Evidence Act 1984)، والذي حلّ بدوره محل قانون الإثبات الجنائي العام لسنة .1965

وحسب ما نصت عليه المادة 69 من القانون البريطاني، فقد اشتُرط لقبول الأدلة الرقمية أن تكون مستوفية للاختبارات الفنية والتقنية المقررة، وتُرفض هذه الأدلة كلياً إذا ثبت الآتي :إذا كانت البيانات أو المخرجات الرقمية غير دقيقة .إذا كانت البيانات المكونة للدليل ناقصة) غير كاملة (أو غير صالحة قانوناً وفنياً .إذا ثبت أن الحاسوب أو النظام الرقمي الذي استُخرج منه الدليل كان لا يعمل بكفاءة كاملة أو شاب تشغيله أي خلل[3] أما في الولايات المتحدة الأمريكية، فقد سارت العديد من الولايات باتجاه سن قوانين وتشريعات خاصة تعنى بتنظيم وقبول الأدلة الرقمية والمعلوماتية، ومن أبرزها :

ولاية" يوتا :(1991) "أقرت تشريعاً يسمح بقبول الأدلة المستمدة والمستخرجة من الحواسب الآلية، فضلاً عن البيانات المخزنة فيها، واعتبارها أدلة إثبات قانونية معتبرة في الدعاوى الجنائية ولاية

---

[1] ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص238 .

[2] خالد ضو، حجية الدليل الإلكتروني وشروط قبوله، مجلة الباحث القانوني في المجلة العلوم القانونية والسياسية، العدد08، المركز الجامعي بغلو، الأغواط، 2022، ص206.

[3] أحمد بن مالك، إبراهيم الخال، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، المجلد05، العدد01، المرجع نفسه، ص110.

"كاليفورنيا :(1983) "نصت تشريعاتها على أن النسخ والمخرجات المستخرجة من البيانات الرقمية تُعد أفضل دليل متاح ومقبول قانوناً لإثبات الوقائع والجرائم المعلوماتية .في النظام الألماني : يُلاحظ أن المشرع لا يلزم الشاهد بطباعة البيانات المخزنة في ذاكرة الحاسوب الآلي، مبرراً ذلك بأن أداء الشهادة في الأصل لا يتضمن فرض هذا الواجب الإجرائي .في النظام التركي : استقر التوجه التشريعي والقضائي على عدم جواز إجبار الشاهد أو إلظامه بكشف كلمات المرور

وينعكس الأثر السلبي لنظام الإثبات المقيد في كونه يكبّل القاضي الجنائي ويقيد سلطته في التقدير واستنباط الأحكام؛ حيث يجد القاضي نفسه مجبراً في كثير من الأحيان على إصدار أحكام وقرارات تخالف عقيدته ويقينه الوجداني لمجرد أن الأدلة المتوافرة لديه لم يقرها المشرع، أو أنها لا تندرج ضمن القوالب الجامدة للنصوص القانونية، مما يحول القاضي إلى مجرد أداة آلية لتطبيق النص دون مراعاة لروح العدالة[1].

الفرع الثاني: حجية الدليل الرقمي في النظام الحر

يقوم نظام الإثبات الحر الذي يجد بيئته الخصبة والأساسية في القوانين الإجرائية اللاتينية على منح القاضي الجنائي سلطة واسعة وحرية مطلقة في تقدير وإثبات الوقائع المعروضة على أنظاره بالاعتماد على كافة الوسائل المتاحة، دون إلزامه بأدلة محددة سلفاً، بل يُترك له الأمر لتكوين قناعته الشخصية والوجدان الخالص وتأسيساً على ذلك، يقبل النظام الفرنسي أمام محاكمه الجنائية مختلف الأدلة الرقمية والتكنولوجية كالتسجيلات الصوتية ومخرجات الأجهزة الإلكترونية ووسائل المراقبة والتصوير، وذلك استناداً إلى ما كرسه قرار محكمة النقض الفرنسية الشهير الصادر عام .1987 ويتم ذلك بالاستعانة بأجهزة وتقنيات خاصة يظّل من الصعب التلاعب بمعطياتها. وبفضل الكفاءة العالية والخبرة الفنية والتقنية التي يتمتع بها الخبراء المتخصصون، بات من الممكن والمتاح كشف أي محاولة للتلاعب أو التزوير أو الإتلاف الرقمي بواسطة أدوات تقنية متطورة وموثوقة.

أما في هولندا، فقد خطى المشرع خطوات متقدمة؛ حيث يتيح قانون الحاسوب لسلطات التحقيق الجنائي صلاحية إصدار أوامر قضائية ملزمة للقائمين على تشغيل الأنظمة المعلوماتية لتقديم وتسهيل الحصول على كافة البيانات والمعلومات الضرورية لاختراق الأنظمة والولوج إليها، باستثناء بيانات

[1] مركز الجامعي علي كافي، تندوف، 2021، ص110.

الحاسوب المسجلة في ملفات الشرطة، حيث أقر القانون أنه إذا كانت إجراءات الحصول على هذه البيانات غير قانونية أو شابتها مخالفات

إجرائية، فإنه يتعين استبعادها كدليل جنائي طبقاً للمبدأ القانوني المستقر استبعاد الأدلة غير القانونية " ثمرة الشجرة الخبيثة".[1]

الفرع الثالث: حجية الدليل الرقمي في النظام المختلط

يقوم هذا النظام الإجرائي على مقاربة توفيقية تجمع بين خصائص ومزايا نظامي الإثبات المقيد والإثبات الحر معاً وهو الاتجاه التشريعي الذي يحاول الربط والمزاوجة بين المدارس الأنجلوسكسونية والمدارس اللاتينية؛ حيث يعتمد أساساً على قيام المشرع بالتدخل لتحديد قوالب وشروط معينة لقبول أدلة بذاتها لإثبات وقائع محددة دون غيرها، وفي الوقت ذاته، يترك للقاضي الجنائي مساحة من الحرية والتقدير في حالات أخرى لتقييم وتقدير القيمة القانونية والبرهانية للأدلة المعروضة أمامه. [2]

الفرع الرابع: موقف المشرع الجزائري

من خلال القراءة التحليلية والاستقراء القانوني لنص المادة 349منق.إ.ج.ج ، نجد أن المشرع قد تبنى مبدأً عاماً وراسخاً ينص على أنه" :يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعاً لاقتناعه الخاص .[3]"ومن هذا المنطلق التشريعي، يتضح جلياً أن المنظومة القانونية في الجزائر قد منحت القاضي الجنائي حرية واسعة وسلطة تقديرية كاملة في تقييم الأدلة الجنائية بناءً على عقيدته واقتناعه الشخصي[4]

بناءً على ما تقدم، يمكن القول إن المشرع الجزائري قد انتهج وسلك المسلك الإجرائي المتبع في النظام اللاتيني (لا سيما القانون الفرنسي)، وذلك عبر فتح الباب لاعتبار الدليل الرقمي دليلاً مشروعاً ومقبولاً كغيره من الأدلة الجنائية التقليدية الأخرى؛ حيث منح سلطة تقديرية واسعة للقاضي الجنائي في تقييم هذه الأدلة الرقمية وبناء الأحكام عليها، ولكن مع إحاطة هذا القبول بضوابط شروط صارمة وضمانات تقنية وقانونية تضمن مصداقيتها

---

[1] خالد ضو، المرجع السابق، ص 206-207.

[2] حميد بلهادي، ص27-28 .

[3] أحمدبن مالك، المرجع السابق، ص110 .

[4] حميد بلهادي، المرجع السابق، ص28 .

وحجيتها، شريطة أن يتم الحصول عليها واستخلاصها بالطرق والمسارات القانونية المشروعة .وتماشياً مع الثورة التكنولوجية، أصبح المشرع الجزائري يضمّن في ترسانته القانونية نصوصاً واضحة وشاملة تستوعب الجرائم المرتبطة بالوسائل التكنولوجية الحديثة والمعلوماتية، حيث بادر بإدراج وسن عدة قوانين محورية في هذا الشأن، وفي مقدمتها القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. [1]

وقد تضمن هذا القانون الخاص مواداً إجرائية وقانونية دقيقة تنظم عمليات التفتيش الجنائي، والتحقيق الرقمي في الجرائم المعلوماتية، مع التأكيد المستمر على ضرورة تكوين وإعداد خبرات قانونية وقضائية وفنية متخصصة في مجال تكنولوجيا الإعلام والاتصال، لضمان مكافحة هذه الجرائم بفعالية واحترافية عالية.[2]

خــاتمة الفصل الأول:

ابعد أن استعرضنا في هذا الفصل الإطار المفاهيمي للتحقيق الإلكتروني والدليل الرقمي، يمكننا القول بأننا قد وضعنا اللبنات الأساسية لتشكيل فهم قانوني متكامل لآليات العمل في بيئة الفضاء الرقمي. لقد اتضح لنا من خلال المبحثين السابقين أن التحقيق الإلكتروني ليس مجرد عمل تقني بحت، بل هو عملية إجرائية مركبة تتطلب توازناً دقيقاً بين المهارة التقنية والالتزام بالنصوص القانونية الإجرائية.

كما خلصنا إلى أن الدليل الإلكتروني، رغم كونه الدليل الأكثر دقة وصدقاً في كشف الجرائم الحديثة بفضل طبيعته التقنية، إلا أنه يظل "هشاً" للغاية؛ إذ إن أي خطأ في إجراءات ضبطه، أو الحفاظ عليه، أو تحليله، قد يؤدي إلى بطلانه وسقوط الإثبات الجنائي برمته. وقد كشف لنا هذا الفصل أن

[1] المادة 349، قانون الاجراءات الجزاءية 14-25، مرجع سابق .

[2] أحمد بن مالك، إبراهيم الخال، المرجع السابق، ص111.

القصور في التعريفات التشريعية لبعض المفاهيم المرتبطة بالفضاء الرقمي لا يزال يطرح إشكالات حول "مشروعية" الإجراءات المتخذة.

إن ما انتهينا إليه في هذا الفصل من نتائج يرسخ قناعة مفادها أن التأسيس النظري للتحقيق الإلكتروني قد تم، ولكن هذا التأسيس يظل "نظرياً" في مواجهة الواقع العملي. فإذا كان المشرع قد وضع المبادئ العامة، فإن "التحدي" يكمن في كيفية تنزيل هذه المبادئ على واقع تقني معقد، يتسم بتطور أدوات الجريمة وتغير وسائلها.

وبناءً على هذه الخلاصة، فإننا نجد أنفسنا أمام ضرورة حتمية للانتقال إلى مستوى أكثر تعقيداً؛ وهو البحث في "العوائق" و"التحديات" التي تحول دون التطبيق الأمثل لهذه المفاهيم التي درسناها. وعليه، سينتقل بنا الفصل الثاني إلى الغوص في التحديات التقنية التي تواجه المحقق، والإشكاليات القانونية التي تفرضها طبيعة الجريمة العابرة للحدود، لنرى كيف يمكن للمنظومة القانونية أن تتفاعل مع هذه العقبات وتتجاوزها.

الفصل الثاني:

إجراءات التحقيق الالكتروني ومعوقاته

إذا كان الفصل الأول قد كرس لتأصيل المفهوم القانوني والتقني للتحقيق الإلكتروني والدليل الرقمي، فإن الغاية من هذا الفصل هي الانتقال من مرحلة التأسيس النظري إلى مرحلة التنزيل الإجرائي حيث ان الانتقال إلى الممارسة الفعلية لعمليات التحقيق في الفضاء الرقمي يكشف عن وجود فجوة كبيرة بين الطموح القانوني والواقع التقني، حيث تواجه جهات الضبط القضائي وسلطات التحقيق تحديات لا تقتصر فقط على تعقيدات التكنولوجيا، بل تمتد لتشمل إشكالات إجرائية وقانونية معقدة.

لقد ارتأينا تقسيم هذا الفصل إلى مبحثين رئيسيين يتكاملان لتشخيص واقع التحقيق الإلكتروني:

حيث ان في المبحث الأول نخصصه لدراسة الإجراءات العملية للتحقيق الإلكتروني، حيث نستعرض كيف تم تكييف الإجراءات الجزائية التقليدية كالتفتيش، الضبط، والحجز لتتوافق مع طبيعة الأدلة الرقمية، مع التركيز على الاجراءات المستحدثة التي جاء بها المشرع تداركا للفجوة والعجز الذي نجم عن الإجراءات التقليدية ايضا الأساليب الدولية اما في المبحث الثاني فسنكرسه لتحليل التحديات الجوهرية التي تعترض التحقيق الإلكتروني، سواء كانت تحديات تقنية تتعلق بالجريمة داتها ، أو المتعلقة بالضحية والجناة او بالمكلفين بالتحقيق تحديات قانونية تتعلق بمشروعية الدليل، بين ضرورة كشف الجريمة وضمان الحقوق والحريات الفردية.

المبحث الأول: إجراءات التحقيق الإلكتروني

شهد العالم طفرة تكنولوجية هائلة أفرزت نمطاً مستحدثاً من الجرائم الرقمية العابرة للحدود، مما فرض على الأنظمة القانونية تطوير آليات الاستقصاء والتحقيق الجنائي لتواكب خصوصية الدليل الإلكتروني وسرعة تلاشيه، ومن هذا المنطلق يسعى هذا المبحث إلى تسليط الضوء على ماهية إجراءات التحقيق الإلكتروني عبر ثلاثة مطالب رئيسية؛ نخصص المطلب الأول منها لبحث الإجراءات التقليدية ومدى قابليتها للتطبيق في البيئة الرقمية، لينتقل المطلب الثاني نحو استعراض الإجراءات المستحدثة التي فرضتها الطبيعة التقنية للجريمة كالتفتيش الرقمي والاعتراض الإلكتروني، وصولاً إلى المطلب الثالث الذي يركز على الإجراءات الدولية وآليات التعاون القضائي والأمني عبر الحدود لمواجهة هذا الامتداد الافتراضي للجريمة.

المطلب الأول: الإجراءات التقليدية في التحقيق الإلكتروني

تستند مواجهة الجريمة الإلكترونية في بيئتها الافتراضية إلى قاعدة إجرائية صلبة تنطلق ابتداءً من القواعد الإجرائية الكلاسيكية التي جرى تطويعها لتتناسب مع البيئة الرقمية، ومن هذا المنطلق يسعى هذا المطلب إلى استعراض الإجراءات التقليدية في التحقيق الإلكتروني من خلال ثلاثة فروع رئيسية؛ نخصص الفرع الأول منها لبحث مرحلة تلقي البلاغات الشكاوى المتعلقة بالجرائم المعلوماتية وكيفية قيدها، لينتقل الفرع الثاني نحو دراسة الخبرة الفنية والمعاينة كآليتين جوهريتين لفحص مسرح الجريمة الرقمي واستخلاص الأدلة بواسطة الخبراء المختصين، وصولاً إلى الفرع الثالث الذي يركز على إجراءات الضبط الإلكتروني للأجهزة والوسائط التقنية المستخدمة في ارتكاب الجريمة تمهيداً لحفظها وتقديمها للعدالة .

الفرع الأول: إجراءات تلقي البلاغات والشكاوى:

تمثل عملية تلقي البلاغات والشكاوى المرتكز الأساسي والخطوة الإستهلاكية في منظومة إجراءات التحري، كونها تشكل جزءا جوهريا من العمل الإستقصائي.

ويعرف البلاغ بمفهومه العام بأنه إخطار الجهات المختصة بوقوع جريمة ما، أو باحتمالية وقوعها الوشيك، أو بوجود اتفاق جنائي يهدف إلى ارتكابها.

وعليه، يشترط في القائم على تلقي هذه البلاغات امتلاك خلفية تقنية ومعرفية واسعة بشبكات التكنلوجيا وآليات عملها، وذلك لضمان القدرة على إدارة نقاش تقني متخصص مع المبلغ حول الجوانب المتصلة بالجريمة.

كما يتوجب على المحقق العمل على إستقاء كافة البيانات والمعلومات الضرورية من المبلغ بهدف تيسير مسار عملية التحقيق، حيث يتم بلورة هذه المعلومات في صورة إجابات دقيقة على مجموعة من التساؤلات المنهجية.[1]

- تاريخ ووقت تلقي البلاغ.
- المعلومات الخاصة بالمبلغ.
- المعلومات الخاصة بملتقى البلاغ.
- طبيعة ونوع جريمة الحاسبة الإلكترونية محل البلاغ.
- الأسئلة الستة المشهورة والمتعلقة بالجريمة: ماذا؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟
- المعلومات ذات العلاقة بالأنظمة الحاسوبية، كطبيعة العتاد ونوعية البرمجيات والمسؤولين عن الأنظمة، وطريقة الإتصال بهم وغيرها.

تستند عملية التخطيط لمواجهة الجريمة الإلكترونية إلى استثمار اليانات المتاحة لوضع تصور استراتيجي وخطة عمل متكاملة تحدد الإجراءات الأمثل للتحقيق، وهو ما يتطلب تشكيل فريق تحقيق متخصص يجمع بين الكفاءات الجنائية التقليدية والخبرات التقنية الدقيقة ويترأس هذا الفريق قائد ذو خبرة معمقة في التحقيق الرقمي، بمؤازرة محققين جنائيين ملمين بأساليب الجرائم المستحدثة، ونخبة من الأخصائيين في الحاسب والسبكات، بالإضافة إلى خبراء في مراجعة الحسابات والأدلة الجنائية التقليدية كالبصمات والتصوير، وذلك لضمان التنفيذ الدقيق لمراحل المعاينة والتفتيش[2].

الفرع الثاني: الخبرة الفنية والمعاينة:

يمثل فحص مسرح الجريمة الرقمية الركيزة الأساسية التي يبنى عليها الدليل الجنائي الإلكتروني، ونظراً للطبيعة التقنية المعقدة وسرعة التلف التي تتسم بها الأدلة الافتراضية، فإن الأمر يتطلب دمج

[1] علي عدنان الفيل، المرجع السابق، ص 11

[2] المرجع نفسه، ص.ص 12-13 .

الجانبين الفني والميداني للوصول إلى الحقيقة؛ ولذلك يسعى هذا الفرع إلى دراسة موضوع الخبرة الفنية والمعاينة من خلال شقين رئيسيين؛ نناقش في أولاً :الخبرة الفنية دور الخبراء والمختصين التقنيين في استخراج الأدلة الرقمية وتحليلها وتفكيك الشفرات، بينما نخصص ثانياً :المعاينة لبيان إجراءات فحص وتوثيق مسرح الجريمة الإلكترونية والوسائط المادية المستخدمة فيه لضمان سلامة الدليل ومنع العبث به.

أولا-الخبرة الفنية:

تعد الاستعانة بالخبراء في المجال لقضائي والتحقيق خطوة جوهرية، لاسيما في مواجهة الجرائم الإلكترونية، حيث يفرض هذا النوع من الجرائم ضرورة الإمام الدقيق والشامل بالأدلة والتحقيقات التقنية، وهو ما يتطلب فهما عميقا للتكنلوجيا والأنظمة الرقمية المعقدة.

وتبرز مساهمة الخبرة الفنية في مجال الجريمة الإلكترونية لدى جهات الأمن العام ذوي الخبرة المتوسطة في كيفية التعامل مع الأدلة الرقمية والحفاظ عليها، نظرا لخصوصيتها التي تميزها عن الأدلة المادية التقليدية. وتلعب هذه الخبرة دورا محوريا في تحديد أنواع الأدلة الرقمية وتحليلها وفق منهجية علمية دقيقة تهدف لكشف ملابسات الجريمة، فضلا عن دورها في تحويل الأدلة غير المرئية إلى أدلة مرئية قابلة للإدراك والفحص مما يسهل من عملية الإثبات الجنائي.[1]

يعرف الخبير الإلكتروني بأنه الكادر الفني المتخصص الذي يجمع بين الخبرة التقنية العميقة والدراية الواسعة بالأنظمة والشبكات الإلكترونية، ويتمتع هذا الخبير بالقدرة على رصد وتحليل وإدراك البيانات الجوهرية اللازمة لعمليات التحقيق، مستندا في ذلك إلى مهاراته التقنية وحواسه المهنية.

كما يمتلك الصلاحية والقدرة الفنية للنفاذ إلى أنظمة المعالجة الآلية للبيانات الرقمية متى استدعت ضرورات التحقيق ذلك، وينقسم الخبراء الإلكترونيون إلى فئات متعددة بحسب التخصص[2]:

-المبرمجون

-المحللون وهم الأشخاص الذين يضعون خطوات العمل ويقومون بتجميع بيانات نظام معين.

-مهندس والصيانة والاتصالات.

-مشغلو الحاسوب الآلي.

---

[1]- بن عمارة فاتن نور الإيمان، التحري والتحقيق في الجرائم الإلكترونية، ميدان الحقوق والعلوم السياسية، التخصص: قانون جنائي والعلوم الجنائية، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية، 2023-2024،

[2]- بوبعاية ابتسام، التحقيق في الجريمة المعلوماتية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر، جامعة محمد البشير الإبراهيمي، برج بوعريرج، 2021-2022، ص 45.

مدير النظام المعلوماتي.

إن على الخبير المعلوماتي أن يقوم بكل ما يمكنه في سبيل التحري الحقيقة والوصول إليها، وفي إطار ما يسمح به عمله، كما يجب عليه استخدام الأساليب العلمية التي يقوم عليها تخصصه والمتمثلة في[1]

- **1-المواقع الإجرامية بذاتها:** وهي المنصات التي محتواها في حد ذاته ركنا ماديا لجريمة ما، كالتهديد، أو النصب والاحتيال، أو القرصنة النسخ غير المشروع، حيث تتيح عملية التحليل الرقمي لهذه المواقع فهم آليات إعدادها، وتتبع حركاتها، وصولا إلى تحديد عنوان بروتكول الإنترنت IP ADDRESS المرتبط بالجهاز المصدر للجريمة.
- **2-المواقع المساعدة على ارتكاب الجريمة:** وهي مواقع قد لا يبدو محتواها إجراميا في الظاهر، إلا أن تتبع نشاط المستفيدين منها يكشف عن ممارسات غير مشروعة، مثل المواقع التي تقدم إرشادات لزراعة المواد المخدرة بعيدا عن الرقابة، أو تلك التي تستخدم لتسهيل الوصول إلى أوكار الرذيلة.

أولى المشرع الجزائري أهمية بالغة لتنظيم أعمال الخبرة، وهو ما تجسد في ق إ ج عبر المواد من 239 إلى252 من ق.ا.ج 14-25 الجديد.

وقد نصت المادة 239 صراحة على صلاحية جهات التحقيق أو الحكم في ندب خبير فني عندما تواجهها مسائل ذات طابع تقني تخصصي، ويتم هذا الندب بناءا على:

-مبادرة من الجهة القضائية تلقائيا.

-طلب من النيابة العامة.

-طلب من أحد أطراف الخصومة[2].

3-أهداف الخبرة الفنية في مجال الجريمة المعلوماتية: تتجلى الأهمية العلمية للخبرة الفنية في التعامل مع الدليل الرقمي من خلال تحقيق مجموعة من الأهداف الجوهرية، وهي:

---

[1]- تابري مختار، الخبرة في الجريمة الإلكترونية، حوار المتوسطي، المجلد 11، العدد 3، ديسمبر 2020، الجزائر، ص 391.

[2]-القانون رقم 14-25 المؤرخ في 9 صفر الموافق 3 غشت سنة 2025 المعدل للامر/155 المؤرخ في 08 يونيو 1966، المعدل والمتمم ل ق إ ج،يتضمن الجريدة الرسمية عدد54 المنشورة في 30-08-2025

•**أ-الكشف عن الأدلة وتحديد ماهيتها:** تمكين جهات التحقيق من العثور على الأدلة الرقمية الكامنة في النظم المعلوماتية وتحديد خصائصها التقنية الفريدة التي تميزها.

•**ب -الإستعادة والمعالجة التقنية:** العمل على إصلاح الأدلة المتضررة أو إعادة تجميع البيانات المجزأة من المكونات المادية للحاسب الآلي لضمان قابليتها للقراءة والاستخدام.

•**ج-تتبع الآثار الرقمية:** استقصاء وجمع كافة الآثار والمعلومات التي يتم تبادلها عبر الشبكات المعلوماتية، والتي قد تشكل خيطا حيويا للوصول إلى الحقيقة.

•**د-توثيق الحجية لضمان السلامة:** إثبات أصالة الدليل الرقمي وموثوقيته من خلال إدراجه ضمن "سلسلة الحيازة"Chain of Custody، مما يضمن عدم تعرضه للعبث من لحظة ضبطه حتى تقديمه للمحكمة.

•**هـ-الفحص المخبري الدقيق:** استخلاص نسخ احتياطية مطابقة للأصل لضمان عدم فقدان البيانات عملية الفحص، واستخدام الخوارزميات البرمجية المتقدمة للتأكد من سلامة الدليل وعدم تعديله.[1]

ثانيا-المعاينة:

تعرف بأنها الإجراء الميداني الذي يقوم به المحقق أو رجال الضبطية القضائية للانتقال إلى مسرح الجريمة، بهدف إثبات حالته المادية، والتحفظ على الأدلة مثل البصمات والأدوات المستخدمة، مما يساعد في كشف هوية الاني وربطه بالجريمة.

1-المعاينة المعلوماتية الرقمية:

هي التطور التقني للمعاينة، وتركز على جمع وتحليل الأدلة الرقمية المستخلصة من الأجهزة الإلكترونية الهواتف، الحواسيب، وسائط التخزين، تهدف هذه العملية إلى استخراج البيانات ذات الصلة بالتحقيق الجنائي السيبراني في تحقيق العدالة.[2] وتتمثل شروطها في:

أ-إذن أو أمر المعاينة المعلوماتية:

[1]- تابري مختار، المرجع السابق، ص 92.

[2]- فلات سمية، حاحا عبد العالي، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد 11، العدد 1، 2023، ص 523.

وهذا ما نصت عليه المادة 97 منق.إ.ج "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن..."[1] جاء في هذه المادة أن من أهم شروط المعاينة أن يكون هناك بإذن المعني بالأمر.

ب-وقت اجراء المعاينة المعلوماتية:

تتميز المعاينة المعلوماتية في الجرائم الإلكترونية بمرونة زمنية تتيح إجراءها في أي وقت من ليل أو نهار، شريطة الحصول على إذن مسبق من وكيل الجمهورية وفقاً للمادة 78 منق.إ.ج ؛ وهذا ما يفرقها عن الجرائم التقليدية التي تتقيد معاينتها بفترة زمنية محددة تمتد من الخامسة صباحاً وحتى الثامنة مساءً[2]

ج-مكان إجراء المعاينة المعلوماتية:

يجب أن تتم المعاينة المعلوماتية في مكان وقوع الجريمة، مع مراعاة مبدأ الشخصية والعينية المنصوص عليهما في المادة 744 من ق.ا.ج 14-25، وكذا المادة 15 من القانون 09/04. كما توجد بعض الحالات التي لا يجوز فيها إجراء معاينة المكان إلا بناءً على اتفاق مسبق.

د-الأشخاص المخول لهم حضور المعاينة المعلوماتية:

يحق حضور المعاينة المعلوماتية لكل من المتهم، والضحية، ومحاميهما، إضافة إلى وكيل الجمهورية، وقاضي التحقيق، وضباط الشرطة القضائية، باعتبارهم أطرافًا أساسية في إجراءات التحقيق.

هـ-محضر المعاينة المعلوماتية:

يُعدّ محضر المعاينة المعلوماتية المرحلة الختامية لإجراءات المعاينة الإلكترونية، حيث يلتزم ضباط الشرطة القضائية بتحرير محاضر تتضمن مختلف الأعمال المنجزة، وذلك وفقًا لما نصّت عليه المادتان 27و73 من ق.ا.ج.

وعليه تشمل المعاينة المعلوماتية ما يلي:

---

[1]- المادة97، من القانون14- 25، مرجع سابق .

[2]- المادة78، من المرجع نفسه .

تتضمن المعاينة المعلوماتية مجموعة من الإجراءات التقنية، من بينها جمع البيانات وتحليلها، وتوثيق الأدلة الرقمية، وإعداد التقارير الفنية، فضلًا عن تقديم الشهادات عند الاقتضاء. كما تستوجب الالتزام بجملة من القواعد والإرشادات الفنية، تتمثل في:

– توثيق الحواسيب الإلكترونية والأجهزة الطرفية المرتبطة بها، مع تصوير محتوياتها والأوضاع العامة لمكان تواجدها.

– توخي الدقة والعناية في ملاحظة الكيفية التي أُعيد بها تشغيل النظام، مع تتبع الآثار الإلكترونية المرتبطة بالتسجيلات الرقمية.

– معاينة حالة التوصيلات والكابلات المرتبطة بمختلف مكونات النظام وإثباتها.

– منع أي شخص غير مختص من الاقتراب أو التعامل مع أجهزة الحاسوب الإلكترونية محل المعاينة.

– المحافظة على كل ما قد يوجد في سلة المهملات من بيانات أو آثار رقمية يمكن أن تفيد التحقيق.

– الامتناع عن نقل أي معلومات من مسرح الجريمة الإلكترونية إلا بعد التأكد من خلوّ المحيط الخارجي من أي مخاطر أو مؤثرات قد تمسّ سلامة الأدلة الرقمية.[1]

الفرع الثالث: التفتيش والضبط الإلكتروني:

نظراً لما تتميز به الكيانات الافتراضية من سرعة الاختفاء والقدرة على المحو عن بُعد؛ وبناءً على ذلك، يهدف هذا الفرع إلى تسليط الضوء على إجرائي التفتيش والضبط الإلكتروني كآليتين حاسمتين في كشف الحقيقة، حيث نتناول من خلالهما الضوابط القانونية والتقنية لتفتيش النظم المعلوماتية والحواسب الآلية وضبط وسائط التخزين والأجهزة المستخدمة في ارتكاب الجريمة، وذلك لبيان كيفية تحقيق التوازن بين كفالة فاعلية العدالة الجنائية من جهة، وصون الحق في حرمة الحياة الخاصة وحماية البيانات المشروعة من جهة أخرى.

[1]– فلات سمية، حاحا عبد العالي، المرجع السابق، ص 528، 529.

أولا-مفهوم التفتيش الإلكتروني:

استهلالاً للحديث عن ماهية التفتيش الإلكتروني، يقتضي المنهج القانوني العودة أولاً إلى الأصل اللغوي والاصطلاحي لمفهوم التفتيش العام. فمن الناحية القانونية، يُقصد بالتفتيش "البحث عن حقيقة أو شيء مكنون في مستودع السر".

كما يُنظر إليه إجرائياً بصفته أحد تدابير التحقيق التي يباشرها موظف مختص قانوناً، وتستهدف أماكن تتمتع بالحرمة القانونية، وذلك بغرض استقصاء وضبط الأدلة المادية المتعلقة بجناية أو جنحة وقعت بالفعل، سواء لإثبات وقوع الجريمة أو لنسبتها إلى المتهم.

أما على صعيد التشريع الجزائري، فنلاحظ أن المشرع قد أحجم عن وضع تعريف جامع ومانع للتفتيش، تاركاً هذه المهمة للفقه القانوني. ومع ذلك، فقد نظمه إجرائياً باعتباره أحد إجراءات التحقيق الابتدائي بموجب المواد 157.158.159من ق.ا.ج 14-25.

وقد تعززت هذه الحماية من خلال الوثيقة الدستورية، حيث نصت المادة 48 من الدستور الجزائري على كفالة الدولة لحرمة المسكن، مقررةً عدم جواز إجراء أي تفتيش إلا بناءً على مقتضيات القانون، وفي إطار الاحترام التام له، مع اشتراط صدور أمر مكتوب من السلطة القضائية المختصة.[1]

1-ضوابط تنفيذ التفتيش الإلكتروني:

نظراً لما تتميز به الكيانات الافتراضية من سرعة الاختفاء والقدرة على المحو عن بُعد؛ وبناءً على ذلك، يهدف هذا الفرع إلى تسليط الضوء على إجرائي التفتيش والضبط الإلكتروني كآليتين حاسمتين في كشف الحقيقة، حيث نتناول من خلالهما الضوابط القانونية والتقنية لتفتيش النظم المعلوماتية والحواسب الآلية وضبط وسائط التخزين والأجهزة المستخدمة في ارتكاب الجريمة، وذلك لبيان كيفية تحقيق التوازن بين كفالة فاعلية العدالة الجنائية من جهة، وصون الحق في حرمة الحياة الخاصة وحماية البيانات المشروعة من جهة أخرى.

يخضع التفتيش الإلكتروني، بوصفه إجراءً من إجراءات التحقيق والتحري، لمجموعة من الضوابط القانونية التي تنقسم إلى شروط موضوعية وأخرى شكلية.

---

[1]- زعزوعة نجاة، التقاضي الالكتروني كآلية لإنجاح نظام العدالة، أطروحة مقدمة لنيل شهادة دكتوراه ل م د، تخصص قانون قضائي، كلية حقوق والعلوم السياسية، جامعة أبي بكر بلقايد، السنة الجامعية 2021-2022، ص

أ-الشروط الموضوعية لتفتيش النظم المعلوماتية: تتمحور هذه الشروط حول مبررات التفتيش ونطاقه (محل التفتيش)، وذلك على النحو الآتي:

1.1. مبرر (سبب) التفتيش الإلكتروني:

لا يجوز إخضاع أي شخص للتفتيش تعسفياً دون وجود مسوغ قانوني. لذا، يعد توفر "السبب" من أهم الأركان الموضوعية، ويتمثل في ضرورة البحث عن أدلة مادية أو رقمية ضمن تحقيق قائم بالفعل لكشف ملابسات جريمة وقعت، وتوجيه الاتهام بناءً على قرائن واضحة لشخص أو مجموعة من الأشخاص.

2.1. نطاق التفتيش الإلكتروني:

يقصد بمحل التفتيش في الجرائم المعلوماتية كافة عناصر المنظومة الحاسوبية، سواء كانت:

-**مادية:** مثل الأجهزة والوحدات الصلبة.

-**معنوية:** مثل البيانات، البرمجيات المخزنة، وشبكات الاتصال الخاصة. كما يشمل البحث في الأقراص المدمجة والوسائط التكنولوجية المختلفة. وقد فرق المشرع الجزائري في هذا

ب-الشروط الشكلية لتفتيش نظم المعلوماتية:

1.1. إلزامية حضور أطراف معينة ومحددة قانوناً: استلزم المشرع الجزائري لصحة إجراءات تفتيش الأنظمة المعلوماتية استيفاء "قاعدة الحضور" المستندة إلى نص المادة 5 من القانون رقم 09/04. وتقضي هذه القاعدة بضرورة تواجد صاحب المسكن المشتبه في ارتكابه الجريمة أثناء عملية المعاينة والتفتيش، وفي حال استحال حضور الشخص المعني عياناً لأسباب قاهرة، يُستعاض عنه وجوباً بحضور شاهدين لضمان سلامة الإجراء.

2.1. توثيق الإجراءات عبر محضر التفتيش الإلكتروني: يُعرف هذا المحضر بأنه تقرير تقني وتوثيقي يجمل كافة النتائج والاستخلاصات التي أسفرت عنها عملية الفحص الرقمي. وتكمن الأهمية القانونية للمحضر في كونه أداة إثبات جوهرية لما تم ضبطه من أدلة رقمية، ويتعين أن يستوعب بشكل تفصيلي ودقيق جميع الخطوات الإجرائية والتقنية التي اتُّبِعت طيلة مراحل التفتيش.

3.1. إسناد العملية لجهات الخبرة التقنية المتخصصة: نظراً للطبيعة الفنية المعقدة للأدلة الرقمية وسرعة تأثرها، يوجب القانون الجزائري إسناد عملية التفتيش إلى خبراء وفنيين متخصصين في

مجال الحاسوب والأنظمة المعلوماتية، والذين يتمتعون بمستوى عالٍ من التكوين والتدريب المتقدم في هذا الحقل المعرفي لضمان دقة التعامل مع البيانات.

2-الضوابط الإجرائية لتفتيش الأنظمة المعلوماتية في التشريع الجزائري

تأسيسًا على القواعد العامة التي تحكم التفتيش، أقر المشرع الجزائري مجموعة من الضوابط الشكلية الجوهرية لضمان مشروعية تفتيش الأنظمة المعلوماتية، وتتمثل هذه الضوابط فيما يلي:

ا- **الوجوب الإجرائي لحضور ذوي الشأن:** استناداً إلى أحكام المادة 05 من القانون رقم 09/04، يتجلى حرص المشرع على حماية الحرمة الخاصة من خلال اشتراط حضور صاحب المسكن المشتبه فيه لعملية التفتيش كأصل عام. وفي الحالات التي يتعذر فيها ذلك، أوجب القانون حضور شاهدين لضمان شفافية الإجراءات وعدم التعسف، مما يضفي صبغة شرعية على ضبط الأدلة الرقمية.[1]

ب- **التوثيق الفني عبر محضر التحرير:** تتجسد القيمة القانونية لعملية التفتيش في محضر التحرير، وهو وثيقة فنية متخصصة تتجاوز مجرد السرد الإداري لتشمل تلخيصاً دقيقاً للنتائج والاستنتاجات التقنية المستخلصة. ويعد هذا المحضر ركيزة إثباتية لا غنى عنها، حيث يجب أن يستوعب كافة التفاصيل الإجرائية والأدلة المادية والرقمية التي أسفر عنها التفتيش.[2]

ج-**إلزامية الاستعانة بالخبرة التقنية المتخصصة:** نظراً للتعقيد الفني المرتبط بالبيانات الرقمية، اشترط المشرع أن تُنفذ هذه العمليات من قبل خبراء وفنيين مؤهلين في علوم الحاسب والأنظمة المعلوماتية. هذا الشرط يضمن الحفاظ على سلامة الأدلة من التلف أو التعديل، ويحقق الدقة التقنية اللازمة للتعامل مع الفضاء السيبراني.[3]

يعد التفتيش الإلكتروني في المنظومة القانونية الجزائرية إجراءً فنياً مستحدثاً يخضع لذات الضوابط الدستورية التي تحكم التفتيش التقليدي، حيث كفلت المادة 40 من الدستور حماية الحريات الشخصية وحرمة المسكن بجعل التفتيش رهناً بصدور أمر قضائي مكتوب وفي إطار ما يسمح به القانون. وتتجلى

---

[1]- رضا هميسي، نفسه، ص 166.

[2]-المرجع نفسه، ص 169.

3-لينداا بن طالب، التفتيش في الجرائم الإلكترونية، مجلة العلوم القانونية والسياسية، العدد 16، 2017، ص454.

4-رضا هميسي، المرجع السابق، ص100.

خصوصية هذا الإجراء في كونه ينصبُّ على محتوى معلوماتي "لا مادي" عابر للحدود الوطنية وقابل للتلف أو التغيير السريع، مما يخرجه من نطاق البحث المادي الكلاسيكي إلى فضاء "التفتيش الافتراضي" للبيانات. ونظراً لهذا التعقيد التقني، فإن تنفيذ هذا الإجراء يتطلب بالضرورة محققاً متخصصاً يمتلك خبرة فنية عالية ودراية تكنولوجية واسعة لضمان سلامة الأدلة الرقمية واستخلاصها بطرق التحقيق الجنائي الفني المعاصرة.[4]

ثانيا-الضبط الإلكتروني:

1-تعريف ضبط الأدلة:

يُقصد بضبط الأدلة الإجرائي وضع اليد على العناصر أو الأشياء المادية التي تُسهم بفعالية في كشف ملابسات الجريمة المرتكبة والوصول إلى الحقيقة الواقعية. وعلى الرغم من أن الضبط يُمثل الغاية الأساسية والإجراء الملازم لعملية التفتيش في معظم الحالات، إلا أنه قد لا ينحصر فيه كسبب وحيد؛ إذ يمكن أن يتأسس الضبط على مسوغات قانونية أخرى مغايرة للتفتيش، مثل ما تسفر عنه المعاينات الميدانية، أو استنادًا إلى ما يُقدمه المتهم أو الشهود طواعية لمأموري الضبط القضائي.

وبناءً على ذلك، يتجه جانب من الفقه القانوني إلى إخراج الضبط من زمرة إجراءات التحري والتمحيص، وإلحاقه بإجراءات الاستدلال، ولا سيما إذا باشرته السلطات المختصة في الأماكن التي يمنحها القانون حق دخولها دون قيود مشددة، كالمركبات والأشياء التي يُعثر عليها في الطريق العام، أو الحقول المفتوحة، أو خارج نطاق المساكن والحرمات الخاصة.

وفي جوهره الإجرائي، لا يخرج الضبط عن كونه استحواذًا ماديًا وقانونيًا على أي أثر أو شيء يتصل بالجريمة المقترفة، بما يفيد في إماطة اللثام عن الحقيقة وتحديد هوية الجناة، بغض النظر عن طبيعة هذا الشيء المستهدف، سواء كان عقاراً أو منقولاً يُضبط طبقاً للقواعد المقررة قانوناً.[1]

2-ضبط الأشياء المادية للحاسب الآلي:

إنَّ ضبط العناصر المادية للحاسوب وملحقاته، والتي تشمل بنية الجهاز الأساسية ومكوناته الثانوية لا يثير أيَّ إشكالات قانونية؛ إذ ينصرف مفهوم الضبط هنا إلى الأعيان المادية الملموسة، كالوسائط المادية للبرمجيات، والأقراص المدمجة، والأشرطة الممغنطة.

---

[1]- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، مصر، د ط، 2012، ص 74.

وعلى الرغم من غياب الخلاف الفقهي والقانوني حول آلية ضبط المكونات المادية للحاسوب وإخضاعها للإجراءات التقليدية، إلا أن بعض التشريعات الغربية قد أفردت نصوصاً خاصة تنظم عملية ضبط هذه المكونات المادية وتوجيهها إجرائياً، حيث تنقسم هذه التوجهات التشريعية إلى مسارين أساسيين:

أ-الاتجاه الأول: منح هذا الاتجاه التشريعي سلطة اتخاذ التدابير والإجراءات اللازمة لجمع الأدلة الجنائية المرتبطة بالجريمة والتحفظ عليها؛ ومن أمثلتها قانون الإجراءات الجنائية الكندي في المادة 487، وق إ ج ي في المادة 251. وفي سياق متصل، يُمكن القول بصفة عامة إن نظام الضبط في لوكسمبورغ يتسع ليشمل كافة المكونات المادية للحاسوب والأشياء ذات الفائدة في كشف الحقيقة وإظهارها[1].

ب-الاتجاه الثاني: ينص هذا الاتجاه صراحةً في تشريعاته على تنظيم عمليات تفتيش وضبط المكونات المادية للحاسوب بشكل مباشر[1]؛ ومن أبرز المرجعيات القانونية في هذا الصدد: قانون إساءة استخدام الحاسوب الصادر في إنجلترا لسنة 1990، وقانون المنافسة في كندا.

حيث تجسد ذلك في المادة 29/7 من ق إ ك، والتي نصت صراحةً على أن: "عمليات تفتيش وضبط الدفاتر والسجلات العائدة للمؤسسات المالية، تقتصر حصراً على تفتيش المكان المحدود بقصد فحصه ومعاينته، والحصول على نسخة من المواد المدونة، دونما تمييز بين أن تكون تلك السجلات محررة في قالب مكتوب ورقي أو محفوظة في شكل إلكتروني".[2]

ضبط الأشياء المعنوية للحاسب الآلي:

تباينت الرؤى التشريعية والاتجاهات الفقهية المعاصرة حول مدى إمكانية إخضاع الأشياء المعنوية والكيانات المنطقية لإجراء "الضبط"، نظراً لطبيعتها الافتراضية وخلوها من المظهر المادي الملموس عند تجردها من دعامتها المادية الحاضنة لها؛ حيث انقسم الفقه في هذا الصدد إلى اتجاهين رئيسيين:

أ. الاتجاه الأول: ويذهب قطاع من الفقه فيه إلى استحالة التصور القانوني لعملية ضبط الكيانات المنطقية؛ وذلك انتفاءً لعنصر المادية عنها. ويترتب على ذلك بالضرورة عدم إمكانية بسط إجراءات

1-المرجع نفسه .

2-سعيداني نعيم، مرجع سابق، ص159 .

3-بوحزمة نصيرة، المرج السابق، ص.ص 331-332 .

الضبط التقليدية على البيانات المخزنة آلياً؛ كون النصوص الإجرائية الكلاسيكية تشترط صراحةً توافر الطابع المادي الملموس، وهو ما تفتقر إليه هذه البيانات بمجرد انفصالها عن دعامتها المادية[3]. ومِن التشريعات التي تبنت هذا التوجه الموضوعي قانون الإجراءات الجنائية الألماني.

ب. الاتجاه الثاني: ويرى أنصار هذا التوجه عدم وجود أي مانع قانوني أو إجرائي يحول دون إمكانية ضبط المكونات غير المادية كالمعلومات والبيانات الافتراضية؛ مستندين في ذلك إلى أن الغاية التشريعية المتوخاة من وراء التفتيش تتمثل في ضبط كل ما يسهم في كشف الحقيقة والوصول إليها، وهو مفهوم مرن يتسع ليشمل كافة البيانات والمعلومات الرقمية[11]

وقد حظي هذا الاتجاه بتأييد واسع في الفقه والتشريع، لا سيما في بلجيكا، وكذا في كندا بموجب المادة 29/7 منقإ ك، والتي نصت صراحةً على أن:

"تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخة من المواد المكتوبة، يستوي في ذلك أن تكون السجلات مكتوبة أم في شكل إلكتروني".

أفرز هذا التباين الفقهي دافعاً ملحاً لدى المشرع الجنائي في العديد من الدول نحو تطوير المنظومة التشريعية الإجرائية، لتتجاوز القواعد التقليدية للضبط والتفتيش القاصرة على الأشياء المادية المحسوسة، وتمتد لتشمل البيانات المعالجة رقمياً، أو إصدار تشريعات مستحدثة خاصة بالجرائم الإلكترونية تتضمن آليات إجرائية تتلاءم مع طبيعة هذه البيانات؛ وهو ما جسدته المادة 39 من قانون تحقيق الجنايات البلجيكي، المُدرجة بمقتضى القانون الصادر في 23/11/2000، إذ يتسع نطاق الحجز وفقاً لهذا النص ليشمل الأشياء المادية وكذا البيانات المعالجة إلكترونيا[2].

المطلب الثاني: الإجراءات المستحدثة في التحقيق الإلكتروني:

الإجراءات المستحدثة في التحقيق الإلكتروني من أهم الركائز التي اعتمدتها التشريعات الحديثة لمواجهةتعد الجريمة المعلوماتية وتطورها المتسارع .ونظراً لقصور القواعد التقليدية للتفتيش والمعاينة عن ضبط الأدلة الرقمية ذات الطبيعة غير المادية وسريعة التلاشي، فقد كان من الضروري تزويد جهات التحقيق بآليات إجرائية تتناسب مع هذه الخصوصية .وتتنوع هذه التدابير الاستقصائية بين الرصد المستمر للأنشطة الرقمية، واختراق سرية الاتصالات السلكية واللاسلكية وفق ضوابط صارمة، وصولاً إلى التغلغل الافتراضي

[1]بوحزمة نصيرة، المرجع السابق، ص.ص332،331.

[2]– علي عدنان الفيل، اللمرجع السابق، ص58.

في الأوساط الإجرامية؛ وهي الإجراءات التي يمكن حصرها وتفصيل أحكامها القانونية وشروط صحتها من خلال الفروع الثلاثة التالية

لفرع الأول :المراقبة الإلكترونيةا

لفرع الثاني :اعتراض المراسلات والتقاط الصورا

الفرع الثالث :التسرب الإلكتروني.

الفرع الأول: المراقبة الإلكترونية:

تعتبر المراقبة الإلكترونية من أبرز الآليات الإجرائية الحديثة التي استحدثتها التشريعات الجنائية لتعقب الجناة وتجميع الأدلة الرقمية في الفضاء الافتراضي .ويقصد بها فرض رقابة تقنية مستمرة ومتطورة على الأنشطة الرقمية للأشخاص المشتبه فيهم أو الأجهزة الوسيطة المستخدمة في ارتكاب الجريمة .ونظراً لأن هذا الإجراء يمس مباشرة بالحق في الخصوصية وحرمة الحياة الخاصة المحمية دستورياً، فقد أحاطه المشرع بضوابط موضوعية وشكلية صارمة لضمان التوفيق بين فاعلية البحث الجنائي وحماية الحريات الفردية.

وللإحاطة بالمرتكزات القانونية والعملية لهذا الإجراء، سنعمد إلى دراسة هذا الفرع من خلال شقين أساسيين:

أولاً :مفهوم المراقبة الإلكترونية.

ثانياً :حالات تطبيق المراقبة الإلكترونية

أولا- المفهوم الإصطلاحي والتشريعي للمراقبة الإلكترونية:

تعرَّف المراقبة الإلكترونية في السياق الإداري والتنظيمي بأنها عملية إشرافية ديناميكية ومستمرة، تُتيح الكشف الفوري والآني عن أي انحرافات أو تجاوزات تشغيلية. وتتحقق هذه الآلية من خلال التدفق المستمر والمنظم للمعلومات، وإيجاد شبكة ترابط تفاعلية تجمع بين الإدارة، والموظفين، والموردين، والمستهلكين؛ الأمر الذي يعزز كفاءة المؤسسات بمختلف أنواعها عبر تمكينها من تتبع المسارات الإجرائية، ودعم آليات اتخاذ القرار، وتقويم الأخطاء بشكل فوري.

كما تُعرف المراقبة الإلكترونية من منظور تقني بأنها ارتكاز المنظومة الرقابية على توظيف تكنولوجيا الحاسبات الآلية في الممارسات الإجرائية، وذلك بالاعتماد على برمجيات حاسوبية متخصصة ومصممة خصيصاً لهذا الغرض، مما يضمن تحقيق الكفاءة الاقتصادية من خلال توفير الوقت والجهد

والتكلفة المادية، فضلاً عن الوصول إلى المخرجات المستهدفة بأعلى مستويات الدقة وبأقل قدر ممكن من المخاطر.

علاوة على ذلك، تُشير المراقبة الإلكترونية إلى التدابير التي يتخذها القائم بالرقابة مستخدماً الشبكات الاتصالية والتقنيات الرقمية لجمع البيانات والمعلومات المتعلقة بشخص مشتبه فيه، أو تحديد موقع مكاني معين، أو رصد وتتبع موضوع محدد يرتبط بطبيعته بجدول زمني، وذلك بغرض تحقيق مستهدفات أمنية أو أي غايات أخر وبائية مبررة.

وبالرجوع إلى البيئة التشريعية الجزائرية، وتحديداً في ضوء أحكام القانون رقم 04-09 ، يُلاحظ أن المشرع الجزائري لم يضع تعريفاً جامعاً مانعاً لمفهوم "المراقبة الإلكترونية" أو "مراقبة الاتصالات الإلكترونية" بعبارات مباشرة، بل اكتفى بضبط وتحديد مفهوم "الاتصالات الإلكترونية" ذاتها؛ حيث نصت المادة 02 على أنها: "أي تراسل أو استقبال لعلامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.[1]

ثانيا-حالات تطبيق الرقابة الإلكترونية:

حصر المشرّع الجزائري الحالات التي يجوز فيها إعمال وتطبيق آلية الرقابة الإلكترونية بموجب المادة 4 من القانون رقم 04-09، وقد وردت هذه الحالات على سبيل المثال لا الحصر، وتتمثل فيما يلي:

1-الوقاية من الجرائم الإرهابية، التخريبية، أو الجرائم الماسة بأمن الدولة:

أجاز المشرّع للسلطات القضائية المختصة اللجوء إلى خيار المراقبة الإلكترونية كإجراء وقائي واستباقي يُطبّق قبل وقوع الجريمة، ويمتد طوال مرحلة التحضير لها وحتى البدء في تنفيذها. وبناءً على ذلك، بمجرد توفر معلومات أو دلائل لدى السلطات تفيد باحتمالية التخطيط لارتكاب جريمة إرهابية، تخريبية، أو ماسة بأمن الدولة، يثبت لها الحق في تفعيل الرقابة الإلكترونية للحد من وقوعها والسيطرة عليها.

ويتضح هنا أن المشرّع قد منح السلطات القضائية صلاحيات واسعة النطاق لمراقبة وسائل وأجهزة الاتصال أو أنظمة التحكم عن بُعد؛ نظراً للطبيعة الخطيرة لهذه الجرائم التي تُدار وتُنفذ في الغالب عبر

[1] زعزوعة نجاة، المرجع السابق، ص.ص 305-306 .

تقنيات الاتصال الحديثة. وتبرز هذه الآلية كأداة وقائية محورية للحد من مخاطر وجرائم الفساد الإلكتروني.

2-توفر معلومات حول احتمال الاعتداء على منظومة معلوماتية:

تُفعل الرقابة الإلكترونية في حال وجود مؤشرات أو معلومات تفيد باحتمال تعرض المنظومات المعلوماتية لاعتداء يهدد النظام العام، أو الدفاع الوطني، أو مؤسسات الدولة والاقتصاد الوطني. وفي هذه الحالة، يتبنى المشرّع هذه الآلية كأداة وقائية حمائية سابقة على الفعل المادي للجريمة، لحماية طيف واسع من المصالح والهيئات الحيوية، ولا سيما قطاعات.

3-مقتضيات التحريات والتحقيقات القضائية:

يُصار إلى المراقبة الإلكترونية عندما تعترض مسار الأبحاث الجارية عقبات يصعب معها الوصول إلى نتائج ملموسة دون الاستعانة بالتقصي الرقمي. ويُعد هذا الإجراء قضائياً بحتاً لارتباطه الوثيق بمرحلتي البحث والتحري، مما يعني أن اللجوء إليه يكون في مرحلة جمع الاستدلالات أو التحقيق القضائي (أي بعد وقوع الجريمة). غير أن الملاحظ من صياغة أحكام المادة 4 فقرة "ج" من القانون رقم 04-09 أنها لم تُقيد الضبط القضائي بنوع محدد من الجرائم، بل جعلت اللجوء للمراقبة الإلكترونية متاحاً في جميع الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو أي جريمة أخرى مرتبطة بجرائم الفساد المعلوماتي.

4-تنفيذ طلبات المساعدة القضائية الدولية المتبادلة:

تُطبق الرقابة الإلكترونية في سياق مكافحة الجريمة العابرة للحدود؛ حيث يُسمح بإجراء المراقبة الإلكترونية داخل الإقليم الوطني بناءً على طلب مساعدة دولية وارد من دولة أخرى، شريطة أن تنحصر المراقبة في نوع محدد من الجرائم. وعموماً، تُطبق هذه الآلية على كافة الجرائم المنصوص عليها في القانون العام، شريطة وجود صعوبة بالغة في الحصول على الأدلة والنتائج دون تفعيل الرقابة الإلكترونية. ومن هذا المنطلق، تظهر الأهمية البالغة للمساعدة القانونية والقضائية، وضرورة تفعيل قنوات التعاون البيني بين الدول لتبادل التحريات والمراقبات والإجراءات القضائية بأعلى كفاءة ممكنة.[1]

1- المادة 4 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009، المتضمن القوا عد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 16 شعبان عام 1430 الموافق لـ 7 أوت سنة 2009، ص 5

الفرع الثالني: اعتراض المراسلات وإلتقاط الصور:

يمثل إجراء اعتراض المراسلات والتقاط الصور أحد أدق وأخطر إجراءات التحقيق الإلكتروني المستحدثة، بالنظر إلى ملامسته المباشرة لسرية المراسلات وحرمة الحياة الخاصة للمواطنين المصونة دستورياً .ولما كانت وسائل الاتصال الحديثة قد تحولت إلى قنوات أساسية للتخطيط للأنشطة الإجرامية وتنفيذها، فقد أضحى من الضروري تمكين جهات التحقيق- وفق تفويض قضائي صارم -من اختراق هذه السرية لضبط الأدلة الرقمية قبل محوها .وينطوي هذا الإجراء على شقين متكاملين؛ أحدهما يتعامل مع المحتوى المتدفق عبر شبكات الاتصال، والآخر يوثق المظاهر المادية للجريمة عبر الوسائط البصرية.

وبناءً عليه، سنقسم دراسة هذا الفرع إلى محورين رئيسيين على النحو التالي

أولاً :اعتراض المراسلات الإلكترونية

ثانياً :التقاط الصور وتوثيقها.

أولا-اعتراض المراسلات:

1-تعريف اعتراض المراسلات

يُقصد باعتراض المراسلات ذلك الإجراء التحقيقي القائم على التتبع السري والمستمر للاتصالات الخاصة بالشخص المشتبه فيه، سواء تم ذلك قبيل ارتكاب السلوك الإجرامي أو بالتزامن معه أو بعد وقوعه، وذلك بهدف ضبطه في حالة تلبس.

وقد ذهب الفقه القانوني، ومثاله الأستاذ "عبد الرحمن خلفي"، إلى تعريف هذه الآلية بأنها:

"عملية رقابة سرية تنصب على المراسلات السلكية واللاسلكية، وتندرج ضمن أطر البحث والتحري عن الجرائم، مستهدفةً جمع الأدلة والاستدلالات والمعلومات المتعلقة بالأشخاص المشتبه في مساهمتهم أو ارتكابهم للفعل الجرمي".[1]

وبناءً عليه، يمكن تصنيف هذا الإجراء كآلية تحقيقية جوهرية تُباشر بشكل خفي، وتنطوي بطبيعتها على مساس بسرية المحادثات الخاصة. ويصدر هذا الإجراء بأمر من السلطة القضائية المختصة وفقاً للأشكال والأوضاع التي حددها القانون، بغرض تحصيل دليل غير مادي (معنوي) يثبت الجريمة. كما

[1] عبد الرحمان خلفي، مرجع سابق ، ص102 .

يشمل الاعتراض في أحد جوانبه التنصت واستراق السمع للأحاديث الشخصية والمكالمات الهاتفية دون علم أو موافقة أطرافها، وذلك بالاستعانة بأجهزة تقنية وإلكترونية حديثة.[1]

بالرجوع إلى موقف المشرع الجزائري، نجد أنه نظم أحكام اعتراض المراسلات بموجب المادة 114 من قانون الإجراءات الجزائية ق.إ.ج الجديد 14-25، حيث حدد من خلالها طبيعة المراسلات الخاضعة للرقابة، وقسمها إلى:

مراسلات سلكية ولاسلكية: وتشمل الهاتف الثابت، الفاكس، والاتصالات اللاسلكية.

وسائل التقنية الحديثة: وتشمل الهاتف النقال، شبكة الإنترنت، البريد الإلكتروني، وغيرها من الوسائط التكنولوجية المعاصرة.

2-النطاق التشريعي لوسائل الاتصال المستهدفة

وفي المقابل، تعمد المشرع الجزائري استبعاد الوسائل البريدية التقليدية (كالخطابات والمراسلات الورقية المكتوبة التي تُنقل عبر البريد) من نطاق هذا الإجراء؛ وذلك رغبةً منه في تكريس الضمانات الدستورية المتعلقة بحرية وسرية المراسلات المكفولة للأفراد.[2]

3-خصائص أسلوب اعتراض المراسلات

يتسم إجراء اعتراض المراسلات بمجموعة من الخصائص البنيوية التي تميزه، ويمكن إيجازها في النقاط التالية:

أ- **السرية المطلقة وعدم العلم:** يُباشر هذا الإجراء خلسةً ودون الحصول على رضا أو علم الشخص المعني (المشتبه فيه). وتعد هذه الخاصية الركيزة الأساسية للإجراء؛ إذ إن علم صاحب الشأن بالرقابة ينفي عن الآلية خاصية "الاعتراض" ويفقدها قيمتها الجنائية.

ب- المساس الاستثنائي بالحق في السرية: يُصنف الاعتراض كإجراء ماسّ بالحق في السرية، وهو ما يمثل تقييداً لحق إنساني أصيل. وعلى الرغم من أن المادة 47 من الدستور تنص صراحةً على حماية حرمة الحياة الخاصة وضمان سرية المراسلات والاتصالات الخاصة دون قيود، إلا أن المشرع

---

[1]-زعزوعة نجاة، مرجع سابق، ص300 .

[2] المادة 114 من القانون رقم 25-14 المؤرخ في 9 صفر عام 1447 الموافق لـ 3 أوت سنة 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 54، الصادرة بتاريخ 19 صفر عام 1447 الموافق لـ 13 أوت سنة 2025.

وضع هذا الاستثناء كضرورة فرضها حسن سير التحريات والتحقيقات الجنائية، والغاية الأسمى هي الحفاظ على النظام العام والأمن العام.

ج-استهداف الدليل المعنوي: ترمي عملية الاعتراض إلى تحصيل أدلة جنائية ذات طبيعة غير مادية؛ فبينما تُعنى عملية التنصت على الأحاديث الهاتفية بالتقاط وتوثيق

الأدلة المعنوية، فإن الهدف النهائي من هذا الاعتراض هو تثبيت هذه الأدلة المعنوية

وتحويلها إلى قرائن مادية دامغة تُسهم في تأكيد اتهام المشتبه فيه.[1]

ثانيا-التقاط صور:

يعتمد هذا الإجراء الجنائي على توظيف الكاميرات الرقمية أو الوسائط التقنية المخصصة لتوثيق وتسجيل البيانات المرئية والصوتية. ويستهدف هذا التدبير رصد الوضعية المادية التي يتواجد عليها الشخص المشتبه فيه وقت مباشرة عملية التصوير، وذلك بغرض استخلاص مادة إثباتية قانونية تُعتمد كدليل قطعي في المسار القضائي.

إن استخدام تقنيات التصوير والمراقبة البصرية بات من الممارسات الإجرائية المألوفة والمستقرة، ولا سيما داخل المؤسسات المصرفية والمالية كالبنوك؛ حيث يُعزى هذا التوسع الإجرائي إلى التزايد الملحوظ في معدلات الجريمة المعاصرة ونوعيتها في الوقت الراهن.

وتماشيًا مع الطفرة التكنولوجية والتقدم العلمي المتسارع، أضحى بمقدور الأجهزة الأمنية الاستعانة بآليات ووسائل تقنية حديثة ومبتكرة تتيح التقاط الصور بجودة ميز وتحديد عالية. ومن أبرز هذه الوسائل التقنية، الأنظمة التي تعمل بالأشعة تحت الحمراء، والمنوط بها توثيق صور الأشخاص بدقة ووضوح عالٍ في الأوقات الليلية وتحت جنح الظلام الدامس، حيث تتميز هذه الأجهزة بقدرتها العالية على نقل الذبذبات الصوتية والمرئية بأسلوب خفي ومستتر تمامًا للحيلولة دون إثارة الانتباه.

أما بالرجوع إلى موقف المشرع الجزائري، فقد نظّم وعرّف هذه الآلية الإجرائية المتمثلة في عمليات التصوير والتقاط الصور الفورية، وضبط أحكامها القانونية تفصيلاً بموجب نص المادة 118 ق.ا.ج.[2]

1-الضوابط الإجرائية الخاصة بها:

1- زعزوعة نجاة، المرجع نفسه، ص301 .

2-المادة 118 من قانون 14-25، المتضمن قانون الإجراءات الجزائية، مرجع سابق.

بيد أن إعمال هذه الترتيبات التقنية والمراقبة البصرية لا يمكن وضعه حيز التنفيذ إلا بناءً على إذن قضائي مسبق وصريح يصدر عن وكيل الجمهورية أو قاضي التحقيق المختص، وتُباشر هذه العمليات تحت رقابتهما المباشرة؛ وذلك استنادًا إلى الأحكام الإلزامية التي قررتها المادة 116 من ق.ا.ج

كما اشترط المشرع أن يصدر هذا الإذن في قالب مكتوب ومحرر رسميًا، محددًا مدته الزمنية بحد أقصى لا يتجاوز أربعة 04 أشهر، مع قابليتها للتجديد وفقًا لمقتضيات التحقيق ومصلحته.[1]

2-الإجراءات المتبعة لمباشرتها:

يهدف إجراء اعتراض المراسلات المكتوبة والالكترونية، وتسجيل الأصوات المحادثة، وتقصي الصور والتقاطها، إلى غاية إجرائية محددة، تتمثل في استيقاف الأدلة الجنائية الصالحة والمنتجة في كشف الحقيقة القضائية، والتي تساهم بشكل جوهري في بناء العقيدة القضائية سواء لإدانة المتهم أو تبرئته من الجرم المنسوب إليه.

وبناءً على ذلك، وتحقيقًا للمشروعية الإجرائية لهذا الأسلوب التحقيقي، استلزم القانون توافر جملة من التدابير والشكليات القانونية الواجبة الاتباع عند مباشرة العمل الميداني، لضمان عدم بطلان الدليل المستمد منها وصون مشروعيته أمام جهات الحكم.

وبالرجوع إلى أحكام المادة 117 من ق.ا.ج، يتبين أن لوكيل الجمهورية أو قاضي التحقيق المختص—بحسب الأحوال—سلطة تسخير أي عون مؤهل يتبع لمصلحة أو وحدة أو هيئة عمومية أو خاصة، تكون منوطة قانونًا بقطاع المواصلات السلكية واللاسلكية، أو متخصصة في الجوانب التقنية،[2] وذلك بهدف التكفل بالجانب الفني والتكنولوجي المرتبط بالعمليات المنصوص عليها في المادة 114 ق.ا.ج على أن يُحرر فور الانتهاء من هذه الأعمال التقنية محضر رسمي يثبت الواقعة.[3]

أ-تسخير الأعوان المؤهلين لدى مصلحة عمومية أو خاصة:

خوّل المشرع الجزائري لكل من وكيل الجمهورية وقاضي التحقيق مكنة قانونية تتيح لهما ندب وتسخير أي عون فني مؤهل قانونًا يعمل لدى جهة أو هيئة أو مصلحة سواء كانت ذات طابع عمومي أو خاص متخصصة في إدارة وسائل المواصلات السلكية واللاسلكية، وذلك ليتولى المهام الفنية والتقنية الدقيقة المصاحبة لعمليات المراقبة والاعتراض الواردة في المادة 114 السالفة الذكر.

---

[1] المادة 116 من المرجع نفسه.

[2] المادة 117، المرجع نفسه

[3] المادة 114، المرجع نفسه

وفي المقابل، يقع على عاتق ضابط الشرطة القضائية المأذون له بموجب الأمر القضائي التزام قانوني صارم بمباشرة وتنفيذ تلك الإجراءات والتدابير بنفسه وبصفة شخصية؛ إذ يمتنع عليه تمامًا تفويض هذه المكنة أو إعادة نقلها إلى الغير، وإنما يقتصر حقه فقط على إمكانية ندب أحد رجال الضبطية القضائية التابعين له، شريطة أن يتضمن الإذن القضائي الصادر له نصًا صريحًا يجيز هذا الندب.

أما فيما يتعلق بالفئات المساعدة من الخبراء والتقنيين والفنيين المؤهلين المذكورين سلفًا، فلا ينطبق عليهم نظام الندب القضائي بمفهومه الضبطي، بل يتم الاستعانة بخدماتهم الفنية التخصصية مع وجوب أداء مهامهم ومباشرة أعمالهم تحت الإشراف والرقابة المباشرة لضابط الشرطة القضائية المسؤول عن الملف.[1]

ب- وضع الترتيبات التقنية اللازمة

كما أوجب المشرع ضرورة المحافظة المطلقة على الطابع السري والسرية التامة للتدابير المتخذة، وذلك تماشيًا مع القواعد العامة المقررة بموجب نص المادة 19من ق.ا.ج، والتي تفرض التزامًا صارمًا بسرية التحري والتحقيق، والتحلي بكتمان السر المهني من قِبل جميع الأشخاص والشركاء المساهمين في تنفيذ هذه الإجراءات.

بموجب أحكام ال مادة114فقرة ر04 من ق.ا.ج، يُمنح لضابط الشرطة القضائية المندوب صلاحية مباشرة إجراءات الترصد الإلكتروني وتنفيذ قرار الندب بالوسائل والكيفية التقنية التي يراها ملائمة ومناسبة لاستظهار الأدلة والوصول إلى الحقيقة المعرفية، وذلك كله في إطار الحدود والضوابط المسموح بها قانونًا.[2]

فإذا انصب الإذن القضائي الصادر على مراقبة المحادثات الهاتفية للمشتبه فيه وتسجيلها، يتعين على ضابط الشرطة القضائية اتخاذ التدابير الفنية والوسائل اللوجستية اللازمة التي تمكنه من عملية التنصت والتوثيق الصوتي بدقة.

ومن بين الأجهزة والوسائل التقنية المعاصرة المستخدمة في هذا الصدد، "الميكروفون الليزري"، وهو جهاز دقيق يُستعمل لغرض التنصت والتقاط المكالمات والأنشطة الصوتية الجارية داخل الغرف والأماكن

---

[1] المادة 19فقرة 4 من القانون نفسه.

[2] المادة 114 فقرة 4 من القانون نفسه.

المغلقة، وذلك عن طريق جهاز إرسال TX؛ حيث تتيح هذه التقنية الولوج إلى الخط الهاتفي المستهدف عن بُعد ودون إثارة أي شبهة أو شعور من الطرف الخاضع للمراقبة.

كما يشمل ذلك استخدام كاميرات فيديو متطورة متناهية الصغر، والتي قد تكون في حجم "حبة العدس" تسهيلاً لإخفائها ونقلها باليد.[1]

3- تحرير المحاضر:

يلتزم ضابط الشرطة القضائية، فور فراغه من إنجاز المهام والتحريات الفنية المنوطة به، بتحرير محضر رسمي يثبت بموجبه تفصيليًا كافة الإجراءات والخطوات التي تم اتخاذها؛ وعلى الرغم من أن القانون لم يشترط شكلية خاصة ومحددة لتدبيج هذا المحضر في شقه الموضوعي، إلا أنه استلزم وجوب توافر الشروط الشكلية العامة المقررة للمحاضر القضائية، ومنها ذكر اسم المحرر، صفتة، وتوقيعه، مع بيان دقيق لتاريخ وساعة بداية العمليات الاستقصائية وساعة انتهائها، وذلك كله وفقًا للقواعد العامة المقررة في المادة 118 من ق.ا ج.[2]

4- نسخ وترجمة التسجيلات:

بالرجوع إلى أحكام المادة119 من ق.ا.ج، يتبين أنها قضت بإلزام ضابط الشرطة القضائية المأذون له، أو المندوب لهذا الغرض، بأن يقوم بوصف أو تفريغ ونسخ المحادثات الصوتية، أو المراسلات المستلمة، أو الصور الملتقطة ذات الفائدة والإنتاجية في إظهار الحقيقة القضائية، وتوثيقها بداخل محضر رسمي مستقل يُودع مباشرةً ضمن ملف القضية.

وبناءً على المقتضيات السابقة، فقد أوجب المشرع الجزائري نقل وتدوين الوقائع والمعاينات التي تمت ملاحظتها وتفريغها بلغة بسيطة، وبأسلوب صياغة واضح ودقيق يخلو من اللبس والغموض. كما أوجب القانون القيام بترجمة كافة المحادثات والاتصالات التي تمت بلغات أجنبية غير الوطنية، والاستعانة في سبيل ذلك بمترجم مؤهل ومحلف يُسخر خصيصًا لملء هذا الغرض الإجرائي.[3]

5- تحرير التسجيلات:

---

[1] زعزوعة نجاة، مرجع سابق، ص304.

[2] المادة118، مرجع سابق.

[3] المادة 119، المرجع نفسه.

يُلاحظ أن المشرع الجزائري لم يتناول بنص صريح ومباشر مصير الأشرطة والتسجيلات الأصلية بعد الفراغ من تحقيق الغرض الإجرائي منها، مما أوجد نوعاً من الفراغ التشريعي؛ إلا أن الفقه القانوني، وفي مقام مواجهته وتغطيته لهذا النقص، استقر على وجوب الانعطاف والرجوع إلى أحكام وقواعد قانون الإجراءات الجزائية الفرنسي. وبوجه دقيق، تم الاستناد إلى نص المادة 706 الفقرة 102 التي تشير إلى أن تلك الدعامات والوسائط التقنية الأصلية يجب أن توضع في حرز مغلق ومختوم رسميًا، على أن يتم إتلافها لاحقاً بناءً على أمر صادر عن المدعي العام.

الفرع الثالث: التسرب الإلكتروني:

يعد التسرب الإلكتروني المعروف قانوناً بالتغلغل الافتراضي أو المجهول من أكثر آليات التحقيق الإلكتروني حداثة وجرأة في مواجهة الجريمة المنظمة وعبر الوطنية، خاصة تلك التي تتخذ من" الإنترنت المظلم Dark Web "والمنصات المشفرة ملاذاً لها .وتكمن خصوصية هذا الإجراء في خروجه عن النمط التقليدي للتحقيق؛ حيث يتطلب دخول رجل الضبط القضائي– أو العميل المختص –إلى البيئة الرقمية للجناة بهوية مستعارة للتغلغل داخل شبكاتهم وتفكيكها من الداخل .ونظراً لطبيعة هذا الإجراء التي تقترب من حدود الخداع والمشروعية، فقد وضع الفقه والتشريع له أُطراً بالغة الدقة لتنظيمه.

وللوقوف على الأبعاد القانونية لهذا الإجراء المستحدث، سنتناول هذا الفرع من خلال محورين رئيسيين

أولاً :تعريف التسرب الإلكتروني مفهومه وطبيعته القانونية

ثانياً :شروط صحة التسرب الإلكتروني وضوابطه.

أولا–تعريف التسرب الإلكتروني:

يتحقق مفهوم التسرب الإلكتروني من خلال قيام ضابط شرطة قضائية مؤهل ومختص باختراق والولوج إلى منظومة معلوماتية، أو نظام اتصالات إلكتروني، أو منصة رقمية؛ بهدف وضع مشتبه فيهم تحت المراقبة نتيجة لضلوعهم في ارتكاب جريمة معلوماتية.

ويُقصد به إجرائياً عملية الدخول الفني إلى البيانات والأنظمة الرقمية للكشف عن هوية الأشخاص المشتبه في ارتكابهم لجرائم محددة.

وقد أولى المشرع عناية خاصة بضبط هذا المفهوم وتأطيره قانوناً، وتحديداً في نص المادة 121 من ق.ا.ج ، حيث نصت على ما يلي: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية

أو جنحة بإيهامهم أنه فاعل مهم أو شريك لهم، ومؤدى ذلك أن المشرع يعتبر هذا الإجراء آلية من آليات التحري الخاصة؛ إذ يتمثل التسرب في الدور الإجرائي الذي يباشره ضابط الشرطة القضائية للتوغل داخل الجماعات الإجرامية واختراقها بعد كسب ثقة أعضائها.[1]

وتأسيساً على ما تقدم، يُصنف التسرب الإلكتروني كعملية دقيقة وحساسة للغاية، تطلب تفعيلها الامتثال لمجموعة صرمة من القواعد والشروط القانونية. فهو يمثل إجراءً سرياً يهدف إلى اختراق الشبكات الإجرامية عن طريق التخفي في صورة شريك يسعى للحصول على ميزة أو خدمة من الضحية، أو عبر

تقمص هوية إجرامية تعرض خدماتها لتنفيذ الجريمة دون وجود ضحية حقيقية على أرض الواقع. وفي هذا الصدد، يمنح القانون تفويضاً لضابط أو عون الشرطة القضائية لاستعمال هوية مستعارة، والقيام عند الضرورة القصوى بالأعمال التالية: "اقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد وأموال أو منتجات أو وثائق ومعلومات متحصل عليها من ارتكاب الجرائم، أو استعمالها، أو وضع الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل والتخزين والاتصال تحت تصرف مرتكبي الجرائم". ومن خلال هذه الصلاحيات، يتضح أن المشرع يسعى لضمان نجاح عملية التسرب الإلكتروني.

ولما كان النجاح في إتمام هذه المهمة يتوقف بالضرورة على كسب ثقة الجماعة الإجرامية[2]، فقد أتاح القانون للمنفذ ارتكاب بعض التجاوزات القانونية استثناءً بغرض تحقيق هذا الهدف المعين.

ثانيا–الشروط الموضوعية والشكلية لإتمام التسرب الإلكتروني:

1–الشروط الموضوعية لإتمام التسرب الإلكتروني:

أ–دوافع اللجوء لعملية التسرب:

---

1 المادة121، المرج نفسه.

[2] مناصرة يوسف، الدليل الالكتروني في القانون الجزاءي، دار الخلدونية، الجزائر، 2021، ص 478

تكمن الغاية الأساسية والمصلحة العليا من اعتماد آلية التسرب في الكشف عن الحقيقة وإماطة اللثام عن الجرائم المعقدة[1]؛ وهو ما كرسّه المشرع الجزائري في نص المادة 120بموجب العبارة القانونية:

"عندما تقتضي ضرورات التحري أو التحقيق". وبناءً عليه، يؤول الاختصاص التقديري في تقييم مدى نجاعة وضرورة إقرار هذه العملية إلى كل من السيد وكيل الجمهورية وقاضي التحقيق المختصين قانوناً.[2]

ب-سرية عملية التسرب الإلكتروني:

يُعد عنصر السرية شرطاً موضوعياً جوهرياً يتوقف عليه نجاح عملية الاختراق السيبراني برمتها، وذ ظراً لأهميتها البالغة، حظر المشرع في المادة125 إشهار أو كشف الهوية الحقيقية لضباط أو أعوان الشر طة القضائية الذين تولوا تنفيذ هذه المهام تحت هويات مستعارة في أي مرحلة من مراحل الخصومة الجنائ ية. كما فرض المشرع الجزاءات جنائية صارمة على كل من يخالف هذا الحظر، حيث نص

على عقوبة الحبس التي تتراوح بين 02 سنتين إلى 10 سنوات وغرامة ما بين 200.000 و500. 000 في حال الكشف عن الهوية الحقيقية للمتسربين. [3]

- الجرائم المقصودة بعملية التسرب:

يُقصد بهذا الشرط حصر نطاق تطبيق آلية التسرب في طائفة محددة من الجرائم النوعية والخطيرة التي تستوجب اللجوء إلى هذا الأسلوب الاستثنائي للبحث والتحري. وقد حددت المادة114 من قانون الإجراءات الجزائية السالفة الذكر هذه الجرائم على سبيل الحصر في الآتي:

- ✓ جرائم المخدرات.
- ✓ الجريمة المنظمة العابرة للحدود الوطنية.
- ✓ الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- ✓ جرائم تبييض الأموال.
- ✓ جرائم الإرهاب.
- ✓ الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد.

---

[1] بن عمارة فاتن نور الايمان، التحقيق والتحري في الجرائم الالكترونية، اطروحة ماستر، كلية الحقوق، جامعة عبد الحميد بن باديس، 2023-2023، ص68.

[2] عزوعة نجاة، مرجع سابق، ص304.

[3] المادة 125 من القانون نفسه.

- ✓ القتل العمدي والمؤثرات العقلية.
- ✓ جرائم الاختطاف الاشخاص والاتجار بالبشر.
- ✓ جراءم تهريب المهاجرين.[1]

2- الشروط الشكلية لإتمام عملية التسرب الإلكتروني

أ- تحرير تقرير مسبق من طرف ضباط الشرطة القضائية:

يلتزم ضابط الشرطة القضائية المكلف بإعداد تقرير مفصل ودقيق قبل الشروع الفعلي في عملية الاختراق، يتم رفعه إلى وكيل الجمهورية، وذلك تكريساً للمبدأ العام الناظم لعمل الشرطة القضائية والمحكوم بنص المادة 27 من قانون الإجراءات الجزائية الجديد 14-25.[2]

وفي ذات السياق، قضت المادة122 ق.إ.ج الجديد 14-25 بأنه: "يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريراً يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي تعرض للخطر أمن الضابط أو العون المتسرب وكذا الأشخاص المسخرين طبقاً للمادة123 أدناه".

ومؤدى ذلك، يتوجب على الضابط صياغة تقرير كتابي يستوعب كافة التفاصيل المحيطة بالعملية، مع تدوين أكبر قدر ممكن من المعطيات المتعلقة بالجريمة المرتكبة، وتقديمه إلى وكيل الجمهورية أو قاضي التحقيق مشفوعاً بطلب رسمي لاستصدار الإذن بمباشرة هذا الإجراء[3]

ب- صدور إذن قضائي بمباشرة الإجراء:

بالنظر إلى الخطورة البالغة التي يكتسيها هذا الإجراء، وضماناً للحقوق والحريات اللصيقة بالمتهم، قيد المشرع الجزائري صلاحيات ضابط الشرطة القضائية بضرورة الحصول على إذن كتابي مسبق صادر عن وكيل الجمهورية أو قاضي التحقيق بحسب الأحوال. ويُعد هذا الإذن شرطاً جوهرياً يبطل الإجراء في حال تخلفه تحت طائلة البطلان[4]. وقد أوجب المشرع الجزائري في المادة124 من قانون الإجراءات الجزائية تضمن هذا الإذن لمجموعة من البيانات الإلزامية وهي:

- ✓ الجريمة محل البحث والتي تبرر اللجوء إلى هذا الإجراء الاستثنائي.
- ✓ الهوية المستعارة لضابط الشرطة القضائية الذي سيتولى تنفيذ العملية.

---

[1] المادة 114 ، المرجع نفسه .

[2] المادة 27 ، المرجع نفسه .

[3] مناصرة يوسف، مرجع سابق، ص478-479 .

[4] المادة 124 ، مرجع سابق .

- ✓ تبيان الأسباب والدواعي القانونية والواقعية المبررة لطلب هذا الإجراء.
- ✓ يجب أن يكون الإذن مكتوباً.

ج- التسرب الإلكتروني مكتوب محدد المدة:

يجب أن يحدد الإذن القضائي الصادر بصفة مكتوبة النطاق الزمني لعملية التسرب بشكل دقيق؛ حيث ضبط المشرع في المادة 124 ق.إ. ج المدة القصوى لعملية التسرب بما لا يتجاوز أربعة04 أشهر.

ومع ذلك، يجوز تجديد هذه العملية وفقاً لمقتضيات التحري أو التحقيق، وبما يتوافق مع الشروط الشكلية والزمنية ذاتها، أي أن مدة التمديد تخضع لذات السقف الزمني المقدر بـ 4 أشهر إضافية إذا اقتضت الضرورة ذلك. كما خول المشرع لوكيل الجمهورية أو قاضي التحقيق الذي أصدر الإذن سلطة الأمر بوقف عملية التسرب في أي وقت إذا استدعت ظروف العملية ذلك.[1]

د-معاملة الضابط المتسرب كشاهد:

قضت المادة 127 ق.إ. ج على أنه: "يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب مسؤوليته دون سواه بوصفه شاهداً عن العملية"، ومفاد ذلك، يجوز لجهة المحكمة في مرحلة المحاكمة استدعاء واعتماد ضابط الشرطة القضائية المسؤول عن العملية بصفته شاهداً في القضية للادلاء بأقواله حول الوقائع المعاينة.[2]

هـ-اشتراط الخبرة في ضابط الشرطة المتسرب:

بغية الحصول على الدليل الرقمي بشكل مشروع وفني سليم، يتطلب الأمر في ضابط الشرطة المتسرب توافر خبرة عالية تمكنه من التعامل الاحترافي مع المنظومات، والمنصات، والأنظمة الإلكترونية؛ حيث يقوم بصياغة وبناء شخصية مستعارة تتيح له اختراق مسرح الاشتباه. وتعد هذه الخبرة الفنية والمعرفية بالتقنيات الحديثة ركيزة أساسية لضمان نجاح عملية التسرب وتحقيق أهدافها.[3]

المطلب الثالث: الأساليب الدولية للتحقيق الجنائي في الجريمة الإلكترونية

---

[1] المادة127 من المرجع نفسه .

[2] بن عمارة فاتن نور الايمان، مرجع سابق، ص71 .

[3] بن عمارة فاتن نور الايمان، مرجع سابق، ص71.

بناءً على ما تقدم، سيتم تقسيم هذا المطلب لتسليط الضوء على هذه الأبعاد وفق الخطة التالي الفرع الأول التعاون الأمني الدولي في مجال الجرائم الإلكترونية .الفرع الثاني التعاون القضائي الدولي في الجرائم الإلكترونية.

الفرع الأول: التعاون الأمني الدولي

يشكل التعاون الأمني الدولي خط الدفاع الأول والآلية الأكثر مرونة وسرعة في مواجهة الجريمة الإلكترونية العابرة للحدود .فبالنظر إلى الطبيعة الافتراضية للأدلة الرقمية وسرعة تعرضها للتعديل أو المحو، فإن الإجراءات القضائية التقليدية قد تتسم بالبطء الذي يخدم مصلحة الجناة؛ الأمر الذي استلزم إيجاد قنوات اتصال أمنية مباشرة وفورية بين الأجهزة الشرطية عبر العالم .(Police–to–Police) ويتيح هذا التنسيق الميداني تبادل المعلومات الاستخباراتية وتقفي أثر الجناة رقمياً في الوقت الحقيقي قبل اتخاذ الإجراءات القضائية الرسمية.

وللإحاطة الشاملة بأبعاد هذا التعاون وأدواته، سنعمد إلى دراسة هذا الفرع من خلال ثلاثة محاور متتالية:

- أولاً :تعريف التعاون الأمني الدولي في الجريمة الإلكترونية
- ثانياً :أهمية التعاون الأمني الدولي في ضبط الأدلة الرقمية
- ثالثاً :صور التعاون الأمني الدولي وآلياته

أولا: تعريف التعاون الأمني الدولي

التعاون الأمني الدولي يُعدّ مصطلح" التعاون الأمني الدولي "من المفاهيم المعقدة التي يَعصُب إخضاع ها لتعريف جامع مانع يحيط بكافة أبعادها؛ ويُعزى هذا الاستعصاء المفاهيمي إلى حزمة من الاعتبارات، أبر زها :الاتساع المطرد في النطاق الجغرافي والموضوعي لهذا التعاون، وتعدّد الصور والأنماط الإجرائية التي ي تجسد من خلالها، فضلاً عن عدم إمكانية حصر أو تقييد الوسائل والآليات المستحدثة والمستجدة التي تمنح هذا التعاون طابعاً ديناميكياً متغيراً ومتطوراً بصفة مستمرة .يضاف إلى ذلك الارتباط الوثيق والجدلي بين فكر ةالتعاون ومفهوم" مصالح الأمن"، والذي يشهد بدوره تباينات وإشكاليات عديدة عند محاولة ضبطه وتحديده

وحيث إن الإرادة الدولية لم تتوافق بعد على صياغة تعريف موحد ومقبول عالمياً للتعاون الأمني بالرغم م ن محوريته وأهميته؛ فإن ذلك يرجع أساساً إلى الطفرات والتحولات المتلاحقة التي طرأت على الظاهرة الأمن ية برمتها بفعل التغيرات الدولية المتسارعة .وتتداخل في هذا السياق عوامل بنيوية متعددة، من بينها :طبيعة

المقاربات والمقارنات الأمنية المعتمدة في حقل الدراسات الأمنية، وتشابك هذا المفهوم مع مصفوفة واسع ة من المفاهيم والمصطلحات المجاورة، وهو ما يفسر غياب الإجماع والاتساق بين الباحثي والدارسين حول و ضع تصور محدد ودقيق لموضوع الأمن وعند تتبّع التعاون الأمني الدولي في أبعاده ومفهومه الواسع، نج د أنه يمتد ليشمل حقولاً ومجالات تشريعية وإجرائية متباينة؛ كالتعاون في الشق الشرطي، والتعاون في المجا ل القانوني والقضائي .ومردّ هذا الشمول هو أن استدامة الأمن وإنفاذه بفاعلية يتطلبان بالضرورة تضافر الجه ود وتكامل الإجراءات والتدابير عبر هذه القطاعات المجتمعة.

ثانيا– أهمية التعاون الأمني الدولي :

تتجلى الأهمية البالغة للتعاون الأمني الدولي، لاسيما في شقها المتعلق بمكافحة الجريمة الإلكترونية بالنظر إلى الطبيعة البنيوية والخصائص الذاتية التي تنفرد بها هذه الجرائم .إذ تُصنّف الجرائم الإلكترونية كواحدة من أخطر النظم الإجرائية المستحدثة، نظراً لما يترتب عليها من تداعيات وخيمة وأضرار جسيمة تمس استقرار ومصالح المجتمع الدولي والوطني على حد سواء.ويُمثّل التعاون الأمني الدولي الركيزة الأساسية والمحور الاستراتيجي الذي تُبنى عليه مقاربات المواجهة الفعّالة للظاهرة الإجرامية الإلكترونية؛ إذ بدون هذا التعاون، سيجد مرتكب الجريمة نفسه محصناً بسياج قانوني يحميه من الملاحقة والمسؤولية الجنائية، وخاصة في الحالات التي تُرتكب فيها الجريمة من خارج الحدود الإقليمية للدولة المتضررة، أو عند فرار الجاني إلى ملاذات دولية أخرى بعد تنفيذ نشاطه الإجرامي .ومن ثم، فإن تفعيل آليات التعاون الدولي يُجهض سلفاً أي حسابات أو تفكير مليّ من قِبل الجناة حول إمكانية الإفلات من العقاب، ويؤكد بما لا يدع مجالاً للشك أن إحكام السيطرة على المجرمين وتتبّعهم أمر حتمي، أياً كانت بيئاتهم الرقمية، ومواقعهم الجغرافية، أو جنسياتهم[1]

وتبرز الأهمية القصوى لهذا النمط من التعاون في التنسيق المشترك بين أجهزة الشرطة الجنائية المتخصصة في مكافحة الجرائم الإلكترونية، كونه يمثل إحدى الأدوات الحيوية لتقويض هذه الجرائم أو الحد من آثارها التدميرية .وتؤكد التحقيقات الجنائية في البيئة الرقمية بصفة عامة، والجرائم الإلكترونية بصفة خاصة، على محورية التعاون الأمني المشترك؛ نظراً لاستحالة استفراد دولة بمفردها بملاحقة وقمع هذا النوع من الإجرام العابر للحدود .فجهاز الأمن الداخلي لأي دولة لا يمكنه، في إطار سيادته الإقليمية الضيقة، تتبع الجناة الدوليين أو ضبطهم وتوقيفهم دون غطاء من التعاون الدولي .وبناءً عليه، فإن تحقيق العدالة

[1] حبيب عباسي، ص520.

الجنائية وإنزال العقاب بالفاعلين يستوجب بالضرورة القيام بإجراءات تحرٍ واستقصاء خارج الحدود الوطنية التي اقترفت الجريمة أو جزء منها على أراضيها؛ وتشمل هذه الإجراءات- على سبيل المثال لا الحصر- المعاينة الفنية لمواقع الإنترنت في الخارج، وضبط الأقراص والوسائط الصلبة وحفظ الأدلة الرقمية ، [1] الفرع

ثالثا-صور التعاون الأمني الدولي لمكافحة الجرائم الإلكترونية

غدت الحاجة ملحة وماسة لصياغة وبناء كيان أمني دولي يأخذ على عاتقه ومسؤوليته القيام بالمهام الحيوية والاستراتيجية في مجال تبادل المعلومات الأمنية .وللتعاون الأمني الدولي في هذا المضمار صور وأنماط متعددة، يمكن إيجاز أبرزها فيما يلي[2] :

1-ربط شبكات الاتصال والمعلومات

تفتقر الاتصالات الشرطية والأمنية إلى الفعالية ما لم تستند إلى وسائل وقنوات اتصال متطورة وذات سرعات فائقة، تضمن تحقيق الاستجابة الفورية، وتمكّن أجهزة العدالة الجنائية وسلطات التحقيق والملاحقة المختلفة من التواصل الآني .ومن هذا المنطلق، عمدت الدول والمنظمات الدولية إلى تطوير منظومات لاتصال وتحديث آليات تبادل المعلومات البينية وتأمينها

2-: تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة:

تواجه دول العالم كافة احتمالات تدفق وأزمات وحوادث مفاجئة وضخمة لا يمكن التنبؤ بها بدقة أو استشراف توقيت حدوثها، وقد يعجز النظام الأمني القومي والقدرات الذاتية للدولة المتضررة عن مواجهتها بمفردها .وفي مثل هذه الكوارث أو المواقف الحرجة، يشكل" عنصر الوقت "العامل الحاسم والفيصل في المواجهة، وهو ما يتطلب تكثيفاً استثنائياً للجهود والخبرات والإمكانات؛ الأمر الذي يصعب تحقيقه على أرض الواقع إلا من خلال تضافر وتكامل الجهود الدولية الإنسانية والأمنية[3] وتُعدّ هذه الصورة من التعاون الأمني من الأنماط البارزة في حقل مكافحة الجرائم الإلكترونية؛ ذلك أن أجهزة العدالة الجنائية والمنظومات الأمنية لا تتمتع بذات القدر من الكفاءة والجاهزية التقنية والفنية في جميع دول العالم .فهناك تفاوت بنيوي واضح؛ إذ تملك بعض الدول منظومات تكنولوجية وتقنية بالغة التطور والتقدم، مستحوذة بذلك على نصيب وافر وخبرة عميقة في مواجهة الإجرام المعلوماتي تشريعياً وفنياً، في حين تفتقر دول أخرى إلى هذه المقومات

---

[1] عادل عبد العال ابراهيم خراشي، المرجع السابق، ص20-21.

[2] المرجع نفسه، ص24.

[3] حسين بن سعيد الغافري، مرجع سابق، ص641-642.

الأساسية .ومن هنا، تتبلور الحتمية الموضوعية لتعزيز التعاون وتبادل الدعم الفني والتقني بين الدول لسد هذه الفجوات الرقمية .

3- القيام ببعض العمليات الشرطية والأمنية المشتركة

تتطلب عمليات تتبع مجرمي المعلوماتية، وملاحقة الشبكات الإجرامية عبر الفضاء السيبراني، وتَعقُّب الأدلة الإلكترونية وضبطها، القيام بعمليات تفتيش دقيقة وعابرة للحدود لمكونات الحاسب الآلي، والمنظومات الرقمية، وشبكات الاتصال؛ وذلك بحثاً عما تحويه من أدلة وقرائن رقمية تبرهن على ارتكاب الجريمة الإلكترونية .وكل هذه الإجراءات المعقدة تستدعي القيام بعمليات شرطية وأمنية مشتركة وممنهجة، تساهم في صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم، وتفضي في نهاية المطاف إلى وضع حد نهائي لأنشطتها.[1]

4- :جهود المنظمة الدولية للشرطة الجنائية الأنتربول

الإنتربول في مجال التعاون الأمني تسعى منظمة" الإنتربول "جاهدة إلى توفير قنوات اتصال آمنة ومس تدامة بين أجهزة الشرطة حول العالم لجعل البيئة الدولية أكثر أماناً، وتحفيز التعاون البيني بين أجهزة الشرط ة في الدول الأطراف على نحو فعال ومثمر في مكافحة الجريمة، وضبط الجناة، وتجميع البيانات والمعلوما ت ذات الصلة بالجريمة والمجرمين وتبادلها .ويتم هذا التنسيق عبر المكاتب المركزية الوطنية للشرطة الدولية الموجودة في الدول الأعضاء، كما تعمل المنظمة على تقديم الدعم الفني والميداني المستمر لأجهزة الشرطة في الدول الأطراف، ودعمها وتحسين قدراتها باستمرار لمنع الإجرام ومحاربته، وتطوير المعارف والمهارات اللازمة لعمل أجهزة الشرطة على الصعيد الدولي بشكل أكثر فاعلية [2]وبهدف إرساء منظومة اتصال فعالة، و آمنة، وآجلة بين أجهزة الشرطة في مختلف الدول، بما يُمكّنها من تبادل المعلومات والبيانات بشكل موثوق و سريع، قامت منظمة الإنتربول بإنشاء وتطوير منظومة عالمية للاتصالات الشرطية المؤمنة؛ تتيح لموظفي انفاذ القانون في جميع الدول الأعضاء الوصول السريع والآمن إلى قواعد بيانات الإنتربول، والاستفادة من خ دماتها المتنوعة على مدار الساعة[3].

---

[1] سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعمومات الدولية، دار النهضة العربية، القاهرة، 2013، ص415.

[2] محمد كمال محمود الدسوقي، الحماية الجنائية للمعلومات الالكترونية، الطبعة الأولى، دار الفكر و القانون، 2015، ص13 . 132-1

[3] المرجع نفسه، ص519.

وقد أحدثت هذه المنظومة المتطورة للاتصالات طفرة نوعية وجذرية في آليات عمل أجهزة الشرطة في الدول الأعضاء؛ حيث مَكّنت المحققين من الوصول المباشر إلى أدوات الإنتربول المتطورة، ومن ثَمَّ الربط لآ ني بين معلومات قد تبدو في ظاهرها منفصلة أو غير مترابطة .ويساهم هذا الربط الشبكي في تيسي التحقيقا ت في الجرائم الإلكترونية، فضلاً عن تمكين أجهزة الشرطة وجهات إنفاذ القانون من تقصي البيانات ومقارنة ها في ثوانٍ معدودة، وذلك عبر وصولهم المباشر إلى قواعد البيانات الدولية المتعلقة بالمجرمين المشبوهين أو الأشخاص المطلوبين [1] وتأسيساً على ما تقدم، يمكن القول إن هذه المنظومة الرقمية تُمثّل إحدى المرتكزا ت الأساسية والمستندات الجوهرية لمكافحة الجرائم الإلكترونية؛ نظراً لما تتطلبه هذه المواجهة من سرعة فائقة في تتبع الأثر الرقمي، وتبادل المعلومات حول الأجهزة المصدرة للهجمات الإلكترونية ومستخدمين أجهزة الـ شرطة في جميع دول العالم ومن الأمثلة التطبيقية الدالة على الدور المحوري لـ" الإنتربول"في مكافحة الجرائم الإلكترونية العابرة للحدود، قيام القضاء اللبناني بتوقيف أحد الطلاب الجامعيين في لبنان بتهمة إنشاء وإرسا ل صور إباحية للقاصرين دون سن العاشرة عبر موقع إلكتروني، وقد تم هذا التوقيف إثر تلقي النيابة العامة اللبنانية برقية رسمية عاجلة من منظمة الإنتربول في ألمانيا بهذا الشأن.[2]

الفرع الثاني: المساعدة القضائية المتبادلة

إذا كان التعاون الأمني يمثل الشق الميداني العاجل لملاحقة الجريمة الإلكترونية، فإن المساعدة القضائية المتبادلة Mutual Legal Assistance تشكل الشق القانوني الرسمي والشرعي الذي يضفي الحجية على الأدلة الرقمية المستمدة من الخارج أمام المحاكم الوطنية .ونظراً لأن اتخاذ إجراءات تحقيق قسرية– كالتفتيش والضبط أو مصادرة الخوادم –على إقليم دولة أجنبية يمس مباشرة بسيادتها الوطنية، فقد استلزم الأمر تنظيم هذه العملية عبر قنوات دبلوماسية وقضائية رسمية تستند إلى المعاهدات الدولية أو مبدأ المعاملة بالمثل، وذلك لضمان مشروعية الدليل الجنائي وحمايته من البطلان. وبناءً على ذلك، سنقوم بتحليل هذا الإجراء القانوني الدولي من خلال تقسيم هذا الفرع إلى محورين أساسيين

---

[1] المرجع نفسه، ص132.

[2] كمال حطاب، الحماية الجزائية للتجارة الالكترونية، اطروحة دوكتوراه في العلوم، تخصص العلوم القانونية، كلية الحقوق والعلوم السياسية، فرع العلوم الجنائية، جامعة جيلالي اليابس، سيدي بلعباس، 2014–2015 ، ص390 .

أولاً :مفهوم المساعدة القضائية المتبادلة في التحقيق الإلكتروني

ثانياً :صور المساعدة القضائية المتبادلة وآلياتها.

أولا: مفهوم المساعدة القضائية المتبادلة

تُعرّف المساعدة القضائية المتبادلة في السياق القانوني والاتفاقي بأنها" :كل إجراء قضائي تباشره سلطات دولة ما، بهدف تسهيل وإسناد المهام القضائية والتحقيقية المنوطة بالمحاكم في دولة أخرى، وذلك بمناسبة نظرها في جريمة من الجرائم [1]."كما يُستخلص لها تعريف إجرائي آخر يفيد بأنها" :قيام سلطة قضائية مختصة تابعة لدولة أجنبية باتخاذ إجراء أو جملة من إجراءات التحقيق الجنائي، وذلك لحساب وبناءً على طلب سلطة قضائية مختصة تابعة لدولة أخرى، بُغية الوصول إلى كشف الحقيقة واستجلاء معالمها في قضايا جنائية معينة"[2] تأسيسًا على ما تقدم، يتضح جليًّا أن آلية المساعدة القضائية المتبادلة تنهض أساسًا على فكرة التنسيق والتعاون الوثيق بين السلطات القضائية التابعة لدولتين على الأقل .ويغدو هذا التعاون مبررًا وإلزاميًّا من أجل اتخاذ تدابير وإجراءات التحقيق القضائي اللازمة في سياق دولة ليست هي الدولة الناظرة في موضوع الجريمة؛ ومرجع ذلك غالبًا يرجع إلى امتداد وتوزع أركان الجريمة أو عناصرها المادية لتشمل إقليم هاتين الدولتين، مما يجعل التعاون حتميًّا لضمان ملاحقة مرتكبي هذه الجرائم وإخضاعهم لمحاكمة عادلة ومنصفة .المراحل الإجرائية لتحقيق المساعدة القضائية :إن إعمال آلية المساعدة القضائية لا يتأتى من الناحية العملية والمسطرية إلا من خلال استيفاء ثلاث خطوات أساسية متتابعة[34]

أ –المرحلة الأولى تقديم الطلب

يُرفع هذا الطلب ابتداءً من قِبل الدولة صاحبة الاختصاص الجنائي في المحاكمة، ويخضع في تصميمه وفحواه للقانون الوطني للدولة الطالبة، كما يتحدد نطاقه بحدود الاتفاقيات الثنائية أو المتعددة الأطراف المبرمة مع الدولة المُوجَّه إليها طلب المساعدة .والأصل المستقر عليه في هذا الصدد أن يتم تقديم وتوجيه هذه الطلبات عبر القنوات الدبلوماسية الرسمية، بيد أنه وعملاً ببعض الاتفاقيات الدولية الحديثة وتيسيرًا للإجراءات، بات يُسمح بالاتصال المباشر بين جهات ووزارات العدل في الدولتين كسباً للوقت واختصاراً للمسافات الزمنية .

ب–المرحلة الثانية فحص ودراسة الطلب:

---

[1] بوحزمة نصيرة، مرجع سابق، ص426.

[2] عادل عبد العال ابراهيم خراشي، مرجع سابق، ص30.

[3] سليمان احمد الفضل، مرجع سابق، ص31–32.

تباشر هذه الخطوة السلطات المختصة في الدولة المدعوة لتقديم المساعدة؛ حيث تتولى عملية التحقق والتثبت من أن الواقعة الجنائية المطلوب التحقيق فيها تُشكل جريمة معاقبًا عليها وفقًا للمنظومة القانونية للدولة الطالبة .وبناءً على مدى مطابقتها للاختصاص الموضوعي المطلوب منها إجابته، يتم البت في الطلب وفقاً لنصوص ومعايير الاتفاقية المعقودة بين الطرفين.

ج-المرحلة الثالثة تنفيذ المساعدة القضائية:

يتم تنفيذ مضامين الإنابة القضائية أو طلب المساعدة وفقاً للقواعد الإجرائية والأنظمة القانونية السارية في الدولة المطلوب منها التنفيذ، حيث تخضع الإجراءات والتدابير لأحكام قانونها الداخلي دون سواه .وفي هذا الإطار، تظل الاتفاقيات الدولية هي الأداة القانونية الوحيدة والمصدر الحصري الذي تنبثق عنه الالتزامات المتبادلة بين الدول في هذا الشأن .وبناءً عليه، فإنه في حال غياب اتفاقية دولية ناظمة، وخروج الطلب عن الشروط والأطر المعمول بها، فلا يمكن إلزام أي دولة بالاستجابة لطلب المساعدة القضائية الموجَّه إليها، ما لم يكن ذلك متوافقاً مع مبادئ القانون الداخلي ومتاحاً في تشريعها الوطني لكلتا الدولتين

2- صور وأشكال المساعدة القضائية المتبادلة تتنوع صور المساعدة القضائية المتبادلة بتنوع التدابير المتبعة

وتأخذ الإجراءات المعتمدة في هذا الشأن الأشكال والتطبيقات التالية :تبادل المعلومات، ونقل الإجراءات[1].

-**آلية تبادل المعلومات** :يُمثل تبادل المعلومات أحد أبرز الركائز الاستراتيجية والوقائية في منظومة مكافحة الجريمة بصفة عامة، والجرائم الإلكترونية والمعلوماتية على وجه الخصوص .وتكمن الأهمية البالغة لهذه الآلية في أن تقاسم المعطيات والبيانات وسرعة الحصول عليها يسهم بشكل فعال ومباشر في تيسير مهام الأجهزة الوطنية، ورفع كفاءتها في التحرك الآني والمناسب لمواجهة ظواهر الإجرام المستحدث .انطلاقاً من هذه المعطيات، يولي المجتمع الدولي أهمية قصوى لتبادل المعلومات بوصفه وسيلة ناجعة وأداة حتمية لكبح جماح الإجرام المنظم والسيبراني؛ نظراً لما تتيحه المعلومات الصحيحة والموثوقة من دعم لوجيستي ومعرفي لأجهزة إنفاذ القوانين في مختلف المجالات، بما في ذلك تتبع أنشطة المنظمات الإجرامية، ورصد

[1] بوحزمة نصيرة، مرجع سابق ، ص429 .

مصادر تمويلها وتتبع حركة الأموال المشبوهة .وفي هذا الصدد، أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين بتطوير أساليب التبادل المنهجي للمعلومات باعتباره عنصراً رئيساً في خطط العمل الدولية لمكافحة الإجرام، كما دعت منظمة الأمم المتحدة إلى إنشاء قواعد بيانات معلوماتية متطورة لإحاطة الدول الأطراف بصورة مستمرة بالاتجاهات العالمية السائدة في مجال الجريمة المستحدثة .وتأسيساً على ما تقدم، يغدو من الضروري تعزيز التعاون الدولي في المسائل الجنائية المرتبطة بالجريمة الإلكترونية عبر توظيف وتطوير نظم وآليات تبادل المعلومات بين الدول الأعضاء، وتقديم الدعم التقني والفني المتبادل، فضلاً عن تكثيف البرامج التدريبية المتخصصة الرامية إلى رفع كفاءة العاملين في قطاع العدالة الجنائية على الصعيد الدولي [1]إن تفعيل التبادل الدولي للمعلومات يُمكن أن يتحقق عملياً من خلال المنظمات والهيئات الدولية المختصة، ويشمل هذا التعاون تبادل البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية بمناسبة نظرها في خصومة جنائية ما، أو للتحقق من صحة الاتهامات الموجهة إلى رعاياها في الخارج، وكذا الإجراءات والتدابير المتخذة ضد المستندات، وقد يمتد ليشمل تبادل السوابق القضائية للجناة[2] .وتتجلى الأهمية البالغة للتعاون الفعال بين الدول في تسريع وتيرة تبادل المعلومات وإنجاز طلبات المساعدة في الحالات العاجلة والحرجة، لا سيما تلك التي يُعتقل فيها المتهمون ثم يُطلق سراحهم مالم ترد المستندات والدلائل القاطعة من الدولة الأخرى في المواعيد المحددة قانوناً. [2]

كما تبرز الأهمية القصوى لتبادل المعطيات في ميدان مكافحة الجرائم الإلكترونية بالنظر إلى لجوء الجناة ومرتكبي هذه الجرائم إلى التخفي الرقمي عبر الشبكات المعلوماتية، واستخدام هويات مزيفة وأسماء مستعارة، مما يفرض تنسيقاً دولياً عابراً للحدود، خاصة في الحالات التي تتوزع فيها الأنشطة الإجرامية بين أكثر من دولة، وذلك لتحديد الهوية الحقيقية للأشخاص المشتبه في ضلوعهم في تلك الجرائم وتحديد أماكن تواجدهم تمهيداً للقبض عليهم .يضاف إلى ذلك أن تبادل المعلومات يمثل ركيزة أساسية للإحاطة بالوسائل والأساليب التقنية المتطورة التي يستخدمها هؤلاء المجرمون في تنفيذ مآربهم، وهي أساليب تتسم بالتغير السريع والتعقيد التكنولوجي المستمر، مما يسهل على أجهزة المواجهة والتصدي كبح هذه الجرائم، الأمر الذي يستوجب تبادل المعطيات بشكل دوري ومرن دون انتظار عقد الاجتماعات والمؤتمرات التقليدية .ومن هذا المنطلق، يمكن إصدار نشرة دورية) شهرية مثلاً (تتضمن أحدث الوسائل والأساليب المبتكرة في مجال

[1] بوحزمة نصيرة، مرجع سابق ، ص429 .

[2] عادل عبد العال ابراهيم الخراشي، مرجع سابق، ص32، .

الجرائم الإلكترونية، على أن يتم تداولها على مستوى الدول إما بطريقة مباشرة من دولة إلى أخرى، أو عبر المنظمات الدولية والإقليمية والتي تتولى بدورها تعميمها على الدول الأعضاء، أو من خلال نشرها في المواقع الإلكترونية الرسمية الخاصة بها، أو عقد اجتماعات وندوات افتراضية عن بعد للتداول والنقاش حول هذه الخبرات والمستجدات .حيث تتيح هذه الآلية لقمع الإجرام استعارة واقتباس الأفكار والحلول الأمنية من تجارب الدول الأخرى، والاطلاع على خبراتهم في مجال الاختراق والتجسس المعلوماتي، سواء من خلال مؤتمراتهم عبر شبكات الإنترنت أو المنتديات والمنابر الرقمية المخصصة لهذا الغرض .وفي هذا السياق العملي، تبرز بعض القضايا الواقعية. [1]

كأمثلة حية على نجاعة هذا التعاون؛ ومنها قضية القرصنة الإلكترونية التي تلقت فيها السلطات الجزائرية في شهر جويلية 2009 معلومات قيمة من سفارة ألمانيا بالجزائر، تفيد بأن مصالح الشرطة الألمانية اكتشفت بأن شخصاً قام بتاريخ 30 جوان2009 ، وفي تمام الساعة الثامنة وخمس وأربعين دقيقة مساءً، باختراق قاعدة بيانات متواجدة بميونيخ في ألمانيا، وقام بتحميل البيانات الرقمية الخاصة بـ 15,000 بطاقة ائتمان باستعمال عنوان بريد إلكتروني موجه .وبشكل مماثل، وتأكيداً لاستمرارية هذا التنسيق الدولي، تلقت ذات السلطات بتاريخ 21 أكتوبر من نفس السنة مراسلة من مكتب الإنتربول بالجزائر مرسلة من مكتب الإنتربول بكندا، تفيد بأن مصالح شرطة كيبك (Québec) تمكنت خلال العام الماضي من القبض على شبكة إجرامية منظمة متخصصة في القرصنة الإلكترونية وتحميل المعطيات الرقمية المتبادلة بين الزبائن والبنوك، وتحويل الأموال من حسابات بنكية .وبناءً على هذه المعلومات المستلمة والتعاون الاستخباري والتقني المشترك، تمكنت المديرية العامة للأمن الوطني من إلقاء القبض على المتهم وهو شاب جزائري، وتقديمه للعدالة بتهمة القرصنة الإلكترونية المرتكبة بحق مراكز معطيات إلكترونية أجنبية متواجدة بكل من ألمانيا وكندا، حيث صدر بحقه حكم قضائي رقم 10/37560 من محكمة عنابة بتاريخ 28 جوان[2] 2010

آلية نقل الإجراءات الجنائية :

يُقصد بنقل الإجراءات الجنائية قيام إحدى الدول بناءً على اتفاقية دولية أو معاهدة مبرمة باتخاذ تدابير وملاحقات قضائية تفيد بالتحقيق في جريمة ارُتكبت في إقليم دولة أخرى، ولصالح هذه الدولة متى توافرت شروط وضوابط قانونية معينة .ومن أهم هذه الشروط مبدأ" التجريم المزدوج"، ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة معاقباً عليها في تشريع كلتا الدولتين) الدولة الطالبة والدولة المطلوب

[1] بوحزمة نصيرة، مرجع سابق، ص429 .

[2] حسين بن سعيد الغافري،مرجع سابق، ص645-646 .

إليها نقل الإجراءات .(هذا بالإضافة إلى ضرورة توافر مشروعية الإجراءات المطلوب اتخاذها، بمعنى أن تكون تلك التدابير متوافقة ومقررة في القانون الداخلي للدولة المطلوب إليها مباشرة الإجراءات .وتكتسي هذه الشروط القانونية أهمية بالغة بالنظر إلى أن صحة الإجراءات المتخذة تؤدي دوراً محورياً وحاسماً في الوصول إلى الحقيقة القضائية وتحقيق العدالة المنصفة .وإعمالاً لهذه القواعد المقررة، يحق للدولة الطالبة أن تلتمس من الدولة المطلوب منها المساعدة القضائية اتخاذ الملاحقات المناسبة، وفق ما تقتضيه المصلحة العامة والاتفاقيات المبرمة بينهما[1].

العابرة للحدود تجعل من تطبيق مبدأ 'سيادة الدولة' على بيانات موزعة في خوادم عالمية أمراً يثير إشكالات قانونية معقدة، خاصة في مجال تنازع الاختصاص القضائي وتحديد الدولة التي لها الحق في الملاحقة والتحقيق.

المبحث الثاني : معوقات التحقيق الإلكتروني

على الرغم من التطور التشريعي والتقني الذي واكب استحداث آليات متطورة للبحث والتحري الرقمي إلا أن مسار التحقيق الجنائي الإلكتروني لا يزال يصطدم بجملة من العقبات والتحديات الجسيمة التي تحد من فاعليته .وتنبثق هذه المعوقات من الطبيعة الاستثنائية والافتراضية للفضاء الرقمي، والتي أفرزت صعوبات متشابكة؛ فبعضها يكمن في الخصائص الذاتية للجريمة الإلكترونية وصعوبة تتبع أثرها الرقمي، وبعضها الآخر يرتبط بالمسلك السلبي للضحايا وعزوفهم عن التبليغ .علاوة على ذلك، يلعب التطور المستمر لذكاء المجرم المعلوماتي واستخدامه لتقنيات التشفير المتقدمة دوراً حاسماً في إفلاته من العقاب، يقابله في كثير من الأحيان نقص في المؤهلات التقنية واللوجستية لدى الجهات التقليدية المكلفة بإنفاذ القانون وللإحاطة الشاملة بهذه التحديات وتفكيك أبعادها، سنعمد إلى دراسة هذا المبحث من خلال أربعة مطالب متكاملة:

المطلب الأول :الصعوبات الراجعة لطبيعة الجريمة الإلكترونية بذاتها.

المطلب الثاني :المعوقات الراجعة لضحايا الجريمة الإلكترونية.

المطلب الثالث :التحديات الراجعة لذكاء وفطنة المجرم المعلوماتي.

---

[1] بوحزمة نصيرة، مرجع سابق، ص431 .

المطلب الرابع :العقبات الراجعة للجهات المختصة باكتشاف الجرائم وضبطها.

المطلب الأول: الصعوبات الراجعة إلى الجريمة المعلوماتية في ذاتها:

تتسم الجريمة المعلوماتية بطبيعة افتراضية تميزها جوهرياً عن الجرائم التقليدية؛ كونها ترتكب بالكامل ضمن بيئة إلكترونية (رقمية). هذا الطابع غير المادي يلقي بظلاله على منظومة العدالة الجنائية، ويفرض تحديات معقدة تبدأ من مرحلة الكشف والتقصي وتصل إلى إثبات الجريمة والتحقيق فيها. ويمكن حصر هذه العقبات في ندرة وخفاء الآثار المادية الملموسة (الفرع الأول)، الطبيعة غير المرئية للأدلة الرقمية (الفرع الثاني)، ضخامة وتدفق المحتوى والبيانات الرقمية (الفرع الثالث)، العابرة للحدود والاصطدام بالسيادة الوطنية (الفرع الرابع)،

الفرع الأول: ندرة وخفاء الآثار المادية الملموسة:

على خلاف الجنايات والجنح الكلاسيكية التي تخلّف وراءها أدلة مادية ملموسة وعينات بيولوجية أو جرمية (كالمقذوفات النارية، الأسلحة البيضاء، أو بقع الدماء والملابس)، فإن الجريمة المعلوماتية تكاد تخلو تماماً من هذه المظاهر الفيزيائية، مما يحرم جهات التحقيق من المؤشرات الحسية المعتادة في مسرح الجريمة.[1]

الفرع الثاني: الطبيعة غير المرئية للأدلة الرقمية:

إن جلّ ما يتركه الجاني خلفه يقتصر على آثار رقمية بحتة قوامها نبضات إلكترونية غير مرئية بالعين المجردة. [2]

هذه الأدلة الافتراضية تتناهى في الصغر من حيث الحجم والحيز، وتصل إلى مستوى "التخيلية"[3]، بحيث يستحيل رصدها أو معاينتها إلا عبر الاستعانة ببرمجيات معقدة وأجهزة تقنية متطورة قادرة على تجسيدها وإظهارها للعيان بصورة مقروءة ومفهومة[4]

---

[1] عائشة بن قارة مصطفى، حجية الدليل الالكتروني، في مجال الاثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، 2010، ص62 .

[2] رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجراءم الالكترونية، ط، المكتب الجامعي الحديث، مصر،2013، ص60 .

[3] رشاد خالد عمر، مرجع سابق، ص60 .

[4] عائشة بن قارة مصطفى، مرجع سابق، ص51 .

الفرع الثالث: ضخامة وتدفق المحتوى والبيانات الرقمية:

يواجه المحققون عقبة كأداء تتمثل في الحجم الهائل والتدفق اللامتناهي للملفات والبيانات المخزنة أو المتداولة عبر البيئة الالكترونية[1]. هذا الاتساع يعقّد من عملية الفرز والتدقيق، ويجعل من استخلاص الملفات المحملة بالنشاط الإجرامي أو تمييز البيانات المجرمة عن تلك المشروعة والمباحة أمراً في غاية الصعوبة، فضلاً عما يثيره هذا التفتيش الموسع من إشكاليات ومخاوف تتعلق بانتهاك الحق الدستوري في الخصوصية وحرمة الحياة الشخصية للأفراد.[1]

الفرع الرابع: العابرة للحدود والاصطدام بالسيادة الوطنية:

تنفذ هذه الجرائم عبر شبكات اتصالات معولمة ومترابطة تتجاوز التقسيمات الجغرافية. هذه الميزة تمنح الجاني القدرة على ولوج الأنظمة وقرصنتها عن بُعد من أي بقعة حول العالم.[3]

وفي المقابل، تجد سلطات الضبط والتحقيق الوطنية نفسها عاجزة عن تتبع هذه البيانات أو ضبطها نظراً لوقوع الخوادم أو مسرح الجريمة خارج النطاق الإقليمي للدولة، مما يؤدي مباشرة إلى اصطدام إجراءات التحقيق بمبدأ سيادة الدول الأخرى.[2]

بحيث إذا كانت النقاط الثلاث الأولى يمكن تجاوزها وتفكيك معضلاتها من خلال الاستعانة بالخبرة الفنية المتخصصة لعلماء الحاسوب والأدلة الرقمية، فإن النقطة الرابعة تظل رهينة بمدى تفعيل التعاون الدولي، وإبرام الاتفاقيات الثنائية والإقليمية لمكافحة الجريمة المنظمة عبر الوطنية لضمان تسليم المجرمين وتبادل المعلومات الجنائية.

المطلب الثاني: الصعوبات الراجعة إلى ضحايا الجرائم المعلوماتية

يمثل المجني عليه 'الضحية'في المحيط الرقمي أحد أكبر التحديات التي تواجه أجهزة التحقيق الجنائي؛ ففي كثير من الأحيان، يسهم سلوك الضحية أو نمطه المعرفي في تعقيد مسار العدالة أو حتى في وقوع الجريمة ابتداءً .وتتعدد العوامل المرتبطة بالضحايا والتي تشكل حجر عثرة أمام اكتشاف الجرائم وضبط أدلتها الرقمية؛ حيث تلعب الأمية الرقمية دوراً أساسياً في تسهيل اختراق الأنظمة، يرافقها في كثير من الأحيان إهمال شديد في تحديث منظومات الحماية الشخصية والمؤسساتية .علاوة على ذلك، فإن عدم استيعاب

---

[1] جميل عبد الباقي الصغير،أدلة الإثبات الجنائيو التكنلوجيا الجديدة، دار النهضة العربية، القاهرة، دار النهضة العربية، القاهرة، 2010، ص115 .

[2] رشاد خالد عمر، مرجع سابق، ص61 .

الضحايا للأبعاد الخطيرة للاعتداءات الإلكترونية يؤدي بالتبعية إلى إحجامهم عن التبليغ، مما يوسع نطاق "الرقم الخفي "في هذا النمط من الجرائم.

ولتشريح هذه الصعوبات وتفصيل أثرها السلبي على منظومة التحقيق، سنقسم هذا المطلب إلى ثلاثة فروع متكاملة

لفرع الأول :قصور الوعي المعرفي والثقافة الرقمية لدى المستخدمين

الفرع الثاني :الإهمال الجسيم والتراخي في اتخاذ التدابير الحمائية

الفرع الثالث :غياب الإدراك لخطورة الفعل الإجرامي المعلوماتي

الفرع الأول: قصور الوعي المعرفي والثقافة الرقمية لدى المستخدمين:

تشكل البيئة الإلكترونية، ولا سيما شبكة الإنترنت، مناخاً مثالياً لاستدراج الضحايا واصطيادهم في بؤرة إجرامية موحدة.[1] وتكمن المعضلة في أن الشريحة الأوسع من مستخدمي هذه الشبكات تفتقر إلى الحد الأدنى من المعرفة التقنية والآليات التحذيرية التي تمكنهم من رصد المؤشرات الأولية للهجمات أو استشعار خطر الاختراق، مما يجعلهم لقمة سائغة لأساليب الخداع الرقمي.[2]

الفرع الثاني: الإهمال الجسيم والتراخي في اتخاذ التدابير الحمائية:

ينجح الجناة في كثير من الأحيان نتيجة غياب الحيطة والحذر من قبل الضحايا، حيث يقع الكثير منهم في فخ ملفات التجسس أو البريد العشوائي والرسائل المفخخة (Spam) التي تحتوي على برمجيات خبيثة وفيروسات دقيقة تنفذ إلى النظام فور فتح الرسالة دون إدراك المستخدم.[3] والأخطر من ذلك هو جهل الضحية بوقوع الاختراق أصلاً، حيث تستمر هذه البرمجيات في العمل بصمت لمدد زمنية طويلة تتيح للجاني استنزاف البيانات والقرصنة قبل أن يتم اكتشاف الأمر، وهو ما يؤدي غالباً إلى فوات الأوان وضياع فرصة تتبع الأثر الرقمي للمجرم. ولا يقتصر هذا الإهمال التقني على الأفراد فحسب، بل يمتد ليشمل المؤسسات المالية والشركات التجارية الكبرى التي قد تتراخي في إجراء التدقيق الدوري والمراجعة الصارمة لحساباتها، مما يحول دون الاكتشاف الفوري لعمليات الاختلاس أو التلاعب المالي إلا بعد مرور أشهر أو سنوات على ارتكابها.[4]

---

[1] رشاد خالد عمر، مرجع سابق، ص61 .

[2] محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، مصر، المجلة الكبرى، 2008 ص108 .

[3] حسين بن سعيد الغافري، مرجع سابق، ص523 .

[4] رشاد خالد عمر، مرجع سابق، ص63 .

الفرع الثالث: غياب الإدراك لخطورة الفعل الإجرامي المعلوماتي:

ثمة تدنٍ واضح في مستوى الوعي المجتمعي بخطورة الجريمة المعلوماتية وتداعياتها؛ إذ يغيب عن أذهان الكثيرين سواء أكانوا أفراداً أم مؤسسات تربوية وتعليمية وإعلامية ضرورة تضافر الجهود لبيان أبعاد هذا الخطر الإجرامي.

ومن ثم، بات من الواجب الحتمي على الدولة صياغة استراتيجيات توعوية شاملة تشارك فيها كافة وسائل الإعلام لتبصير المجتمع بمخاطر هذه الجرائم وطرق الوقاية منها، إعمالاً للتوصيات الدولية الصادرة عن مؤتمرات الأمم المتحدة ذات الصلة (مثل مؤتمر الأونكتاد لعام 2005).[1]

المطلب الثالث: الصعوبات الراجعة إلى فطنة وذكاء مجرمي المعلوماتية:

يتميز المجرم المعلوماتي أو الجاني الرقمي بخصائص سلوكية وفنية فريدة ترفعه عن مصاف المجرمين التقليديين؛ فهو غالباً ما يتمتع بمستوى عالٍ من الذكاء، والفطنة، والخبرة التقنية المتخصصة في التعامل مع الأنظمة البرمجية وشبكات الاتصال .هذا التفوق المعرفي يمنح الجاني القدرة على ابتكار أساليب معقدة تسبق أحياناً الوسائل الأمنية المتاحة لجهات إنفاذ القانون .وتتجلى خطورة فطنة هذا المجرم في قدرته العالية على طمس هويته الحقيقية خلف ستار من العناوين الوهمية، واستخدامه لتقنيات متطورة تجعل من عملية تتبع أثره الرقمي أو إثبات التهمة في مواجهته أمراً بالغ الصعوبة والتعقيد.

وبناءً على ذلك، سنقوم بتفكيك هذه العقبات ومظاهر ذكاء الجاني من خلال الفروع التالية:

الفرع الأول :التخفي الفني وانتحال الهويات الافتراضية

الفرع الثاني :استخدام تقنيات التشفير والبرمجيات المعقدة لإعاقة التحقيق

الفرع الثالث :القدرة على المحو السريع للأدلة الرقمية وتدميرها

الفرع الأول: استخدام تقنيات التشفير المتقدمة للبيانات:

يعمد الجاني بفضل مهاراته العالية إلى تشفير الملفات والبيانات الإلكترونية محل الجريمة أو وسائل الاتصال المستخدمة فيها. هذا التشفير يحجب محتوى البيانات ويمنع غير المصرح لهم من الاطلاع

[1] رشاد خالد عمر، مرجع سابق،ص64 .

عليها أو كشف طبيعتها الإجرامية، وهي ذات الحيلة التي تبرز بوضوح في عمليات غسيل الأموال عبر الإنترنت وتداول العملات الافتراضية.[1]

كما يلجأ الجناة إلى استخدام برمجيات خبيثة متخصصة مثل برامج رصد ضربات المفاتيح (Key\,\,Logger\,\,System) بهدف اقتناص كلمات السر وتمرير الرسائل الإلكترونية بصورة سرية ومحمية قانونياً ببرامج التشفير ذاتها.[2]

الفرع الثاني: سرعة محو وإتلاف الأدلة الرقمية:

يمتلك المجرم المعلوماتي القدرة على طمس معالم جريمته بمرونة وسرعة فائقة عقب التنفيذ مباشرة. إذ يتيح له النظام تعديل البيانات، أو محو سجلات النشاط الرقمي، أو تفعيل برامج تجميد وتصفير الأنظمة بمجرد استشعار الخطر (مثل برامج Deep\,\,Freeze). وتتم هذه العمليات التقنية المضادة في أجزاء من الثانية ومن خلال ضغطات بسيطة، مما يترك المحققين أمام أنظمة فارغة خالية من أي دليل إثبات يُعتد به قانوناً.[3]

الفرع الثالث: التخفي الفني وانتحال الهويات الافتراضية:

يقوم الجاني بتمويه هويته الحقيقية وموقعه الجغرافي عبر استخدام هويات زائفة، أو أسماء مستعارة، أو عبر الولوج من خلال خوادم بروكسي متعددة وشبكات وهمية تعيق أي محاولة لتتبعه، مما يصعّب من مهمة ربط الفعل المادي لشخصه الحقيقي.

المطلب الرابع: الصعوبات الراجعة إلى الجهات المختصة باكتشاف الجرائم المعلوماتية

يواجه جهاز الضبط القضائي (الشرطة والادعاء العام) معوقات هيكلية وتنظيمية تحد من فاعلية أدائه في مواجهة الطفرة المتسارعة للجريمة الرقمية.

الفرع الأول: نقص ونقصان المعرفة الفنية والخبرة التخصصية لدى جهات الضبط:

---

[1] رشاد خالد عمر،المرجع نفسه، ص63 .

[2] جميل عبد الباقي الصغير، مرجع سابق، ص115 .

[3] شيماء عبد الغاني محمد عطا الله ، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص115 .

إن المهام الملقاة على عاتق مأموري الضبط القضائي تتطلب إلماماً واسعاً بالمنظومات المعلوماتية وبرمجياتها، وهو ما يفتقر إليه قطاع واسع من الكوادر الأمنية الكلاسيكية.[1]

هذا العجز المعرفي قد يدفع المحققين في بعض الأحيان – عن جهل وبدون قصد – إلى تدمير الأدلة الرقمية أثناء محاولة فحص الأجهزة أو التعامل مع مسرح الجريمة الافتراضي بطريقة غير مهنية، مما يترتب عليه ضياع الدليل وتفتته. ولمواجهة هذه المعضلة[2]، تباينت استراتيجيات الدول؛ حيث اتجهت الدول المتقدمة مبكراً (مثل كندا منذ عام 1980، والولايات المتحدة الأمريكية عبر تشكيل مكاتب متخصصة تابعة لمكتب التحقيقات الفيدرالي FBI وقسم مكافحة جرائم الحاسوب وحقوق الملكية الفكرية التابع لوزارة العدل عام 1991، تلتها فرنسا) نحو تأسيس وحدات أمنية نخبوية، لا تعتمد في تأهيلها على التدريب العسكري والبدني التقليدي، بل ترتكز على الكفاءة العلمية والتقنية العالية لخوض غمار الملاحقة الرقمية عبر الفضاء الإلكتروني. بالمقابل، ما زالت العديد من الدول النامية (ومنها المشرع العراقي) تعتمد بصورة أساسية على أجهزتها التقليدية الساكنة دون تأهيل تقني كافٍ لمواكبة هذه الجرائم، وهو ما يستدعي التدخل التشريعي العاجل لإنشاء أجهزة شرطية متخصصة ومستقلة للتحري عن الجرائم المعلوماتية، على غرار ما تبناه المشرع السوداني في قانون جرائم المعلوماتية لعام 2007. [3]

الفرع الثاني: غياب وقصور الثقافة القانونية والتشريعية المتخصصة:

تعاني سلطات إنفاذ القانون من ضعف حاد في الإدراك القانوني لطبيعة وخطورة الأنماط المستحدثة للجرائم الإلكترونية، وهو تحدٍ يزداد تعقيداً في الدول التي تفتقر حتى الآن إلى تشريعات موضوعية وإجرائية خاصة بمكافحة الجرائم المعلوماتية وتحديد صورها وأركانها بدقة. لذا، يثور التأكيد الفقهي على ضرورة تدارك المشرع لهذا النقص عبر إصدار قوانين رادعة، مع ضرورة النص صراحة على منح صفة الضبطية القضائية للموظفين الفنيين العاملين في قطاع المعلوماتية والاتصالات وتحديد اختصاصاتهم بدقة، وذلك أسوة بالنهج الذي سلكه المشرع الإماراتي في قانون مكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006 (والتعديلات والإجراءات اللاحقة)، والذي ساهم في تسريع وتيرة الكشف عن هذه الجرائم وملاحقة مرتكبيها.

---

[1] علي بن عبد الله العسيري، الآثار الأمنية لإستخدام الشباب للأنترنت، ط1، مركز الدراسات والبحوث، جامعة نايفالعربية للعلوم الأمنية، الرياض، 2004 ، ص 59 .

[2] رشاد خالد عمر، مرجع سابق، ص66 .

[3] رشاد خالد عمر، مرجع سابق، ص66 .

الفرع الثالث: شح الإمكانات التقنية واللوجستية:

إن مجرد توافر المعرفة النظرية لدى مأموري الضبط القضائي يظل غير كافٍ ما لم يدعم بتوفير بنية تحتية تقنية مكافئة وقادرة على مجابهة الأدوات التي يستعملها الجناة.

فالأمر يقتضي وجوباً تزويد الأجهزة الأمنية بأحدث البرمجيات التحليلية، ومنظومات الفحص الجنائي الرقمي المتطورة، ووسائل تتبع الشبكات، لتمكينهم من أداء مهامهم بفاعلية وإعادة التوازن لصالح منظومة العدالة الجنائية في مواجهة مجرمي الفضاء الافتراضي.[1]

المطلب الرابع: تأثير مشكلات الدليل الرقمي على اقتناع القاضي

يتبوأ الدليل الرقمي مكانة مركزية كأحد أبرز وسائل الإثبات في العصر الراهن، مدفوعاً بالطفرة التكنولوجية المتسارعة؛ بيد أن توظيفه القضائي يصطدم بجملة من العقبات التي تؤثر بشكل مباشر على عقيدة قاضي الموضوع ويقينه الجنائي، أو ما يصطلح عليه فقهياً بـ "الاقتناع الشخصي للقاضي". وتكمن هذه الإشكاليات في طبيعة الدليل الرقمي التكوينية من جهة، وفي الآليات الإجرائية المتبعة للحصول عليه من جهة أخرى، وهو ما ينعكس سلباً على قيمته الثبوتية في منظومة الإثبات الجنائي.

إن حظر وتجريم الأنشطة غير المشروعة عبر الوسائط الرقمية يتأثر طردياً بالخصائص الذاتية لهذه الجرائم، وكذا بالوسائل العلمية المستحدثة في ارتكابها؛ الأمر الذي يؤدي في كثير من الأحيان إلى ترسيخ ظاهرة الإفلات من العقاب نتيجة عدم اكتشاف الجريمة وقت اقترافها، أو العجز عن تحديد الهوية الرقمية للجناة، أو تعذر بناء دليل مادي مستوفٍ للشروط القانونية لإدانتهم، مما يترتب عليه أضرار بالغة تمس الأفراد والمجتمع على حد سواء.[2]

وعليه، سنعمل على تفكيك هذه الإشكاليات وبيان مدى تأثيرها من خلال تصنيفها إلى نوعين رئيسيين: مشكلات موضوعية، ومشكلات إجرائية.

الفرع الأول: المشكلات الموضوعية للدليل الرقمي

تتمحور العقبات الموضوعية للدليل الرقمي حول ماهيته الذاتية، ومضمونه، والخصائص الفيزيائية والمادية التي تشكله. فقد أضحى هذا الدليل ركيزة جوهرية في الخصومة الجنائية نظراً لاستخراجه من الأجهزة الذكية، والحواسب الآلية، والكاميرات الرقمية، وشبكات الإنترنت. إلا أن ارتباطه الوثيق بالتقنيات

---

[1] درابلة العمري سليم، مرجع سابق، ص237 .

[2] عائشة بن قارة مصطفى، مرجع سابق، ص252 .

الحديثة أفرز تحديات موضوعية تمس جوهره وتؤثر في حجيته وقيمته التدليلية أمام الهيئات القضائية، وتتجمل أبرز هذه المشكلات فيما يلي:[1]

اولا- غياب الدليل الرقمي المرئي:

يتصف الدليل الرقمي بأنه دليل غير مرئي؛ إذ هو في حقيقته نبضات وإشارات مخزنة كهرومغناطيسية داخل الأنظمة الحاسوبية في قالب ثنائي.

وتتجلى خطورة هذه الخصائص في البيئة الرقمية (مثل شبكة الإنترنت) في أنها تتيح للمستخدمين ميزة الاتصال وحجب هوياتهم الحقيقية، مما يجعله دليلاً غير ملموس يفتقر إلى المادية الجسدية التي تتمتع بها الأدلة التقليدية (كالأسلحة أو المحررات الورقية). هذا الغياب المادي يضعف من أثره النفسي والإقناعي لدى القاضي، لا سيما في الأنظمة القضائية التي تتبنى مبدأ القناعة لشخصية الوجدانية، مما قد يسوق إلى استبعاده أو التشكيك في قيمته القانونية.[2]

علاوة على ذلك، فإن الجرائم الواقعة على العمليات الرقمية غالباً ما تنصب على جوانب معنوية ترتبط بالمعالجة الآلية للبيانات والمعطيات الرقمية. فإذا ما وقعت جرائم اعتداء على هذا الجانب المعنوي (كالسرقة، أو الغش، أو التزوير المعنوي)، فإن إقامة الدليل تغدو مسألة معقدة نظراً للطبيعة الافتراضية للمحل الذي وقعت عليه الجريمة، ولأنها تعتمد في موضوعها على التشفير والرموز السرية والنبضات المغنطيسية التي يصعب ترك آثار مرئية لها يمكن معاينتها بالطرق التقليدية، أو الاستدلال منها على الجناة. ومن أمثلة ذلك إرسال الرسائل الإلكترونية مجهولة الهوية أو المصدر، والتي يسهل في الغالب تعديلها والتلاعب ببياناتها بغرض قطع الصلة بين المجرم وسلوكه الإجرامي، مما يشكل عائقاً حقيقياً أمام جهات التحقيق والتحري، والقضاة على حد سواء، والذين اعتادوا في عقيدتهم القضائية على الإثبات المادي للجريمة.[3]

ثانيا- الدليل الرقمي ذو طبيعة ديناميكية:

يمتاز الدليل الرقمي بطبيعته الديناميكية المتغيرة (غير الثابتة)، وهي خاصية تميزه بنيوياً عن الأدلة التقليدية، وتعد من أعقد الإشكاليات الموضوعية المؤثرة في حجيته. فالمقصود بالديناميكية هنا هو أن

---

[1] درابلة العمري سليم، مرجع سابق، ص239 .

[2] درابلة العمري سليم، مرجع سابق، ص239 .

[3] المرجع نفسه، ص240 .

البيانات الرقمية قابلة للتعديل، أو الحذف، أو التحديث المستمر؛ إذ يمكن نقلها عبر شبكات الاتصال بسرعة فائقة، كما يمكن تخزين هذه المعلومات والمعطيات في خوادم تقع خارج حدود الدولة (خارج الاختصاص الإقليمي).

يترتب على هذه الديناميكية صعوبة بالغة في تتبع الأدلة الرقمية وضبطها؛ إذ يتطلب الأمر اتخاذ تدابير إجرائية عابرة للحدود الوطنية، كمعاينة المواقع الإلكترونية المخالفة، أو تفتيش نظم الحاسب الآلي، أو ضبط الأقراص الصلبة التي قد تحوي مواد غير مشروعة (كالصور الإباحية مثلاً).

ويزداد الأمر تعقيداً عندما تصطدم هذه الإجراءات بسيادة الدول الأخرى التي قد ترفض الاستجابة، مما دفع المجتمع الدولي إلى إبرام العديد من الاتفاقيات والمعاهدات الدولية في مجال التعاون الدولي والقضائي، والتي تهدف إلى تقريب القوانين الجنائية، وتنسيق الجهود في إطار مكافحة الجرائم العالمية والسيبرانية العابرة للحدود.[1]

ثالثا- مشكلة الأصالة في الدليل الرقمي:

تعتبر الأصالة شرطاً جوهرياً لقبول الدليل الرقمي أمام القضاء، والمقصود بها هو التحقق من أن البيانات المعروضة هي ذاتها التي نُشئت أو استُقبلت من قِبل أطراف الدعوى، دون أن يلحقها أي تغيير أو تعديل منذ لحظة إنتاجها في البيئة الرقمية. وتكتسب الأصالة أهمية بالغة بالنظر إلى ما تتميز به المعطيات الرقمية من سهولة في النسخ، والإرسال، والتعديل دون ترك آثار ملموسة، بخلاف المستندات الورقية التي تحمل توقيعاً حياً أو ختماً رسمياً يسهل كشف تزويره.

فالملفات الرقمية لا تظهر عليها علامات التلاعب ما لم تخضع لفحص تقني دقيق؛ لكونها عبارة عن تعداد غير محدود لأرقام ثنائية موحدة في الصفر والواحد (0-1). فمثلاً، الصورة في العالم الافتراضي ليس لها وجود مادي ملموس كالصورة الفوتوغرافية الورقية، بل هي مجموعة من الأرقام الرمزية التي تعود في أصلها الجوهري إلى الرقم الثنائي (0-1)، أي أنها عبارة عن نبضات إلكترونية متواصلة تستمد حيويتها وتفاعلها من الطاقة.

لأجل ذلك، ثارت إشكالات فقهية وقانونية متعددة حول مدى الاعتداد بالنسخة الرقمية لتقوم مقام الدليل الكامل الأصيل. وقد اتجهت التشريعات المقارنة إلى تبني منطق افتراض أصالة الدليل الرقمي، كما هو الحال في قانون الإجراءات الجنائية الفيدرالي في الولايات المتحدة الأمريكية، حيث نصت القاعدة

[1] المرجع نفسه، ص 241-242.

القانونية 1001 البند 3 على قبول الدليل الرقمي باعتباره مستنداً أصلياً ما دامت البيانات صادرة عن حاسوب آلي أو جهاز مماثل، وسواء كانت مطبوعة أو مسجلة على دعامات أخرى. وبذلك ساوى المشرع بين الكتابة المادية التقليدية من حيث الأصالة وبين مخرجات لحاسوب، على الرغم من أن طبيعة الكتابة عبر الحاسوب تكون مجرد نسخ للأصل الموجود رقمياً في نظام الحاسب أو عبر شبكة الإنترنت.[1]

رابعا- صعوبة فهم الدليل الرقمي:

يعد فهم الدليل الرقمي من أبرز العقبات الموضوعية في القضاء الحديث؛ إذ غالباً ما يتضمن هذا النوع من الأدلة بيانات تقنية بالغة التعقيد، مثل سجلات النظام (Logs)، البصمات الرقمية (Digital Footprints)، بيانات السيرفرات، وتقارير التحليل الجنائي الرقمي. هذه البيانات لا يمكن قراءتها أو استيعابها بسهولة دون خلفية معلوماتية دقيقة، وبالتالي يتوقف فهمها على توافر خبرة فنية متخصصة، وقدرة تقنية عالية على معالجة المعلومات وتفكيك الغموض الناشئ عن الجرائم الإلكترونية الواقعة على وسائط التكنولوجيا.

بناءً على ذلك، يتطلب استيعاب الدليل الرقمي تدريباً تخصصياً مستمراً للجهات القضائية وسلطات التحقيق، يُمكّنهم من فهم طبيعة المعطيات الرقمية، وآليات جمع مكونات الحاسب الآلي، وكيفية عمل البرمجيات، ومعرفة لغات البرمجة والأنظمة التي يتم التعامل بها، نظراً لأن غالبية هذه الوسائط تعتمد على رموز وشفرات برمجية شديدة التعقيد.[2]

خامسا- سهولة إخفاء الدليل الرقمي:

تتميز الأدلة الرقمية بأنها من أكثر الأدلة عرضة للإخفاء أو الإزالة السريعة دون ترك أي أثر مادي ظاهر، وذلك بسبب طبيعتها غير الملموسة واعتمادها الكامل على الوسائط الإلكترونية والرقمية، بخلاف الدليل التقليدي الذي يصعب إخفاؤه كالمستندات أو الأدوات الجرمية. ففي البيئة الرقمية، يمكن للجناة بنقرة واحدة حذف الملفات الرقمية، أو تشفيرها، أو نقلها إلى خوادم وسحبها إلى خدمات سحابية Cloud services متعددة، مما يجعل الوصول إليها من الصعوبة بمكان، ويحول دون تنفيذ أوامر التفتيش القضائية الدولية.[3]

---

[1] أسامة محي الدين عبد العال، ص707 .

[2] مايدي شهرة –مسعودي أمال، ص 118 .

[3] المرجع نفسه، ص 118-119 .

سادسا- المعاينة وصعوبتها في النظام الرقمي:

تثير المعاينة في العالم الرقمي عدة عقبات قانونية وعملية:

1-عدم انتقال المحقق مادياً:

المعاينة الافتراضية تتطلب فحص الأنظمة عبر الشبكات (الإنترنت) دون الحاجة لتقييد المحقق بالانتقال الجغرافي، مما يطرح تساؤلاً حول مدى مشروعية ذلك إذا لم ينص القانون صراحة على هذا الإجراء.

2-**سرعة الشبكات والتدفق الفوري:** تتميز البيئة الرقمية بالسرعة الفائقة وقصر زمن العمليات، مما يقلل من الفارق الزمني للمعاينة مقارنة بالجرائم التقليدية، لكنه يتطلب استجابة فورية لمنع ضياع الدليل.

3-**انتهاك الخصوصية وسرية البيانات:** الأنظمة والحواسيب تحتوي على كميات ضخمة من البيانات الشخصية التي قد لا علاقة لها بالجريمة، مما يجعل فحصها مظنة المساس بحقوق الأفراد وحرياتهم.

4-**عقبة الحدود والسيادة الوطنية:** الجريمة المعلوماتية عابرة للحدود؛ فقد يكون نظام الحواسب مستضافاً في دولة أخرى (خارج السيادة الإقليمية للدولة)، مما يخلق نزاعاً دولياً يتطلب اتفاقيات تعاون دولي حديثة لتنظيم الفحص والتحقيق المشترك (مثل اتفاقية بودابست عام 2001).[1]

رابعا. المعوقات الفنية والتنظيمية

نقص المعرفة الفنية والتقنية: يفتقر العديد من موظفي ومحققي الجهات المختصة إلى الكفاءة التكنولوجية والمهارات الرقمية اللازمة للتعامل مع الأنظمة المعقدة وفحص مسرح الجريمة الافتراضي.

الحاجة إلى وحدات متخصصة: تبرز ضرورة إنشاء أقسام وشعب أمنية متخصصة بمكافحة الجرائم المعلوماتية وتدريب كوادرها (على غرار الأجهزة الأمنية في فرنسا والولايات المتحدة).

[1] درابلة العمري سليم، مرجع سابق، ص264 .

خطورة ضبط الأدلة الإلكترونية: تُعد خطوة فحص وضبط الأدلة الرقمية من أدق المراحل؛ نظراً لطبيعتها غير المادية وسهولة تعرضها للتلف أو التغيير أثناء المعاينة الفنية، مما يفتح الباب لإشكالات قانونية متعددة أثناء المحاكمة.[1]

الفرع الثاني التفتيش التحقيقي

يُمكن تعريف التفتيش التحقيقي في السياق القانوني العام بأنه: إجراء إجرائي ذو طبيعة قضائية تباشره السلطة المختصة بالتحقيق، يستهدف الكشف عن العناصر المادية والأدلة التي تساهم في إثبات الجريمة، أو تحديد وتتبع كل ما يُحتمل أنه أسهم في تسهيل ارتكابها أو ارتبط بها، شريطة أن ينصب هذا الإجراء على أماكن تتمتع بحرمة قانونية وسرية محمية.[2]

ومن هذا المنطلق، يكتسب التفتيش التحقيقي طابعاً قضائياً بحتاً يُدرجه ضمن آليات التحقيق الابتدائي.

وتبعاً لذلك، فإن الصلاحية الأصلية لمباشرته تنعقد حصرياً لجهات التحقيق المختصة، ولا يجوز لغيرها من السلطات اتخاذه إلا في إطار الاستثناءات التشريعية الصارمة والضيقة التي حددها القانون على سبيل الحصر.

وتتمثل الغاية التشريعية المتوخاة من التفتيش التحقيقي، في الغالب الأعم، في ضبط الموجودات والمتحصلات المادية المرتبطة بالواقعة الإجرامية، وفي بعض الأحيان تمتد لتشمل إلقاء القبض على المتهم نفسه.[3]

وبصفة عامة، فإن إعمال هذا الإجراء في بيئة الجرائم المعلوماتية يثير جملة من الإشكاليات القانونية والتطبيقية، ونستعرضها على النحو الآتي:

أولاً: سبب التفتيش

---

[1] صالح عبد الزهرة الحسون، أحكام التفتيش وأثاره في القانون العراقي، ط1، مطبعة الأديب البغدادية، بغداد، 1979، ص39-40.

[2] عباس الحسني، شرح قانون أصول المحاكمات الجزائية الجديد، المجلد1، مطبعة الإرشاد، بغداد، بلا سنة نشر، ص167.

[3] رشاد خالد عمر، مرجع سابق، ص128.

يُجمع الفقه والتشريع على أن مشروعية إجراء التفتيش التحقيقي وصحته ترتبط ارتباطاً وثيقاً بتوافر شروط موضوعية ثلاثة تمثل السبب القانوني لارتكازه، وهي:

- قيام واقعة إجرامية متحققة وثابتة فعلاً.
- قيام أسباب ودلائل كافية ومعقولة تبرر اللجوء إلى هذا الإجراء القسري وتسوغ انتهاك الحرمة.
- تحقق فائدة ومصلحة تحقيقية مرجوة ومباشرة من وراء تفعيل هذا الإجراء

ومع ذلك، فإن هذه الشروط الثلاثة تثير إشكاليات قانونية معقدة عند إسقاطها على منظومة الجرائم المعلوماتية؛ ففيما يتعلق بالشرط الأول، وفي ظل غياب تشريع خاص ينظم مكافحة الجرائم السيبرانية في العراق مثلاً، تبرز صعوبة بالغة أمام جهات التحقيق والقائمين بإنفاذ القانون في التحقق واليقين من وقوع الجريمة من عدمه، ولا سيما عند وجود خلاف فقهي واسع حول الطبيعة القانونية للأفعال المكونة لهذه الجرائم، وهو ما تم تفصيله مسبقاً في الفصل الأول.[1]

أما فيما يخص الشرطين الثاني والثالث، فإنهما يثيران إشكالية توازن دقيقة في بيئة الجرائم المعلوماتية؛ حيث إن اتخاذ إجراء التفتيش التحقيقي بناءً على مجرد الشبهات قد يؤدي في كثير من الأحيان إلى إلحاق أضرار مادية ومعنوية بالغة الجسامة بالجهة الصادر بحقها أمر التفتيش، مما قد يحمل الدولة (ممثلة بسلطاتها القضائية والتحقيقية) المسؤولية والتعويض في حال لم تثبت تلك الشبهات.

مثال تطبيقي: ولعل الشاهد الأبرز في هذا السياق هو الواقعة الشهيرة التي حدثت عام 1990 في الولايات المتحدة الأمريكية، عندما اشتبهت سلطات التحقيق في تورط أحد العاملين في شركة (ستيف جاكسون) للألعاب في إحدى الجرائم السيبرانية. وبناءً على ذلك، قامت السلطات بتفتيش مقر الشركة وضبطت كافة الأجهزة والأنظمة الحاسوبية وملحقاتها، مما تسبب بشكل مباشر في شلل تام لأعمال الشركة وتوقف نشاطها، وإلحاق خسائر مالية فادحة بها. وهو ما دفع القضاء لاحقاً إلى الحكم بتعويض الشركة تعويضاً مجزياً عن تلك الأضرار بعد أن ثبتت براءتها التامة من التهم المنسوبة إليها.

إضافة إلى ما تقدم، فإن الشرط الثالث—والذي يقضي بضرورة وجود فائدة ومصلحة حقيقية مرجوة من التفتيش من خلال ضبط الموجودات المتعلقة بالجريمة—يثير خلافاً فقهياً عميقاً حول مدى إمكانية خضوع المكونات والبيانات الإلكترونية للتفتيش؛ باعتبار أن الغاية التقليدية للتفتيش هي ضبط الأدلة المادية الملموسة، وليس الأدلة الرقمية غير المادية ذات الطبيعة المعنوية.

---

[1] رشاد خالد عمر، مرجع نفسه، ص130.

بيد أننا نرى أن جوهر الإشكالية هنا لا يرتبط بمدى خضوع المكونات الإلكترونية للتفتيش من عدمه، بقدر ما يرتبط بمدى إمكانية فحص ومعاينة هذه المكونات من الناحية العملية دون المساس بالحق في الخصوصية وحرمة المراسلات، وهو الأمر الذي يدعونا إلى دراسة مشكلات الضبط في جرائم المعلوماتية بشيء من التفصيل في الفقرات اللاحقة.[1]

ثانياً: وقت إجراء التفتيش

يُلاحظ من استقراء التشريعات الإجرائية الحديثة أنها تنص بصفة عامة على حظر تنفيذ أوامر تفتيش المساكن في أوقات محددة (كالليل أو أيام العطل والأعياد)، وذلك رعايةً لحرمة السكن ونأياً بالقاطنين فيه عن المباغتة والأضرار النفسية[1]، مع النص في الوقت ذاته على بعض الحالات الاستثنائية التي يجوز فيها التفتيش ليلاً، كحالات التلبس بالجريمة أو وجود أسباب معقولة يقدرها القاضي، أو وجود نصوص استثنائية تسمح بإجراء التفتيش التحقيقي في أي وقت ومن دون استثناء، كما هو الحال في قانون الإجراءات الجنائية المصري والإماراتي، بالإضافة إلى قانون أصول المحاكمات الجزائية العراقي، حيث لم يقيد إجراء التفتيش بوقت معين.[2]

ورغم أن الأخذ بحظر التفتيش الليلي يمثل مظهراً إنسانياً مهماً لحماية حريات الأفراد وخصوصياتهم، إلا أنه يشكل في بيئة جرائم المعلوماتية عائقاً كبيراً أمام فاعلية التحقيق.

فبما أن الجرائم الرقمية يمكن ارتكابها من قبل الجناة في أي وقت ومن أي مكان—بحيث يمكن أن يتزامن ارتكاب الجريمة مع منتصف الليل في دولة ما بينما يكون الوقت منتصف النهار في دولة أخرى نتيجة لاختلاف النطاقات الزمنية—فإن هذا التباين الإقليمي يؤدي في كثير من الأحيان إلى جعل الجريمة المعلوماتية المرتكبة في بلد ما، تقع خارج الساعات المسموح فيها بالتفتيش قانوناً في بلد آخر.

علاوة على ذلك، تتميز الجرائم المعلوماتية بأنها نادراً ما تكون مشهودة، وأن الأدلة الرقمية المرتبطة بها تتسم بالسيولة وسرعة التلف والسهولة الفائقة في المحو والتعديل، مما يرفع من احتمالية قيام

---

[1] سمير إبراهيم جميل العزاوي، المسؤولية الجنائية الناشئة عن إساءة استخدام الأنترنت، كلية القانون، جامعة بغداد، 2005، ص107-108

[2] رشاد خالد عمر، مرجع سابق، ص131.

المجرم بمسح الدليل فوراً. ومن ثم، يصبح من الضروري بمكان إجازة التفتيش الفوري وعلى وجه السرعة للحيلولة دون إفلات الجاني من العقاب.[1]

لذا، وبغية إيجاد صيغة توازن مرنة بين اعتبارات حماية الخصوصية وحظر التفتيش الليلي للمساكن، وبين متطلبات مكافحة الجرائم المعلوماتية الخطيرة، سلكت بعض التشريعات مسلكاً وسطاً؛ حيث استثنت بعض الجرائم الخطيرة—ومن بينها الجرائم المعلوماتية—من حظر التفتيش الليلي، مرخصةً للجهات المختصة فحص المساكن ومعاينتها ليلاً.[2]

ونحن بدورنا نؤيد هذا التوجه التشريعي ونفضله، لكونه يقترب من المنطق القانوني السليم ويحقق التوازن المطلوب بين حماية الحريات الفردية وخطورة الجرم المرتكب، لاسيما وأن هذا الإجراء يتفق مع أهمية وخطورة الجريمة، والأهم من ذلك كله أنه يتماشى مع ضرورة إجراء التفتيش على وجه السرعة في الجرائم المعلوماتية. ومن هنا، فإننا ندعو المشرع العراقي إلى أن يحذو حذو هذه التشريعات في هذا الصدد.[3]

ثالثاً: حضور إجراءات التفتيش

تتجه غالبية التشريعات الإجرائية الحديثة ومن ضمنها التشريعات المقارنة—إلى النص الصريح على وجوب حضور المتهم أو من ينيبه عند إجراء التفتيش إن أمكن ذلك، وفي حال تعذر ذلك، يتعين إجراء التفتيش بحضور شاهدين؛ وذلك كضمانة جوهرية لصيانة حق المتهم في الدفاع عن نفسه، وتعزيزاً لمنسوب الثقة واليقين في الأدلة المستخلصة من عملية التفتيش.

ولكن إذا كانت قاعدة الحضور هذه لا تثير إشكالات تذكر في بيئة الجرائم التقليدية، فإنها لا تبدو كذلك بالنسبة للجرائم المعلوماتية، وذلك بالنظر لخطورة حضور هؤلاء الأشخاص على الأدلة الرقمية المراد ضبطها. فبالنظر لخصوصية وسرعة إمكانية محو أو إتلاف هذه الأدلة أو التلاعب بها[4]، فإن حضور الخاضع للتفتيش قد يمنحه فرصة لتدمير الأدلة بمجرد كبسة زر واحدة على لوحة المفاتيح أو الفأرة، أو إعطاء أمر حاسوبي سريع يمحو البيانات تماماً من نطاق الذاكرة والحفظ.

---

[1] المرجع نفسه، نفس الصفحة.

[2] سردار علي عزيز ص241

[3] حسين بن سعيد الغافري، مرجع سابق، ص241 .

[4] عائشة بن قارة مصطفى، مرجع سابق، ص109.

ولكل ذلك، فإننا نرى ضرورة استبعاد الجرائم المعلوماتية من نطاق قاعدة الحضور هذه، وذلك تماشياً مع نهج المشرع الجزائري الذي استثنى مجموعة من الجرائم الخطيرة (ومن ضمنها الجرائم المعلوماتية) من الخضوع لقاعدة الحضور هذه، حيث يكتفي المشرع في مثل هذه الحالات بحضور الشاهدين والمختار أو من يقوم مقام الأخير إن أمكن إحضارهم. ويستهدف هذا التعديل الإجرائي الحفاظ على هذه الضمانة المهمة، سواء بالنسبة للمتهم وضمان صحة الإجراءات، أو بالنسبة لسلامة الدليل الرقمي وضمان عدم التلاعب به.[1]

رابعاً: نطاق أمر التفتيش من حيث تفتيش الشبكات

لقد ساهمت الطفرة التكنولوجية المعاصرة والتحول الرقمي في عصرنا الحالي في إمكانية امتداد وانتشار الأدلة الإلكترونية عبر شبكات معلوماتية متعددة من أجهزة حاسوب قد تقع أغلبها خارج النطاق الإقليمي للدولة. ويمثل هذا التمدد العابر للحدود تحدياً إجرائياً وقانونياً واضحاً أمام سلطات التفتيش والتحقيق، خصوصاً إذا ما صدر أمر التفتيش القضائي مستهدفاً جهاز حاسوب معين في مكان محدد دون غيره، في حين تكتشف جهة التحقيق أثناء التنفيذ وجود حواسب أخرى مرتبطة بالشبكة وموصولة بالحاسوب المأذون بتفتيشه.

وفي هذه الحالة، يثور تساؤل قانوني دقيق حول مدى جواز امتداد التفتيش ليشمل الحواسب الأخرى المرتبطة بناءً على الإذن القضائي الأول، وموقف المشرع والقضاء من هذه الإشكالية. وفي سبيل تذليل هذه العقبة القانونية، نرى ضرورة التفرقة بين فرضيتين أساسيتين[2]:

1-**الفرضية الأولى: إذا كانت الحواسب الأخرى الموصولة بالشبكة موجودة داخل النطاق الإقليمي للدولة.** وفي معالجة هذه الحالة، اختلفت التشريعات المقارنة؛ فالمشرع الفرنسي عالجها من خلال إجازته امتداد إذن التفتيش الأول ليشمل جميع الحواسب والأنظمة الأخرى الموجودة في المكان الذي يوجد فيه الحاسوب المأذون بتفتيشه، وذلك وفقاً للتعديل الإجرائي المعمول به. وفي المقابل، نجد أن القانون الأمريكي يرفض هذا الامتداد التلقائي؛ إذ يشترط صدور أمر تفتيش مستقل ومنفصل لكل جهاز على حدة، ما .[1]

---

[1] المادة 76 من قانون إجراءات الجزائية الجزائري، مرجع سابق.

[2] رشاد خالد عمر، مرجع سابق، ص134 .

لم توجد حالة طارئة أو استثنائية تبرر ذلك، حيث لم نجد في القانون الأمريكي أي نص تشريعي صريح يعالج هذه المسألة، ولكن في المقابل نجد أن التوجيهات الداخلية الخاصة بإجراءات التفتيش في الولايات المتحدة الأمريكية قد أجازت امتداد الإذن الصادر بتفتيش مقر شركة معينة ليشمل كافة فروعها الكائنة في نفس العقار.[1]

وبذات المنحى، عالج المشرع العراقي هذه المسألة من خلال النصوص التقليدية المنظمة للتفتيش، فأجاز التفتيش الفجائي لجميع الأماكن المرتبطة ببعضها البعض، طالما كان هذا الشيء متاحاً وموجوداً في المكان المأذون بتفتيشه أو في ملحقاته، أو كان ذو صلة بالجريمة التي يجري التفتيش من أجلها. وينطبق هذا الحكم بطبيعة الحال على تفتيش الحواسب والشبكات المحلية المتصلة ببعضها.[2]

2-**الفرضية الثانية: وجود الأنظمة أو الحواسب الأخرى خارج إطار المكان المأذون بتفتيشه، (الأنظمة السحابية أو الموزعة).** وفي هذا الصدد، معالجة بعض التشريعات الإجرائية الحديثة هذه الحالة أيضاً؛ حيث أجازت امتداد إذن التفتيش الصادر بحق مكان معين ليشمل جميع الحواسب المتصلة

والموجودة في مكان آخر غير المكان المأذون بتفتيشه، ولو كانت تلك الحواسب متواجدة في نطاق دولة أخرى كبلجيكا مثلاً، شريطة أن يكون هذا الامتداد ضرورياً ومبرراً لكشف حقيقة الجريمة وضبط أدلتها المهددة بالضياع.[3]

وفي السياق ذاته، نجد أن المشرع الفرنسي قد عالج هذه الحالة أيضاً من خلال القوانين والاتفاقيات الدولية المنظمة للتفتيش العابر للحدود، والاتفاقيات الأمنية المشتركة.

وفيما يتعلق بالقانون المصري، فقد ذهب جانب من الفقه إلى إمكانية معالجة هذه الحالة استناداً إلى تطبيق نص المادة (71/2) من قانون الإجراءات الجنائية المصري، والتي أجازت للقائم بالتفتيش أن يجري أي عمل من أعمال التحقيق—ومن ضمنها تفتيش مكان آخر—وذلك في الأحوال التي يخشى فيها من فوات الوقت، أو متى ما كان ذلك متصلاً بالتفتيش الذي يجريه ولازماً في كشف الحقيقة، أو في الحالات التي يؤدي تأخير الإجراء فيها إلى زوال أو ضياع أو فقدان الدليل.

---

[1] شيماء عبد الغني عطا الله ص298 .

[2] رشاد خالد عمر، مرجع سابق، ص135 .

[3] المرجع نفسه، نفس الصفحة.

وهو في هذه الحالة لا يستمد سلطته الاستثنائية تلك من قرار ندبه، وإنما يستمدها مباشرة من نص القانون المذكور بناءً على توفر حالة من حالات الضرورة أو الاستعجال[1]. إلا أن هذا الرأي انتقد من قِبل رأي آخر من الشراح؛ باعتبار أنه يخالف نص المادة (44) من الدستور المصري، الذي يقضي بعدم جواز تفتيش المنازل بغير رضا أصحابها إلا بناءً على أمر قضائي مسبب.

وأما فيما يتعلق بمعالجة هذه الفرضية في القانون العراقي، فيُلحظ أن النصوص الحالية للتفتيش في قانون أصول المحاكمات الجزائية لا تسمح بامتداد التفتيش لغير المكان المأذون بتفتيشه وملحقاته إلا في صورتين:

الأولى: إذا كان القائم بالتفتيش هو قاضي التحقيق نفسه، أو كان حاضراً أثناء إجراء التفتيش، فعندها يجوز له وبمقتضى المواد (56 و75 و76) من قانون أصول المحاكمات الجزائية إصدار الأمر بتفتيش أي مكان حتى ولو كان خارج سلطة اختصاصه، على أنه ينبغي عليه في الحالة الأخيرة أن يخطر فيما بعد قاضي تحقيق تلك المنطقة بما اتخذه من إجراءات في منطقة الآخر.

الثانية: إذا كانت الكمبيوترات الأخرى موجودة في منزل شخص متهم بجناية أو جنحة عمدية ومشهودة، أو في أي مكان آخر تحت حيازته؛ ففي هذه الحالة يجوز مدّ الإذن الصادر بالتفتيش حتى ولو كان القائم بالتفتيش هو المحقق.[2]

وبالتالي، فلا يجوز في غير هاتين الصورتين تفتيش الكمبيوترات الأخرى المرتبطة بالكمبيوتر المتواجد في المكان المأذون بتفتيشه، ما دامت تلك الكمبيوترات متواجدة خارج ذلك المكان، حتى ولو كان من الممكن الولوج إليها من خلال ذلك الكمبيوتر.

ومثل هذا الأمر له مضاره في مجال التحقيق في الجرائم المعلوماتية، لما سينجم عنه لا محالة من تأخير في إجراء التفتيش، مما يستدعي معه ضرورة سلك المشرع العراقي المسلك ذاته الذي سلكه المشرع البلجيكي الآنف الذكر بهذا الصدد.

الحالة الثانية: إذا كانت الكمبيوترات الأخرى موجودة خارج حدود إقليم الدولة:

---

[1] جلال ثروت ص 356

[2] رشاد خالد عمر، مرجع سابق، ص137.

في هذه الحالة، إذا كانت البيانات المراد تفتيشها موجودة في نظام أو موقع إلكتروني متاح للجمهور، فإنها لا تثير الإشكالية؛ حيث يجوز مدّ التفتيش إليها من دون الحاجة إلى أي إذن آخر من الجهات المختصة في الدولة الأخرى، حسبما نصت عليها الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية الصادرة في بودابست عام 2001. [1]

ولكن المشكلة تثور فيما إذا كانت تلك البيانات موجودة في كمبيوترات أو مواقع غير متاحة للجمهور، فمدّ التفتيش في هذه الحالة سيؤدي لا محالة إلى المساس بسيادة الدولة أو الدول الأخرى التي تتواجد على إقليمها تلك الكمبيوترات أو المواقع؛ إلا إذا كان هناك في القانون الدولي ما يجيز ذلك، حسبما أوصى المجلس الأوروبي في توصيته المرقمة R 95 13، وذلك في الحالات المستعجلة.

وهو ما نصت عليه أيضاً الاتفاقية الأوروبية المذكورة أعلاه في المادة (32) منها. ولما كانت فرنسا من الدول الموقعة على الاتفاقية المتقدمة، فقد أجاز المشرع الفرنسي للسلطات التحقيقية مدّ نطاق التفتيش إلى الكمبيوترات المرتبطة بالكمبيوتر المأذون بتفتيشه والموجودة خارج الإقليم الفرنسي، فيما إذا كان من الممكن الولوج إليها من خلال الكمبيوتر متاح للجمهور، على أن يتم ذلك في جميع الأحوال وفق الشروط المنصوص عليها في الاتفاقيات الدولية المعمول بها في فرنسا في هذا الصدد.[2]

فيما لم نجد نصاً قانونياً صريحاً في القانون الأمريكي بهذا الصدد، مع أن الولايات المتحدة الأمريكية هي الأخرى أيضاً من الدول الموقعة على الاتفاقية المذكورة. وكذلك لم نجد أيضاً في كل من القانونين المصري والعراقي ما يستدل منه على معالجتهما لهذه المسألة، وهو ما يُعدّ ثغرة في التشريع العراقي لابد من سدّها في المستقبل القريب، على أن تحقيق ذلك يستلزم بالضرورة دخول الحكومة العراقية في اتفاقيات دولية وثنائية تنظم هذه المسألة، في سبيل الحرص من جهة على عدم خرق سيادة الدول الأخرى وعدم إتاحة الفرصة من جهة أخرى أمام مجرمي المعلوماتية للإفلات من العقاب من خلال تعمّد تخزين الملفات والبيانات التي تشكل دليل إدانة ضدهم في كمبيوترات متواجدة في إقليم دولة أخرى.[3]

الإشكاليات القانونية المتعلقة بالخصوم أو أطراف الدعوى الجزائية

---

[1] المرجع نفسه، نفس الصفحة.

[2] المادة 32، من اتفاقية الأوروبية (بودابست)لمكافحة الجرائم لاإلكترونية، المعتمدة من مجلس أوروبا، الصادرة بتاريخ 23نوفمبر 2001، ودخلت حيز التنفيذ في 1 يوليو 2004.

[3] رشاد خالد عمر، مرجع سابق، ص138.

تثير منظومة الخبرة القضائية المنتدبة في نطاق الجرائم المعلوماتية جملة من العقبات القانونية والعملية التي تمس أطراف الخصومة الجنائية؛ إذ لا تقتصر هذه الإشكالات على الجهات القضائية (سواء جهات التحقيق أو الحكم)، بل تمتد لتمس بظلالها الضمانات الدستورية والقانونية المقررة للخصوم. ويمكن حصر هذه المشكلات الجوهرية في المحاور الآتية:

رابعا- مدى مشروعية حضور الخصوم أثناء مباشرة الخبير المعلوماتي لمهامه الفنية

أقرت الغالبية العظمى من التشريعات الإجرائية الحديثة حق الخصوم في حضور إجراءات التحقيق الجنائي، ويشمل ذلك بالضرورة مواكبة أعمال الخبرة الفنية؛ كونه ركيزة أساسية من ركائز حق الدفاع كضمانة دستورية.[1]

موقف المشرع المصري: أجاز المشرع في مصر بنص صريح أحقية الخصوم في الحضور أثناء قيام الخبير بأعماله الفنية، غير أنه منح الخبير في الوقت ذاته مكنة مباشرة مأموريته دون حضورهم إذا اقتضت الضرورة ذلك، شريطة أن يتم توجيه الدعوة رسمياً للخصوم لحضور الإجراء.[2]

موقف المشرع الفرنسي: يلاحظ أن القانون الفرنسي لم ينص صراحة على كفالة حق الخصوم في الحضور الفعلي المباشر أثناء تنفيذ الخبير لأعماله، بيد أنه استعاض عن ذلك بتقرير حزمة من الحقوق والضمانات الإجرائية الأخرى التي سيتم تبيانها لاحقاً في موضعها، في حين لم يتبنَّ المشرع الأمريكي هذا الحق أو ينص عليه صراحة.

نتائج الفصل الأول

الإطار المفاهيمي للتحقيق الإلكتروني والدليل الرقمي قصور المفاهيم التقليدية أمام الجريمة المعلوماتية أثبتت الدراسة أن التحقيق الجنائي التقليدي لم يعد كافياً بمفرده لاستيعاب طبيعة الجريمة الإلكترونية، مما

[1] فتحي محمد انورعزت، الحماية الجنائية الموضوعية والإجرائية والإعتداء على المصنفات والحق في الخصوصية والكمبيوتر والأنترنت في نطاق التشريعات الوطنية والتعاون الدولي، ط1، دار النهضة العربية، القاهرة، 2007، ص694-696.

[2] رشاد خالد عمر، مرجع سابق، ص171.

استلزم تبني مفهوم" التحقيق الإلكتروني "كآلية فنية مستحدثة تتناسب مع الطبيعة غير المادية للفضاء الافتراضي.

مرونة شرط مسرح الجريمة :تبيّن أن مسرح الجريمة الإلكترونية لم يعد محصوراً في حيز جغرافي مادي ضيق، بل أصبح ممتداً وعابراً للحدود الوطنية، وهو بيئة رقمية تتسم بالحركية والافتراضية الكاملة . خصوصية الدليل الرقمي) المنشأ والهشاشة :(خلص الفصل إلى أن الدليل الرقمي يتميز بخصائص فريدة تجعله مختلفاً جوهرياً عن الأدلة المادية؛ فهو دليل خفي، سريع الزوال، وسهل المحو أو التعديل بكبسة زر واحدة، مما يجعله" هشاً "ويتطلب حيطة تقنية فائقة أثناء التعامل معه ومعاينته لمنع تشويهه أو إسقاط حجيته القانونية .

التكامل بين القواعد الإجرائية والتقنية :إن تبيان الركن الشرعي للجرائم الإلكترونية في التعديلات المتلاحقة لقانون العقوبات الجزائري وقانون09-04 ، يظل رهيناً بمدى قدرة المحقق على ضبط الأدلة وصونها تقنياً، فالنص القانوني لا يتحرك عملياً إلا بوجود فضاء رقمي موثق ومحمٍ إجرائياً.

ثانياً :نتائج الفصل الثاني

إجراءات وعوائق التحقيق الإلكتروني

التحول الإجرائي التكنولوجي للمشرع الجزائري :أظهرت الدراسة مواكبة المشرع الجزائري للتطور التقني من خلال تدعيم قانون الإجراءات الجزائية بآليات مستحدثة استثنائية مثل :التفتيش والضبط الإلكتروني للبيانات المخزنة في الأنظمة المعلوماتية، واعتراض المراسلات، والمراقبة التقنية عبر التقاط الصور وتسجيل الأصوات .

الحاجة الحتمية للخبرة الفنية المتخصصة :استجلاء غموض الجرائم المعلوماتية والانتقال للمعاينة الرقمية أثبت حتمية الاستعانة بفريق تحقيق رقمي متخصص وشرطة قضائية مدربة فنيّاً؛ حيث إن الأسئلة الستة المنهجية للمحقق لا يمكن الإجابة عليها في الفضاء الافتراضي بآليات البحث والتحري التقليدية . التفتيش الإلكتروني بين الشرعية القضائية والخصوصية :خلص الفصل إلى أن التفتيش وضبط النظم المعلوماتية يوازنان بدقة بين الشروط الشكلية والموضوعية الصارمة لحماية حقوق الأفراد والدستور كحرمة الحياة الخاصة، وبين مقتضيات الفاعلية في ملاحقة الجناة .التشفير كأبرز العوائق التقنية :تمخضت الدراسة عن تحديد عوائق موضوعية جسيمة تقف أمام جهات التحقيق، أبرزها تقنيات التشفير المعقدة التي يستخدمها الجناة لإخفاء معالم الدليل، ومحو البيانات الفوري، بالإضافة إلى نقص التأهيل التقني لبعض الهيئات المكلفة بالتحقيق مقارنة بالاحترافية الإجرامية لمرتكبي هذه الجرائم .قصور آليات التعاون الدولي التقليدية :تبين أن

الطابع العابر للحدود للجريمة الإلكترونية يجعل آليات المساعدة القضائية المتبادلة والتعاون الدولي التقليدي بطيئة وإجراءاتها معقدة، وهو ما يتنافى مع صفة" السرعة "اللصيقة بالدليل الرقمي، مما يسهل على الجناة الإفلات من العقاب في حالة غياب اتفاقيات دولية مرنة ومباشرة

خـــاتمة الفصل الثاني:

بوصولنا إلى ختام هذا الفصل، نكون قد استكملنا تشريح الإجراءات المتبعة في التحقيق الإلكتروني، وسلطنا الضوء على جملة التحديات الجسيمة التي تواجه هذا المسار. لقد أثبت تحليلنا أن الإجراءات القانونية، رغم أهميتها في ضمان مشروعية الدليل، تظل محفوفة بالمخاطر التقنية التي قد تُفقد الإجراء قيمته القانونية أو تجعله عرضة للبطلان.

لقد أوضح هذا الفصل أن التحدي الحقيقي ليس فقط في "كيفية جمع الدليل"، بل في "كيفية الحفاظ على سلامته" في بيئة متغيرة ومتحركة لا تعترف بالحدود، وفي ظل تقنيات تشفير متطورة تحصن الجاني وتجعل الوصول إليه مهمة بالغة التعقيد. كما اتضح أن التشريعات الحالية، رغم محاولاتها لمسايرة التطور، لا تزال تعاني من بطء في استيعاب سرعة التحولات الرقمية، وهو ما يضع جهات التحقيق في موقف يتأرجح بين "الجمود النصي" و"ضرورة الفعل".

لقد خلصنا من خلال دراسة التحديات التقنية والقانونية إلى أن التحقيق الإلكتروني يتطلب "فلسفة إجرائية جديدة"، تتجاوز الأطر التقليدية وتعتمد على التخصص الدقيق، والتعاون الدولي العابر للحدود، والتوازن الصارم بين مقتضيات الضبط القضائي وحقوق الأفراد. إن العقبات التي عرضناها لم تكن مجرد عوائق نظرية، بل هي تحديات واقعية يومية يواجهها قضاة التحقيق وضباط الشرطة القضائية، مما يجعل من تجاوزها ضرورة ملحة لاستعادة فعالية العدالة في الفضاء الرقمي.

وبهذا الفصل، نكون قد أحيطنا بالجانبين الإجرائي والواقعي لموضوع دراستنا، بعد أن تأصلنا مفاهيمياً في الفصل الأول. ومع انتهاء هذا التحليل، ننتقل الآن إلى صياغة النتائج النهائية والتوصيات التي تمخضت عن هذا البحث، والتي نأمل أن تشكل مرجعاً قانونياً أو فكرةً للمشرع من أجل تطوير منظومتنا الإجرائية بما يخدم مصلحة المجتمع ويحقق العدالة الرقمية المنشود.

الخاتمة العامة

الخاتمة العامة

لقد أفرزت الثورة الرقمية واقعاً إجرامياً جديداً تجاوز الحدود التقليدية للزمان والمكان، وأصبحت الجريمة الإلكترونية من أخطر التحديات التي تواجه أنظمة العدالة الجنائية، لما تتسم به من تعقيد تقني، وسرعة في التنفيذ، وطابع عابر للحدود، الأمر الذي فرض على التشريعات الوطنية إعادة النظر في وسائل وآليات البحث والتحقيق الجنائي بما يضمن حماية الحقوق والحريات من جهة، وتحقيق الفعالية في كشف الجرائم وملاحقة مرتكبيها من جهة أخرى.

ومن خلال هذه الدراسة، تبيّن أن التحقيق الإلكتروني لم يعد مجرد وسيلة إجرائية حديثة، بل أصبح ضرورة قانونية وتقنية تفرضها طبيعة البيئة الرقمية، حيث أثبتت الدراسة أن القواعد التقليدية للتحقيق الجنائي لم تعد كافية لمواجهة الجرائم المعلوماتية، بالنظر إلى خصوصية مسرح الجريمة الإلكتروني، والطبيعة الفنية والهشة للدليل الرقمي، الذي يتطلب أساليب علمية دقيقة في جمعه وحفظه وتحليله، حفاظاً على سلامته وحجيته أمام القضاء.

كما كشفت الدراسة أن المشرع الجزائري قد خطا خطوات مهمة في سبيل مواكبة هذا التحول من خلال إدراج إجراءات استثنائية للتحقيق الإلكتروني، وتطوير المنظومة القانونية بما يسمح باللجوء إلى وسائل تقنية حديثة كالتفتيش الإلكتروني، واعتراض المراسلات، والمراقبة التقنية، غير أن فعالية هذه النصوص تبقى رهينة بتوفير الإمكانات البشرية والتقنية الكفيلة بحسن تطبيقها، وبمدى قدرة أجهزة إنفاذ القانون على مواكبة التطور المتسارع لأساليب الإجرام الإلكتروني.

وفي المقابل، أبرزت الدراسة جملة من التحديات التي لا تزال تحد من فعالية التحقيق الإلكتروني، وفي مقدمتها التشفير المتطور، وسرعة إتلاف الأدلة الرقمية أو تغييرها، والقصور في التأهيل التقني لبعض القائمين على التحقيق، إضافة إلى بطء آليات التعاون القضائي الدولي مقارنة بالسرعة الفائقة التي تنتقل بها الجرائم الإلكترونية عبر الحدود، وهو ما يستوجب تعزيز التعاون الدولي، وتطوير الاتفاقيات الثنائية ومتعددة الأطراف، وتوحيد قواعد تبادل الأدلة الرقمية بما يحقق سرعة الاستجابة ويحافظ على حقوق الدول والأفراد.

وعليه، فإن نجاح التحقيق الإلكتروني لا يتحقق بمجرد سن النصوص القانونية، وإنما يتطلب بناء منظومة متكاملة ترتكز على ثلاثة أبعاد متلازمة، هي: تشريع مرن يواكب التطورات

التقنية، وأجهزة تحقيق تمتلك الكفاءة والخبرة الرقمية، وتعاون دولي فعال قادر على تجاوز القيود الإقليمية التي لم تعد تعترف بها الجرائم المعلوماتية.

وفي الأخير، فإن مستقبل العدالة الجنائية في العصر الرقمي لن يُقاس بمدى صرامة العقوبات فحسب، وإنما بقدرتها على تطوير وسائل الإثبات والتحقيق بما يضمن الوصول إلى الحقيقة الرقمية وفق الضمانات القانونية الواجبة. فكلما تطورت وسائل الجريمة، كان لزاماً أن تتطور وسائل العدالة بالسرعة ذاتها، حتى يبقى القانون قادراً على أداء رسالته في حماية المجتمع وصون الحقوق والحريات، وترسيخ الثقة في القضاء في مواجهة أحد أخطر أشكال الإجرام المعاصر.

وبذلك، فإن التحقيق الإلكتروني لم يعد خياراً تشريعياً أو إجراءً استثنائياً، وإنما أصبح حجر الزاوية في مكافحة الجرائم الإلكترونية، والضمان الحقيقي لتحقيق عدالة جنائية عصرية تستجيب لمتطلبات الدولة الرقمية، وتوازن بين حماية الأمن المعلوماتي واحترام الحقوق الأساسية للأفراد، في ظل عالم أصبحت فيه المعلومة أغلى من المادة، وأصبح الدليل الرقمي مفتاح الوصول إلى الحقيقة القضائية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولاً: النصوص القانونية

1. الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم.
2. الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.
3. القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
4. القانون رقم 05-10 المؤرخ في 20 يونيو 2005، المعدل لقانون الإجراءات الجزائية.
5. القانون رقم 14-25 المؤرخ في 3 أوت 2025، المتضمن قانون الإجراءات الجزائية.
6. المرسوم الرئاسي رقم 19-172 المؤرخ في 6 جوان 2019.
7. قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.
8. قانون العقوبات الفرنسي.(Article 323-1 Code pénal)
9. اتفاقية بودابست بشأن الجريمة الإلكترونية لسنة 2001.

ثانياً: الكتب العامة

1. ابن منظور، لسان العرب، دار صادر، بيروت، ط3، 1994.
2. إبراهيم مكبور، المعجم الوجيز، مجمع اللغة العربية، مصر، ط1، 1973.
3. جميل صليبا، المعجم الفلسفي، دار الكتاب اللبناني، بيروت، ط1، 1970.
4. فؤاد الأفرام البستاني، منجد الطلاب، دار المشرق، بيروت، ط45، 1997.
5. جيلالي بغدادي، التحقيق دراسة مقارنة نظرية وتطبيقية، الديوان الوطني للأشغال التربوية، الجزائر.
6. دليلة جلول، الأسس النفسية للتحقيق الجنائي، دار الهدى، الجزائر، 2015.
7. حسن جوفندار، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، دار الثقافة، عمان، 2008.

8. حمد أبو الروس، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، المكتب الجامعي الحديث، الإسكندرية.
9. محمد سعيد نمور، أصول الإجراءات الجزائية، دار الثقافة، عمان، ط2، 2012.
10. محمد أنور عاشور، المبادئ الأساسية في التحقيق الجنائي العملي، عالم الكتب، القاهرة، 1987.
11. جباري عبد المجيد، دراسات قانونية عن المادة الجزائية، دار هومة، الجزائر، 2012.

ثالثاً: الكتب المتخصصة

1. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2018.
2. خالد ممدوح إبراهيم، أمن الجرائم الإلكترونية، الدار الجامعية، مصر.
3. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة، الأردن، 2011.
4. مصطفى محمود موسى، التحقيق الجنائي في الجريمة الإلكترونية.
5. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006.
6. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دار الكتب والوثائق القومية، مصر، 2012.
7. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، 2009.
8. محمد زهير، الحجية القانونية للدليل الرقمي في الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، 2021.
9. مناصرة يوسف، الدليل الإلكتروني في القانون الجزائي، دار الخلدونية، الجزائر، 2021.
10. فراح مناني، أدلة الإثبات الحديثة في القانون، دار العمري، الجزائر، 2013.
11. رشاد خالد عمر، المشكلات القانونية والفنية للتحقيق في الجرائم الإلكترونية، المكتب الجامعي الحديث، مصر، 2013.

12. سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2013.

13. محمد كمال محمود الدسوقي، الحماية الجنائية للمعلومات الإلكترونية، دار الفكر والقانون، 2015.

14. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2010.

15. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة.

16. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007.

17. علي بن عبد الله العسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

18. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، مصر، 2012.

19. صالح عبد الزهرة الحسون، أحكام التفتيش وآثاره في القانون العراقي، بغداد، 1979.

20. عباس الحسني، شرح قانون أصول المحاكمات الجزائية الجديد، بغداد.

21. فتحي محمد أنور عزت، الحماية الجنائية الموضوعية والإجرائية للاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت، دار النهضة العربية، القاهرة، 2007.

رابعاً: الرسائل الجامعية (دكتوراه – ماجستير – ماستر)

22. بوحزمة نصيرة، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه، جامعة جيلالي اليابس، سيدي بلعباس.

23. عمارة فوزي، قاضي التحقيق، أطروحة دكتوراه، جامعة الإخوة منتوري، قسنطينة.

24. مراد بن عيسى، حجية الدليل الرقمي في المادة الجزائية، أطروحة دكتوراه، جامعة الجزائر 1

25. كمال حطاب، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه، جامعة جيلالي اليابس.
26. زعزوعة نجاة، التقاضي الإلكتروني كآلية لإنجاح نظام العدالة، أطروحة دكتوراه، جامعة تلمسان.
27. هدى أحمد العوضي، استجواب المتهم في مرحلة التحقيق الابتدائي، رسالة ماجستير.
28. سعيد بن نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير.
29. خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه.
30. أجعود فطيمة، خصوصية التحقيق في الجريمة الإلكترونية، مذكرة ماستر.
31. درابلة العمري سليم، حجية الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر.
32. مايدي شهرة ومسعودي آمال، الدليل الرقمي ودوره في الإثبات الجنائي، مذكرة ماستر.
33. خلود فراحتية، دور الدليل الرقمي في الإثبات في الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر.
34. بن عمارة فاتن نور الإيمان، التحري والتحقيق في الجرائم الإلكترونية، مذكرة ماستر.
35. بوبعاية ابتسام، التحقيق في الجريمة المعلوماتية، مذكرة ماستر.

خامساً: المقالات العلمية (المجلات)

1. بوضياف إسمهان، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية.
2. سهيلة بوزبرة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، المجلة النقدية للقانون والعلوم السياسية.
3. طلاح عبد القادر، آيت عبد المالك، "التحقيق الجنائي للجرائم الإلكترونية في التشريع الجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية.
4. تابري مختار، "الخبرة في الجريمة الإلكترونية"، مجلة الحوار المتوسطي.
5. فلات سمية، حاحا عبد العالي، "مقتضيات المعاينة المعلوماتية في التشريع الجزائري"، مجلة الحقوق والحريات.

6. ليندا بن طالب، "التفتيش في الجرائم الإلكترونية"، مجلة العلوم القانونية والسياسية.
7. أحمد أبو القاسم، "المفهوم العلمي والتطبيقي للدليل الجنائي"، مجلة مركز البحوث الشرطية.
8. أسامة محي الدين عبد العال، "حجية الدليل الرقمي في الإثبات الجنائي"، مجلة البحوث القانونية والاقتصادية.
9. وهيبة لعوارم، "الدليل الرقمي في مجال الإثبات الجنائي وفقاً للتشريع الجزائري"، المجلة الجنائية القومية.
10. خالد ضو، "حجية الدليل الإلكتروني وشروط قبوله"، مجلة الباحث القانوني.
11. أحمد بن مالك، إبراهيم الخال، "دور الأدلة الرقمية في الإثبات الجنائي"، مجلة العلوم الإنسانية.

سادساً: المؤتمرات والندوات العلمية

1. طارق محمد الجميلي، *الدليل الرقمي في مجال الإثبات الرقمي*، ورشة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون، 2009.
2. أشرف صلاح الدين، *طرق الحماية التكنولوجية بأنواعها المختلفة*، أعمال مؤتمر مكافحة الجريمة عبر الإنترنت، المنظمة العربية للتنمية الإدارية، القاهرة، 2010.

سابعاً: المواقع الإلكترونية

1. قاموسCambridge Dictionary ، تعريف الدليل الرقمي(Digital Evidence) ، تاريخ الاطلاع: 2026/04/15

الفهرس

الفهرس

الفصل الثاني:إجراءات التحقيق الالكتروني ومعوقاته

الملخص

الملخص:

تتناول هذه الدراسة الموسومة بـ "**تحديات التحقيق الإلكتروني في ظل الفضاء الرقمي** "موضوع التحقيق الإلكتروني باعتباره إحدى أهم الآليات القانونية المستحدثة لمواجهة الجرائم الإلكترونية، وذلك من خلال بيان الإطار المفاهيمي للتحقيق الإلكتروني والدليل الرقمي، وتحليل التنظيم القانوني الذي أقره المشرع الجزائري، مع إبراز أهم التحديات القانونية والتقنية التي تواجه سلطات التحقيق في جمع الأدلة الرقمية وحفظها.

اعتمدت الدراسة على المنهج الوصفي التحليلي، وتوصلت إلى أن التحقيق الإلكتروني أصبح ضرورة حتمية تفرضها طبيعة الجرائم الإلكترونية، وأن الدليل الرقمي يمثل الركيزة الأساسية للإثبات الجنائي، إلا أن فعاليته ترتبط بسلامة إجراءات جمعه وحفظه. كما خلصت الدراسة إلى أن المشرع الجزائري عزز المنظومة القانونية بآليات حديثة، غير أن التحقيق الإلكتروني لا يزال يواجه تحديات، أبرزها التشفير، وسرعة زوال الأدلة الرقمية، ونقص الخبرة التقنية، وصعوبة التعاون الدولي في الجرائم العابرة للحدود.

الكلمات المفتاحية :التحقيق الإلكتروني، الفضاء الرقمي، الجريمة الإلكترونية، الدليل الرقمي، الإثبات الجنائي، التشريع الجزائري.

Abstract

This study, entitled **"Challenges of Electronic Investigation in the Digital Space,"** examines electronic investigation as one of the most important legal mechanisms developed to combat cybercrime. It analyzes the conceptual framework of electronic investigation and digital evidence, the legal framework adopted by the Algerian legislator, and the main legal and technical challenges faced by investigative authorities in collecting and preserving digital evidence.

The research adopts a descriptive and analytical approach and concludes that electronic investigation has become an essential necessity due to the unique nature of cybercrime. It also finds that digital evidence is the cornerstone of criminal proof, provided that it is collected and preserved according to proper legal and technical procedures. Furthermore, despite the legislative developments introduced by the Algerian legislator, electronic investigation still faces significant challenges, including encryption technologies, the rapid disappearance of digital evidence, limited technical expertise, and difficulties in international judicial cooperation.

Keywords: Electronic Investigation, Digital Space, Cybercrime, Digital Evidence, Criminal Evidence, Algerian Legislation.