

جامعة عبد الحميد بن باديس مستغانم

المرجع:

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة نهاية الدراسة لنيل شهادة ماستر

الاثبات القضائي في الجرائم السيبرانية في ضوء القانون الجزائري

ميدان الحقوق والعلوم السياسية

التخصص: القانون القضائي

الشعبة: الحقوق

تحت اشراف الاستاذ (ة):

من اعداد الطالب (ة):

- كعيبش بومدين

- عبد الله بن سلوى أمينة

اعضاء لجنة المناقشة

الاستاذ (ة) بن عودة يوسف.....رئيسا

الأستاذ (ة) كعيبش بومدين.....مشرفا مقرر

الاستاذ (ة) زواتين خالد.....مناقشا

السنة الجامعي: 2026/2025

نوقشت في: 2026/06/11



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة عبد الحميد بن باديس - مستغانم



كلية الحقوق والعلوم السياسية
مصلحة التبرعات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية في إنجاز البحث

أنا الممضي أدناه، الطالب (ة):

اللقب: عبد الله بن بادي الاسم: أ. مينة

الحامل (ة) لبطاقة التعريف الوطنية رقم: 412192454 والصادرة بتاريخ: 14.07.2024

المسجل (ة) بكلية: الحقوق والعلوم السياسية قسم: قانون خاص

والمكلف (ة) بإنجاز مذكرة ماستر بعنوان:

الإثبات الجنائي في الجرائم السيبرانية في ضوء القانون

الجزائري

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

م. النصفية على التوقيع السيد
عبد الله بن بادي
412192454
14/07/2024



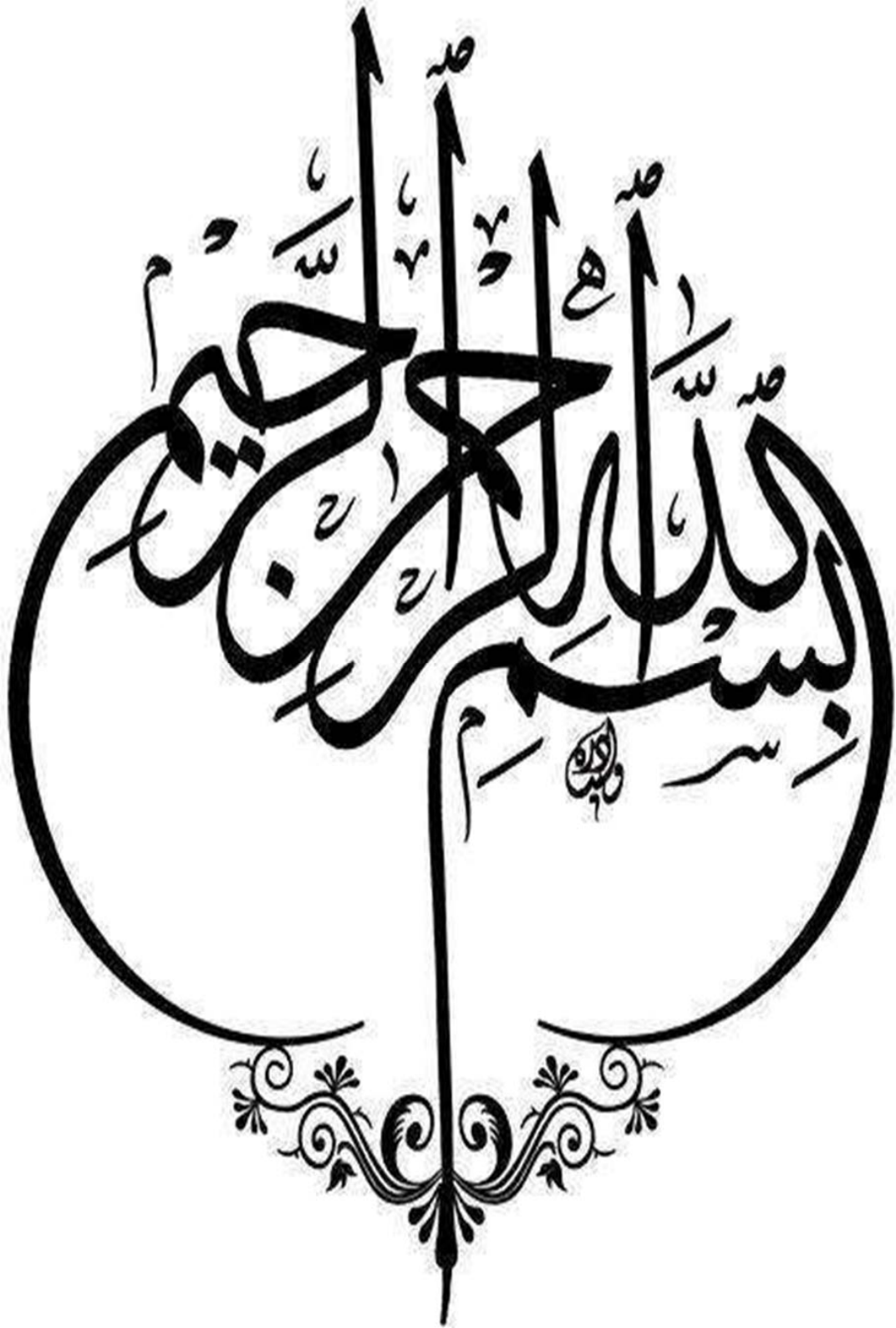
امضاء المعني

9 جوان 2026

عن رئيس المجلس الأعلى
و بالتفويض منه
رئيس مصلحة الخالة
معمّر إبراهيم

التاريخ:

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها.



إهداء

إلى أبي العزيز،

سندي في هذه الحياة، ومصدر العزم والإرادة، الذي كان دائماً مثلاً للتضحية
والعطاء، أسأل الله أن يحفظه ويدعم عليه الصحة والعافية.

إلى أُمِّي الغالية،

نبع الحنان والرحمة، وصاحبة الفضل الكبير فيما وصلت إليه، التي أحاطتني
بدعائها وتشجيعها في كل مراحل حياتي، حفظها الله وأدامها تاجاً فوق رأسي.
وإلى إخوتي وأخواتي، وعائلتي الكريمة جميعاً، وإلى كل من ساندني وشجعني ووقف إلى
جانبي طوال مسيرتي الدراسية.

وإلى أصدقائي وزملائي، وكل من حمل لي مشاعر المودة والدعم، أهدي ثمرة هذا
الجهد المتواضع، راجياً من الله أن يجعله عملاً نافعاً ومباركاً.

أمنية

الشكر والتقدير

شكر وعرفان

بسم الله الرحمن الرحيم، الحمد لله الذي وفقنا لإتمام هذا العمل، والصلاة والسلام

على سيدنا محمد صلى الله عليه وسلم.

أتقدم بأسمى عبارات الشكر والتقدير والاحترام إلى الأستاذ المشرف كعيبش بومدين، على ما قدمه من توجيهات علمية قيمة، وما أبداه من صبر واهتمام ومتابعة طوال فترة إعداد هذه المذكرة، فكان لتوجيهاته الأثر البالغ في إنجاز هذا

العمل.

كما أتوجه بالشكر إلى كل من ساعدني وساندني في مسيرتي الدراسية، وساهم بكلمة طيبة أو نصيحة نافعة أو دعم معنوي في إنجاز هذا البحث. وأسأل الله تعالى أن يجزي الجميع خير الجزاء وأن يوفقهم لما فيه الخير والنجاح.

أمنية

مقدمة

مقدمة:

شهد العالم خلال العقود الأخيرة تطورًا تكنولوجيًا هائلًا مسّ مختلف مجالات الحياة، حيث أصبحت الوسائل الرقمية والأنظمة المعلوماتية جزءًا أساسيًا من النشاط اليومي للأفراد والمؤسسات والدول، وذلك بفضل الانتشار الواسع لشبكة الإنترنت وتكنولوجيا الإعلام والاتصال الحديثة¹. وقد ساهم هذا التطور في تسهيل المعاملات وتبادل المعلومات وتحقيق سرعة التواصل، إلا أنه في المقابل أدى إلى ظهور نوع جديد من الجرائم يُعرف بالجرائم السيبرانية أو الجرائم الإلكترونية، التي تُرتكب باستعمال الوسائط الرقمية أو تستهدف الأنظمة المعلوماتية والبيانات الإلكترونية².

وتُعد الجرائم السيبرانية من أخطر الجرائم المستحدثة في العصر الحديث، لما تتميز به من طبيعة خاصة تختلف عن الجرائم التقليدية، إذ غالبًا ما ترتكب عن بعد، وتتجاوز الحدود الجغرافية للدول، كما يصعب اكتشاف مرتكبيها أو تعقبهم بسبب اعتمادهم على وسائل تقنية متطورة تساعدهم على إخفاء هوياتهم ومحو آثارهم الرقمية³. كما أن هذه الجرائم تتنوع صورها لتشمل الاختراق الإلكتروني، وسرقة البيانات، والاحتيال الإلكتروني، والتزوير الرقمي، وانتهاك الخصوصية، والابتزاز الإلكتروني، ونشر البرمجيات الخبيثة وغيرها من الجرائم التي تهدد الأمن المعلوماتي للأفراد والدول⁴.

¹ - محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2010، ص 15.

² - عبد الفتاح بيومي حجازي، الجرائم الإلكترونية في التشريع المقارن، دار الفكر الجامعي، الإسكندرية، 2007، ص 22.

³ - أحمد شوقي الشلقاني، الجرائم المعلوماتية وإثباتها الجنائي، دار النهضة العربية، القاهرة، 2012، ص 41.

⁴ - عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، 2011، ص 88.

وقد أدى تزايد هذا النوع من الجرائم إلى بروز تحديات قانونية وقضائية كبيرة، خاصة في مجال الإثبات الجنائي، باعتبار أن الإثبات يمثل جوهر الدعوى الجزائية والأساس الذي تبنى عليه الأحكام القضائية¹. فالقواعد التقليدية للإثبات الجنائي أصبحت في كثير من الأحيان غير كافية للتعامل مع الجرائم السيبرانية، نظرًا لخصوصية الدليل الرقمي الذي يتميز بكونه غير مادي وقابلًا للتعديل أو الحذف بسهولة، مما يستوجب اعتماد وسائل تقنية وقانونية حديثة تتلاءم مع طبيعة البيئة الإلكترونية².

ومن هنا ظهر مفهوم الدليل الإلكتروني باعتباره من أهم وسائل الإثبات الحديثة في الجرائم السيبرانية، حيث أصبح يشكل عنصرًا أساسيًا في كشف الحقيقة وإثبات وقوع الجريمة ونسبتها إلى مرتكبها³. ويشمل الدليل الإلكتروني مختلف البيانات والمعلومات المخزنة أو المنقولة عبر الوسائط الرقمية، مثل الرسائل الإلكترونية، والسجلات الرقمية، والمحادثات الإلكترونية، وعناوين بروتوكول الإنترنت، والبيانات المستخرجة من الحواسيب والهواتف الذكية وغيرها⁴.

¹ - محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2013، ص 455.

² - محمد الأمين البشري، الإثبات الجنائي بالأدلة الرقمية، دار الكتب القانونية، مصر، 2015، ص 61.

³ - عبد الفتاح بيومي حجازي، الدليل الإلكتروني وحجته في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، 2008، ص 33.

⁴ - فيصل عبد الله الكندري، الجرائم الإلكترونية والتقنيات الحديثة للتحقيق الجنائي، منشورات الحلبي الحقوقية، بيروت، 2017، ص 74.

غير أن الاعتماد على الدليل الإلكتروني يثير العديد من الإشكالات القانونية والتقنية، خاصة فيما يتعلق بمدى حجته القانونية أمام القضاء، وشروط صحته، وطرق جمعه وتحليله، ومدى إمكانية التلاعب به أو المساس بسلامته¹. كما أن عملية الحصول على الأدلة الرقمية تستوجب اتباع إجراءات دقيقة تراعي احترام الحقوق والحريات الأساسية للأفراد، وفي مقدمتها الحق في الخصوصية وسرية المراسلات².

ولمواجهة هذه التحديات، اتجهت التشريعات الحديثة إلى تطوير منظومة الإثبات الجنائي بما يسمح بالاعتراف بالأدلة الرقمية وتنظيم إجراءات التعامل معها، وذلك من خلال سن نصوص قانونية خاصة بالجرائم الإلكترونية والإثبات الرقمي³. وفي هذا الإطار، سعى المشرع الجزائري إلى مواكبة التطورات التكنولوجية من خلال إصدار القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلى جانب إدخال تعديلات على قانون الإجراءات الجزائية وقانون العقوبات بما يتلاءم مع طبيعة الجرائم السيبرانية⁴.

كما أصبح للخبرة الفنية الرقمية دور بالغ الأهمية في مجال الإثبات السيبراني، حيث يعتمد القضاء بشكل متزايد على المختصين في تحليل الأدلة الرقمية واستخراج البيانات

¹ - مصطفى عبد الله كامل، حجية الدليل الإلكتروني في الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2016، ص 53.

² - محمد صبحي نجم، شرح قانون أصول المحاكمات الجزائية، دار الثقافة للنشر والتوزيع، عمان، 2014، ص 210.

³ - أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، دار النهضة العربية، القاهرة، 2016، ص 512.

⁴ - القانون رقم 04-09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية، العدد 47، سنة 2009.

الإلكترونية وتفسيرها¹. فالخبرة الرقمية تُمكن الجهات القضائية من فهم الجوانب التقنية للجريمة وتحديد كيفية وقوعها وربط الأدلة الرقمية بمرتكبيها، وهو ما يجعلها عنصراً أساسياً في تحقيق العدالة الجنائية في البيئة الإلكترونية².

إلى جانب ذلك، فإن الجرائم السيبرانية غالباً ما تتخذ طابعاً عابراً للحدود، الأمر الذي يجعل التعاون الدولي ضرورة حتمية لمكافحتها، سواء من خلال تبادل المعلومات أو تسليم المجرمين أو توحيد الجهود التقنية والقانونية بين الدول³. وقد ساهمت الاتفاقيات الدولية، وعلى رأسها اتفاقية بودابست لمكافحة الجرائم المعلوماتية، في وضع إطار قانوني دولي للتعاون في مجال مكافحة الجرائم الإلكترونية والإثبات الرقمي⁴.

وتبرز أهمية دراسة وسائل الإثبات القضائي في الجرائم السيبرانية في كونها تمثل الوسيلة الأساسية لتحقيق التوازن بين حماية المجتمع من الجرائم الإلكترونية وضمان حقوق الأفراد وحرياتهم الأساسية⁵. كما أن هذه الدراسة تكتسي أهمية علمية وعملية بالنظر إلى التطور السريع للتكنولوجيا وما يرافقه من تطور مستمر في أساليب ارتكاب الجرائم الإلكترونية، الأمر الذي يفرض على الأنظمة القانونية والقضائية مواكبة هذه المستجدات⁶.

¹ - عبد الحميد الشواربي، الخبرة الجنائية في الجرائم الإلكترونية، منشأة المعارف، الإسكندرية، 2018، ص 91.

² - محمد سعيد نمور، أصول الإجراءات الجزائية، دار الثقافة للنشر والتوزيع، عمان، 2015، ص 333.

³ - سامي عبد الحميد، التعاون الدولي في مكافحة الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2019، ص 119.

⁴ - اتفاقية بودابست بشأن الجرائم المعلوماتية لسنة 2001، المعتمدة من مجلس أوروبا بتاريخ 23 نوفمبر 2001.

⁵ - علي عبد القادر القهوجي، قانون العقوبات - القسم العام، منشورات الحلبي الحقوقية، بيروت، 2010، ص 67.

⁶ - عمر سالم، الحماية الجنائية للمعلومات عبر الإنترنت، دار النهضة العربية، القاهرة، 2014، ص 102.

وتتمثل إشكالية هذه الدراسة في التساؤل الرئيسي الآتي:

إلى أي مدى استطاعت وسائل الإثبات القضائي مواكبة خصوصية الجرائم السيبرانية وضمان فعاليتها في كشف الحقيقة وتحقيق العدالة الجنائية؟

ويتفرع عن هذه الإشكالية عدد من التساؤلات الفرعية، أهمها:

ما المقصود بالدليل الإلكتروني وما مدى حجيته القانونية؟

ما هي إجراءات جمع وتحليل الأدلة الرقمية؟

ما دور الجهات القضائية والخبرة الرقمية في الإثبات السيبراني؟

ما أبرز التحديات العملية التي تواجه الإثبات في الجرائم السيبرانية؟

وما هي الآفاق المستقبلية لتطوير الإطار القانوني والتقني للإثبات الرقمي؟

وللإجابة عن هذه الإشكالية تم الاعتماد على المنهج التحليلي من خلال تحليل النصوص القانونية المتعلقة بالإثبات الرقمي، إضافة إلى المنهج الوصفي لعرض المفاهيم التقنية المرتبطة بالأدلة الرقمية، والاستعانة بالمنهج المقارن من خلال الإشارة إلى بعض التشريعات والاتفاقيات الدولية ذات الصلة¹.

وقد تم تقسيم هذه الدراسة إلى فصلين رئيسيين، حيث تناول الفصل الأول وسائل الإثبات الرقمية في الجرائم السيبرانية، من خلال دراسة الدليل الإلكتروني وحجيته القانونية، وإجراءات

¹ - رمضان أبو السعود، أصول البحث العلمي في الدراسات القانونية، دار الجامعة الجديدة، الإسكندرية، 2011، ص 55.

جمع وتحليل الأدلة الرقمية. أما الفصل الثاني فقد خُصص لدراسة دور الجهات القضائية والخبرة الفنية في الإثبات السيبراني، إضافة إلى التحديات العملية والآفاق المستقبلية لتطوير وسائل الإثبات في الجرائم الإلكترونية.

الفصل الأول:

الإطار المفاهيمي والقانوني للإثبات في الجرائم السيبرانية

الفصل الأول: الإطار المفاهيمي والقانوني للإثبات في الجرائم السيبرانية

يُمثل الإثبات في مجال الجرائم السيبرانية أحد أخطر التحديات التي تواجه العدالة الجنائية المعاصرة، ذلك لأن هذه الجرائم تتم في فضاء رقمي غير مادي، وتتخذ أشكالاً متطورة تختلف جوهرياً عن الجرائم التقليدية¹. وإذ يسعى المشرع إلى ملاحقة مرتكبي هذه الأفعال الإجرامية وتقديمهم للعدالة، فإنه يصطدم بإشكاليات قانونية وتقنية تعيق كشف الحقيقة وإقامة الدليل². ومن هنا، تبرز الحاجة الملحة إلى فهم دقيق للإطار المفاهيمي لهذه الجرائم، واستقراء الأسس القانونية التي تحكم إثباتها، وذلك تمهيداً لتحليل آليات الإثبات الرقمي وسبل تطويرها.

ويتناول هذا الفصل الجوانب النظرية والقانونية المرتبطة بإثبات الجرائم السيبرانية، وذلك من خلال مبحثين رئيسيين: يعرض الأول منهما لمفهوم الجرائم السيبرانية وطبيعتها القانونية وخصائصها المؤثرة على الإثبات، بينما يحلّل الثاني الأساس القانوني للإثبات في هذا المجال، مستعرضاً قواعد الإثبات العامة في قانون الإجراءات الجزائية الجزائري، ثم النصوص الخاصة بالجرائم السيبرانية والدليل الرقمي.

¹ - بلعباس، مصطفى. "الدليل الرقمي كحجية للإثبات أمام القاضي الجزائري في المعاملات الإلكترونية". مجلة صوت القانون، المجلد 7، العدد 1، الصفحات 471-493. (ص 472).

² - زاوي، محمد الطاهر، "الجريمة الإلكترونية في ضوء اتفاقية بودابست: الإطار المفاهيمي والتصنيفي". مجلة البحوث القانونية والاقتصادية، المجلد 9، العدد 1، الصفحات 944-965. (ص 945).

المبحث الأول: مفهوم الجرائم السيبرانية

قبل الخوض في دراسة آليات الإثبات في الجرائم السيبرانية، يتعين الوقوف عند تحديد المفهوم الدقيق لهذه الجرائم، ذلك أن غموض المصطلحات أو تداخلها قد يؤدي إلى خلل في فهم طبيعة الإشكاليات القانونية المطروحة¹. ويشكل هذا المبحث مدخلاً نظرياً ضرورياً يهدف إلى تعريف الجرائم السيبرانية في الفقه والتشريع، ثم بيان طبيعتها القانونية، وتمييزها عن الجرائم التقليدية، وذلك في مطلب أول، يليه مطلب ثانٍ مخصص لخصائص هذه الجرائم وأثرها على عمليات الإثبات.

المطلب الأول: تعريف الجرائم السيبرانية وطبيعتها القانونية

يعد تحديد المقصود بالجرائم السيبرانية الخطوة المنهجية الأولى لفهم طبيعة الإشكالات التي تطرحها على مستوى الإثبات². وقد اختلفت آراء الفقهاء في تعريف هذه الجرائم، كما تعددت صياغات المشرعين لها، مما يستوجب عرضاً تحليلياً لهذه التعاريف، ثم بيان الطبيعة القانونية للجرائم السيبرانية، وأخيراً تمييزها عن الجرائم التقليدية.

الفرع الأول: تعريف الجرائم السيبرانية في الفقه والتشريع

أولاً: الإشكالات المصطلحية: لا يخلو موضوع الجرائم السيبرانية من إشكالات مصطلحية تعكس تطور الظاهرة وتشعبها³. فقد استعمل الفقه والمشرع عدة مصطلحات للإشارة إلى هذه الأفعال الإجرامية، منها "جرائم الحاسوب"، و"جرائم المعلوماتية"، و"جرائم الإنترنت"، و"الجرائم

¹ - زاوي محمد الطاهر، المرجع السابق، ص 946.

² - بلعباس مصطفى، المرجع السابق، ص 474.

³ - زاوي محمد الطاهر، المرجع السابق، ص 948.

الإلكترونية"، و"الجرائم الرقمية"، و"جرائم تكنولوجيا المعلومات والاتصال"¹. ويعود هذا التعدد إلى عاملين رئيسيين: أولهما تطور الوسائل التقنية المستخدمة في ارتكاب الجريمة، وثانيهما تعدد زوايا النظر إلى هذه الظاهرة².

غير أن المصطلح الأكثر شيوعاً في الوقت الراهن هو "الجرائم السيبرانية" (Cybercrime)، وهو مصطلح مشتق من كلمة "سايبير" (Cyber) التي تعني الفضاء الإلكتروني³. ويمتاز هذا المصطلح بشموليته النسبية، إذ يشير إلى كافة الأفعال غير المشروعة التي تستهدف أو تستخدم نظم المعلومات أو شبكات الاتصال⁴.

ثانياً: التعريف الفقهي: اختلف الفقه في تعريف الجرائم السيبرانية وفق منظورين أساسيين، يمكن إجمالهما على النحو التالي:

1- المنظور الضيق: يقتصر هذا المنظور على الأفعال التي تستهدف نظم المعلومات والبيانات المعالجة آلياً بوصفها محلاً للاعتداء⁵. فالجريمة السيبرانية، وفق هذا التصور، هي "كل سلوك غير مشروع يقع على نظام المعلومات أو البيانات المخزنة فيه أو المتبادلة عبر شبكات الحاسوب"⁶. وتندرج تحت هذا التعريف الجرائم التي لا يمكن ارتكابها إلا باستخدام

¹ - القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 47، 16 غشت 2009.

² - القانون رقم 04-09، المرجع السابق، المادة الثانية.

³ - زاوي محمد الطاهر، المرجع السابق، ص 950.

⁴ - بلعباس مصطفى، المرجع السابق، ص 475.

⁵ - عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، ديوان المطبوعات الجامعية، الجزائر، 2018، ص 112.

⁶ - أحمد فتحي سرور، الوسيط في قانون العقوبات، دار النهضة العربية، القاهرة، 2016، ص 245.

الحاسوب أو شبكاته، كالاختراق غير المشروع لنظم المعلومات، وتعطيل المواقع الإلكترونية، والتجسس المعلوماتي¹.

2- المنظور الواسع: يتسع هذا المنظور ليشمل كل فعل إجرامي تستخدم فيه وسائل تكنولوجيا المعلومات والاتصال كأداة لارتكاب الجريمة، سواء كان هذا الفعل موجهاً ضد نظام معلوماتي أم لا². فالجريمة السيبرانية، بهذا المعنى، هي "كل سلوك غير مشروع يرتكب باستخدام الحاسوب أو الشبكة المعلوماتية، أو يقع على الحاسوب أو الشبكة المعلوماتية"³. ويشمل هذا التعريف جرائم مثل الاحتيال عبر الإنترنت، وانتحال الشخصية، والابتزاز الإلكتروني، ونشر المحتويات غير المشروعة⁴.

ويرى جانب من الفقه أن المنظور الواسع هو الأقرب إلى الواقع العملي، ذلك أن الجاني قد يستخدم الوسائل الرقمية لارتكاب جرائم تقليدية كالسرقة والسب والقتل، مما يستوجب إخضاع هذه الأفعال لنظام قانوني يراعي خصوصية البيئة الرقمية⁵.

ثالثاً: التعريف التشريعي في القانون الجزائري: تبني المشرع الجزائري تعريفاً موسعاً للجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، وذلك في القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، والمتضمن القواعد الخاصة للوقاية من هذه الجرائم

¹ - القانون رقم 25-14 المؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، عدد 54، 3 أوت 2025.

² - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المعتمدة في ديسمبر 2024، المادة الثانية.

³ - محمود نجيب حسني، شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 2015، .310.

⁴ - Robert chesmey, cybercrime and the law, Oxford Université press, 2018,p54.

⁵ - زاوي محمد الطاهر، المرجع السابق، ص 955.

ومكافحتها¹. تنص المادة الثانية من هذا القانون على أن المقصود بهذه الجرائم هو: "الجرائم المساس بأنظمة المعالجة الآلية للبيانات كما هي معرّفة بموجب قانون العقوبات، وكذا كل جريمة أخرى تُرتكب أو يُسهّل ارتكابها بواسطة نظام معلوماتي أو نظام اتصال إلكتروني"².

وقد جاء هذا التعريف جامعاً بين شقي التعريف الفقهي: الضيق والواسع. فالشق الأول منه يتعلق بالجرائم المساس بأنظمة المعالجة الآلية للبيانات (المنظور الضيق)، بينما الشق الثاني يشمل كل جريمة يسهل ارتكابها باستخدام نظام معلوماتي أو نظام اتصال إلكتروني (المنظور الواسع)³.

رابعاً: تعريف الجريمة السيبرانية في الاتفاقيات الدولية: على المستوى الدولي، تبنّت اتفاقية بودابست لمكافحة الجريمة المعلوماتية لسنة 2001 مقارنة تقوم على تعداد الأفعال الإجرامية بدلاً من تقديم تعريف جامع⁴. وقد صنفت الاتفاقية الجرائم المعلوماتية في أربع فئات رئيسية: جرائم تتعلق بسرقة وسلامة واستعمال نظم المعلومات (كالوصول غير المشروع، والاعتراض غير المشروع)، والجرائم المرتبطة بالحاسوب (كتزوير البيانات المعلوماتية واحتيال الحاسوب)، والجرائم المتصلة بالمحتوى (كجرائم تتعلق بالأطفال)، والجرائم المتعلقة بانتهاك حقوق المؤلف والحقوق المجاورة⁵.

¹ - بلعباس مصطفى، المرجع السابق ص 480.

² - زاوي محمد الطاهر، المرجع السابق، ص 957.

³ - القانون رقم 09-04 المرجع السابق، المادة الثالثة.

⁴ - بلعباس مصطفى، المرجع السابق، ص 482.

⁵ - زاوي محمد الطاهر، المرجع السابق، ص 960.

أما اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية التي اعتمدت في ديسمبر 2024، والتي وقعت عليها الجزائر في 25 أكتوبر 2025، فقد عرفت في مادتها الثانية "نظام تكنولوجيا المعلومات والاتصالات" بأنه "أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة التي يقوم واحد منها أو أكثر، وفقاً لبرنامج ما، بجمع وتخزين بيانات إلكترونية ومعالجتها آلياً"، وعرفت "البيانات الإلكترونية" بأنها "أي تمثيل لحقائق أو معلومات أو مفاهيم في شكل يتيح معالجتها في نظام تكنولوجيا معلومات واتصالات"¹.

الفرع الثاني: الطبيعة القانونية للجرائم السيبرانية

تشير الجرائم السيبرانية إشكالات قانونية تتعلق بتحديد طبيعتها، وهل هي جرائم مستقلة بذاتها تستوجب تنظيمًا خاصاً، أم أنها تندرج ضمن الأصناف التقليدية للجرائم (جنايات، جنح، مخالفات)².

أولاً: استقلالية الجرائم السيبرانية: يذهب جانب من الفقه إلى القول باستقلالية الجرائم السيبرانية، وذلك للأسباب التالية³:

1. اختلاف محل الجريمة: فمحل الجريمة السيبرانية هو البيانات والمعلومات ذات الطابع غير المادي، بينما محل الجريمة التقليدية هو الأشياء والأموال المادية⁴. وهذا الاختلاف ينعكس على طبيعة الإثبات ووسائله.

¹ - القانون رقم 14-25 المرجع السابق ، المواد من 1 إلى 5.

² - القانون رقم 14-25 المرجع السابق ، المادة الأولى.

³ - القانون رقم 14-25، المرجع السابق ، المادة الثالثة.

⁴ - زاوي محمد الطاهر، المرجع السابق ، ص 962.

2. اختلاف كيفية ارتكاب الجريمة: تتم الجريمة السيبرانية في بيئة رقمية لا تعترف بالحدود الجغرافية، ويمكن ارتكابها عن بُعد ودون حاجة إلى تواجد مادي للجاني في مسرح الجريمة¹.

3. صعوبة إخضاعها للقواعد التقليدية: أظهرت القواعد التقليدية في قانون العقوبات والإجراءات الجزائية قصوراً في مواجهة الجرائم السيبرانية، مما استوجب تدخلاً تشريعياً خاصاً².
غير أن هذا الاتجاه ليس بمنأى عن الانتقادات، ذلك أن استقلالية الجرائم السيبرانية لا تعني انفصالها التام عن المفاهيم الجنائية العامة، بل إنها لا تزال تستند إلى نفس المبادئ (كشرعية الجرائم والعقوبات، والمسؤولية الجزائية، والركن المعنوي)³.

ثانياً: طبيعة الجرائم السيبرانية في القانون الجزائري: لم يخرج المشرع الجزائري عن التقسيم الثلاثي التقليدي للجرائم (جنايات، جنح، مخالفات) عند تجريم الأفعال السيبرانية⁴. فقد وزع هذه الأفعال في قانون العقوبات وفي القانون 04-09 بحسب شدة العقوبة المقررة لكل فعل⁵.

فعلى سبيل المثال، يعاقب على جريمة الدخول غير المشروع إلى نظام معالجة آلي للبيانات بغرامة فقط (مخالفة أو جنحة بسيطة)، بينما يعاقب على جريمة عرقلة سير النظام

¹ - بلعباس مصطفى، المرجع السابق ، ص 484.

² - القانون رقم 04-09 المرجع السابق ، المادة الثالثة.

³ - القانون رقم 04-09 المرجع السابق ، المادة الرابعة.

⁴ - القانون رقم 14-25 المرجع السابق ، المادة 120.

⁵ - بلعباس مصطفى، المرجع السابق ، ص 486.

المعلوماتي بالسجن (جنحة أو جناية بحسب النتيجة المترتبة)¹. وهذا يعني أن الجريمة السيبرانية - في القانون الجزائري - ليست نوعاً مستقلاً من الجريمة يتجاوز التقسيم الثلاثي، بل هي "وصف" لفعل إجرامي وقع في بيئة رقمية، يظل خاضعاً لتصنيفه وفقاً للعقوبة المقررة له².

وتأسيساً على ما تقدم، يمكن القول إن الطبيعة القانونية للجرائم السيبرانية هي طبيعة مزدوجة: فهي من ناحية تخضع للمبادئ العامة للقانون الجنائي (كالعقاب الشخصي، وشرعية الجرائم والعقوبات)، ومن ناحية أخرى تتصف بخصوصيات تستوجب معاملة قانونية مختلفة فيما يتعلق بوسائل الإثبات وقواعد الاختصاص القضائي والتعاون الدولي³.

إذا كان تحديد مفهوم الجرائم السيبرانية يثير صعوبة على مستوى الفقه والتشريع بسبب اتساع نطاقها وتعدد صورها، فإن هذه الصعوبة تتضاعف عند محاولة ضبط طبيعتها القانونية، ذلك أن هذا النوع من الجرائم لا يخضع للمنطق التقليدي للجريمة كما استقر في القانون الجنائي الكلاسيكي، بل يقوم على منطق رقمي افتراضي تتداخل فيه الوسيلة بالنتيجة، والمكان بالزمان، والفاعل بالفعل، مما يجعلها جرائم ذات بنية مركبة ومعقدة في آن واحد⁴. وتكمن أهمية دراسة الطبيعة القانونية للجرائم السيبرانية في كونها المدخل الأساسي لفهم كيفية التعامل معها إجرائياً، خاصة في مجال الإثبات، إذ إن اختلاف طبيعتها يفرض بالضرورة اختلافاً في وسائل الإثبات وأساليبه، وهو ما دفع العديد من التشريعات المقارنة إلى إفراد تنظيم خاص بها أو إدخال تعديلات على القواعد العامة للقانون الجنائي لتتلاءم مع خصوصيتها

¹ - زاوي محمد الطاهر، المرجع السابق، ص 965.

² - بلعباس مصطفى، المرجع السابق، ص 488.

³ - اتفاقية بودابست لمكافحة الجريمة المعلوماتية (2001)، المواد من 14 إلى 21.

⁴ - محمود نجيب حسني، شرح قانون العقوبات - القسم العام، دار النهضة العربية، القاهرة، 2015، ص 315.

التقنية.

وفي هذا السياق، يرى جانب من الفقه أن الجرائم السيبرانية تمثل نمطاً جديداً من "الإجرام الذكي"، لأنها تعتمد على المعرفة التقنية العالية وتوظيف الوسائل الرقمية بطريقة دقيقة ومنظمة، مما يجعلها تختلف جذرياً عن الجرائم التقليدية التي تعتمد غالباً على القوة المادية أو الوسائل المباشرة¹. كما أن هذا النوع من الجرائم لا يتطلب بالضرورة وجود انتهاك مادي بين الجاني والضحية، وهو ما يعزز طابعها الافتراضي ويزيد من صعوبة ضبطها قانونياً.

ومن الخصائص البارزة أيضاً أن الجرائم السيبرانية تتسم بما يمكن تسميته بـ "تداخل الحدود القانونية"، حيث يمكن أن ينطلق الفعل الإجرامي من دولة معينة، بينما تقع النتيجة في دولة أخرى، ويتم تخزين الأدلة في دولة ثالثة، وهو ما يخلق حالة من التشتت القانوني الذي يصعب معه تحديد القانون الواجب التطبيق أو المحكمة المختصة، ويجعل من التعاون الدولي في المجال الجنائي ضرورة ملحة².

كما أن هذه الجرائم تتميز بكونها قابلة للتطور المستمر، إذ أن التطور التكنولوجي السريع يؤدي إلى ظهور صور جديدة من السلوك الإجرامي لم تكن معروفة سابقاً، مثل جرائم الفدية الإلكترونية (Ransomware) أو الاحتيال عبر الذكاء الاصطناعي أو التلاعب بالخوارزميات، وهو ما يجعل الطبيعة القانونية لهذه الجرائم في حالة "ديناميكية دائمة" لا تستقر على شكل واحد.

¹- عبد الفتاح بيومي حجازي، الجريمة المعلوماتية في التشريع المقارن، دار الفكر الجامعي، الإسكندرية، 2017، ص 88.

²- محمد زكي أبو عامر، قانون العقوبات الدولي، دار الجامعة الجديدة، الإسكندرية، 2019، ص 142.

ومن جهة أخرى، فإن الجرائم السيبرانية تطرح إشكالية مهمة تتعلق بعنصر الزمن في القانون الجنائي، إذ أن الفعل الإجرامي قد يتم في جزء من الثانية، بينما تمتد آثاره لفترة طويلة، مما يثير تساؤلاً حول اللحظة القانونية لقيام الجريمة، هل هي لحظة الدخول غير المشروع للنظام المعلوماتي أم لحظة تحقق الضرر أم استمرار التأثير؟ وهي مسألة ما تزال محل نقاش فقهي وقضائي واسع¹ وتجدر الإشارة أيضاً إلى أن هذه الجرائم غالباً ما ترتبط بمفهوم "النية التقنية" أو القصد المعلوماتي، حيث لا يكفي مجرد استعمال الوسيلة الرقمية لقيام الجريمة، بل يجب أن تتجه إرادة الجاني إلى تحقيق نتيجة غير مشروعة عبر النظام المعلوماتي، وهو ما يعقد عملية الإثبات ويجعلها تعتمد بشكل كبير على تحليل السلوك الرقمي للجاني بدل الأدلة المادية التقليدية.

الفرع الثالث: تمييز الجرائم السيبرانية عن الجرائم التقليدية

يُعد تمييز الجرائم السيبرانية عن الجرائم التقليدية خطوة منهجية ضرورية لفهم طبيعة التحديات التي تطرحها هذه الجرائم على مستوى الإثبات². ويمكن إجمال أوجه التمايز بين الفئتين كما يلي:

أولاً: من حيث محل الجريمة: محل الجريمة التقليدية هو الأشياء المادية المحسوسة التي يمكن رؤيتها ولمسها، كالأموال المنقولة والعقارات والأشخاص³. أما محل الجريمة السيبرانية، فهو في الغالب غير مادي، ويتعلق بالبيانات والمعلومات المخزنة إلكترونياً، أو بحرمة النظم

¹ -حمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2016، ص 203.

² - اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق، المواد من 25 إلى 32.

³ - محمد نجيب حسني، المرجع السابق، ص 322.

المعلوماتية ذاتها¹. وهذا التمايز يستتبع اختلافاً في كيفية ارتكاب الجريمة وآليات اكتشافها وإثباتها.

ثانياً: من حيث مكان وزمان ارتكاب الجريمة: تتم الجريمة التقليدية في مكان مادي محدد (كمسرح جريمة القتل أو السرقة)، ويرتبط زمانها بلحظة مادية معينة². أما الجريمة السيبرانية، فيمكن أن يرتكبها شخص موجود في بلد ضد شخص أو نظام موجود في بلد آخر، في زمن يستحيل معه الجزم بال لحظة الدقيقة للفعل الإجرامي³. يقول أحد الباحثين في هذا الصدد: "إن الجريمة السيبرانية لا تعترف بالحدود الجغرافية التقليدية، بل تمتد عبر القارات في ثوان معدودة، مما يصعب مهمة تحديد السلطة القضائية المختصة"⁴.

ثالثاً: من حيث مرتكب الجريمة: قد يكون مرتكب الجريمة التقليدية أي شخص تتوافر فيه الأهلية الجزائية، وغالباً ما يترك أثراً مادية في مسرح الجريمة (كالبصمات، والحمض النووي)⁵. أما مرتكب الجريمة السيبرانية، فغالباً ما يكون ذا مهارات تقنية متقدمة، وقد يستخدم وسائل إخفاء متطورة (كالشبكات الافتراضية الخاصة، والتشغيل عبر خوادم وسيطة) تصعب عملية التعرف عليه وتحديد هويته⁶.

رابعاً: من حيث الإثبات: يعتمد إثبات الجريمة التقليدية على الأدلة المادية التقليدية (الشهادات، المحاضر، التقارير الفنية، المعاينات)، بينما يعتمد إثبات الجريمة السيبرانية على

¹-زاوي محمد الطاهر، المرجع السابق، ص 968.

²-بلعباس مصطفى، المرجع السابق، ص 490.

³-زاوي محمد الطاهر، المرجع السابق، ص 970.

⁴- اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق.

⁵- اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق، المواد 8 إلى 12.

⁶- محمد نجيب حسني، المرجع السابق، ص 210.

الأدلة الرقمية التي تتميز بقابليتها للتلف والتغيير والعبث¹. كما أن إثبات الجريمة السيبرانية يتطلب خبراء في المجال التقني، وغالباً ما تتوقف نتائج الدعوى على تقاريرهم الفنية².

خامساً: من حيث الضرر: قد يكون ضرر الجريمة التقليدية محدوداً ومادياً (كفقدان مبلغ من المال أو التعرض لإصابة جسدية)، بينما قد يكون ضرر الجريمة السيبرانية واسع الانتشار وغير مادي (كالاعتداء على الخصوصية، والتشهير، وسرقة الهوية، وتعطيل خدمات أساسية)³.

إن التمييز بين الجرائم السيبرانية والجرائم التقليدية لا يقتصر فقط على اختلاف الوسيلة، بل يمتد إلى اختلاف فلسفة التجريم ذاتها، إذ إن الجرائم التقليدية تقوم على فكرة الاعتداء المادي المباشر على الأشخاص أو الأموال أو النظام العام، في حين تقوم الجرائم السيبرانية على الاعتداء على "المعلومة" باعتبارها قيمة قانونية مستقلة، وهو تحول جوهري في الفكر الجنائي الحديث⁴.

فالجرائم التقليدية تتطلب في الغالب وجود اتصال مادي بين الجاني والمجني عليه، مثل السرقة التي تستلزم الاستيلاء المادي على الشيء، أو الضرب الذي يتطلب تماساً جسدياً، بينما في الجرائم السيبرانية يتم الاعتداء دون أي تماس مادي مباشر، بل عبر أوامر رقمية أو برمجيات خبيثة يتم تنفيذها عن بعد، وهو ما يخلق قطيعة مع المفهوم التقليدي للجريمة. كما أن عنصر الإثبات في الجرائم التقليدية يعتمد على وسائل حسية ملموسة مثل البصمات أو

¹ - زاوي محمد الطاهر، المرجع السابق، ص 972.

² - بلعباس مصطفى، المرجع السابق، ص 492.

³ - القانون رقم 09-04 المرجع السابق، المادة 12.

⁴ - Robert Chesney, Cybercrime and the Law, Oxford University Press, 2018, p. 54.

الشهود أو المعاينة، بينما يعتمد في الجرائم السيبرانية على أدلة رقمية غير مرئية مثل سجلات الخوادم، البيانات الوصفية (Meta data) ، وعناوين الاتصال، وهي أدلة تتطلب خبرة تقنية متخصصة لفهمها وتفسيرها، مما يجعل القاضي في هذه القضايا أكثر اعتماداً على الخبرة التقنية مقارنة بالقضايا التقليدية¹

ومن الفوارق الجوهرية كذلك أن الجرائم التقليدية غالباً ما تكون محدودة النطاق من حيث المكان، إذ تقع في نطاق جغرافي محدد، بينما الجرائم السيبرانية تتميز بالعالمية المطلقة، حيث يمكن للجاني أن يكون في دولة، والضحية في دولة أخرى، والخادم في دولة ثالثة، مما يجعلها جرائم "عابرة للسيادة".

إضافة إلى ذلك، فإن الجرائم السيبرانية تتميز بقدرتها العالية على الإخفاء والتخفي، إذ يستخدم الجناة أدوات تقنية مثل التشفير وإخفاء الهوية (Anonymisation) والشبكات المظلمة (Dark Web)، مما يجعل تتبعهم أكثر تعقيداً مقارنة بالجرائم التقليدية التي تترك آثاراً مادية واضحة.

وبالتالي، فإن هذا التمييز لا يهدف فقط إلى الجانب النظري، بل له آثار عملية مباشرة على مستوى الإثبات الجنائي، حيث يستوجب تطوير وسائل تحقيق رقمية متخصصة قادرة على التعامل مع الطبيعة غير المادية لهذه الجرائم، وهو ما بدأ المشرع الجزائري في التوجه إليه تدريجياً من خلال إدخال قواعد تتعلق بالدليل الإلكتروني²

¹ - عبد الله سليمان، شرح قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2018، ص 277.

² - القانون رقم 04-09، المرجع السابق

المطلب الثاني: خصائص الجرائم السيبرانية وأثرها على الإثبات

تتصف الجرائم السيبرانية بخصائص تميزها عن غيرها من الجرائم، وتؤثر هذه الخصائص بشكل كبير على عمليات البحث والتحري والإثبات¹. ويمكن إجمال هذه الخصائص في ثلاث خصائص رئيسية: الطابع الرقمي وغير المادي للجريمة، والسرعة والعالمية في ارتكاب الجريمة، وصعوبة تحديد الفاعل ومكان الجريمة.

الفرع الأول: الطابع الرقمي وغير المادي للجريمة

أولاً: طبيعة الدليل الرقمي: إن أهم ما يميز الجريمة السيبرانية هو طابعها الرقمي غير المادي². فكيان الجريمة بأكمله - أدواتها، مسرحها، وآثارها - يتخذ شكلاً رقمياً. فالمعتدى عليه قد يكون موقعاً إلكترونياً أو حساباً مصرفياً أو ملفات وبيانات مخزنة على خادم معلوماتي³. والسلوك الإجرامي يتمثل في تدفقات بيانات وأوامر برمجية لا تُرى ولا تُلمس. وحتى "آثار الجريمة"، التي تشكل جوهر الإثبات الجنائي التقليدي، تتخذ شكلاً رقمياً يتجسد في سجلات الاتصالات وبيانات الدخول وسجلات النظام، وهي بطبيعتها غير مادية يصعب إدراكها بالحواس⁴.

وهذا الطابع غير المادي يمثل إشكالية حقيقية للإثبات، ذلك أن مفهوم "مسرح الجريمة" التقليدي، الذي يقتضي وجود مكان مادي يمكن معاينته ورفع الآثار منه، يصبح مفهوماً غير

¹ - القانون رقم 25-14 المرجع السابق، المادة 150.

² - بلعباس مصطفى، المرجع السابق، ص 491.

³ - زاوي محمد الطاهر، المرجع السابق، ص 973.

⁴ - القانون رقم 09-04، المرجع السابق، المادة 15.

ملائم في البيئة الرقمية¹. يمكن القول إن "مسرح الجريمة" في الجرائم السيبرانية يمتد ليشمل عدة مواقع: جهاز الجاني، والخوادم الوسيطة، والخادم المستهدف، وسجلات مقدمي الخدمة². وهذا التوزع المكاني يعقد مهمة ضبط الدليل والحفاظ عليه.

ثانياً: هشاشة الدليل الرقمي: تتسم الأدلة الرقمية بدرجة عالية من الهشاشة، فهي قابلة للتلف أو التغيير أو الإتلاف بسهولة³. فمجرد تشغيل جهاز الحاسوب المتعلق بالجريمة قد يؤدي إلى تعديل "الطابع الزمني" للملفات أو مسح بعض البيانات الحيوية⁴. وهذا الوضع يتطلب تدخلاً فورياً من مختصين في المجال التقني لضبط الدليل الرقمي والحفاظ على سلامته، وبالتالي ضمان مقبوليته أمام القضاء⁵.

ويلاحظ أن هذه الخاصية تفرض على أعضاء الشرطة القضائية، الذين اعتادوا على جمع الأدلة المادية، ضرورة اكتساب مهارات تقنية جديدة، وإلا فإنهم معرضون لخطر إتلاف الدليل أثناء جمعه⁶. وقد أشارت المادة الثالثة من القانون 04-09 إلى إمكانية "إجراء عمليات مراقبة للاتصالات الإلكترونية، وجمع محتواها وتسجيله في وقت حقيقي، وكذا إجراء تفتيش وحجز في

¹ - القانون رقم 25-14، المرجع السابق، المادة 160.

² - بلعباس مصطفى، المرجع السابق، ص 493.

³ - زاوي محمد الطاهر، المرجع السابق، ص 975.

⁴ - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق، المادة 40.

⁵ - محمد نجيب حسني، المرجع السابق، ص 148.

⁶ - بلعباس مصطفى، المرجع السابق، ص 472.

نظام معلوماتي"¹، غير أن النص القانوني وحده لا يكفي، بل لا بد من تكوين تقني متخصص لتنفيذ هذه الإجراءات².

الفرع الثاني: السرعة والعالمية في ارتكاب الجريمة

أولاً: تجاوز الحدود الوطنية: تتميز الجرائم السيبرانية بقدرتها على تجاوز الحدود الجغرافية في زمن قياسي، بفضل شبكات الإنترنت والاتصالات الحديثة التي تنقل البيانات بين القارات في أجزاء من الثانية³. هذه الخاصية تطرح إشكالية قانونية كبرى تتعلق بتحديد القانون الواجب التطبيق والسلطة القضائية المختصة⁴.

فإذا ارتكب شخص جريمة سيبرانية من بلد (أ) ضد نظام معلوماتي في بلد (ب)، مروراً بخوادم في بلد (ج)، واستقرت آثار الجريمة في بلد (د)، فأى هذه الدول تملك الاختصاص القضائي؟ هل الدولة التي انطلق منها الهجوم؟ أم الدولة التي وقع فيها الضرر؟ أم الدولة التي عبرتها البيانات أثناء انتقالها؟⁵

لقد حاولت القواعد التقليدية للاختصاص القضائي (كقاعدة الإقليمية، وشخصية الجاني أو المجني عليه) الإجابة عن هذه الأسئلة، غير أن تطبيقها الصارم على الجريمة السيبرانية قد يؤدي إلى نتائج غير مرضية، ذلك أن الجريمة الواحدة قد تخضع لاختصاص عدة دول، مما يخلق نزاعات إيجابية أو سلبية للاختصاص⁶.

¹ - زاوي محمد الطاهر، المرجع السابق، ص 945.

² - بلعباس مصطفى، المرجع السابق، ص 474.

³ - زاوي محمد الطاهر، المرجع السابق، ص 948.

⁴ - القانون رقم 04-09 المرجع السابق.

⁵ - القانون رقم 14-25 المرجع السابق.

⁶ - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق.

ثانياً: صعوبة التعاون الدولي: إن عالمية الجريمة السيبرانية تستلزم تعاوناً دولياً سريعاً وفعالاً لتبادل الأدلة وتحديد مكان الجاني وربما تسليمه¹. غير أن آليات التعاون التقليدية (كالإنابات القضائية) تتصف بالبطء، وقد تستغرق شهوراً أو سنوات، مما يتعارض مع طبيعة الدليل الرقمي الذي قد يتلف أو يُعَدَّل في غضون أيام أو حتى ساعات².

ولهذا السبب، ركزت الاتفاقيات الدولية، كاتفاقية بودابست واتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، على ضرورة إنشاء شبكات تعاون سريع بين السلطات الوطنية، تشمل إمكانية تقديم طلبات الحصول على الأدلة على مدار الساعة، والتعاون "العفوي" أي دون انتظار طلب رسمي³. ومع ذلك، تظل الفروق بين التشريعات الوطنية عقبة رئيسية أمام التعاون الفعال، إذ تختلف الدول في تعريفها للجريمة السيبرانية، وفي الضمانات الإجرائية التي تفرضها على جمع الأدلة الرقمية⁴.

الفرع الثالث: صعوبة تحديد الفاعل ومكان الجريمة

أولاً: إشكالية إثبات هوية الفاعل: تمثل مسألة تحديد الفاعل في الجرائم السيبرانية تحدياً كبيراً للأجهزة القضائية، وذلك للأسباب التالية⁵:

1. عدم وجود اتصال مادي بين الجاني والضحية: يمكن ارتكاب الجريمة السيبرانية دون أي لقاء أو اتصال مباشر بين الجاني والضحية، مما يحرم المحققين من وسائل الإثبات التقليدية كشهادة الضحية أو معاينتها للجاني¹.

¹ - بلعباس مصطفى، المرجع السابق ، ص 476.

² - زاوي محمد الطاهر، المرجع السابق ، ص 950.

³ - القانون رقم 09-04 المرجع السابق ، المادة الثانية.

⁴ - بلعباس مصطفى، المرجع السابق ، ص 478.

⁵ - زاوي محمد الطاهر، المرجع السابق ، ص 952.

2. استخدام وسائل إخفاء الهوية: يستخدم مرتكبو الجرائم السيبرانية وسائل متطورة لإخفاء هوياتهم، كاستخدام الشبكات الافتراضية الخاصة (VPN) التي تخفي عنوان الآي بي الحقيقي، أو اختراق أجهزة الغير واستخدامها كـ "دمى" لشن الهجمات، أو استخدام شبكة "تور" (TOR) التي تجعل تتبع النشاط الإلكتروني شبه مستحيل².

3. صعوبة ربط النشاط الإلكتروني بشخص معين: حتى لو نجحت السلطات في تحديد عنوان الآي بي المستخدم في ارتكاب الجريمة، فإن هذا لا يعني بالضرورة تحديد هوية الشخص الذي ارتكبها. فقد يكون الجهاز مخترقاً، أو مستخدماً من قبل عدة أشخاص، أو يكون الجاني قد استخدم نقطة وصول لاسلكية مفتوحة³.

ثانياً: إشكالية تحديد مكان الجريمة: ترتبط الإشكالية السابقة بإشكالية تحديد مكان الجريمة، التي تشكل بدورها شرطاً لتحديد السلطة القضائية المختصة⁴. في الفضاء السيبراني، يصبح مفهوم "المكان" نسبياً وغير مستقر، ذلك أن جريمة واحدة - كالاختراق - قد يرتكبها شخص جالس في مقهى إنترنت بالجزائر العاصمة، ضد خادم موجود في أمريكا، وتظهر آثارها على حواسيب مستخدمين في فرنسا وبريطانيا. فأى من هذه المواقع يعتبر "مكان ارتكاب الجريمة"⁵؟

¹ - القانون رقم 14-25، المرجع السابق، المواد من 1 إلى 5.

² - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق، المادة الثانية.

³ - محمد نجيب حسني، المرجع السابق، ص 233.

⁴ - بلعباس مصطفى، المرجع السابق، ص 480.

⁵ - زاوي محمد الطاهر، المرجع السابق، ص 955.

لقد تباينت الحلول الفقهية والقضائية لهذه الإشكالية. فمنهم من يرى أن مكان ارتكاب الجريمة هو المكان الذي يوجد فيه الجاني وقت ارتكاب الفعل المادي (نظرية الفعل). ومنهم من يرى أنه المكان الذي تتحقق فيه النتيجة الإجرامية (نظرية النتيجة). ومنهم من يتبنى نظرية "الوجود الممتد" التي تقول إن الجاني موجود - افتراضاً - في كل مكان تصل إليه أفعاله الإجرامية¹. وقد أخذت بعض التشريعات، ومنها التشريع الجزائري، بنظرية النتيجة، مما يعني أن القضاء الجزائري يعتبر مختصاً إذا وقع أثر الجريمة في الجزائر، بغض النظر عن مكان وجود الجاني وقت ارتكاب الفعل².

ولكن هذا الحل ليس مثالياً، إذ قد يؤدي إلى تضخيم الاختصاص القضائي للدول، حيث قد تصبح أي جريمة سيبرانية ذات تأثير عالمي خاضعة لاختصاص عشرات الدول، مما يخلق حالة من عدم اليقين القانوني ويعرقل الملاحقة الجنائية الفعالة³.

إن صعوبة تحديد الفاعل في الجرائم السيبرانية تُعد من أخطر الإشكالات التي تواجه العدالة الجنائية الحديثة، ذلك أن البيئة الرقمية تسمح بقدر كبير من التخفي وإخفاء الهوية، مما يجعل الجاني في كثير من الأحيان غير مرئي قانونياً رغم كونه فاعلاً فعلياً للجريمة. فالتقنيات الحديثة مثل الشبكات الافتراضية الخاصة (VPN)، وخوادم البروكسي، وتقنيات التشفير المتقدم، إضافة إلى استخدام الحسابات الوهمية أو المسروقة، كلها وسائل تتيح للجاني قطع الصلة الظاهرة بين الفعل الإجرامي وهويته الحقيقية، وهو ما يعقد بشكل كبير عملية الإثبات

¹ - القانون رقم 09-04، المرجع السابق، المادة الثالثة.

² - القانون رقم 25-14 المرجع السابق، المادة الأولى.

³ - بلعباس مصطفى، المرجع السابق، ص 482.

الجنائي¹

ويترتب على ذلك أن سلطة التحقيق لم تعد تعتمد فقط على الوسائل التقليدية في تحديد هوية الجاني، بل أصبحت تعتمد على ما يسمى بالأثر الرقمي“ أو “البصمة الإلكترونية“، وهي مجموعة من البيانات التقنية التي يتركها المستخدم أثناء تفاعله مع النظام المعلوماتي، مثل عنوان بروتوكول الإنترنت (IP) وسجلات الدخول (Logs) وبيانات الجهاز المستخدم. غير أن هذه الأدلة تبقى في كثير من الأحيان غير كافية بمفردها لإثبات الهوية بشكل قاطع، نظراً لإمكانية التلاعب بها أو إخفائها أو حتى نسبتها إلى غير الفاعل الحقيقي².

كما أن إشكالية تحديد الفاعل تتعدّد أكثر في ظل ما يُعرف بالإجرام العابر للوسيط“، حيث يتم تنفيذ الجريمة عبر عدة مراحل تقنية موزعة على أكثر من جهاز وأكثر من دولة، مما يجعل تتبع السلسلة الرقمية للجريمة أمراً في غاية الصعوبة، ويستلزم خبرات تقنية عالية المستوى قد لا تكون متوفرة لدى أجهزة التحقيق التقليدية. ومن هنا تظهر الحاجة إلى تطوير منظومة التحقيق الجنائي الرقمي بما يتناسب مع طبيعة هذا النوع من الجرائم.

أما من حيث تحديد مكان ارتكاب الجريمة، فإن الجرائم السيبرانية تطرح إشكالاً قانونياً بالغ التعقيد، ذلك أن الفعل الإجرامي يتم في فضاء افتراضي لا يخضع لمفهوم المكان المادي التقليدي. فالجريمة قد تُرتكب من جهاز موجود في دولة معينة، بينما يكون الخادم المستهدف

¹—عبد الفتاح بيومي حجازي، الدليل الرقمي في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، 2018، ص 63.

²—محمد عيد الغريب، الإثبات الجنائي الحديث، دار النهضة العربية، القاهرة، 2017، ص 190.

في دولة أخرى، والضحية في دولة ثالثة، وهو ما يؤدي إلى تشتت عناصر الجريمة جغرافياً، ويجعل من الصعب تحديد مكان واحد لوقوعها¹

هذا التداخل المكاني يؤدي بدوره إلى صعوبة تطبيق القواعد التقليدية للاختصاص القضائي، حيث تعتمد هذه القواعد غالباً على معيار مكان ارتكاب الجريمة أو مكان تحقق النتيجة. غير أن الطبيعة السيبرانية للجريمة تجعل هذين المعيارين غير حاسمين في كثير من الحالات، مما دفع بعض التشريعات والاتفاقيات الدولية إلى تبني معايير مرنة مثل معيار أثر الجريمة أو معيار مكان وجود النظام المعلوماتي المتضرر.

وفي هذا السياق، يظهر أثر هذه الخصائص بشكل مباشر على قواعد الإثبات الجنائي، إذ إن صعوبة تحديد الفاعل والمكان تؤدي إلى اعتماد القضاء بشكل متزايد على الأدلة الرقمية والتحليل الفني للبيانات بدل الأدلة التقليدية. غير أن هذا التحول يطرح بدوره إشكالات تتعلق بحجية هذه الأدلة ومدى موثوقيتها، خاصة في ظل إمكانية التلاعب بها أو تعديلها دون ترك أثر ظاهر.

كما أن الطبيعة المتغيرة والمتطورة للبيئة الرقمية تجعل من عملية الإثبات عملية ديناميكية وليست ثابتة، إذ إن الأدلة الرقمية قد تتغير أو تُمحي أو تُستبدل خلال فترة زمنية قصيرة جداً، مما يفرض على سلطات التحقيق التدخل السريع لحفظ الأدلة قبل ضياعها. ولهذا السبب، أصبح ما يعرف بالحفظ الفوري للبيانات أو "التجميد التقني للمعلومات" إجراءً أساسياً في التحقيق في الجرائم السيبرانية.

¹ -محمود نجيب حسني، شرح قانون العقوبات - القسم العام، دار النهضة العربية، القاهرة، 2015، ص 322.

ومن جهة أخرى، فإن هذه الخصائص أدت إلى بروز دور الخبرة التقنية بشكل كبير في المجال الجنائي، حيث أصبح الخبير المعلوماتي شريكاً أساسياً في عملية الإثبات، يقوم بتحليل البيانات الرقمية وتفسيرها للقاضي، الذي غالباً ما يفتقر إلى التكوين التقني اللازم لفهم هذه المعطيات. وهو ما يطرح تساؤلاً حول مدى استقلالية القاضي في تقدير الأدلة الرقمية في ظل اعتماده المتزايد على الخبرة الفنية¹

وبناءً على ما سبق، يمكن القول إن خصائص الجرائم السيبرانية، وعلى رأسها الطابع غير المادي، والسرعة، والعالمية، وصعوبة تحديد الفاعل والمكان، قد أحدثت تحولاً جذرياً في قواعد الإثبات الجنائي، حيث انتقل النظام التقليدي القائم على الأدلة المادية إلى نظام جديد يعتمد على الأدلة الرقمية والتقنية، وهو ما يستوجب تطويراً مستمراً للقواعد القانونية لمواكبة هذا التطور.

المبحث الثاني: الأساس القانوني للإثبات في الجرائم السيبرانية

بعد الوقوف على مفهوم الجرائم السيبرانية وخصائصها المؤثرة على الإثبات، ينتقل هذا المبحث لتحليل الأساس القانوني الذي يحكم إثبات هذه الجرائم². وسيتم التطرق أولاً إلى التنظيم القانوني العام للإثبات في قانون الإجراءات الجزائية الجزائري، ثم إلى النصوص الخاصة التي وضعها المشرع لمواكبة خصوصية الإثبات الرقمي.

¹ - أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2016، ص 289.

² - زاوي محمد الطاهر، المرجع السابق، ص 957.

المطلب الأول: التنظيم القانوني للإثبات في القانون الجزائري

لا ينفصل إثبات الجرائم السيبرانية عن قواعد الإثبات العامة المنصوص عليها في قانون الإجراءات الجزائية. فهذا القانون يحدد الإطار الإجرائي الذي تباشر بموجبه الدعوى العمومية، وتجمع الأدلة، ويُفصل فيها¹. إلا أن هذه القواعد قد لا تكون ملائمة تماماً لطبيعة الأدلة الرقمية، مما دفع المشرع إلى إدخال تعديلات عليها، كان آخرها صدور القانون رقم 14-25 المؤرخ في 3 غشت 2025 المتضمن قانون الإجراءات الجزائية الجديد².

الفرع الأول: قواعد الإثبات في قانون الإجراءات الجزائية رقم 14-25

أولاً: مبدأ حرية الإثبات في المواد الجزائية: يقوم قانون الإجراءات الجزائية على مبدأ أساسي هو "حرية الإثبات"، وهو ما يعني أن القاضي الجزائي غير مقيد بوسائل إثبات معينة، بل يمكنه الأخذ بأي دليل يقدم إليه، شرط أن يكون قد تم الحصول عليه بطرق مشروعة، وأن يكون له صلة بالوقائع المطلوب إثباتها، وأن تتاح للخصوم فرصة مناقشته³. هذا المبدأ يتسق مع طبيعة الدليل الرقمي الذي لم يكن موجوداً عند وضع قواعد الإثبات التقليدية، إذ يسمح للقاضي بقبول الأدلة الرقمية كالمطبوعات الإلكترونية وسجلات الاتصالات وتقارير الخبرة التقنية⁴.

¹ - القانون رقم 09-04، المرجع السابق ، المادة الثالثة.

² - القانون رقم 14-25، المرجع السابق ، المادة الثالثة.

³ - بلعباس مصطفى، المرجع السابق ، ص 484.

⁴ - زاوي محمد الطاهر، المرجع السابق ، ص 960.

وقد كرس قانون الإجراءات الجزائية الجديد رقم 14-25 هذا المبدأ في مواده الأولى التي تؤكد على "المحاكمة العادلة واحترام كرامة وحقوق الإنسان"¹، وتتص على أن "كل شخص يعتبر بريئاً ما لم تثبت إدانته بحكم قضائي حائز لقوة الشيء المقضي فيه"². وهذا الإعلان عن قرينة البراءة لا يمنع من الأخذ بأي دليل، ولكنه يضع عبء الإثبات على عاتق النيابة العامة، ويحرم القاضي من إدانة المتهم بناء على شك أو احتمال³.

ثانياً: دور أعضاء الشرطة القضائية في جمع الأدلة: خول قانون الإجراءات الجزائية لأعضاء الشرطة القضائية صلاحيات واسعة في البحث والتحري وجمع الأدلة، بما في ذلك سلطة إجراء التفتيش والحجز والاستماع إلى الشهود⁴. غير أن هذه الصلاحيات، عندما تمارس في مجال الجرائم السيبرانية، تتطلب (كما سبقت الإشارة) مهارات تقنية متخصصة، وهو ما قد لا يتوفر لدى عضو الشرطة القضائية التقليدي⁵.

وقد حاول المشرع تدارك هذا القصور من خلال النص (في القانون 04-09) على إمكانية الاستعانة بخبراء في مجال تكنولوجيا المعلومات والاتصال عند إجراء التحريات، وكذلك من خلال إنشاء وحدات متخصصة في مكافحة الجرائم السيبرانية تابعة للشرطة القضائية⁶.

¹ - القانون رقم 14-25، المرجع السابق ، المادة 120.

² - بلعباس مصطفى، المرجع السابق ، ص 486.

³ - زاوي محمد الطاهر، المرجع السابق ، ص 962.

⁴ - القانون رقم 04-09، المرجع السابق ، المادة الرابعة.

⁵ - القانون رقم 14-25، المرجع السابق ، المادة 150.

⁶ - بلعباس مصطفى، المرجع السابق ، ص 488.

بيد أن هذه الوحدات لا تزال، حسب بعض الآراء، بحاجة إلى مزيد من التكوين والإمكانات المادية لمواكبة تطور أساليب الجناة¹.

ثالثاً: ضمانات حقوق الدفاع في مرحلة جمع الأدلة: لا تعني حرية الإثبات أن النيابة العامة أو الشرطة القضائية يمكنها جمع الأدلة كيفما اتفقت، بل إن القانون يفرض ضمانات متعددة لحماية حقوق الدفاع². فالتفتيش، مثلاً، لا يجوز إلا بإذن من قاضي التحقيق أو النيابة العامة، ويجب أن يتم بحضور الشخص المتعلق به الإجراء أو من ينوب عنه. والحجز لا يشمل إلا الأشياء ذات الصلة بالجريمة³. وهذه الضمانات تثير إشكاليات في مجال الأدلة الرقمية، التي قد تكون موجودة على خوادم تقع خارج الإقليم الوطني، أو قد تكون مشفرة لا يمكن فك تشفيرها إلا بتعاون المتهم، مما يطرح مسألة "حق المتهم في عدم إدانة نفسه"⁴.

يقر قانون الإجراءات الجزائية الجزائري مبدأ حرية الإثبات في المواد الجزائية، وهو مبدأ يسمح للقاضي الجنائي بتكوين قناعته بناءً على أي دليل يراه مناسباً، دون التقيد بوسيلة إثبات محددة. ويهدف هذا المبدأ إلى تمكين القاضي من الوصول إلى الحقيقة الواقعية للجريمة، باعتبار أن الحقيقة الجنائية لا يمكن حصرها في وسيلة إثبات واحدة⁵.

غير أن تطبيق هذا المبدأ في مجال الجرائم السيبرانية يطرح صعوبات كبيرة، لأن الأدلة الرقمية تختلف في طبيعتها عن الأدلة التقليدية، فهي أدلة غير مادية، قابلة للتغيير أو الإتلاف

¹ - زاوي محمد الطاهر، المرجع السابق، ص 965.

² - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق، المواد من 25 إلى 32.

³ - بلعباس مصطفى، المرجع السابق، ص 490.

⁴ - زاوي محمد الطاهر، المرجع السابق، ص 968.

⁵ - أحسن بوسقيعة، التحقيق القضائي في المواد الجزائية، دار هومة، الجزائر، 2019، ص 120.

أو التلاعب، مما يجعلها تحتاج إلى معالجة تقنية دقيقة قبل عرضها على القضاء¹ كما أن قانون الإجراءات الجزائية لم يتناول بشكل مفصل إجراءات جمع الدليل الرقمي أو شروط صحته أو كيفية حفظه، بل ترك ذلك للاجتهاد القضائي والخبرة التقنية، وهو ما أدى إلى تفاوت في التطبيق العملي بين الجهات القضائية².

ومن ثم، فإن القاضي الجزائي في الجرائم السيبرانية يعتمد بشكل كبير على الخبرة التقنية لفهم طبيعة الدليل الرقمي، مما يجعل دوره في هذه القضايا غير مباشر في تقييم الدليل، بل يقوم على تحليل نتائج الخبرة الفنية المقدمة إليه³.

الفرع الثاني: حجية الأدلة في القانون الجزائري

أولاً: مفهوم الحجية: "الحجية" في القانون تعني القوة الإلزامية للدليل، أي قدرته على إقناع القاضي بوقوع فعل معين أو وجود علاقة قانونية معينة⁴. وتختلف حجية الأدلة في المواد الجزائية وفقاً لنوع الدليل وطبيعته ومصدره⁵.

فالشهادة، مثلاً، تخضع لمبدأ "حرية الإقناع" للقاضي، فهو غير ملزم بأخذ شهادة معينة بمجرد تقديمها، بل يقدر قيمتها بناء على ضميره وظروف الدعوى⁶. أما المحاضر والتقارير الرسمية التي يحررها أعضاء الشرطة القضائية أو الخبراء، فتتمتع بحجية خاصة تنص على

¹ - محمد عيد الغريب، الإثبات الجنائي الحديث، دار النهضة العربية، القاهرة، 2017، ص 177.

² - عبد العزيز سعد، طرق الإثبات في المواد الجزائية، دار هومة، الجزائر، 2017، ص 134.

³ - عبد الله سليمان، المرجع السابق، ص 203.

⁴ - القانون رقم 09-04، المرجع السابق، المادة 12.

⁵ - القانون رقم 25-14، المرجع السابق، المادة 160.

⁶ - بلعباس مصطفى، المرجع السابق، ص 492.

أنها "تبرر ما ورد فيها إلى أن يثبت عكسها"¹، أي أنها تفترض صحتها ما لم يطعن فيها بالتزوير.²

ثانياً: حجية الدليل الرقمي: يشير الدليل الرقمي إشكالية خاصة فيما يتعلق بحجيته، وذلك للأسباب التالية³:

1. سهولة التزوير: يمكن تزوير البيانات الرقمية وتحريفها بدرجة يصعب معها كشف التزوير بالطرق التقليدية. فالرسالة الإلكترونية، مثلاً، يمكن تغيير محتواها وتاريخ إرسالها وهوية مرسلها⁴. ومن ثم، يحتاج القاضي إلى التأكد من سلامة الدليل وسلسلة حيازته قبل أن يعطي له حجية⁵.

2. الطابع الفني للدليل: لا يمكن للقاضي أن يفهم الدليل الرقمي ويعرف قيمته إلا بمساعدة خبير تقني. وهذا يعني أن حجية الدليل الرقمي تصبح "حجية غير مباشرة"، إذ يتوقف قبولها على مدى إقناع القاضي بتقرير الخبير وبمنهجية عمله⁶.

3. التعارض المحتمل مع مبدأ شخصية العقاب: قد يكون الدليل الرقمي (كعنوان الآي بي) مرتبطاً بجهاز أو عنوان وصول، وليس بشخص بعينه. فإعطاء حجية مطلقة لمثل هذا

¹ - زاوي محمد الطاهر، المرجع السابق، ص 970.

² - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق، المادة 40.

³ - محمد نجيب حسني، المرجع السابق، ص 240.

⁴ - بلعباس مصطفى، المرجع السابق، ص 472.

⁵ - زاوي محمد الطاهر، المرجع السابق، ص 973.

⁶ - القانون رقم 09-04، المرجع السابق، المادة 15.

الدليل قد يؤدي إلى إدانة شخص لم يرتكب الجريمة، بل استُخدم جهازه في ارتكابها دون علمه (مثلاً، في حالة اختراق شبكة الواي فاي المنزلية)¹.

ولمواجهة هذه الإشكاليات، اشترط المشرع والقضاء الجزائري، لقبول الدليل الرقمي، توافر شروط عدة: ألا يكون قد تم التلاعب به، وأن يكون قد تم الحصول عليه بطرق مشروعة، وأن يكون له صلة مباشرة بالوقائع محل التحقيق، وأن يُعرض على القاضي في إجراءات علنية تتاح فيها للخصوم فرصة مناقشته². كما اشترطت المادة الثالثة من القانون 04-09 أن تكون إجراءات جمع الأدلة الرقمية "مبررة بحماية النظام العام أو لضرورات التحقيق"، مما يضيف عليها مشروعية إجرائية تعزز حجيتها³.

تقوم السياسة الجنائية في الجزائر على مبدأ حرية القاضي في تقدير الأدلة، وهو ما يعني أن القاضي غير ملزم بأي دليل معين، بل له كامل السلطة في تقدير مدى كفاية الأدلة المطروحة أمامه لتكوين قناعته. غير أن هذه الحرية ليست مطلقة، بل مقيدة باحترام قواعد المشروعية وعدم الاعتماد على أدلة غير قانونية⁴.

وفيما يتعلق بالدليل الرقمي، فإن الإشكال لا يكمن فقط في قبوله، بل في مدى حجيته وقوته الإثباتية. فالقاضي قد يقبل الدليل الرقمي كعنصر من عناصر الإثبات، لكنه قد لا يعتبره كافياً وحده للإدانة، خاصة إذا لم يكن مدعوماً بأدلة أخرى أو بخبرة تقنية تؤكد صحته. كما أن التطور التقني جعل من الممكن تعديل البيانات الرقمية دون ترك أثر ظاهر، وهو ما

¹ - القانون رقم 25-14، المرجع السابق، المادة 160.

² - بلعباس مصطفى، المرجع السابق، ص 493.

³ - زاوي محمد الطاهر، المرجع السابق، ص 975.

⁴ - محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2015، ص 233.

يضعف الثقة المطلقة في هذا النوع من الأدلة، ويدفع القضاء إلى التعامل معه بحذر شديد، مع ضرورة التحقق من مصدره وسلسلة انتقاله منذ لحظة جمعه إلى غاية عرضه أمام المحكمة¹ ومن ثم، فإن حجية الدليل الرقمي في القانون الجزائري ليست حجية مطلقة، بل هي حجية نسبية تخضع لتقدير القاضي، الذي يوازن بين قوة الدليل من جهة، ومدى سلامته القانونية والتقنية من جهة أخرى.

الفرع الثالث: سلطة القاضي في تقدير وسائل الإثبات

أولاً: مبدأ الاقتناع الشخصي للقاضي: يؤكد قانون الإجراءات الجزائية على أن القاضي يحكم في الدعوى وفقاً لـ "اقتناعه الشخصي" المستمد من الأدلة المقدمة أمامه، وليس وفقاً لقواعد فنية جامدة تحدد مسبقاً قيمة كل دليل². هذا المبدأ يمنح القاضي سلطة تقديرية واسعة في الموازنة بين الأدلة وترجيح بعضها على بعض³.

وفي مجال الجرائم السيبرانية، تتجلى سلطة القاضي التقديرية بشكل خاص، إذ يصبح مضطراً إلى تقييم أدلة تقنية معقدة، قد تكون متناقضة، وتقدم بتقارير خبراء متضاربة. والقاضي غير ملزم باتباع رأي خبير بعينه، بل يمكنه أن يفضل تقريراً على آخر، أو أن يرفضها جميعاً إذا لم تقنعه⁴.

¹ - عبد الله سليمان، شرح قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2018، ص 240.

² - اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق، المادة 40.

³ - بلعباس مصطفى، المرجع السابق، ص 474.

⁴ - زاوي محمد الطاهر، المرجع السابق، ص 948.

ثانياً: حدود السلطة التقديرية للقاضي: رغم اتساع سلطة القاضي التقديرية، فهي ليست مطلقة، بل تخضع لحدود موضوعية وإجرائية¹:

1. الالتزام بسببية قراره: يجب على القاضي أن يبين في حكمه الأسباب التي دفعته إلى الاقتناع بوقوع الجريمة أو انتفاءها، والأدلة التي اعتمد عليها. هذا الإلزام بالتعليل هو ضمانة ضد التحكم، ووسيلة للمراقبة من قبل محكمة النقض. فإذا بنى القاضي قناعته على أدلة رقمية دون أن يشرح كيف تحقق من صحتها وسلامتها، فإن حكمه يكون معرضاً للنقض².

2. احترام الضمانات الإجرائية: لا يمكن للقاضي أن يعتد بدليل تم الحصول عليه بطرق غير مشروعة، كالتتصت غير المأذون به قانوناً، أو اختراق نظام معلوماتي دون إذن قضائي³. وهذا ما يسمى بـ "نظرية شجرة السموم" في القانون المقارن، والتي تقول إن أي دليل مستمد من دليل غير مشروع هو أيضاً غير مقبول⁴.

3. وجوب عرض الأدلة على الخصوم: من مبادئ المحاكمة العادلة أن تتاح لجميع الأطراف فرصة مناقشة الأدلة المقدمة. وإذا أحاط القاضي علماً بدليل دون أن يعرضه على المتهم ودفاعه، فإنه يكون قد انتهك حق الدفاع، وقراره يصبح قابلاً للإبطال⁵.

يتمتع القاضي الجزائي في النظام القانوني الجزائري بسلطة تقديرية واسعة في تقييم الأدلة، حيث يكون قناعته الحرة بناءً على مجموع ما يعرض عليه من أدلة وقرائن، دون أن يكون ملزماً

¹ - القانون رقم 04-09، المرجع السابق .

² - القانون رقم 14-25، المرجع السابق .

³ - اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق .

⁴ - بلعباس مصطفى، المرجع السابق ، ص 476.

⁵ - زاوي محمد الطاهر، المرجع السابق ، ص 950.

بدليل معين أو بنوع محدد من وسائل الإثبات. وهذه السلطة تعد من أهم ضمانات العدالة الجنائية، لأنها تسمح للقاضي بالوصول إلى الحقيقة الواقعية بعيداً عن القيود الشكلية¹ غير أن هذه السلطة في مجال الجرائم السيبرانية تواجه تحديات كبيرة، نظراً للطبيعة التقنية المعقدة للأدلة الرقمية، التي لا يمكن فهمها أو تقييمها دون الاستعانة بخبراء متخصصين في مجال المعلوماتية. وبالتالي، فإن القاضي في هذه القضايا يعتمد بشكل كبير على نتائج الخبرة التقنية، مما يجعل دوره في تقييم الدليل غير مباشر²

كما أن الاعتماد الكبير على الخبرة التقنية يثير إشكالاً يتعلق بمدى استقلالية القاضي في تكوين قناعته، إذ إن تحويل الدليل الرقمي إلى تقرير فني قد يؤدي إلى تأثير غير مباشر على قناعة القاضي، خاصة إذا كانت الخبرة ذات طابع تقني معقد لا يمكن مناقشته بسهولة. ومع ذلك، فإن القضاء الجزائري يسعى إلى تحقيق توازن بين الاعتماد على الخبرة التقنية وبين الحفاظ على السلطة التقديرية للقاضي، بحيث تبقى الخبرة مجرد عنصر من عناصر الإثبات وليس دليلاً ملزماً للقاضي³

المطلب الثاني: النصوص الخاصة بالجرائم السيبرانية والإثبات الرقمي

استجابة للخصوصيات التي تميز الجرائم السيبرانية، لم يكتف المشرع الجزائري بالقواعد العامة لقانون الإجراءات الجزائية، بل وضع نصوصاً خاصة تهدف إلى مواكبة تطور هذه الجرائم وتوفير إطار قانوني ملائم لإثباتها⁴. وتتمثل هذه النصوص أساساً في أحكام القانون

¹ - أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية، ديوان المطبوعات الجامعية، الجزائر، 2016، ص 260.

² - عبد الفتاح بيومي حجازي، المرجع السابق، ص 118.

³ - أحسن بوسقيعة، المرجع السابق، ص 168.

⁴ - القانون رقم 09-04، المرجع السابق، المادة الثانية.

04-09، وفي تنظيم الدليل الإلكتروني في التشريع الجزائري، فضلاً عن دور الاتفاقيات الدولية في دعم التعاون والإثبات.

الفرع الأول: أحكام القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

أولاً: نطاق القانون وأهدافه: صدر القانون رقم 04-09 في 5 غشت 2009 ليكون بمثابة قانون إجرائي خاص يهدف إلى وضع قواعد وقائية وزجرية لمكافحة الجرائم المرتكبة باستخدام تكنولوجيا الإعلام والاتصال¹. وقد جاء ليكمل أحكام قانون العقوبات وقانون الإجراءات الجزائية، وليزودهما بآليات تتناسب مع خصوصية الفضاء الإلكتروني².

ويتضمن هذا القانون عدة أحكام تتصل مباشرة بالإثبات، منها ما يسمح للسلطات القضائية بمراقبة الاتصالات الإلكترونية في الوقت الحقيقي، وحجز البيانات المخزنة في النظم المعلوماتية، والاستعانة بخبراء لتحليل هذه البيانات³. كما يضع أحكاماً لتنظيم مسؤولية مزودي الخدمات في الاحتفاظ ببيانات الاتصالات وإتاحتها للسلطات القضائية عند الطلب⁴.

ثانياً: إجراءات الضبط القضائي الخاصة: من أبرز ما أتى به القانون 04-09 هو توسيع صلاحيات الضبط القضائي لتشمل إجراءات تقنية لم تكن معروفة من قبل، والمتمثلة في⁵:

¹ - بلعباس مصطفى، المرجع السابق ، ص 478.

² - زاوي محمد الطاهر، المرجع السابق ، ص 952.

³ - القانون رقم 14-25، المرجع السابق .

⁴ - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق.

⁵ - محمد نجيب حسني، المرجع السابق ص 333.

1. مراقبة الاتصالات الإلكترونية: نصت المادة الثالثة من القانون على إمكانية "إجراء عمليات مراقبة للاتصالات الإلكترونية، وجمع محتواها وتسجيله في وقت حقيقي"¹، وذلك بقرار من السلطة القضائية المختصة، وبمراعاة الضمانات القانونية التي تحمي سرية المراسلات. وهذه المراقبة هي بمثابة "تفتيش" في الفضاء الرقمي، إلا أنها تثير حساسية خاصة لأنها تمس بخصوصية الأفراد². ولذا، اشترط المشرع أن تكون هناك دوافع جدية تحتملها حماية النظام العام أو ضرورات التحقيق، وألا تتجاوز مدة المراقبة ما هو ضروري للتحقيق³.

2. الحجز في نظام معلوماتي: أجاز القانون للسلطات القضائية "إجراء تفتيش وحجز في نظام معلوماتي"⁴. وهذا الحجز يختلف عن الحجز التقليدي، ذلك أن القيمة المادية للجهاز الحاسوبي (الخادم، القرص الصلب، الهاتف الذكي) قد تكون ضئيلة مقارنة بقيمة البيانات المخزنة فيه. ومن ثم، قد تكفي السلطات بنسخ البيانات ("حجز بالنسخ") بدلاً من مصادرة الجهاز نفسه، وهو ما يعرف بـ "الحجز المرآة"، الذي يضمن الحفاظ على الدليل دون حرمان الغير من استخدام جهازه⁵.

ثالثاً: التعاون الإجرائي مع مزودي الخدمات: ألزم القانون 04-09 مزودي الخدمات (مقدمي خدمات الاتصال والإنترنت) بالتعاون مع السلطات القضائية، والاحتفاظ ببيانات الاتصالات لمدة معينة، وتقديمها عند الطلب⁶. وبيانات الاتصالات هذه - كما عرفها القانون

¹ - بلعباس مصطفى، المرجع السابق، ص 480.

² - زاوي محمد الطاهر، المرجع السابق، ص 955.

³ - القانون رقم 04-09، المرجع السابق، المادة الثالثة.

⁴ - القانون رقم 14-25، المرجع السابق، المادة الأولى.

⁵ - بلعباس مصطفى، المرجع السابق، ص 482.

⁶ - زاوي محمد الطاهر، المرجع السابق، ص 957.

- تشمل "بيانات المرور" (مصدر الاتصال، وجهته، مساره، توقيته، تاريخه، حجمه ومدته)، وهي أدلة حاسمة في تحديد هوية الجاني وتعبق نشاطه الإجرامي¹.

غير أن هذا الإلزام يثير تساؤلات حول مدى احترامه للخصوصية وحماية البيانات الشخصية، خاصة مع تزايد القدرة على جمع وتحليل كميات هائلة من البيانات². كما يطرح إشكاليات عملية، إذ قد لا يتعاون مزودو الخدمات الواقعون خارج الإقليم الوطني (كشركات البريد الإلكتروني العالمية)، مما يُخرج القانون الوطني عن نطاقه الفعال³.

يُعد القانون رقم 04-09 الإطار التشريعي الأساسي لمكافحة الجرائم السيبرانية في الجزائر، حيث جاء ليواكب التطور التكنولوجي المتسارع ويعالج الفراغ القانوني الذي كانت تعاني منه المنظومة التشريعية في مواجهة الجرائم المعلوماتية. وقد نص هذا القانون على تجريم مجموعة من الأفعال التي تمس بالأنظمة المعلوماتية، مثل الدخول غير المشروع إلى نظم المعالجة الآلية للمعطيات، أو البقاء فيها دون إذن، أو تعديل أو إتلاف البيانات أو تعطيل سير النظام المعلوماتي⁴.

كما أقر القانون وسائل خاصة للتحقيق في هذه الجرائم، من بينها إمكانية اللجوء إلى الوسائل التقنية لجمع الأدلة الرقمية، وهو ما يمثل اعترافاً صريحاً بالدليل الإلكتروني كوسيلة إثبات في المجال الجنائي، غير أن المشرع لم يحدد بدقة الإجراءات التقنية الواجب اتباعها لضمان سلامة هذا الدليل، مما يترك المجال مفتوحاً للاجتهاد القضائي والخبرة الفنية⁵.

¹ - القانون رقم 04-09، المرجع السابق، المادة الثالثة.

² - القانون رقم 14-25، المرجع السابق، المادة الثالثة.

³ - بلعباس مصطفى، المرجع السابق، ص 484.

⁴ - القانون رقم 04-09، المواد 2 إلى 7.

⁵ - محمد عيد الغريب، الإثبات الجنائي الحديث، دار النهضة العربية، القاهرة، 2017، ص 219.

ويلاحظ أن هذا القانون يتبنى مقاربة وقائية وعقابية في آن واحد، حيث لا يقتصر على تجريم الأفعال بعد وقوعها، بل يسعى أيضاً إلى الوقاية من الجرائم المعلوماتية من خلال وضع آليات للمراقبة والتتبع، غير أن فعالية هذه الآليات تبقى مرتبطة بمدى توفر الإمكانيات التقنية والبشرية لدى الجهات المختصة¹

كما يعكس القانون 04-09 توجهاً تشريعياً نحو الاعتراف بالخصوصية التقنية للجرائم السيبرانية، من خلال التعامل معها كنمط إجرامي مستقل له قواعده الخاصة، وليس مجرد امتداد للجرائم التقليدية.

الفرع الثاني: تنظيم الدليل الإلكتروني في التشريع الجزائري

أولاً: اعتراف المشرع بالدليل الإلكتروني: لم يعرف المشرع الجزائري، في نصوص صريحة، "الدليل الإلكتروني" كمصطلح قانوني موحد. غير أنه اعترف به واقعاً من خلال عدة نصوص متفرقة، أبرزها²:

· قانون المعاملات الإلكترونية (الأمر رقم 03-23 المؤرخ في 26 غشت 2003)، الذي نص على أن "الكتابة الإلكترونية لها نفس الحجية المقررة للكتابة الورقية" متى تم التوقيع عليها بتوقيع إلكتروني آمن³. وهذا النص ينطبق على الإثبات في المواد المدنية والتجارية، غير أنه قد يسترشد به القاضي الجزائري في تقدير الأدلة الرقمية⁴.

¹ - أحسن بوسقيعة، التحقيق القضائي في المواد الجزائية، دار هومة، الجزائر، 2019، ص 144.

² - زاوي محمد الطاهر، المرجع السابق، ص 960.

³ - القانون رقم 14-25، المرجع السابق، المادة 120.

⁴ - بلعباس مصطفى، المرجع السابق، ص 486.

· قانون حماية الأشخاص الطبيعيين في مجال معالجة البيانات الشخصية (القانون رقم 07-18 المؤرخ في 10 جوان 2018)، الذي نظم شروط جمع البيانات الشخصية ومعالجتها، بما في ذلك البيانات التي قد تستخدم كأدلة في الدعوى الجزائية¹.

ولكن على المستوى التقني، يظل القانون 04-09 هو النص الأهم الذي أقر بإمكانية استخدام الأدلة الرقمية في التحقيقات الجزائية، وأعطى للقاضي سلطة الاعتداد بها، وإن كان بطريقة غير مباشرة عبر تنظيم وسائل الحصول عليها².

ثانياً: شروط قبول الدليل الإلكتروني: بالرجوع إلى أحكام القانون 04-09 والمبادئ العامة للإجراءات الجزائية، يمكن استخلاص الشروط التالية لقبول الدليل الإلكتروني³:

1. شرط المشروعية: يجب أن يتم جمع الدليل الإلكتروني بموجب إذن قضائي، وباحترام القواعد الإجرائية (كتسبيب قرار المراقبة، تحديد مدتها، إلخ). فالدليل الذي يتم جمعه دون إذن أو عن طريق تجاوز السلطات المقررة يكون غير مقبول، ويترتب عليه بطلان الإجراءات⁴.

2. شرط السلامة: يجب أن يثبت أن الدليل الإلكتروني لم يتم التلاعب به أو تغييره منذ لحظة جمعه حتى عرضه على القضاء. ويتحقق ذلك من خلال "سلسلة الحيازة" (Chain of Custody) الموثقة، وهي وثيقة تسجل كل انتقال للدليل من شخص لآخر، والإجراءات التي تمت عليه. وأي انقطاع في هذه السلسلة أو غموض فيها يضعف حجية الدليل أو يفقده إياها⁵.

¹ - زاوي محمد الطاهر، المرجع السابق، ص 962.

² - القانون رقم 04-09، المرجع السابق، المادة الرابعة.

³ - القانون رقم 14-25، المرجع السابق، المادة 150.

⁴ - بلعباس مصطفى، المرجع السابق، ص 488.

⁵ - زاوي محمد الطاهر، المرجع السابق، ص 965.

3. شرط الصلة: يجب أن يكون الدليل الإلكتروني مرتبطاً بالوقائع محل الدعوى، وقادراً على إثباتها أو نفيها. فلا يجوز قبول دليل لا صلة له بالقضية، أو يكون قد تم جمعه لأغراض أخرى غير تحقيق العدالة¹.

ثالثاً: حجية الدليل الإلكتروني أمام القاضي الجزائي: تتفاوت حجية الدليل الإلكتروني بحسب نوعه وطريقة الحصول عليه. فأدلة "بيانات المرور" التي تقدمها شركات الاتصالات بناء على التزاماتها القانونية تتمتع بحجية أقوى من رسالة إلكترونية قدمها شخص مجهول دون إثبات مصدرها². غير أن القاضي يظل هو صاحب السلطة التقديرية في تقييم حجية كل دليل، وفقاً لـ "اقتناعه الشخصي"³.

وهذا يعني أن حجية الدليل الإلكتروني في القانون الجزائري هي "حجية مادية" لا "حجية قانونية". بمعنى أن القانون لا يفرض على القاضي أخذ دليل معين بمجرد وجوده، بل يترك له حرية تقدير قيمته الإثباتية⁴. وهذا يتناقض مع بعض التشريعات المدنية التي تعطي حجية قانونية للكتابة الإلكترونية المعتمدة على التوقيع الإلكتروني الآمن (كاعتبارها بمثابة محرر عرفي). في القانون الجزائري، لا توجد مثل هذه الحجية المسبقة، لأن القاضي في المواد الجزائية يبحث عن "حقيقة مطلقة" وليس عن مجرد توازن بين أطراف عقد⁵.

¹ - اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق ، المواد من 25 إلى 32.

² - بلعباس مصطفى، المرجع السابق ، ص 490.

³ - زاوي محمد الطاهر، المرجع السابق ، ص 968.

⁴ - القانون رقم 09-04، المرجع السابق ، المادة 12.

⁵ - القانون رقم 25-14، المرجع السابق ، المادة 160.

لم يضع المشرع الجزائري تنظيماً شاملاً ومفصلاً للدليل الإلكتروني، بل اكتفى بوضع قواعد عامة تسمح باستخدام الوسائل التقنية في الإثبات، خاصة في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. وهذا ما يظهر من خلال القانون 04-09 الذي أقر إمكانية اللجوء إلى وسائل تقنية لجمع الأدلة الرقمية، دون تحديد إجراءات دقيقة لكيفية التعامل معها¹

ويُعد هذا الغموض التشريعي أحد أبرز التحديات التي تواجه القضاء الجزائري في هذا المجال، حيث يضطر القضاة إلى الاعتماد على الاجتهاد والخبرة التقنية لتحديد مدى قبول الأدلة الرقمية. كما أن غياب تنظيم تفصيلي يؤدي أحياناً إلى تفاوت في التطبيق القضائي بين مختلف الجهات القضائية.

وفي المقابل، فقد حاول الفقه والقضاء تطوير معايير عملية لضبط الدليل الإلكتروني، من بينها ضرورة توثيق مصدر الدليل، وضمان سلامته التقنية، وتحديد هوية من قام بجمعه، بالإضافة إلى الحفاظ على تسلسل زمني دقيق لعملية جمعه وتحليله²

كما أن التنظيم الجزائري للدليل الإلكتروني يتأثر بشكل واضح بالاتجاهات الدولية، خاصة اتفاقية بودابست التي وضعت مبادئ أساسية للتعامل مع الأدلة الرقمية، مثل ضرورة حفظ البيانات بشكل عاجل، وتسهيل التعاون الدولي في نقل الأدلة بين الدول.

الفرع الثالث: دور الاتفاقيات الدولية في دعم الإثبات السيبراني

أولاً: اتفاقية بودابست لمكافحة الجريمة المعلوماتية (2001): تعد اتفاقية بودابست، التي انضمت إليها أكثر من 60 دولة، الصك الدولي الأكثر شمولاً في مجال مكافحة الجريمة

¹ - القانون رقم 04-09، المواد 3 و4 و5.

² - أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية، ديوان المطبوعات الجامعية، الجزائر، 2016، ص 274.

السيبرانية¹. وقد وضعت الاتفاقية معايير مشتركة لتجريم الأفعال السيبرانية، وصلاحيات إجرائية للسلطات الوطنية (كإصدار أوامر الإنتاج، والبحث والحجز على النظم المعلوماتية، والمراقبة في الوقت الفعلي)، وآليات للتعاون الدولي السريع (كشبكة الاتصال على مدار الساعة، والمساعدة المتبادلة في جمع الأدلة، وحتى تسليم المجرمين)².

ولم توقع الجزائر على اتفاقية بودابست بعد، وهو موقف تشاركها فيه العديد من الدول العربية والإسلامية (باستثناء تونس والمغرب وموريتانيا اللواتي انضمن إليها)³. ترجع أسباب عدم الانضمام إلى اعتبارات تتعلق بالسيادة الوطنية، وإلى تحفظات على بعض أحكام الاتفاقية التي تسمح بـ "الاختراق العابر للحدود" (أي اختراق نظام معلوماتي في دولة أخرى دون إذن مسبق منها في حالات الطوارئ)، وهو ما تراه بعض الدول انتهاكاً لسيادتها⁴.

ثانياً: اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية (2024-2025): في خطوة تاريخية، اعتمدت الجمعية العامة للأمم المتحدة في ديسمبر 2024 أول معاهدة عالمية لمكافحة الجريمة السيبرانية، بعد مفاوضات استمرت ثلاث سنوات ترأست الجزائر لجنتها التحضيرية وشاركت في قيادة مسارها التفاوضي⁵. وقد وقعت الجزائر على هذه المعاهدة في 25 أكتوبر 2025، إلى جانب 64 دولة أخرى⁶.

¹ - بلعباس مصطفى، المرجع السابق ، ص 492.

² - زاوي محمد الطاهر، المرجع السابق ، ص 970.

³ - اتفاقية الامم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق ، المادة 40.

⁴ - محمد نجيب حسني، المرجع السابق ص 345.

⁵ - بلعباس مصطفى، المرجع السابق ، ص 472.

⁶ - زاوي محمد الطاهر، المرجع السابق ، ص 945.

تعتبر هذه المعاهدة تطوراً نوعياً مقارنة باتفاقية بودابست لعدة أسباب¹:

1. الشمول الجغرافي: كونها معاهدة أممية، فهي مفتوحة لجميع الدول الأعضاء في الأمم المتحدة، مما يزيد من عدد الدول المنضمة ويحقق إجماعاً دولياً أوسع².
 2. مراعاة احتياجات الدول النامية: تركز المعاهدة على المساعدة التقنية وبناء القدرات لمساعدة الدول النامية على تطوير تشريعاتها وقدراتها في مكافحة الجريمة السيبرانية³.
 3. مواءمة أحكامها مع حقوق الإنسان: تؤكد المعاهدة في ديباجتها على "الحق في الحماية من التدخل التعسفي أو غير القانوني في خصوصيات الأفراد، وبأهمية حماية البيانات الشخصية"، وهو ما يعالج بعض الانتقادات الموجهة لاتفاقية بودابست⁴.
 4. تجريم أفعال جديدة: أضافت المعاهدة جرائم سيبرانية لم تكن واردة في اتفاقية بودابست، كالجرائم المتعلقة بالاتجار بالأشخاص عبر الإنترنت، والاحتيال في مجال المدفوعات الإلكترونية، والتأثير الخبيث على البنية التحتية الحيوية⁵.
- ثالثاً: أثر هذه الاتفاقيات على نظام الإثبات الجزائي: على الرغم من أن الجزائر لم تنضم بعد إلى اتفاقية بودابست، فإن انضمامها إلى اتفاقية الأمم المتحدة سيكون له أثر كبير على نظام الإثبات الوطني، وذلك من خلال⁶:

¹ - القانون رقم 09-04 المرجع السابق.

² - القانون رقم 14-25، المرجع السابق.

³ - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق.

⁴ - بلعباس مصطفى، المرجع السابق، ص 474.

⁵ - زاوي محمد الطاهر، المرجع السابق، ص 948.

⁶ - القانون رقم 09-04، المرجع السابق، المادة الثانية.

1. تعديل التشريعات الوطنية: ستضطر الجزائر إلى تعديل قوانينها (قانون العقوبات، قانون الإجراءات الجزائية، القانون 04-09) لمواءمتها مع أحكام المعاهدة، خاصة فيما يتعلق بتوسيع صلاحيات جمع الأدلة الرقمية (كبيانات المرور والمراقبة الفورية)، وإدخال آليات تعاون دولي سريعة¹.

2. تعزيز التعاون القضائي: ستتيح المعاهدة للسلطات القضائية الجزائرية تقديم طلبات للحصول على أدلة رقمية من دول أخرى (كالحصول على بيانات من خادم موجود في أوروبا أو أمريكا)، كما ستلزم الجزائر بالاستجابة لطلبات مماثلة من دول أخرى، مما يعزز فعالية الملاحقة الجزائية².

3. وضع معايير مشتركة: ستوحد المعاهدة المعايير الدولية لقبول الأدلة الرقمية، مما يساعد القضاء الجزائري على تطوير ممارساته في هذا المجال، وتدريب قضاته وخبرائه على أحدث الأساليب في جمع وتحليل الأدلة الرقمية³.

ومن المتوقع، مع دخول هذه المعاهدة حيز التنفيذ، أن يسرع المشرع الجزائري إلى إصدار نصوص تعديلية لقانون الإجراءات الجزائية وللقانون 04-09، لتتماشى مع الالتزامات الدولية الجديدة، مما سينعكس إيجاباً على واقع الإثبات في الجرائم السيبرانية في الجزائر⁴.

أصبح التعاون الدولي في مجال مكافحة الجرائم السيبرانية ضرورة حتمية، نظراً للطبيعة العابرة للحدود لهذه الجرائم، حيث لا يمكن لأي دولة مواجهة هذا النوع من الإجرام بمفردها.

¹ - القانون رقم 14-25، المرجع السابق، المواد من 1 إلى 5.

² - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق، المادة الثانية.

³ - محمد نجيب حسني، المرجع السابق ص 355.

⁴ - بلعباس مصطفى، المرجع السابق، ص 476.

وتُعد اتفاقية بودابست بشأن الجريمة السيبرانية لسنة 2001 أهم إطار دولي في هذا المجال، إذ وضعت قواعد موحدة للتعاون الدولي في جمع الأدلة الرقمية وتبادلها¹

وقد ساهمت هذه الاتفاقية في تطوير مفهوم الدليل الإلكتروني على المستوى الدولي، من خلال التأكيد على ضرورة حفظ البيانات الرقمية بشكل سريع، وتمكين السلطات القضائية من الوصول إلى الأدلة المخزنة في دول أخرى عبر آليات التعاون القضائي. كما شجعت الدول على تطوير تشريعاتها الوطنية بما يتماشى مع طبيعة الجرائم السيبرانية²

ورغم أن الجزائر ليست طرفاً في هذه الاتفاقية، إلا أن تأثيرها يظهر بشكل غير مباشر في تطور التشريع الوطني، خاصة في ما يتعلق بالاعتراف بالدليل الإلكتروني وتبني بعض المبادئ المتعلقة بحفظ البيانات والتعاون الدولي في المجال الجنائي.

ومن ثم، فإن الاتفاقيات الدولية تلعب دوراً مكماً للنصوص الوطنية، حيث تساهم في سد الفراغ التشريعي وتعزيز فعالية الإثبات في الجرائم السيبرانية، خاصة في ظل الطبيعة العالمية لهذا النوع من الجرائم.

¹– Convention on Cybercrime (Budapest Convention), 2001

²– Robert Chesney, Cybercrime and the Law, Oxford University Press, 2018, p. 119.

خلص هذا الفصل إلى أن الجرائم السيبرانية تمثل نقلة نوعية في مفهوم الإجرام، تتسم بطابع رقمي لا مادي، وسرعة وعالمية في الارتكاب، وصعوبة في تحديد الفاعل ومكان الجريمة¹. وهذه الخصائص تفرض تحديات حقيقية على أنظمة الإثبات التقليدية التي تطورت في بيئة مادية. كما تبين أن المشرع الجزائري، بموجب القانون 04-09 ثم قانون الإجراءات الجزائية الجديد 14-25، قد خطا خطوات مهمة في اتجاه ملائمة قواعد الإثبات مع خصوصية هذه الجرائم، من خلال إقرار إجراءات خاصة كالمراقبة الفورية للاتصالات الإلكترونية والحجز في النظم المعلوماتية، وإنشاء وحدات شرطة قضائية متخصصة².

غير أن هذه الجهود تظل غير كافية في ظل غياب تنظيم تشريعي واضح لحجية الدليل الرقمي وشروط قبوله، وبقاء سلطة القاضي في تقديره خاضعة لمعايير عامة قد لا تستوعب تعقيدات الأدلة التقنية³. كما أن عدم انضمام الجزائر إلى اتفاقية بودابست، وكون اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لا تزال في مرحلة التوقيع والتصديق، يضع نظام الإثبات الوطني في عزلة نسبية عن التطورات الدولية، رغم أن الجزائر لعبت دوراً محورياً في صياغة المعاهدة الأممية⁴.

من هذا المنطلق، يبقى الطريق ممهداً لمزيد من التطوير التشريعي والقضائي، خاصة على صعيد ضمان سلامة الأدلة الرقمية وسلسلة حيازتها، وضبط آليات التعاون الدولي في

¹ - زاوي محمد الطاهر، المرجع السابق، ص 950.

² - القانون رقم 04-09، المرجع السابق، المادة الثالثة.

³ - القانون رقم 14-35، المرجع السابق، المادة الأولى.

⁴ - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المرجع السابق.

جمع الأدلة، وتكوين القضاة وأعضاء النيابة العامة والشرطة القضائية في مجال التقنيات الرقمية، وهو ما سيكون محور الفصول القادمة من هذه الدراسة¹.

¹ - بلعباس مصطفى، المرجع السابق ، ص 478.

الفصل الثاني:

وسائل الإثبات القضائي في الجرائم السيبرانية وتقييمها

بعد أن استعرضنا في الفصل الأول الإطار المفاهيمي والقانوني للجرائم السيبرانية، وتبين لنا خصوصية هذه الجرائم من حيث طبيعتها الرقمية غير المادية، وتجاوزها للحدود الوطنية، وصعوبة تحديد الفاعل ومكان الجريمة¹، ننتقل في هذا الفصل إلى صميم الإشكالية التي تطرحها هذه الجرائم على مستوى العدالة الجنائية، ألا وهو جانب الإثبات².

فإذا كانت الجريمة السيبرانية لا تترك آثاراً مادية بالمعنى التقليدي - كأثار الأقدام أو بصمات الأصابع - فإنها تترك آثاراً رقمية يمكن تعقبها وجمعها وتحليلها، شريطة توفر الإجراءات القانونية والتقنية المناسبة³.

وتتجلى أهمية هذا الفصل في كونه ينتقل من النظري إلى التطبيقي، حيث يعرض لوسائل الإثبات الفعلية المعتمدة في مواجهة الجرائم السيبرانية، ويقيم مدى فعاليتها في ظل التحديات الراهنة⁴.

وقد قسمنا هذا الفصل إلى مبحثين رئيسيين: يتناول المبحث الأول وسائل الإثبات الرقمية من حيث مفهوم الدليل الإلكتروني وحجيته وشروطه، ثم إجراءات جمعه وتحليله. ويتناول

¹ - د. عبد الفتاح بيومي حجازي، الدليل الجنائي الرقمي وحجيته في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2010، ص 15.

² - د. محمد أمين البشري، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، القاهرة، الطبعة الثانية، 2018، ص 22.

³ - د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون الدولي، دار الكتب القانونية، مصر، الطبعة الأولى، 2007، ص 48.

⁴ - د. أحمد عبد الكريم سلامة، الحماية الجنائية للمعلوماتية، دار النهضة العربية، القاهرة، الطبعة الأولى، 2015، ص 33.

المبحث الثاني دور الجهات القضائية والأمنية، من خلال الضبطية القضائية المتخصصة والخبرة الرقمية، ثم التحديات العلمية وآفاق التطوير¹.

¹ - د. محمود نجيب حسني، شرح قانون الإجراءات الجزائية، دار النهضة العربية، القاهرة، الطبعة السادسة، 2016، ص

المبحث الأول: وسائل الإثبات الرقمية في الجرائم السيبرانية

يمثل الدليل الرقمي العمود الفقري لعملية الإثبات في الجرائم السيبرانية¹. فقد شهد مفهوم الدليل الرقمي تطوراً كبيراً خلال العقدين الماضيين، حيث انتقل من كونه وسيلة إثبات ثانوية أو تكميلية إلى أن أصبح، في كثير من القضايا السيبرانية، الدليل الوحيد المتاح لإثبات الجريمة². وتتميز الأدلة الرقمية بخمس خصائص جوهرية تميزها عن الأدلة التقليدية: الطابع غير المادي (فهي مجرد بيانات وإشارات إلكترونية)، والهشاشة وسهولة التلف (فمجرد تشغيل الجهاز قد يعدل البيانات)، والانتشار والتوزيع المكاني (قد تكون موزعة على خوادم في عدة دول)، والحاجة إلى وسيط تقني وخبير لقراءتها وتفسيرها، والضخامة من حيث حجم البيانات (قد تصل إلى تيرابايت)³.

المطلب الأول: الدليل الإلكتروني وحجيته القانونية

أصبح الدليل الإلكتروني من أهم وسائل الإثبات في الجرائم السيبرانية نظراً لارتباط هذه الجرائم بالبيئة الرقمية. وقد فرض التطور التكنولوجي الاعتراف بهذا النوع من الأدلة ومنحه

¹ - د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، منشأة المعارف، الإسكندرية، الطبعة الأولى، 2009، ص 57.

² - د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الثالثة، 2014، ص 278.

³ - د. خالد ممدوح إبراهيم، التحقيق الجنائي الرقمي والأدلة الرقمية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2017، ص 66.

قيمة قانونية أمام القضاء . لذلك يقتضي الأمر دراسة مفهومه وشروط حجته القانونية في الإثبات الجنائي.

الفرع الأول: مفهوم الدليل الإلكتروني وحجته القانونية

اختلف الفقه في تعريف الدليل الإلكتروني تبعاً لاختلاف زوايا النظر إليه¹. فمنهم من عرّفه تعريفاً موضوعياً بأنه "كل أثر رقمي ناتج عن استخدام نظام معلوماتي أو شبكة اتصال، يمكن الاستناد إليه لإثبات واقعة قانونية أو دحضها"². ويشمل هذا التعريف البيانات المخزنة على الأجهزة الإلكترونية، وسجلات الاتصالات، والرسائل الإلكترونية، والصور والمقاطع الرقمية، وبيانات المرور، والبيانات الوصفية³.

ومنهم من عرّفه تعريفاً إجرائياً بأنه "المعلومات التي يتم جمعها من الأجهزة الإلكترونية أو شبكات الاتصال وفقاً للإجراءات القانونية والقواعد التقنية المتخصصة، والتي يُمكن تقديمها أمام

¹ - د. عبد الفتاح بيومي حجازي، الدليل الإلكتروني في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2012، ص 39.

² - د. محمد سعيد نمور، أصول الإجراءات الجزائية، دار الثقافة للنشر والتوزيع، عمان، الطبعة الخامسة، 2013، ص 352.

³ - د. خالد ممدوح إبراهيم، حجية الدليل الإلكتروني في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2011، ص 74.

القضاء كوسيلة إثبات¹. ويرى أنصار هذا التعريف أنه الأكثر ملاءمة للسياق الجنائي، لأنه يشدد على ضرورة أن يتم جمع الدليل بطرق قانونية سليمة، وإلا فإنه يفقد قيمته الإثباتية².

أما المشرع الجزائري، فلم يقدم تعريفاً جامعاً للدليل الإلكتروني في نصوص صريحة، سواء في قانون الإجراءات الجزائية الجديد رقم 14-25 أو في القانون 04-09³. غير أنه اعترف به ضمناً من خلال النصوص التي تنظم إجراءات الحصول عليه، كالمراقبة الإلكترونية والحجز في نظام معلوماتي المنصوص عليها في المادة الثالثة من القانون 04-09⁴.

فيما يتعلق بحجية الدليل الإلكتروني في القانون الجزائري، لم ينص المشرع صراحة على ذلك، غير أن الفقه الجزائري ذهب إلى أن حجية الدليل الإلكتروني تخضع للمبدأ العام في المواد الجزائية، وهو "حرية الإثبات"⁵. وهذا المبدأ يعني أن القاضي الجزائي غير مقيد بوسائل

¹ - د. محمد الأمين البشري، الجرائم الإلكترونية والتحقيق فيها، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، 2016، ص 91.

² - د. فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة العاشرة، 2014، ص 522.

³ - الجريدة الرسمية للجمهورية الجزائرية، القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47، سنة 2009، ص 5.

⁴ - الجريدة الرسمية للجمهورية الجزائرية، القانون رقم 14-25 المعدل والمتمم لقانون الإجراءات الجزائية، العدد 32، سنة 2025، ص 12.

⁵ - د. أحسن بوسقيعة، التحقيق القضائي في القانون الجزائري، دار هومة، الجزائر، الطبعة التاسعة، 2017، ص 214.

إثبات معينة، بل يمكنه الأخذ بأي دليل يقدم إليه، شريطة أن يكون قد تم الحصول عليه بطرق مشروعة، وأن يكون له صلة بالوقائع المطلوب إثباتها، وأن تتاح للخصوم فرصة مناقشته¹. وتكون حجية الدليل الإلكتروني "حجية مادية" وليست "حجية قانونية"². فالحجية المادية تعني أن القانون لا يفرض على القاضي أخذ دليل معين بمجرد وجوده، بل يترك له حرية تقدير قيمته الإثباتية وفقاً لاقتناعه الشخصي³.

لقد أدى التطور الهائل في وسائل الاتصال الحديثة إلى اتساع نطاق الاعتماد على الدليل الإلكتروني في الإثبات الجنائي، خاصة مع انتقال جزء كبير من النشاط الإنساني إلى الفضاء الرقمي⁴. فأصبحت المعاملات التجارية، والمراسلات المهنية، والعلاقات الاجتماعية، وحتى الأنشطة الإجرامية تتم عبر الوسائط الإلكترونية، الأمر الذي جعل الدليل الرقمي أكثر تعبيراً عن الواقع الإجرامي المعاصر من الأدلة التقليدية⁵. وتظهر أهمية هذا الدليل بصورة خاصة في

¹ - د. عبد العزيز سعد، أبحاث تحليلية في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، الطبعة الثانية، 2018، ص 301.

² - د. محمود نجيب حسني، نظرية الإثبات الجنائي، دار النهضة العربية، القاهرة، الطبعة الثانية، 2011، ص 129.

³ - د. أحمد شوقي الشلقاني، مبادئ الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، الطبعة الأولى، 2010، ص 198.

⁴ - د. عبد الفتاح بيومي حجازي، الدليل الإلكتروني في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2012، ص 55.

⁵ - د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، منشأة المعارف، الإسكندرية، الطبعة الأولى، 2009، ص 88.

في الجرائم التي تُرتكب بالكامل داخل البيئة المعلوماتية، حيث لا يترك الجاني أثراً مادياً ملموساً يمكن الاعتماد عليه، وإنما يترك أثراً رقمية كامنة داخل الأنظمة المعلوماتية وقواعد البيانات¹. ولهذا السبب، اتجهت التشريعات الحديثة إلى الاعتراف الضمني أو الصريح بالدليل الإلكتروني، وإلى منح القاضي سلطة تقديرية واسعة في الاستناد إليه متى توفرت ضمانات المشروعية والسلامة التقنية². كما ساهم الاجتهاد القضائي المقارن، خصوصاً في فرنسا والولايات المتحدة، في تكريس حجية الدليل الرقمي، من خلال الاعتراف بالرسائل الإلكترونية وسجلات الدخول والبيانات الوصفية كوسائل إثبات معتبرة متى تم جمعها وفق الإجراءات القانونية³.

كما أن القيمة العملية للدليل الإلكتروني لا تكمن فقط في إثبات وقوع الجريمة، وإنما تمتد إلى تحديد هوية الجاني وربط النشاط الإجرامي به بصورة دقيقة⁴. فبيانات الاتصال وعناوين الآي بي وسجلات الولوج إلى الأنظمة تتيح تتبع مسار النشاط الإجرامي زمنياً ومكانياً، كما تسمح

¹ Casey Eoghan, Digital Evidence and Computer Crime, Academic Press, Third Edition, 2011, p. 73.

² د. خالد ممدوح إبراهيم، حجية الدليل الإلكتروني في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2011، ص 93.

³ Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations, Cengage Learning, Fifth Edition, 2015, p. 132.

⁴ د. محمد الأمين البشري، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، القاهرة، الطبعة الثانية، 2018، ص 111.

بتحديد الأجهزة المستخدمة والحسابات المرتبطة بها¹. ويزداد الأمر أهمية في الجرائم المنظمة والعبارة للحدود، حيث يعتمد المحققون بشكل شبه كامل على التحليل الرقمي لتفكيك الشبكات الإجرامية وكشف الروابط بين المتورطين². غير أن الاعتماد المفرط على الأدلة الرقمية يثير إشكالات تتعلق بإمكانية التلاعب بها أو اصطناعها باستخدام تقنيات متقدمة، وهو ما يفرض ضرورة إخضاعها للرقابة القضائية الدقيقة والاستعانة بالخبرة الفنية المتخصصة³. ولذلك فإن الاتجاه الحديث في الفقه الجنائي يدعو إلى وضع قواعد خاصة بالإثبات الرقمي تختلف عن القواعد التقليدية، نظراً للطبيعة التقنية المعقدة لهذا النوع من الأدلة⁴.

الفرع الثاني: شروط صحة الدليل الإلكتروني وأنواعه

لكي يكون الدليل الإلكتروني صحيحاً ومقبولاً أمام القضاء، يجب أن تتوافر فيه ثلاثة شروط رئيسية، أجمع عليها الفقه والخبراء التقنيون⁵.

الشرط الأول هو شرط المشروعية، ويقصد به أن يتم الحصول على الدليل الإلكتروني وفقاً للإجراءات القانونية المقررة، وليس عن طريق تجاوز السلطات أو انتهاك الحقوق

¹- Brian Carrier, File System Forensic Analysis, Addison-Wesley, First Edition, 2005, p. 281.

²- Convention on Cybercrime (Budapest Convention), Council of Europe, 2001, p. 9.

³- د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الثالثة، 2014، ص 341.

⁴- د. محمود نجيب حسني، نظرية الإثبات الجنائي، دار النهضة العربية، القاهرة، الطبعة الثانية، 2011، ص 212.

⁵- د. خالد ممدوح إبراهيم، الدليل الرقمي في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2018، ص 88.

والحريات¹. فإذا تم جمع الدليل عن طريق التنصت غير المأذون به، أو اختراق نظام معلوماتي دون إذن قضائي، فإنه يكون غير مشروع، ويترتب عليه بطلان الإجراءات².

وينبغي التفريق هنا بين عدم المشروعية المطلقة - كجمع الدليل دون أي سند قانوني - مما يؤدي إلى بطلان الدليل والإجراءات اللاحقة المبنية عليه (نظرية ثمرة الشجرة المسمومة)، وعدم المشروعية النسبية - كجمع الدليل بإذن قضائي مع تجاوز حدود الإذن - فيكون الدليل غير المشروع فقط هو الذي يبطل³.

الشرط الثاني هو شرط الصحة والسلامة، ويقصد به أن يكون الدليل الإلكتروني سليماً لم يتم التلاعب به أو تعديله أو إتلاف جزء منه، منذ لحظة ضبطه وحتى عرضه على القضاء⁴. ويتحقق هذا الشرط من خلال إثبات "سلسلة الحيازة" (Chain of Custody) و"التوقيع الرقمي" (Hash Value)⁵.

¹- د. محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، الطبعة السابعة، 2015، ص 265.

²- د. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الفكر العربي، القاهرة، الطبعة السابعة، 2013، ص 317.

³- د. محمد عيد الغريب، الدليل الإلكتروني أمام القضاء الجنائي، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، 2014، ص 101.

⁴- د. خالد ممدوح إبراهيم، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2019، ص 144.

⁵- Casey Eoghan, Digital Evidence and Computer Crime, Academic Press, Third Edition, 2011,

p. 221.

وسلسلة الحيازة هي وثيقة تسجل كل من تناول الدليل منذ لحظة ضبطه، مع تحديد وقت ومكان وتسليم كل شخص للآخر، والإجراءات التي تمت عليه¹. وهي تهدف إلى إثبات أن الدليل لم يتم التلاعب به، وتحديد المسؤولية في حال ثبوت التلاعب، وتمكين الخصوم من تتبع تاريخ الدليل².

أما التوقيع الرقمي (Hash) فهو قيمة رقمية فريدة تُستخرج من ملف أو قرص صلب باستخدام خوارزمية رياضية (كالـ SHA-256). فإذا تغير الملف بأي شكل، ولو بتغيير حرف واحد، تتغير قيمة الـ Hash بالكامل، مما يتيح التأكد من سلامة النسخة المقدمة للقضاء³.

الشرط الثالث هو شرط الصلة، ويقصد به أن يكون الدليل الإلكتروني مرتبطاً بالوقائع محل الدعوى، وقادراً على إثباتها أو نفيها⁴. فلا يجوز قبول دليل إلكتروني لا علاقة له بالقضية، أو تم جمعه عن طريق الصدفة دون أن يكون له مساس بالوقائع المطلوب إثباتها⁵.

¹ - Brian Carrier, File System Forensic Analysis, Addison-Wesley, First Edition, 2005, p. 367.

² - Kruse Warren & Heiser Jay, Computer Forensics: Incident Response Essentials, Addison-Wesley, Second Edition, 2002, p. 198

³ - Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations, Cengage Learning, Fifth Edition, 2015, p. 254.

⁴ - د. عبد الفتاح بيومي حجازي، الإثبات الجنائي الإلكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2016، ص

⁵ - د. عبد الله سليمان، شرح قانون العقوبات الجزائري، ديوان المطبوعات الجامعية، الجزائر، الطبعة السادسة، 2012، ص

فيما يتعلق بأنواع الدليل الإلكتروني، يمكن تصنيفها إلى سبعة أنواع رئيسية¹.

البيانات المخزنة (Stored Data): وتشمل الملفات والوثائق والصور والمقاطع البرمجية المخزنة على الأجهزة الإلكترونية. وهي أكثر أنواع الأدلة الرقمية شيوعاً².

بيانات المرور (Traffic Data): وتشمل البيانات التي تولدها الاتصالات الإلكترونية، كمصدر الاتصال ووجهته ومساره وتوقيته وتاريخه ومدته. تحتفظ بها شركات الاتصالات ومقدمو خدمات الإنترنت (ISP)، وتعتبر أدلة حاسمة في تتبع النشاط الإجرامي لأنها تكشف "من اتصل بمن ومتى وكم استغرق"³.

البيانات الواردة في سجلات النظام (System Logs): وهي سجلات آلية تسجل الأحداث على النظام المعلوماتي، كعمليات الدخول والخروج والمحاولات الفاشلة والتغييرات التي تطرأ على الملفات. لا يمكن التلاعب بها بسهولة لأنها تُكتب تلقائياً⁴.

البيانات الواردة في سجلات مقدمي الخدمات (ISP Logs): وهي البيانات التي يحتفظ بها مقدمو خدمات الإنترنت عن عملائهم، كعنوان الآي بي المخصص لكل عميل، ومواعيد اتصاله بالإنترنت¹.

¹ - Casey Eoghan, Handbook of Digital Forensics and Investigation, Academic Press, First Edition, 2010, p. 89.

² - Brian Carrier, File System Forensic Analysis, مرجع سابق، ص 172.

³ - Convention on Cybercrime (Budapest Convention), Council of Europe, 2001, Article 1, p. 3.

⁴ - Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations, مرجع

سابق، ص 318.

البيانات المتعلقة بالمحتوى (Content Data): وهي البيانات التي تعبر عن مضمون الاتصالات، كمحتوى الرسائل الإلكترونية والرسائل النصية والمكالمات الصوتية عبر الإنترنت. وهي الأكثر حساسية من حيث الخصوصية، وتتطلب إذنًا قضائيًا خاصاً².

البيانات الوصفية (Metadata): وهي بيانات تصف بيانات أخرى، كاسم المؤلف وتاريخ الإنشاء والتعديل والجهاز المستخدم. حاسمة في إثبات نسب المستندات الإلكترونية وكشف التزوير، فإذا كان تاريخ تعديل ملف يسبق تاريخ إنشائه، فهذا دليل على التلاعب³.

الأدلة الرقمية المستعادة (Deleted/Recovered Data): وهي البيانات التي تم مسحها ولكن لا تزال قابلة للاستعادة تقنياً، لأن عملية المسح لا تمحو البيانات فعلياً بل تشير إلى أن المساحة أصبحت متاحة للكتابة فوقها. مهمة جداً لأن المجرمين غالباً ما يحاولون مسح الأدلة⁴.

تعد مسألة سلامة الدليل الإلكتروني من أكثر المسائل تعقيداً في مجال الإثبات الجنائي، لأن البيانات الرقمية بطبيعتها قابلة للتعديل أو النسخ أو الإتلاف دون أن يترك ذلك أثراً ظاهراً كما هو الحال في الأدلة التقليدية⁵. ولذلك تعتمد المختبرات الجنائية الحديثة على بروتوكولات

¹ - د. محمد الأمين البشري، جرائم الإنترنت وطرق مكافحتها، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2017، ص 133.

² - Convention on Cybercrime (Budapest Convention)، مرجع سابق، المادة 21، ص 18.

³ - Eoghan Casey, Digital Evidence and Computer Crime، مرجع سابق، ص 412.

⁴ - Brian Carrier, File System Forensic Analysis، مرجع سابق، ص 401.

⁵ - Casey Eoghan, Digital Evidence and Computer Crime، مرجع سابق، ص 146.

تقنية صارمة لضمان سلامة الأدلة الرقمية، من بينها استخدام وسائل الحماية من الكتابة (Write Blockers) التي تمنع أي تعديل على وسائط التخزين أثناء عملية الفحص¹. كما يتم الاعتماد على تقنيات التحقق الرياضي بواسطة قيم الـ Hash للتأكد من أن النسخة الجنائية مطابقة تماماً للأصل². وتبرز أهمية هذه الإجراءات في منع الطعن في الدليل أمام القضاء، إذ يمكن لأي خلل في سلسلة الحيازة أو في إجراءات النسخ والتحليل أن يؤدي إلى استبعاد الدليل بالكامل³. ولهذا السبب، أصبحت عملية جمع الأدلة الرقمية علماً قائماً بذاته يخضع لقواعد ومعايير دولية دقيقة⁴

ومن جهة أخرى، فإن تنوع الأدلة الرقمية يفرض على القاضي والخبير فهماً واسعاً لطبيعة كل نوع من هذه الأدلة وحدوده التقنية والقانونية⁵. فالبيانات المخزنة تختلف في قيمتها الإثباتية عن بيانات المرور أو البيانات الوصفية، كما أن لكل نوع منها طريقة خاصة في الجمع

¹ - Brian Carrier, File System Forensic Analysis, مرجع سابق، ص 304.

² - Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations, مرجع سابق، ص 268.

³ - د. خالد ممدوح إبراهيم، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2019، ص 187.

⁴ - Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, First Edition, 2010, p. 118.

⁵ - د. عبد الفتاح بيومي حجازي، الإثبات الجنائي الإلكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2016، ص 144.

والتحليل والتفسير¹. وتعتبر البيانات الوصفية من أخطر أنواع الأدلة الرقمية لأنها تكشف تفاصيل خفية قد لا تظهر في محتوى الملف نفسه، مثل تاريخ الإنشاء والتعديل ومصدر الملف والجهاز المستخدم². كما أن البيانات المسترجعة من الملفات المحذوفة تمثل دليلاً بالغ الأهمية في القضايا السيبرانية، لأنها غالباً ما تعكس محاولة الجاني إخفاء نشاطه الإجرامي³. غير أن الاعتماد على هذا النوع من الأدلة يتطلب خبرة تقنية متقدمة، لأن استرجاع البيانات وتحليلها بصورة خاطئة قد يؤدي إلى نتائج مضللة أو غير دقيقة⁴.

الفرع الثالث: القيمة القانونية للدليل الرقمي أمام القضاء

لم يستقر القضاء الجزائري بعد على موقف موحد بشأن القيمة القانونية للدليل الرقمي، وذلك لقلة القضايا السيبرانية التي وصلت إلى المحاكم، ولحدثة الموضوع⁵. غير أنه يمكن استخلاص بعض المبادئ من الأحكام الصادرة في القضايا المتعلقة بالسب والقذف عبر الإنترنت أو الاحتيال الإلكتروني⁶.

¹ - Convention on Cybercrime (Budapest Convention)، المرجع سابق، المادة 18، ص 15.

² - Casey Eoghan, Digital Evidence and Computer Crime، المرجع سابق، ص 233.

³ - Brian Carrier, File System Forensic Analysis، المرجع سابق، ص 421.

⁴ - د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، مرجع سابق، ص 176.

⁵ - د. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، الطبعة الخامسة عشرة، 2019، ص 522.

⁶ - د. عبد العزيز سعد، الجرائم الواقعة على نظم المعالجة الآلية للمعطيات، دار هومة، الجزائر، الطبعة الأولى، 2016، ص 95.

فقد قبل القضاء الجزائري المطبوعات الإلكترونية (كصفحات مواقع التواصل الاجتماعي) كدليل في الدعوى، بشرط التأكد من عدم تلاعب الخصوم بها، وأن يتم تقديمها في صورة تقرير رسمي من خبير أو مسؤول عن النظام المعلوماتي¹. كما اعتدى بسجلات الاتصالات المقدمة من شركات الهاتف المحمول ومقدمي خدمات الإنترنت، بحكم أن هذه الشركات تخضع لرقابة الدولة وتتمتع بقرينة الصدق والموثوقية².

غير أن القضاء الجزائري شدد على عدم الاعتداد بالأدلة الرقمية التي يتم جمعها بوسائل غير مشروعة، كاختراق حساب شخص على مواقع التواصل لاستخراج رسائل خاصة، أو استخدام برمجيات تجسس دون إذن قضائي³. كما شددت المحكمة العليا على ضرورة تعليل الأحكام فيما يتعلق بالدليل الرقمي، وعدم الاكتفاء بالإشارة العامة إلى "ما ورد في تقرير الخبير"⁴.

يخضع تقدير القاضي للدليل الرقمي لثلاثة ضوابط رئيسية⁵. أولها حرية الاقتناع الشخصي، فالقاضي له السلطة التقديرية الكاملة في تقدير قيمة الدليل الرقمي، وهو غير ملزم

¹ - المحكمة العليا الجزائرية، غرفة الجناح والمخالفات، قرار رقم 128745، بتاريخ 12 مارس 2021، مجلة المحكمة العليا، العدد 1، 2022، ص 76.

² - المحكمة العليا الجزائرية، قرار رقم 135221، بتاريخ 15 سبتمبر 2022، مجلة القضاء، العدد 3، 2023، ص 91.

³ - د. محمد حسين منصور، الإثبات الإلكتروني، مرجع سابق، ص 208.

⁴ - المحكمة العليا الجزائرية، قرار رقم 140812، بتاريخ 7 جانفي 2024، مجلة المحكمة العليا، العدد 2، 2024، ص 102.

⁵ - د. محمود نجيب حسني، نظرية الإثبات الجنائي، مرجع سابق، ص 144.

باتباع رأي خبير بعينه¹. وثانيها ضرورة التعليل، حيث يلتزم القاضي بتعليل حكمه، مبيناً الأسباب التي دفعته إلى الأخذ بدليل معين أو رفضه، وكيفية تأكده من سلامة الدليل الرقمي². وثالثها احترام الضمانات الإجرائية، فلا يمكن للقاضي أن يعتد بدليل تم الحصول عليه بطرق غير مشروعة³.

لا يمكن القول بحجية مطلقة للدليل الرقمي أمام القضاء الجزائي، بل هي حجية نسبية. وذلك لسهولة تزوير الدليل الرقمي أو التلاعب به، ولطابع التقني للدليل مما يصعب فهمه على القاضي غير المختص، ولأن القاضي يعتمد في معظم القضايا السيبرانية على تقارير الخبراء مما يجعل الحجية غير مباشرة⁴.

تتأثر القيمة القانونية للدليل الرقمي بدرجة كبيرة بمدى اقتناع القاضي بسلامة الإجراءات التي رافقت جمعه وتحليله وتقديمه أمام المحكمة⁵. فالقاضي الجزائي، وإن كان يتمتع بحرية واسعة في تكوين اقتناعه الشخصي، إلا أنه يبقى مطالباً بالتحقق من أن الدليل الرقمي قد تم الحصول عليه وفق الضمانات القانونية والتقنية التي تكفل عدم المساس بحقوق الأفراد أو التلاعب بالبيانات⁶. ولذلك فإن المحاكم الحديثة لم تعد تكتفي بمجرد تقديم ملف إلكتروني أو

¹- د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، مرجع سابق، ص 301.

²- د. أحمد شوقي الشلقاني، مبادئ الإجراءات الجنائية، مرجع سابق، ص 241.

³- د. فتحي سرور، الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص 547.

⁴- د. خالد ممدوح إبراهيم، حجية الدليل الإلكتروني في الإثبات الجنائي، مرجع سابق، ص 169.

⁵- د. محمود نجيب حسني، نظرية الإثبات الجنائي، دار النهضة العربية، القاهرة، الطبعة الثانية، 2011، ص 228.

⁶- د. فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة العاشرة، 2014، ص 588.

صورة رقمية، بل تشترط أن تكون هذه الأدلة مدعمة بتقارير فنية وخبرة متخصصة تبين مصدر الدليل وكيفية استخراجهِ وسلامته التقنية¹. كما أن بعض المحاكم المقارنة اتجهت إلى اعتماد معايير خاصة لتقييم الأدلة الرقمية، تقوم على فحص مصداقية البرمجيات المستخدمة في التحليل، وكفاءة الخبير، ومدى احترام سلسلة الحيازة². ويظهر من ذلك أن حجية الدليل الرقمي ليست حجية تلقائية، وإنما تخضع لرقابة دقيقة من السلطة القضائية التي توازن بين فعالية الإثبات من جهة، وضمان حقوق الدفاع والخصوصية من جهة أخرى³

ومن ناحية أخرى، فإن التطور التقني الحديث أوجد تحديات جديدة أمام القضاء فيما يتعلق بتقدير القيمة القانونية للدليل الرقمي، خاصة مع انتشار تقنيات التزييف العميق (Deepfake) والذكاء الاصطناعي القادر على إنشاء صور ومقاطع صوتية وفيديوهات يصعب تمييزها عن الحقيقة⁴. وقد أدى ذلك إلى تزايد الدعوات الفقهية إلى ضرورة تعزيز

¹-د. خالد ممدوح إبراهيم، حجية الدليل الإلكتروني في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2011، ص 211.

²- Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations, Cengage Learning, Fifth Edition, 2015, p. 347.

³-د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الثالثة، 2014، ص 396.

⁴-د. محمد الأمين البشري، الجرائم الإلكترونية والتحقيق فيها، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، 2016، ص 244.

الوسائل التقنية والقانونية للتحقق من أصالة الأدلة الرقمية قبل اعتمادها قضائياً¹. كما برز اتجاه قضائي حديث يشدد على ضرورة دعم الدليل الرقمي بأدلة أخرى كلما أمكن، وعدم بناء الإدانة على دليل رقمي منفرد إذا كانت هناك شكوك تقنية تحيط به². ولهذا أصبحت الخبرة الرقمية تحتل مكانة محورية في الدعوى الجزائية السيبرانية، لأنها تمثل الوسيلة الأساسية التي تساعد القاضي على فهم الجوانب التقنية المعقدة وتقييم مدى موثوقية الأدلة المعروضة أمامه³. كما أن احترام معايير التوثيق والشفافية في إعداد التقارير الفنية يعزز ثقة القضاء في الدليل الرقمي ويمنحه قوة إثباتية أكبر⁴.

¹ Casey Eoghan, Digital Evidence and Computer Crime, Academic Press, Third Edition, 2011, p. 521.

² د. أحمد شوقي الشلقاني، مبادئ الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، الطبعة الأولى، 2010، ص 334.

³ Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, First Edition, 2010, p. 366.

⁴ د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، منشأة المعارف، الإسكندرية، الطبعة الأولى، 2009، ص 287.

المطلب الثاني: إجراءات جمع وتحليل الأدلة الرقمية

لا يكفي مجرد وجود دليل رقمي لإثبات الجريمة، بل لا بد من جمعه وتحليله وفق إجراءات قانونية وتقنية سليمة تضمن سلامته ومقبوليته أمام القضاء¹. فالدليل الرقمي يتميز بالهشاشة، وأي خطأ في عملية جمعه أو تحليله قد يؤدي إلى فقدان الدليل أو إضعاف حجته².

الفرع الأول: تفتيش وضبط الأجهزة الإلكترونية

تختلف عملية تفتيش الأجهزة الإلكترونية اختلافاً جوهرياً عن عملية تفتيش الأشياء المادية التقليدية³. فالجهاز الإلكتروني الواحد يمكن أن يحتوي على ملايين الملفات، مما يستدعي نقله إلى المختبر بدلاً من تفتيشه في مسرح الجريمة⁴. كما أن الجهاز غالباً ما يحتوي على بيانات شخصية حساسة لا علاقة لها بالجريمة، وتفتيشها دون سبب قد يشكل انتهاكاً خطيراً

¹ - د. محمد الأمين البشري، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 155.

² - Casey Eoghan, Digital Evidence and Computer Crime، مرجع سابق، ص 243.

³ - Brian Carrier, File System Forensic Analysis، مرجع سابق، ص 53.

⁴ - Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations، مرجع

سابق، ص 291.

للخصوصية¹. بالإضافة إلى ذلك، فإن أي تشغيل خاطئ للجهاز قد يؤدي إلى تعديل الطوابع الزمنية للملفات أو مسح بيانات حيوية².

في القانون الجزائري، يخضع تفتيش الأجهزة الإلكترونية لضوابط قانونية صارمة³. فلا يجوز التفتيش إلا بإذن من قاضي التحقيق أو النيابة العامة، إلا في حالتين استثنائيتين: حالة التلبس بالجريمة، أو حالة الاستعجال القصوى⁴. ويجب أن يكون الإذن القضائي كتابياً ومسبباً، وأن يحدد بدقة الجهاز المراد تفتيشه والمكان ونطاق التفتيش⁵.

كما يجب أن يتم التفتيش بحضور صاحب الجهاز أو من يمثله قانونياً، وذلك لضمان حقوق الدفاع⁶. ويلتزم ضابط الشرطة القضائية بحدود التفتيش (مبدأ التناسب)، فلا يجوز الاطلاع على ملفات شخصية لا صلة لها بالجريمة⁷. كما يحظر استخدام أي وسائل إكراه لإجبار صاحب الجهاز على فتحه أو فك تشفيره⁸.

¹ - د. عبد الفتاح بيومي حجازي، الحماية الجنائية للحياة الخاصة عبر الإنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2015، ص 73.

² - Eoghan Casey, Handbook of Digital Forensics and Investigation- مرجع سابق، ص 154.

³ - الجريدة الرسمية للجمهورية الجزائرية، قانون الإجراءات الجزائية الجزائري، آخر تعديل 2025، ص 65.

⁴ - د. أحسن بوسقيعة، التحقيق القضائي في القانون الجزائري، مرجع سابق، ص 238.

⁵ - د. عبد العزيز سعد، أبحاث تحليلية في قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 329.

⁶ - د. محمد زكي أبو عامر، الإجراءات الجنائية، مرجع سابق، ص 302.

⁷ - د. رؤوف عبيد، مبادئ الإجراءات الجنائية، مرجع سابق، ص 355.

⁸ -

أما الإجراءات التقنية الواجب اتباعها أثناء تفتيش الأجهزة الإلكترونية (البروتوكول الميداني) فتشمل خمس خطوات رئيسية¹.

الخطوة الأولى: توثيق مسرح الجريمة الرقمي، وذلك بتصوير المكان الذي يوجد فيه الجهاز بالفيديو والصور الفوتوغرافية من زوايا متعددة، وتوثيق وضعية الجهاز (مفتوح أو مغلق، موصل بالكهرباء أو بالإنترنت)، وتوثيق كل ما هو موصل بالجهاز، وتسجيل اسم الجهاز ونوعه وطراره ورقمه التسلسلي².

الخطوة الثانية: عزل الجهاز عن مصادر الاتصال والطاقة فوراً، وذلك بفصل كابل الطاقة، وفصل البطارية إذا كان الجهاز محمولاً، وفصل كابل الشبكة، ثم وضع الجهاز في "حقيبة فاراداي" (Faraday Bag) وهي كيس معزول كهربائياً يمنع أي إشارات من الدخول أو الخروج³.

الخطوة الثالثة: عدم تشغيل الجهاز أو إجراء أي عملية عليه تحت أي ظرف، سواء كان مفتوحاً أو مغلقاً، لأن أي تشغيل قد يؤدي إلى تعديل الطوابع الزمنية للملفات أو مسح بيانات حيوية⁴.

¹ - Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations , مرجع سابق، ص 344.

² - Casey Eoghan, Digital Evidence and Computer Crime , مرجع سابق، ص 287.

³ - Kruse Warren & Heiser Jay, Computer Forensics , مرجع سابق، ص 221.

⁴ - Brian Carrier, File System Forensic Analysis , مرجع سابق، ص 77.

الخطوة الرابعة: نقل الجهاز إلى المختبر في أسرع وقت ممكن، بوضعه في كيس معزول مكتوب عليه رقم القضية وتاريخ الضبط وتوقيع الضابط، مع مراعاة عدم تعريضه للاهتزاز أو الصدمات¹.

الخطوة الخامسة: تحرير محضر التفتيش والضبط، ويتضمن أسباب التفتيش وسنده القانوني، وتاريخ ووقت بدء وانتهاء التفتيش، ووصفاً دقيقاً للجهاز، ووصفاً لكل إجراء تم عليه، وملاحظات صاحب الجهاز².

فيما يتعلق بحجز الأجهزة الإلكترونية، يجوز للسلطات الاكتفاء بـ"الحجز المرآة" أو "التصوير الجنائي" (Forensic Imaging)، وهو عمل نسخة طبق الأصل عن محتويات الجهاز ثم تحليل النسخة وإعادة الجهاز إلى صاحبه³. وهذا الإجراء مقبول قانوناً في الجزائر، لأنه يحقق التوازن بين حاجة العدالة إلى الدليل وحق صاحب الجهاز في الانتفاع به⁴.

غير أن هناك حالات تستدعي حجز الجهاز نفسه: إذا كان الجهاز هو أداة الجريمة، أو كان صغير الحجم وسهل التخفي أو الإتلاف، أو كان صاحب الجهاز غير متعاون، أو كانت البيانات مشفرة ولا يمكن نسخها دون فك التشفير⁵.

¹—Eoghan Casey, Handbook of Digital Forensics and Investigation, مرجع سابق، ص 201.

²—د. خالد ممدوح إبراهيم، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، مرجع سابق، ص 211.

³—د. محمد الأمين البشري، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 188.

⁴—د. عبد الفتاح بيومي حجازي، الدليل الجنائي الرقمي وحجيته في الإثبات الجنائي، مرجع سابق، ص 164.

⁵—Casey Eoghan, Digital Evidence and Computer Crime, مرجع سابق، ص 315.

تثير عملية تفتيش الأجهزة الإلكترونية إشكالات قانونية دقيقة تتعلق بالتوازن بين مقتضيات البحث والتحري من جهة، وضمان الحق في الخصوصية وحماية الحياة الخاصة من جهة أخرى¹. فالأجهزة الرقمية الحديثة، كالهواتف الذكية والحواسيب المحمولة، لم تعد مجرد وسائل تقنية، بل أصبحت مخازن ضخمة للبيانات الشخصية والمهنية والعائلية، بما في ذلك الصور والمراسلات والحسابات البنكية والوثائق الخاصة². ولهذا فإن أي تفتيش غير مشروع لهذه الأجهزة قد يشكل اعتداءً خطيراً على الحقوق والحريات الأساسية المكفولة دستورياً³. ومن هذا المنطلق، شددت التشريعات المقارنة على ضرورة احترام مبدأ التناسب أثناء التفتيش، بحيث يقتصر البحث على البيانات المرتبطة بالجريمة محل التحقيق دون التوسع في فحص البيانات الشخصية غير المتعلقة بها⁴. كما أصبح الإذن القضائي المسبق شرطاً أساسياً في أغلب الأنظمة القانونية الحديثة، مع ضرورة أن يكون الإذن محدداً من حيث نوع الجهاز والبيانات المطلوب الوصول إليها والمدة الزمنية للتفتيش⁵.

¹-د. عبد الفتاح بيومي حجازي، الحماية الجنائية للحياة الخاصة عبر الإنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2015، ص 102.

²-د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، منشأة المعارف، الإسكندرية، الطبعة الأولى، 2009، ص 194.

³-د. فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة العاشرة، 2014، ص 621.

⁴-د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الثالثة، 2014، ص 411.

⁵-د. محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، الطبعة السابعة، 2015، ص 356.

وعلى المستوى التقني، فإن نجاح عملية ضبط الأجهزة الإلكترونية يعتمد بدرجة كبيرة على سرعة تدخل المحققين وكفاءتهم الفنية¹. فبعض البيانات الرقمية تكون مؤقتة أو متطايرة (Volatile Data)، مثل البيانات المخزنة في الذاكرة العشوائية أو الاتصالات النشطة، والتي قد تضيع فور إيقاف تشغيل الجهاز². ولذلك يقتضي الأمر أحياناً التعامل مع الجهاز وهو في حالة تشغيل، مع اتخاذ تدابير دقيقة لمنع تغيير البيانات أو إتلافها³. كما أن المجرمين السيبرانيين يلجؤون في كثير من الأحيان إلى وسائل متطورة لإخفاء الأدلة، كالتشفير أو برامج التدمير الذاتي للبيانات، مما يفرض على المحققين استخدام أدوات وتقنيات متقدمة لاستخراج المعلومات دون المساس بسلامتها⁴. ويؤدي أي خطأ أثناء التفتيش أو النقل أو الحفظ إلى إمكانية الطعن في الدليل لاحقاً أمام القضاء، الأمر الذي يبرز أهمية الالتزام الصارم بالبروتوكولات التقنية والقانونية المعتمدة دولياً⁵

الفرع الثاني: استخراج البيانات الرقمية وتحليلها

¹ - Casey Eoghan, Digital Evidence and Computer Crime, Academic Press, Third Edition, 2011, p. 281.

² - Brian Carrier, File System Forensic Analysis, Addison-Wesley, First Edition, 2005, p. 339.

³ - Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations, Cengage Learning, Fifth Edition, 2015, p. 371.

⁴ - Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, First Edition, 2010, p. 244.

⁵ - د. خالد ممدوح إبراهيم، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2019، ص 268.

بعد حجز الجهاز الإلكتروني، تنقل عملية استخراج البيانات وتحليلها إلى مختبر متخصص¹. تبدأ عملية استخراج البيانات بعمل نسخة جنائية (Forensic Imaging)، وهي نسخة طبق الأصل (bit-for-bit copy) عن كامل محتويات الجهاز، بما في ذلك الملفات المحذوفة والمساحات غير المخصصة، باستخدام برمجيات متخصصة².

وتتم عملية التصوير الجنائي عادةً بطريقتين³. الأولى هي النسخ المباشر (Live Imaging) وتستخدم للخوادم التي لا يمكن إيقافها، ولكنها محفوفة بالمخاطر لأن أي نشاط على الجهاز أثناء النسخ قد يغير البيانات⁴. والثانية هي النسخ بعد الإغلاق (Dead Imaging) وهي الأكثر أماناً، حيث يتم إغلاق الجهاز ثم نزع القرص الصلب ونسخ البيانات⁵.

¹—Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations، مرجع سابق، ص 402.

²—Brian Carrier, File System Forensic Analysis، مرجع سابق، ص 411.

³—Eoghan Casey, Handbook of Digital Forensics and Investigation، مرجع سابق، ص 229.

⁴—Kruse Warren & Heiser Jay, Computer Forensics: Incident Response Essentials، مرجع سابق، ص 244.

⁵—Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations، مرجع سابق، ص 415.

بعد الانتهاء من النسخ، يتم حساب قيمة التوقيع الرقمي (Hash Value) للأصل وللنسخة، فإذا تطابقت القيم، فهذا يعني أن النسخة مطابقة تماماً للأصل¹. ثم يتم وضع القرص الصلب الأصلي في مكان آمن، وجميع عمليات التحليل تتم على النسخة الجنائية².

أما تحليل البيانات الرقمية فيشمل عدة تقنيات³. تحليل سجلات النظام لتحديد متى تم الدخول إلى النظام، ومن الذي دخل، وما هي الملفات التي تم الوصول إليها⁴. تحليل بيانات المرور لتحديد مصدر الهجوم ووجهته، والمسارات التي سلكتها البيانات⁵. تحليل البيانات الوصفية لفحص تاريخ إنشاء الملف وتاريخ تعديله، واسم المؤلف، والجهاز المستخدم⁶. تحليل الأنشطة الزمنية لترتيب الأحداث في جدول زمني واحد لرسم صورة متكاملة لمسار الجريمة⁷.

¹– Casey Eoghan, Digital Evidence and Computer Crime، مرجع سابق، ص 337.

²– Brian Carrier, File System Forensic Analysis، مرجع سابق، ص 438.

³– د. خالد ممدوح إبراهيم، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، مرجع سابق، ص 247.

⁴– Eoghan Casey, Handbook of Digital Forensics and Investigation، مرجع سابق، ص 263.

⁵– Convention on Cybercrime (Budapest Convention), Council of Europe, 2001, Article 20, p. 17.

⁶– Casey Eoghan, Digital Evidence and Computer Crime، مرجع سابق، ص 429.

⁷– Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations، مرجع

سابق، ص 461.

واستعادة الملفات المحذوفة لأن نظام التشغيل لا يسمح البيانات فعلياً بل يشير إلى أن المساحة أصبحت متاحة للكتابة فوقها¹.

بعد الانتهاء من التحليل، يجب توثيق كل خطوة في تقرير فني مفصل يُقدم إلى القضاء². يتضمن التقرير مقدمة (الجهة الطالبة، تاريخ التعيين، الأسئلة المطلوب الإجابة عنها)، ووصف الأدوات والأجهزة المستخدمة، ووصف الإجراءات المتبعة (كيف تم الاستلام، النسخ، التحليل، قيمة الـ Hash)، ونتائج التحليل، والاستنتاجات، والملاحق (صور، قوائم، سلسلة الحيازة)³.

تُعد مرحلة استخراج البيانات الرقمية وتحليلها من أكثر مراحل التحقيق السيبراني تعقيداً، لأنها تمثل المرحلة التي تتحول فيها البيانات الخام إلى أدلة يمكن الاستناد إليها أمام القضاء⁴. ولا يقتصر عمل الخبراء في هذه المرحلة على استرجاع الملفات أو قراءة محتويات الأجهزة، بل يمتد إلى تحليل العلاقات بين البيانات، وتتبع النشاط الرقمي للمشتبه فيه، وربط الوقائع التقنية بالسلوك الإجرامي محل المتابعة⁵. ويستخدم الخبراء في ذلك برمجيات متخصصة قادرة على تحليل ملايين الملفات والبيانات خلال فترة زمنية قصيرة، مع تصنيفها وفق أهميتها وعلاقتها

¹– Brian Carrier, File System Forensic Analysis، مرجع سابق، ص 492.

²– د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، مرجع سابق، ص 221.

³– د. خالد ممدوح إبراهيم، التحقيق الجنائي الرقمي والأدلة الرقمية، مرجع سابق، ص 273.

⁴– د. خالد ممدوح إبراهيم، التحقيق الجنائي الرقمي والأدلة الرقمية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2017، ص 291.

⁵– Casey Eoghan, Digital Evidence and Computer Crime، مرجع سابق، ص 329.

بالجريمة¹. كما تعتمد المختبرات الحديثة على تقنيات الذكاء الاصطناعي والتعلم الآلي للمساعدة في اكتشاف الأنماط المشبوهة وتحليل السلوك الإجرامي الرقمي بصورة أكثر دقة وسرعة². غير أن الاعتماد على هذه التقنيات لا يلغي دور العنصر البشري، لأن تفسير النتائج التقنية وربطها بالسياق القانوني يظل من اختصاص الخبير المختص³

كما أن تحليل البيانات الرقمية لا يهدف فقط إلى إثبات وقوع الجريمة، وإنما يساعد أيضاً في إعادة بناء التسلسل الزمني للأحداث وتحديد دور كل شخص شارك في النشاط الإجرامي⁴. فالجداول الزمنية المستخرجة من سجلات النظام وبيانات الاتصال تتيح للمحققين معرفة توقيت الدخول إلى الأنظمة، والملفات التي تم تعديلها، والأوامر التي تم تنفيذها⁵. ويُعتبر هذا النوع من التحليل مهماً بشكل خاص في الجرائم المنظمة والهجمات الإلكترونية المعقدة، حيث يكون تحديد تسلسل الأحداث ضرورياً لفهم طريقة تنفيذ الجريمة وتحديد المسؤوليات⁶. كما أن عملية استرجاع البيانات المحذوفة أصبحت أداة فعالة في كشف محاولات إخفاء الأدلة، لأن حذف

¹ - Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations, مرجع سابق، ص 448.

² - Eoghan Casey, Handbook of Digital Forensics and Investigation, مرجع سابق، ص 389.

³ - د. محمد الأمين البشري، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، القاهرة، الطبعة الثانية، 2018، ص 242.

⁴ - Brian Carrier, File System Forensic Analysis, مرجع سابق، ص 463.

⁵ - Casey Eoghan, Digital Evidence and Computer Crime, مرجع سابق، ص 355.

⁶ - Convention on Cybercrime (Budapest Convention), Council of Europe, 2001, p. 14.

الملفات لا يؤدي بالضرورة إلى زوالها الكامل من وسائط التخزين¹. ومع ذلك، فإن أي خطأ في تفسير البيانات أو الربط بينها قد يؤدي إلى نتائج غير دقيقة، مما يجعل الدقة العلمية والحياد المهني من أهم المبادئ التي يجب أن تحكم عمل الخبير الرقمي²

الفرع الثالث: ضمان سلامة الأدلة الرقمية من العبث

تعتبر سلسلة الحيازة (Chain of Custody) العنصر الأهم في ضمان سلامة الدليل الرقمي ومقبوليته أمام القضاء³. فبدون سلسلة حيازة موثقة بشكل صحيح، يمكن للدفاع أن يطعن في الدليل بأنه قد تم التلاعب به⁴.

سلسلة الحيازة هي الوثيقة التي تسجل كل من تناول الدليل منذ لحظة ضبطه، مع تحديد وقت ومكان تسلمه، ومن قام بتسليمه، وإلى من تم تسليمه، والغرض من التسليم، وأي إجراء تم على الدليل⁵.

تهدف سلسلة الحيازة إلى أربعة أهداف رئيسية¹: إثبات أن الدليل لم يتم التلاعب به، وتحديد المسؤولية في حال ثبوت التلاعب، وتمكين الخصوم من تتبع تاريخ الدليل والتحقق من سلامته، وإضفاء المصادقية على الدليل في نظر القضاء².

¹ - Brian Carrier, File System Forensic Analysis, مرجع سابق، ص 501

² - د. عبد الفتاح بيومي حجازي، الإثبات الجنائي الإلكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2016، ص 233.

³ - Casey Eoghan, Digital Evidence and Computer Crime- مرجع سابق، ص 351.

⁴ - Kruse Warren & Heiser Jay, Computer Forensics- مرجع سابق، ص 267.

⁵ - Eoghan Casey, Handbook of Digital Forensics and Investigation, مرجع سابق، ص 284.

تبنى سلسلة حياة سليمة من خلال خمسة إجراءات³: التوثيق الأولي (تسجيل تاريخ ووقت الضبط، مكان الضبط، من قام بالضبط، وصف الجهاز، حالة الجهاز، والتوقيع)⁴، وضع الدليل في حاوية آمنة (حقيبة فاراداي أو صندوق مختوم) مكتوب عليها رقم القضية وتاريخ الضبط وتوقيع الضابط⁵، تسجيل كل انتقال (نموذج نقل الحياة) بتوقيع المسلم والمستلم⁶، تسجيل كل إجراء تم على الدليل (من قام به، تاريخه، وصفه، نتيجته)⁷، والتوقيع الرقمي (Hash) كضمان إضافي⁸.

يتحمل أعضاء الشرطة القضائية والخبراء مسؤولية كبيرة في الحفاظ على سلامة الأدلة الرقمية⁹. وفي القانون الجزائري، يمكن مساءلتهم على ثلاثة مستويات¹⁰: المساءلة الجنائية (إذا

¹- د. عبد الفتاح بيومي حجازي، الإثبات الجنائي الإلكتروني، مرجع سابق، ص 197.

²- د. محمد عيد الغريب، الدليل الإلكتروني أمام القضاء الجنائي، مرجع سابق، ص 168.

³- Nelson Phillips & Stuart Christopher, Guide to Computer Forensics and Investigations , مرجع سابق، ص 487.

⁴- Casey Eoghan, Digital Evidence and Computer Crime- مرجع سابق، ص 362.

⁵- Kruse Warren & Heiser Jay, Computer Forensics- مرجع سابق، ص 281.

⁶- Brian Carrier, File System Forensic Analysis- مرجع سابق، ص 511.

⁷- Eoghan Casey, Handbook of Digital Forensics and Investigation- مرجع سابق، ص 301.

⁸- Casey Eoghan, Digital Evidence and Computer Crime- مرجع سابق، ص 374.

⁹- د. عبد العزيز سعد، أبحاث تحليلية في قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 352.

¹⁰- د. أحسن بوسقيعة، التحقيق القضائي في القانون الجزائري، مرجع سابق، ص 267.

ثبت تعمدهم تزوير الدليل أو إتلافه)، والمساءلة التأديبية (إذا ثبت إهمالهم في الحفاظ على الدليل)، والمساءلة المدنية (إذا ترتب على إهمالهم ضرر لشخص كإدانة بريء)¹.

تُعد سلامة الأدلة الرقمية من الركائز الأساسية التي يقوم عليها الإثبات في الجرائم السيبرانية، لأن أي تشكيك في أصالة الدليل أو سلامته يؤدي إلى إضعاف قيمته القانونية وربما استبعاده بالكامل من ملف الدعوى². ولهذا السبب، تعتمد الأنظمة الجنائية الحديثة على مبدأ "سلسلة الحيازة" باعتباره الضمان الأساسي للحفاظ على موثوقية الدليل منذ لحظة ضبطه إلى غاية عرضه أمام المحكمة³. ويقتضي هذا المبدأ توثيق جميع المراحل التي مر بها الدليل، بما في ذلك الأشخاص الذين تعاملوا معه، والأماكن التي تم حفظه فيها، والإجراءات التي أُجريت عليه⁴. كما يتم اللجوء إلى وسائل تقنية متطورة لضمان عدم تعديل البيانات، مثل أنظمة التشفير والتوقيع الرقمي وأجهزة الحفظ المؤمنة⁵. وتبرز أهمية هذه الإجراءات بصورة خاصة في القضايا التي تعتمد بشكل أساسي على الأدلة الرقمية دون وجود أدلة مادية تقليدية داعمة⁶.

¹ - د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 489.

² - Casey Eoghan, Digital Evidence and Computer Crime, مرجع سابق، ص 381.

³ - Eoghan Casey, Handbook of Digital Forensics and Investigation, مرجع سابق، ص 297.

⁴ - Nelson Phillips & Stuart Christopher, Guide to Computer Forensics and Investigations, مرجع سابق، ص 482.

⁵ - Brian Carrier, File System Forensic Analysis, مرجع سابق، ص 528.

⁶ - د. خالد ممدوح إبراهيم، حجية الدليل الإلكتروني في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى،

2011، ص 244.

ومن جهة أخرى، فإن الحفاظ على سلامة الأدلة الرقمية لا يرتبط فقط بالإجراءات التقنية، وإنما يتطلب أيضاً وجود إطار قانوني وتنظيمي واضح يحدد مسؤوليات مختلف المتدخلين في عملية الإثبات¹. فالإهمال في حفظ الأجهزة أو سوء التعامل مع البيانات قد يؤدي إلى ضياع أدلة مهمة أو إلى تغيير محتواها بشكل غير مقصود². كما أن نقل الأدلة الرقمية بين الجهات الأمنية والمختبرات والمحاكم يجب أن يتم وفق ضوابط دقيقة تمنع الوصول غير المصرح به إليها³. ولهذا تتجه التشريعات الحديثة إلى فرض عقوبات صارمة على كل من يعبث بالأدلة الرقمية أو يتسبب في إتلافها عمداً أو نتيجة الإهمال الجسيم⁴. كما تدعو الاتجاهات الفقهية الحديثة إلى اعتماد معايير دولية موحدة في مجال حفظ الأدلة الرقمية، بما يضمن توحيد الممارسات وتعزيز الثقة في هذا النوع من الإثبات أمام القضاء الوطني والدولي⁵

¹-د. عبد العزيز سعد، أبحاث تحليلية في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، الطبعة الثانية، 2018، ص 401.

²-د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة السادسة، 2016، ص 566.

³-د. محمد زكي أبو عامر، الإجراءات الجنائية، مرجع سابق، ص 403.

⁴-د. رؤوف عبيد، مبادئ الإجراءات الجنائية، دار الفكر العربي، القاهرة، الطبعة السابعة، 2013، ص 471.

⁵- ISO/IEC 27037:2012, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, International Organization for Standardization, Geneva, 2012, p. 11.

المبحث الثاني: دور الجهات القضائية والأمنية في الإثبات السيبراني

لا يمكن الحديث عن الإثبات في الجرائم السيبرانية دون التطرق إلى دور الجهات القضائية والأمنية الفاعلة في هذا المجال¹. فهذه الجهات هي التي تمتلك صلاحية جمع الأدلة الرقمية وتحليلها، وتقديمها إلى القضاء الذي يفصل في الدعوى².

المطلب الأول: دور الضبطية القضائية والخبرة الرقمية

تلعب الضبطية القضائية والخبرة الرقمية دورًا محوريًا في الكشف عن الجرائم السيبرانية وإثباتها. فنجاح التحقيق في هذا النوع من الجرائم يعتمد إلى حد كبير على الكفاءة التقنية في التعامل مع الأدلة الرقمية. لذلك سنوضح اختصاصات الضبطية القضائية وأهمية الخبرة الفنية في مجال الإثبات السيبراني.

الفرع الأول: اختصاصات الضبطية القضائية في الجرائم السيبرانية

تطلبت مواجهة الجرائم السيبرانية وجود أجهزة شرطة قضائية متخصصة ذات مهارات تقنية عالية، لأن عضو الشرطة التقليدي لا يمتلك المعرفة اللازمة للتعامل مع الأدلة الرقمية³. استجاب المشرع الجزائري لهذا الطلب بموجب القانون 09-04، حيث أنشأ الوحدة الوطنية للبحث في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (تابعة للأمن الوطني)،

¹ - د. محمد الأمين البشري، الجرائم الإلكترونية والتحقيق فيها، مرجع سابق، ص 233.

² - د. عبد الفتاح بيومي حجازي، الدليل الإلكتروني في الجرائم المعلوماتية، مرجع سابق، ص 211.

³ - د. خالد ممدوح إبراهيم، التحقيق الجنائي الرقمي والأدلة الرقمية، مرجع سابق، ص 301.

ومركز البحث والتحليل في الجرائم السيبرانية (تابع للدرك الوطني)، بالإضافة إلى خلايا مماثلة في المديریات والأفواج الإقليمية¹.

تتمتع هذه الوحدات باختصاصات متعددة: تلقي البلاغات والإشعارات المتعلقة بالجرائم السيبرانية، وإجراء التحريات والتحقيقات الأولية وجمع الأدلة الرقمية، والاستعانة بخبراء تقنيين عند الحاجة، وتبادل المعلومات مع الوحدات المماثلة في الدول الأخرى².

يمنح القانون 04-09 أعضاء الضبطية القضائية المتخصصة صلاحيات أوسع من تلك المقررة لأعضاء الضبطية القضائية التقليدية³. فيمكنهم، بإذن قضائي، الدخول إلى النظم المعلوماتية للبحث عن أدلة⁴. كما يمكنهم، بإذن قضائي مسبب ومحدد المدة، مراقبة الاتصالات الإلكترونية في الوقت الحقيقي وجمعها وتسجيلها⁵. ولهم الحق في الإطلاع على بيانات المرور من مزودي الخدمات، وحجز البيانات المخزنة (بالنسخ أو المصادرة)⁶.

¹ - الجريدة الرسمية للجمهورية الجزائرية، القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47، سنة 2009، ص 7.

² - د. عبد العزيز سعد، الجرائم الواقعة على نظم المعالجة الآلية للمعطيات، مرجع سابق، ص 142.

³ - د. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص 544.

⁴ - الجريدة الرسمية للجمهورية الجزائرية، القانون رقم 04-09، المادة 3، ص 8.

⁵ - Convention on Cybercrime (Budapest Convention) -، مرجع سابق، المادة 20، ص 17.

⁶ - د. محمد الأمين البشري، جرائم الإنترنت وطرق مكافحتها، مرجع سابق، ص 191.

غير أن هذه الصلاحيات ليست مطلقة، بل تخضع لضمانات قانونية صارمة¹. فلا تجوز إلا بإذن قضائي مسبب، ويجب أن يكون الإذن محدداً من حيث الإجراء والمدة والجهاز المستهدف². وتتم الإجراءات بسرية، ولا يجوز إطلاع الشخص المستهدف عليها إلا بعد انتهائها³. كما لا يجوز استخدام هذه الصلاحيات للبحث عن جرائم أخرى غير الجريمة المصرح بها⁴. وللشخص المستهدف الحق في الطعن في قرار الإذن القضائي أمام محكمة أعلى⁵.

فيما يتعلق بالتعاون بين الضبطية القضائية ومقدمي الخدمات، فقد ألزم القانون 04-09 مقدمي الخدمات (شركات الاتصالات، مزودي الإنترنت، منصات التواصل) بالتعاون الفوري مع السلطات القضائية، والاحتفاظ ببيانات الاتصالات لمدة لا تقل عن سنة، وتقديمها خلال 48 ساعة⁶. غير أن هذا الإلزام لا يسري إلا على المزودين الموجودين في الجزائر، أما المزودون الأجانب فلا يمكن إجبارهم إلا عبر آليات التعاون الدولي⁷.

¹- د. فتحي سرور، الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص 655.

²- د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، مرجع سابق، ص 377.

³- د. رؤوف عبيد، مبادئ الإجراءات الجنائية، مرجع سابق، ص 402.

⁴- د. محمد زكي أبو عامر، الإجراءات الجنائية، مرجع سابق، ص 344.

⁵- د. أحمد شوقي الشلقاني، مبادئ الإجراءات الجنائية، مرجع سابق، ص 289.

⁶- الجريدة الرسمية للجمهورية الجزائرية، القانون رقم 04-09، مرجع سابق، ص 10.

⁷- د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون الدولي، مرجع سابق، ص 223.

الفرع الثاني: دور الخبرة الرقمية في الإثبات

الخبرة الرقمية (Digital Forensics) هي عملية علمية منهجية تهدف إلى جمع الأدلة الرقمية وتحليلها وتقديمها بشكل مقبول أمام القضاء¹. تتميز الخبرة الرقمية عن غيرها من أنواع الخبرات بالتطور السريع، والحاجة إلى أجهزة وبرمجيات متخصصة، والحاجة إلى تدريب مستمر وفهم قانوني².

يتم تعيين الخبير الرقمي من قبل السلطة القضائية (قاضي التحقيق أو محكمة الموضوع)³. ويجب أن تتوفر فيه المؤهل العلمي (شهادة في علوم الحاسوب أو مجال ذي صلة)، والتدريب المهني (شهادات مهنية متخصصة كـ GCFA، EnCE)، والخبرة العملية (3-5 سنوات على الأقل)، والنزاهة والاستقلالية (لا صلة له بالخصوم)، والقبول لدى الجهات القضائية (مقيد لدى وزارة العدل)⁴.

يمر عمل الخبير الرقمي بست مراحل رئيسية⁵.

¹- Casey Eoghan, Digital Evidence and Computer Crime, مرجع سابق، ص 17.

²- Eoghan Casey, Handbook of Digital Forensics and Investigation, مرجع سابق، ص 41.

³- د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 522.

⁴- Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations, مرجع سابق، ص 529.

⁵- د. خالد ممدوح إبراهيم، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، مرجع سابق، ص 317.

المرحلة الأولى: تحديد نطاق المهمة، حيث يجتمع الخبير مع السلطة القضائية لتحديد الأسئلة التي يجب الإجابة عنها (مثال: هل جهاز المتهم يحتوي على برمجيات اختراق؟ هل تم إرسال رسالة التهديد من حساب المتهم؟)¹.

المرحلة الثانية: جمع الأدلة، حيث يقوم الخبير (أو أعضاء الضبطية القضائية بإشرافه) بتفتيش الأجهزة وضبطها، وعمل النسخ الجنائية، وتوثيق سلسلة الحيازة².

المرحلة الثالثة: تحليل الأدلة، باستخدام تقنيات التحليل المختلفة (سجلات النظام، بيانات المرور، البيانات الوصفية، الجدول الزمني، استعادة الملفات المحذوفة)³.

المرحلة الرابعة: صياغة التقرير، حيث يصوغ الخبير تقريره كتابياً بلغة واضحة ومفهومة للقاضي غير الخبير، متضمناً مقدمة ووصف الإجراءات والنتائج والاستنتاجات والملاحق⁴.

المرحلة الخامسة: مراجعة التقرير، للتأكد من عدم وجود أخطاء لغوية أو فنية أو منهجية⁵.

¹ Casey Eoghan, Digital Evidence and Computer Crime- مرجع سابق، ص 58.

² Brian Carrier, File System Forensic Analysis- مرجع سابق، ص 533.

³ Eoghan Casey, Handbook of Digital Forensics and Investigation- مرجع سابق، ص 336.

⁴ د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، مرجع سابق، ص 266.

⁵ Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations- مرجع

سابق، ص 551.

المرحلة السادسة: الإدلاء بالشهادة أمام القضاء، حيث يحضر الخبير الجلسة، ويحلف اليمين، ويشرح تقريره، ويجيب على أسئلة القاضي والنيابة العامة والدفاع¹.

تكمن أهمية الخبرة الرقمية في ترجمة الدليل التقني إلى لغة قانونية يفهمها القاضي، وكشف التلاعب والتزوير باستخدام البيانات الوصفية والتوقيع الرقمي، وربط الجاني بالجريمة من خلال تحليل سجلات الدخول وبيانات المرور، وتوثيق الأدلة بشكل مقبول قضائياً من خلال سلسلة الحيازة والتوقيع الرقمي².

الفرع الثالث: تقييم تقارير الخبراء أمام القضاء

تقرير الخبير هو رأي فني وليس دليلاً قاطعاً، والقاضي غير ملزم باتباعه³. يتمتع تقرير الخبير بحجية "قرينة بسيطة" تفترض صحته ما لم يثبت العكس⁴.

للقاضي أن يرفض تقرير الخبير كلياً أو جزئياً إذا وجد فيه خطأ فادحاً (كاستخدام برمجية غير مناسبة)، أو تناقضاً داخلياً (بين النتائج الجزئية والنتيجة النهائية)، أو مخالفة للقانون (كاستخدام وسيلة جمع غير مشروعة)، أو انحيازاً ظاهراً (كتعبير الخبير عن رأي قانوني أو استخدام لغة غير موضوعية)⁵.

¹ - د. عبد الفتاح بيومي حجازي، الإثبات الجنائي الإلكتروني، مرجع سابق، ص 245.

² - د. خالد ممدوح إبراهيم، حجية الدليل الإلكتروني في الإثبات الجنائي، مرجع سابق، ص 233.

³ - د. فتحي سرور، الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص 701.

⁴ - د. محمود نجيب حسني، نظرية الإثبات الجنائي، مرجع سابق، ص 193.

⁵ - د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، مرجع سابق، ص 421.

من أهم ضمانات حقوق الدفاع، إمكانية مناقشة الخبير في تقريره أمام القضاء¹. يحضر الخبير الجلسة بأمر من المحكمة، ويحق للمتهم ومحاميه طرح أسئلة حول منهجية العمل، وصحة الإجراءات، واستنتاجات الخبير (هل هناك تفسير بديل للبيانات؟)، ومؤهلاته². كما يحق للمتهم طلب تعيين خبير آخر (خبرة مضادة) أو إعادة التحليل³.

في حال تعارض تقارير الخبراء (يقدم خبيران تقريرين متعارضين)، على القاضي أن يوازن بين التقريرين ويرجح أيهما أقوى بناءً على مؤهلات الخبراء وخبراتهم، ومنهجية العمل (هل اتبع الخبير البروتوكولات المعتمدة؟)، ودقة الإجراءات (هل قام بعمل نسخة جنائية؟ هل وثق سلسلة الحياة؟)، واتساق النتائج مع باقي الأدلة في الدعوى، والموضوعية (هل لغة الخبير موضوعية أم متحيزة؟)⁴.

المطلب الثاني: التحديات العلمية وآفاق تطوير الإثبات السيبراني

يواجه الإثبات في الجرائم السيبرانية العديد من الصعوبات القانونية والتقنية الناتجة عن التطور المستمر للتكنولوجيا وظهور أساليب إجرامية حديثة. وقد دفع ذلك إلى البحث عن حلول تشريعية وتقنية أكثر فعالية. ومن ثم سنتناول أبرز التحديات المطروحة والآفاق المستقبلية لتطوير منظومة الإثبات السيبراني.

¹ - د. محمد زكي أبو عامر، الإجراءات الجنائية، مرجع سابق، ص 391.

² - د. أحمد شوقي الشلقاني، مبادئ الإجراءات الجنائية، مرجع سابق، ص 317.

³ - د. رؤوف عبيد، مبادئ الإجراءات الجنائية، مرجع سابق، ص 437.

⁴ - د. عبد العزيز سعد، أبحاث تحليلية في قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 389.

الفرع الأول: الصعوبات العملية في إثبات الجرائم السيبرانية

تواجه عملية الإثبات السيبراني عدة صعوبات عملية¹.

أولاً: التطور التقني السريع. تتطور وسائل ارتكاب الجرائم السيبرانية بسرعة تفوق قدرة الأجهزة القضائية على مواكبتها². فبينما تستغرق الدول سنوات لسن قوانين جديدة، تظهر تقنيات إجرامية جديدة في غضون أشهر³. من أبرز هذه التقنيات: التشفير القوي (End-to-End Encryption) الذي يجعله تطبيقات مثل واتساب وسيجنال، مما يجعل الأدلة غير قابلة للقراءة بدون تعاون المتهم⁴. وشبكة تور (TOR) التي تسمح بالتصفح المجهول، مما يجعل تتبع النشاط شبه مستحيل⁵. والعملات المشفرة (Cryptocurrencies) التي تعيق تتبع الأموال في جرائم الاحتيال⁶. والذكاء الاصطناعي (AI) المستخدم في إنشاء رسائل تصيد متطورة و"ديب فيك"⁷.

¹ - د. محمد الأمين البشري، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 277.

² - د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون الدولي، مرجع سابق، ص 251.

³ - د. خالد ممدوح إبراهيم، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، مرجع سابق، ص 344.

⁴ - Casey Eoghan, Digital Evidence and Computer Crime- مرجع سابق، ص 471.

⁵ - Eoghan Casey, Handbook of Digital Forensics and Investigation- مرجع سابق، ص 392.

⁶ - د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، مرجع سابق، ص 301.

⁷ - د. خالد ممدوح إبراهيم، التحقيق الجنائي الرقمي والأدلة الرقمية، مرجع سابق، ص 355.

ثانياً: ندرة الكوادر البشرية المؤهلة. لا يتوفر في الجزائر عدد كافٍ من خبراء الأدلة الرقمية المؤهلين تأهيلاً عالياً¹. وغالباً ما يُعهد بمهمة الخبرة الرقمية إلى مهندسين حاسوب أو تقنيين، دون أن يكون لديهم تدريب في الجانب الجنائي (كقواعد الإثبات، وسلسلة الحياة، والشهادة أمام القضاء)². وهذا النقص يؤدي إلى تأخر إنجاز التقارير، وأخطاء فادحة، وعدم القدرة على مواكبة التطورات³.

ثالثاً: ضعف التنسيق بين النيابة العامة والجهات التقنية. يعاني المحققون (أعضاء النيابة العامة والشرطة القضائية) والقضاة من ضعف في الفهم التقني، ويتعاملون مع الأدلة الرقمية بنفس طريقة تعاملهم مع الأدلة المادية، مما قد يؤدي إلى إتلافها أو فقدانها⁴. كما أن الخبراء التقنيين قد لا يفهمون المتطلبات القانونية للإثبات، كأهمية توثيق سلسلة الحياة أو ضرورة الحصول على إذن قضائي قبل التفتيش⁵.

رابعاً: ضعف البنية التحتية التقنية. لا تمتلك كثير من النيابة والمحاكم الجزائرية معامل جنائية رقمية مجهزة بأحدث الأجهزة والبرمجيات⁶. فمعمل الأدلة الرقمية يحتاج إلى أجهزة حاسوب عالية الأداء، وبرمجيات متخصصة (كالـ EnCase التي تكلف آلاف الدولارات

¹ - د. عبد العزيز سعد، الجرائم الواقعة على نظم المعالجة الآلية للمعطيات، مرجع سابق، ص 181.

² - د. أحسن بوسقيعة، التحقيق القضائي في القانون الجزائري، مرجع سابق، ص 298.

³ - د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، مرجع سابق، ص 448.

⁴ - د. فتحي سرور، الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص 736.

⁵ - د. محمد زكي أبو عامر، الإجراءات الجنائية، مرجع سابق، ص 429.

⁶ - د. خالد ممدوح إبراهيم، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، مرجع سابق، ص 377.

سنوياً)، وأجهزة مادية (كموازن الأقراص وكيس فاراداي)، وغرفة محكمة مجهزة لعرض الأدلة الرقمية¹. كما أن بعض المحاكم لا تزال تتعامل بالطرق الورقية التقليدية، مما يصعب تقديم الأدلة الرقمية في شكلها الإلكتروني².

خامساً: غياب معايير وطنية موحدة. لا توجد في الجزائر معايير وطنية موحدة لجمع وتحليل الأدلة الرقمية، تلتزم بها كل وحدات الضبطية القضائية والخبراء³. وهذا الغياب يؤدي إلى تباين في الممارسات (وحدة شرطة تعمل بطريقة وأخرى بطريقة مختلفة)، وتباين في قبول الأدلة (محكمة في ولاية تقبل دليلاً ومحكمة أخرى ترفضه)، وصعوبة تدريب الكوادر في غياب معايير موحدة⁴.

الفرع الثاني: التعاون الدولي في التحقيق السيبراني

لا تعترف الجرائم السيبرانية بالحدود الوطنية⁵. فالدليل الرقمي قد يكون موزعاً على خوادم في عدة دول، والجاني قد يكون في دولة والمجني عليه في دولة أخرى، وأثر الجريمة قد يظهر

¹ Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations- مرجع

سابق، ص 603.

² د. محمد الأمين البشري، جرائم الإنترنت وطرق مكافحتها، مرجع سابق، ص 233.

³ د. عبد الفتاح بيومي حجازي، الإثبات الجنائي الإلكتروني، مرجع سابق، ص 288.

⁴ د. عبد العزيز سعد، أبحاث تحليلية في قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 417.

⁵ Convention on Cybercrime (Budapest Convention), Council of Europe, 2001, Preamble, p. 1.

في دولة ثالثة¹. لذلك، لا يمكن لأي دولة بمفردها أن تحقق في جريمة سيبرانية عابرة للحدود، بل لا بد من تعاون دولي فعال وسريع².

تتعدد آليات التعاون الدولي في مجال الجرائم السيبرانية³. أولها الاتفاقيات الثنائية والمتعددة الأطراف، كاتفاقية بودابست لمكافحة الجريمة المعلوماتية (2001) التي يتبعها أكثر من 60 دولة، واتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية (2024) التي وقعت عليها الجزائر في أكتوبر 2025⁴. وتوفر هذه الاتفاقيات أطراً قانونية متقدمة للتعاون، تشمل شبكات الاتصال على مدار الساعة (Network 7/24) للتعاون السريع، حيث تعين كل دولة نقطة اتصال وطنية تعمل 24 ساعة يومياً لاستقبال الطلبات العاجلة والرد عليها في غضون ساعات⁵.

ثانيها الإنابات القضائية (Letters Rogatory)، وهي الطلب الرسمي من محكمة في دولة إلى محكمة في دولة أخرى للحصول على أدلة، غير أن هذه الآلية تتصف بالبطء الشديد وقد تستغرق شهراً⁶. ثالثها تسليم المجرمين (Extradition)، حيث يمكن للدولة التي يوجد بها

¹ - د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، مرجع سابق، ص 322.

² - د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون الدولي، مرجع سابق، ص 271.

³ - د. خالد ممدوح إبراهيم، حجية الدليل الإلكتروني في الإثبات الجنائي، مرجع سابق، ص 266.

⁴ - United Nations Convention against Cybercrime, United Nations, 2024, p. 5.

⁵ - Convention on Cybercrime (Budapest Convention), مرجع سابق، المادة 35، ص 28.

⁶ - د. أحمد شوقي الشلقاني، مبادئ الإجراءات الجنائية، مرجع سابق، ص 361.

الجاني أن تسلمه إلى الدولة التي وقعت فيها الجريمة¹. رابعها المساعدة المتبادلة (Mutual Legal Assistance - MLA)، وهي آلية أكثر مرونة من الإنابة القضائية تسمح للسلطات القضائية بطلب مساعدة نظيراتها في جمع الأدلة ومراقبة الاتصالات وتجميد الحسابات، غير أنها لا تزال بطيئة نسبياً لأنها تمر عبر القنوات الدبلوماسية².

رغم أهمية التعاون الدولي، إلا أنه يواجه عقبات عدة³. من أبرزها اختلاف التشريعات الوطنية، فالدول تختلف في تعريف الجرائم السيبرانية وفي العقوبات المقررة وفي الضمانات الإجرائية المطلوبة لجمع الأدلة، مما قد يدفع دولة إلى رفض تلبية طلب دولة أخرى إذا اعتبرت أن الفعل غير مجرم في قانونها (مبدأ الجريمتين)⁴. والخلاف حول الاختصاص القضائي، فقد تتنافس عدة دول على الاختصاص بنفس الجريمة (تنازع إيجابي)، أو تتنازع كل دولة وتقول إن الأخرى هي المختصة (تنازع سلبي)⁵. والبطء الإجرائي، فحتى في إطار المساعدة المتبادلة، قد تستغرق الطلبات وقتاً طويلاً للترجمة والتدقيق والتنفيذ، مما قد يؤدي إلى إتلاف الأدلة الرقمية⁶. وعدم تعاون بعض الدول لأسباب سياسية أو لعدم وجود معاهدة مع الدولة الطالبة⁷. وحماية البيانات والخصوصية، فبعض الدول (كالدول الأعضاء في الاتحاد الأوروبي)

¹ - د. رؤوف عبيد، مبادئ الإجراءات الجنائية، مرجع سابق، ص 468.

² - د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، مرجع سابق، ص 497.

³ - د. محمد الأمين البشري، الجرائم الإلكترونية والتحقيق فيها، مرجع سابق، ص 301.

⁴ - د. عبد الله سليمان، شرح قانون العقوبات الجزائري، مرجع سابق، ص 511.

⁵ - د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 588.

⁶ - د. عبد الفتاح بيومي حجازي، الدليل الجنائي الرقمي وحجتيه في الإثبات الجنائي، مرجع سابق، ص 295.

⁷ - د. خالد ممدوح إبراهيم، التحقيق الجنائي الرقمي والأدلة الرقمية، مرجع سابق، ص 391.

الأوروبي) لديها قوانين صارمة لحماية البيانات الشخصية (كلائحة GDPR)، وقد ترفض تسليم بيانات إذا اعتبرت أن الدولة طالبة لا توفر حماية كافية¹.

الفرع الثالث: مقترحات لتطوير الإطار القانوني والتقني للإثبات

انطلاقاً من الصعوبات والتحديات التي تم استعراضها، يمكن تقديم مجموعة من المقترحات لتطوير الإثبات في الجرائم السيبرانية على ثلاثة مستويات².

أولاً: المقترحات التشريعية. يجب إصدار قانون خاص بالدليل الرقمي يستقل عن القواعد العامة للإثبات، يحدد تعريفاً واضحاً للدليل الرقمي، وشروطه (المشروعية، الصحة، الصلة)، وحجيته، وإجراءات جمعه، وسلسلة حيازته³. كما يجب تعديل قانون العقوبات وقانون الإجراءات الإجرائية الجزائية لمواءمتهما مع اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، خاصة فيما يتعلق بتوسيع صلاحيات جمع الأدلة الرقمية وإدخال آليات التعاون الدولي السريعة⁴. وتنظيم مسؤولية مقدمي الخدمات (الموجودين في الجزائر والأجانب الذين يقدمون خدمات لسكان الجزائر) بالاحتفاظ بالبيانات لمدة معقولة وتقديمها عند الطلب خلال أجل قصير، مع

¹ – Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), Official

Journal of the European Union, 2016, p. 1.

² – د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، مرجع سابق، ص 337.

³ – د. عبد الفتاح بيومي حجازي، الإثبات الجنائي الإلكتروني، مرجع سابق، ص 311.

⁴ – United Nations Convention against Cybercrime, مرجع سابق، ص 14.

ضمانات تحمي خصوصية المستخدمين¹. وإدخال نظام التوقيع الرقمي وسلسلة الحيازة في القانون، والنص على أن الأدلة الرقمية لا تقبل ما لم تكن مصحوبة بسلسلة حيازة موثقة وتوقيع رقمي².

ثانياً: المقترحات التقنية والتنظيمية. إنشاء معامل وطنية للأدلة الرقمية مجهزة بأحدث الأجهزة والبرمجيات، معتمدة وفق المعايير الدولية (كمعيار ISO 17025 للمختبرات الجنائية)³. وضع بروتوكولات وطنية موحدة لجمع وتحليل الأدلة الرقمية تلزم بها كل وحدات الضبطية القضائية والخبراء، وتُراجع وتُحدث كل عامين لمواكبة التطورات التقنية⁴. تدريب مستمر لأعضاء الضبطية القضائية والنيابة العامة والقضاة، وإدراج مادة "الأدلة الرقمية والجرائم السيبرانية" في مناهج التكوين، وتنظيم دورات تدريبية مستمرة كل 6-12 شهراً⁵. تخصص القضاة بإنشاء دوائر قضائية متخصصة في الجرائم السيبرانية يرأسها قضاة تلقوا تكويناً متقدماً في هذا المجال، ويتوفرون على مساعدين تقنيين (خبراء مقيمين)⁶. وإنشاء وحدة تعاون دولي

¹ - د. خالد ممدوح إبراهيم، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، مرجع سابق، ص 404.

² - Casey Eoghan, Digital Evidence and Computer Crime, مرجع سابق، ص 498.

³ - ISO/IEC 17025:2017, General Requirements for the Competence of Testing and Calibration

Laboratories, International Organization for Standardization, Geneva, 2017, p. 6.

⁴ - Eoghan Casey, Handbook of Digital Forensics and Investigation, مرجع سابق، ص 421.

⁵ - د. محمد الأمين البشري، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 329.

⁶ - د. عبد العزيز سعد، أبحاث تحليلية في قانون الإجراءات الجزائية الجزائري، مرجع سابق، ص 442.

سريعة (7/24) تابعة للنيابة العامة أو وزارة العدل للرد على طلبات المساعدة الدولية وتقديم الطلبات الجزائية إلى الخارج.¹

ثالثاً: المقترحات الدولية. المصادقة السريعة على اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية (بعد التوقيع)، وتعديل التشريعات الوطنية تمهيداً لتطبيقها، والمشاركة الفاعلة في اجتماعات الدول الأطراف لوضع آليات تنفيذية فعالة.² إنشاء منصة إلكترونية عربية لتبادل الأدلة الرقمية، على غرار النموذج الأوروبي (SIRIUS)، تسمح للدول العربية بتبادل طلبات المساعدة والأدلة الرقمية في الوقت الفعلي مع ترجمة فورية وتحديثات لحظية.³ توحيد التشريعات العربية في مجال مكافحة الجرائم السيبرانية، على الأقل في ما يتعلق بتجريم الأفعال الأساسية (كالاختراق غير المشروع والاحتيال الإلكتروني)، ووضع ضوابط مشتركة لجمع الأدلة الرقمية (سلسلة الحيازة والتوقيع الرقمي)، وتحديد عقوبات دنيا وعليا للجرائم السيبرانية.⁴

خلص هذا الفصل إلى أن وسائل الإثبات في الجرائم السيبرانية تختلف جوهرياً عن وسائل الإثبات التقليدية، حيث يشكل الدليل الرقمي العنصر المحوري في كشف الحقيقة.⁵ فقد تبين أن

¹–Convention on Cybercrime (Budapest Convention)، مرجع سابق، المادة 35، ص 28.

²–United Nations Convention against Cybercrime، مرجع سابق، ص 22.

³–د. خالد ممدوح إبراهيم، حجية الدليل الإلكتروني في الإثبات الجنائي، مرجع سابق، ص 299.

⁴–د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون الدولي، مرجع سابق، ص 318.

⁵–د. محمد حسين منصور، الإثبات الإلكتروني في المنازعات المدنية والجنائية، مرجع سابق، ص 351.

أن الدليل الرقمي يتمتع بحجية نسبية تخضع لتقدير القاضي، ولا يمكن قبوله إلا بتوافر شروط المشروعية والصحة والصلة، مع ضرورة توثيق سلسلة حيازته بدقة والتوقيع الرقمي عليه¹.

كما أظهر الفصل أن إجراءات جمع وتحليل الأدلة الرقمية تتطلب خبرة تقنية عالية، والالتزام ببروتوكولات صارمة تهدف إلى الحفاظ على سلامة الدليل ومنع إتلافه أو العبث به. ويقع هذا العبء بشكل رئيسي على وحدات الضبطية القضائية المتخصصة (كالوحدة الوطنية للبحث في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال) والخبراء الرقميين².

أما على مستوى دور الجهات القضائية والأمنية، فقد تبين أن هناك تقدماً ملحوظاً في الجرائر من خلال إنشاء وحدات متخصصة وتعيين خبراء رقميين، إلا أن الواقع لا يزال يعاني من ندرة الكوادر المؤهلة، وضعف التنسيق بين القضاة والمحققين والخبراء، وغياب المعايير الوطنية الموحدة، وضعف البنية التحتية التقنية³.

كما تبين أن التعاون الدولي، رغم أهميته القصوى لمكافحة الجرائم السيبرانية العابرة للحدود، يواجه عقبات تشريعية (اختلاف القوانين) وإجرائية (البطء) وسياسية (عدم التعاون)⁴.

من هذا المنطلق، تبرز الحاجة الملحة إلى تطوير الإطار القانوني والتقني للإثبات السيبراني في الجزائر، من خلال إصدار تشريع خاص بالدليل الرقمي، وإنشاء معامل وطنية، ووضع بروتوكولات موحدة، وتدريب الكوادر البشرية تدريباً مستمراً، وتفعيل آليات التعاون

¹ Casey Eoghan, Digital Evidence and Computer Crime- مرجع سابق، ص 517.

² د. محمد الأمين البشري، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 344.

³ د. عبد العزيز سعد، الجرائم الواقعة على نظم المعالجة الآلية للمعطيات، مرجع سابق، ص 205.

⁴ Convention on Cybercrime (Budapest Convention- مرجع سابق، ص 31.

الدولي، لا سيما في ضوء التزامات الجزائر بموجب اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لسنة 2024¹.

وهذه التطورات، إذا تمت بشكل جاد ومنسق، ستعكس إيجاباً على واقع الإثبات في الجرائم السيبرانية في الجزائر، وتساهم في تحقيق العدالة الجنائية في هذا المجال الحيوي².

¹–United Nations Convention against Cybercrime، مرجع سابق، ص 27.

²–د. عبد الفتاح بيومي حجازي، الدليل الجنائي الرقمي وحجبه في الإثبات الجنائي، مرجع سابق، ص 337.

الخاتمة

خاتمة

وفي ختام هذه الدراسة الموسومة بـ وسائل الإثبات القضائي في الجرائم السيبرانية وتقييمها، يتضح أن التطور التكنولوجي الذي شهده العالم في العقود الأخيرة أدى إلى ظهور بيئة رقمية حديثة ساهمت في تسهيل مختلف مجالات الحياة، غير أنها في المقابل أفرزت نوعاً جديداً من الجرائم يتمثل في الجرائم السيبرانية التي أصبحت تشكل تهديداً حقيقياً للأفراد والمؤسسات والدول. وقد فرضت هذه الجرائم تحديات قانونية وقضائية معقدة، خاصة في مجال الإثبات الجنائي، نظراً لخصوصية الدليل الرقمي وطبيعة الجرائم المرتكبة عبر الفضاء الإلكتروني.

وقد بينت هذه الدراسة أن وسائل الإثبات التقليدية لم تعد كافية لمواجهة الجرائم السيبرانية، الأمر الذي أدى إلى بروز الدليل الإلكتروني كوسيلة أساسية في الكشف عن الحقيقة وإثبات الجرائم الإلكترونية. كما تبين أن فعالية الإثبات الرقمي ترتبط بمدى احترام الإجراءات القانونية والتقنية الخاصة بجمع الأدلة الرقمية وتحليلها وحفظها، إضافة إلى أهمية الخبرة الفنية الرقمية في مساعدة القضاء على فهم الجوانب التقنية المعقدة للجرائم الإلكترونية.

كما أظهرت الدراسة أن المشرع الجزائري حاول مواكبة التطورات التكنولوجية من خلال سن مجموعة من النصوص القانونية المتعلقة بمكافحة الجرائم الإلكترونية، إلا أن التطور المتسارع للتكنولوجيا يفرض ضرورة تحديث هذه النصوص بصورة مستمرة، خاصة في ظل ظهور تقنيات حديثة وأساليب إجرامية أكثر تعقيداً. كذلك تبين أن الجرائم السيبرانية غالباً ما تتخذ طابعاً عابراً للحدود، مما يجعل التعاون الدولي عنصراً أساسياً في مجال التحقيق والإثبات.

ومن خلال هذه الدراسة تم التوصل إلى مجموعة من النتائج المهمة، يمكن تلخيصها فيما

يلي:

النتائج

• الجرائم السيبرانية تتميز بطبيعة خاصة تختلف عن الجرائم التقليدية من حيث الوسيلة والمكان وسرعة التنفيذ.

• وسائل الإثبات التقليدية أصبحت غير كافية لمواجهة الجرائم الإلكترونية.

• الدليل الإلكتروني أصبح من أهم وسائل الإثبات في الجرائم السيبرانية.

• الدليل الرقمي يتميز بكونه سريع الزوال وقابلًا للتعديل أو الإتلاف.

• حجية الدليل الإلكتروني مرتبطة بسلامة إجراءات جمعه وتحليله وحفظه.

• الإثبات الرقمي يحتاج إلى خبرة تقنية متخصصة لفهم وتحليل الأدلة الإلكترونية.

• للخبرة الفنية الرقمية دور أساسي في مساعدة القضاء على كشف الجرائم السيبرانية.

• المشرع الجزائري حاول مواكبة التطور الرقمي من خلال سن قوانين خاصة بالجرائم

الإلكترونية.

• ما تزال بعض النصوص القانونية بحاجة إلى التحديث لمواكبة التطورات التقنية الحديثة.

• الجرائم السيبرانية غالبًا ما تكون عابرة للحدود، مما يصعب إجراءات التحقيق والإثبات.

• التعاون الدولي أصبح ضرورة أساسية لمكافحة الجرائم الإلكترونية.

• التطور التكنولوجي المستمر يؤدي إلى ظهور صور جديدة ومعقدة من الجرائم السيبرانية.

الختامة

- حماية الدليل الرقمي تتطلب وسائل تقنية حديثة وإجراءات دقيقة.
- تحقيق التوازن بين مكافحة الجرائم الإلكترونية وحماية الحقوق والحريات يعد من أهم التحديات القانونية.
- الإثبات الرقمي أصبح عنصرًا أساسيًا لتحقيق العدالة الجنائية في البيئة الإلكترونية.
- وبناءً على هذه النتائج، يمكن تقديم مجموعة من التوصيات والاقتراحات التي من شأنها المساهمة في تطوير منظومة الإثبات الرقمي وتعزيز فعالية مكافحة الجرائم السيبرانية، وتتمثل فيما يلي:

التوصيات

- تحديث التشريعات المتعلقة بالإثبات الرقمي والجرائم السيبرانية بصورة مستمرة.
- وضع قواعد قانونية دقيقة لتنظيم إجراءات جمع الأدلة الرقمية وحفظها.
- تعزيز تكوين القضاة وأعضاء الضبطية القضائية في مجال الجرائم الإلكترونية.
- إنشاء مخابر جنائية رقمية متخصصة ومجهزة بأحدث التقنيات.
- دعم الخبرة الفنية الرقمية وتكوين خبراء مختصين في الأمن السيبراني.
- تعزيز التعاون الدولي في مجال تبادل المعلومات والأدلة الإلكترونية.
- الاستفادة من الاتفاقيات الدولية والتجارب المقارنة في مجال مكافحة الجرائم السيبرانية.
- تطوير البنية التحتية الرقمية للجهات القضائية والأمنية.
- تكييف برامج التوعية بمخاطر الجرائم الإلكترونية وطرق الوقاية منها.
- تشجيع البحث العلمي والدراسات الأكاديمية المتعلقة بالإثبات الرقمي.

- توفير وسائل تقنية حديثة لحماية الأدلة الرقمية من التلاعب أو الإتلاف.
 - تعزيز التنسيق بين الجهات القضائية والأمنية والتقنية في مجال التحقيق الرقمي.
 - اعتماد برامج تدريبية دورية لمواكبة التطورات التقنية الحديثة.
 - العمل على تسريع إجراءات التعاون القضائي الدولي في الجرائم السيبرانية.
 - تطوير آليات الكشف المبكر عن الجرائم الإلكترونية والحد من مخاطرها.
- وفي الأخير، يمكن القول إن نجاح العدالة الجنائية في مواجهة الجرائم السيبرانية لم يعد مرتبطاً فقط بوجود نصوص قانونية تجرم الأفعال الإلكترونية، وإنما أصبح مرتبطاً بمدى قدرة الأنظمة القضائية على تطوير وسائل الإثبات الرقمي والاستفادة من التقدم التقني والخبرة الفنية والتعاون الدولي، بما يضمن حماية المجتمع وتحقيق الأمن المعلوماتي وصيانة الحقوق والحريات في البيئة الرقمية الحديثة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

قائمة المراجع

أولاً: المصادر

أ- القوانين

القانون رقم 04-09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، سنة 2009.

القانون رقم 14-25 المؤرخ في 03 أوت 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية.

اتفاقية بودابست بشأن الجرائم المعلوماتية لسنة 2001، المعتمدة من مجلس أوروبا بتاريخ 23 نوفمبر 2001.

اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المعتمدة سنة 2024.

ثانياً: المراجع

أ- الكتب

- أبو عامر، محمد زكي، الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، 2015.

- أبو عامر، محمد زكي، قانون العقوبات الدولي، دار الجامعة الجديدة، الإسكندرية، 2019.

قائمة المصادر والمراجع

- إبراهيم، خالد ممدوح، الأدلة الرقمية والتحقيق الجنائي الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2019.
- إبراهيم، خالد ممدوح، التحقيق الجنائي الرقمي والأدلة الرقمية، دار الفكر الجامعي، الإسكندرية، 2017.
- إبراهيم، خالد ممدوح، الدليل الرقمي في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2018.
- إبراهيم، خالد ممدوح، حجية الدليل الإلكتروني في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، 2011.
- البشري، محمد الأمين، الجرائم الإلكترونية والتحقيق فيها، دار الجامعة الجديدة، الإسكندرية، 2016.
- البشري، محمد الأمين، جرائم الإنترنت وطرق مكافحتها، دار الفكر الجامعي، الإسكندرية، 2017.
- البشري، محمد الأمين، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، القاهرة، 2018.
- البشري، محمد أمين، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، القاهرة، 2018.
- البشري، محمد الأمين، الإثبات الجنائي بالأدلة الرقمية، دار الكتب القانونية، مصر، 2015.
- بوسقيعة، أحسن، التحقيق القضائي في القانون الجزائري، دار هومة، الجزائر، 2017.

قائمة المصادر والمراجع

- بوسقيعة، أحسن، التحقيق القضائي في المواد الجزائية، دار هومة، الجزائر، 2019.
- بوسقيعة، أحسن، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، 2019.
- بيومي حجازي، عبد الفتاح، الإثبات الجنائي الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2016.
- بيومي حجازي، عبد الفتاح، الجرائم الإلكترونية في التشريع المقارن، دار الفكر الجامعي، الإسكندرية، 2007.
- بيومي حجازي، عبد الفتاح، الدليل الإلكتروني في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2012.
- بيومي حجازي، عبد الفتاح، الدليل الإلكتروني وحجيته في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، 2008.
- بيومي حجازي، عبد الفتاح، الدليل الجنائي الرقمي وحجيته في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، 2010.
- بيومي حجازي، عبد الفتاح، الحماية الجنائية للحياة الخاصة عبر الإنترنت، دار الفكر الجامعي، الإسكندرية، 2015.

قائمة المصادر والمراجع

- بيومي حجازي، عبد الفتاح، مكافحة جرائم الكمبيوتر والإنترنت في القانون الدولي، دار الكتب القانونية، مصر، 2007.
- حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2015.
- حسني، محمود نجيب، شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 2015.
- حسني، محمود نجيب، نظرية الإثبات الجنائي، دار النهضة العربية، القاهرة، 2011.
- حجازي، عبد الفتاح بيومي، الدليل الرقمي في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، 2018.
- سعد، عبد العزيز، أبحاث تحليلية في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، 2018.
- سعد، عبد العزيز، الجرائم الواقعة على نظم المعالجة الآلية للمعطيات، دار هومة، الجزائر، 2016.

قائمة المصادر والمراجع

- سلامة، أحمد عبد الكريم، الحماية الجنائية للمعلوماتية، دار النهضة العربية، القاهرة، 2015.
- سليمان، عبد الله، شرح قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2018.
- سليمان، عبد الله، شرح قانون العقوبات الجزائري، ديوان المطبوعات الجامعية، الجزائر.
- سرور، أحمد فتحي، الوسيط في قانون العقوبات، دار النهضة العربية، القاهرة، 2016.
- سرور، فتحي، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2014.
- الشلقاني، أحمد شوقي، الجرائم المعلوماتية وإثباتها الجنائي، دار النهضة العربية، القاهرة، 2012.
- الشلقاني، أحمد شوقي، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2016.
- الشلقاني، أحمد شوقي، مبادئ الإجراءات الجزائية في التشريع الجزائري والمقارن، ديوان المطبوعات الجامعية، الجزائر، 2016.
- الشلقاني، أحمد شوقي، مبادئ الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2010.
- الشواربي، عبد الحميد، الخبرة الجنائية في الجرائم الإلكترونية، منشأة المعارف، الإسكندرية، 2018.

قائمة المصادر والمراجع

- عبيد، رؤوف، مبادئ الإجراءات الجنائية في القانون المصري، دار الفكر العربي، القاهرة، 2013.
- القهوجي، علي عبد القادر، قانون العقوبات، القسم العام، منشورات الحلبي الحقوقية، بيروت، 2010.
- الكندري، فيصل عبد الله، الجرائم الإلكترونية والتقنيات الحديثة للتحقيق الجنائي، منشورات الحلبي الحقوقية، بيروت، 2017.
- كامل، مصطفى عبد الله، حجية الدليل الإلكتروني في الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2016.
- الغريب، محمد عيد، الإثبات الجنائي الحديث، دار النهضة العربية، القاهرة، 2017.
- الغريب، محمد عيد، الدليل الإلكتروني أمام القضاء الجنائي، دار الجامعة الجديدة، الإسكندرية، 2014.
- منصور، محمد حسين، الإثبات الإلكتروني في المنازعات المدنية والجنائية، منشأة المعارف، الإسكندرية، 2009.
- منصور، محمد حسين، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2010.
- مهدي، عبد الرؤوف، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، 2014.
- نجم، محمد صبحي، شرح قانون أصول المحاكمات الجزائية، دار الثقافة للنشر والتوزيع، عمان، 2014.

قائمة المصادر والمراجع

- نمور، محمد سعيد، أصول الإجراءات الجزائية، دار الثقافة للنشر والتوزيع، عمان، 2013.
- سالم، عمر، الحماية الجنائية للمعلومات عبر الإنترنت، دار النهضة العربية، القاهرة، 2014.
- عبد الحميد، سامي، التعاون الدولي في مكافحة الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2019.
- ب- المراجع الأجنبية

- 1- Brian Carrier, File System Forensic Analysis, Addison-Wesley, 2005.
- 2- Casey Eoghan, Digital Evidence and Computer Crime, Academic Press, 2011.
- 3- Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2010.
- 4- Kruse Warren & Heiser Jay, Computer Forensics: Incident Response Essentials, Addison-Wesley, 2002.
- 5- Nelson Phillips & Steuart Christopher, Guide to Computer Forensics and Investigations, Cengage Learning, 2015.
- 6- Robert Chesney, Cybercrime and the Law, Oxford University Press, 2018.

الفهرس والمحتويات

قائمة الفهرس والمحتويات

الموضوعات	الصفحة
الإهداء	
الشكر والعرفان	
المقدمة	1
الفصل الأول الإطار المفاهيمي والقانوني للإثبات في الجرائم السيبرانية	
المبحث الأول: مفهوم الجرائم السيبرانية	9
المطلب الأول: تعريف الجرائم السيبرانية وطبيعتها القانونية	9
الفرع الأول: تعريف الجرائم السيبرانية في الفقه والتشريع	9
الفرع الثاني: الطبيعة القانونية للجرائم السيبرانية	13
الفرع الثالث: تمييز الجرائم السيبرانية عن الجرائم التقليدية	17
المطلب الثاني: خصائص الجرائم السيبرانية وأثرها على الإثبات	20
الفرع الأول: الطابع الرقمي وغير المادي للجريمة	21
الفرع الثاني: السرعة والعالمية في ارتكاب الجريمة	22
الفرع الثالث: صعوبة تحديد الفاعل ومكان الجريمة	24
المبحث الثاني: الأساس القانوني للإثبات في الجرائم السيبرانية	29
المطلب الأول: التنظيم القانوني للإثبات في القانون الجزائري	29
الفرع الأول: قواعد الإثبات في قانون الإجراءات الجزائية رقم 14-25	29

قائمة الفهرس والمحتويات

32	الفرع الثاني: حجية الأدلة في القانون الجزائري
35	الفرع الثالث: سلطة القاضي في تقدير وسائل الإثبات
37	المطلب الثاني: النصوص الخاصة بالجرائم السيبرانية والإثبات الرقمي
38	الفرع الأول: أحكام القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال
41	الفرع الثاني: تنظيم الدليل الإلكتروني في التشريع الجزائري
44	الفرع الثالث: دور الاتفاقيات الدولية في دعم الإثبات السيبراني
الفصل الثاني وسائل الإثبات القضائي في الجرائم السيبرانية وتقييمها	
54	المبحث الأول: وسائل الإثبات الرقمية في الجرائم السيبرانية
54	المطلب الأول: الدليل الإلكتروني وحجيته القانونية
55	الفرع الأول: مفهوم الدليل الإلكتروني وحجيته القانونية
59	الفرع الثاني: شروط صحة الدليل الإلكتروني وأنواعه
65	الفرع الثالث: القيمة القانونية للدليل الرقمي أمام القضاء
70	المطلب الثاني: إجراءات جمع وتحليل الأدلة الرقمية
70	الفرع الأول: تفتيش وضبط الأجهزة الإلكترونية
75	الفرع الثاني: استخراج البيانات الرقمية وتحليلها
80	الفرع الثالث: ضمان سلامة الأدلة الرقمية من العبث

84	المبحث الثاني: دور الجهات القضائية والأمنية في الإثباتات السيبراني
84	المطلب الأول: دور الضبطية القضائية والخبرة الرقمية
84	الفرع الأول: اختصاصات الضبطية القضائية في الجرائم السيبرانية
87	الفرع الثاني: دور الخبرة الرقمية في الإثبات
89	الفرع الثالث: تقييم تقارير الخبراء أمام القضاء
90	المطلب الثاني: التحديات العلمية وآفاق تطوير الإثباتات السيبراني
91	الفرع الأول: الصعوبات العملية في إثبات الجرائم السيبرانية
91	الفرع الثاني: التعاون الدولي في التحقيق السيبراني
96	الفرع الثالث: مقترحات لتطوير الإطار القانوني والتقني للإثباتات
10	الخاتمة
2	
10	قائمة المصادر والمراجع
7	
11	فهرس المحتويات
5	
11	الملخص
9	

الملخص

الملخص:

تناولت هذه الدراسة موضوع وسائل الإثبات القضائي في الجرائم السيبرانية وتقييمها، باعتبارها من المواضيع القانونية الحديثة التي فرضتها الثورة الرقمية والتطور المتسارع لتكنولوجيات الإعلام والاتصال. وقد هدفت الدراسة إلى إبراز خصوصية الجرائم السيبرانية وبيان مدى فعالية وسائل الإثبات القضائي في الكشف عنها وإثباتها، مع التركيز على الدليل الإلكتروني باعتباره الوسيلة الأساسية للإثبات في البيئة الرقمية. واعتمدت الدراسة على المنهج التحليلي من خلال تحليل النصوص القانونية المنظمة للإثبات الرقمي، إلى جانب المنهج الوصفي لعرض مختلف المفاهيم المتعلقة بالجرائم السيبرانية والأدلة الرقمية. كما تناولت الدراسة حجية الدليل الإلكتروني، وإجراءات جمع الأدلة الرقمية وتحليلها، ودور الجهات القضائية والخبرة الفنية في الإثبات السيبراني، بالإضافة إلى التحديات العملية التي تواجه التحقيق والإثبات في الجرائم الإلكترونية. وتوصلت الدراسة إلى أن الدليل الإلكتروني أصبح يحتل مكانة محورية في الإثبات الجنائي المعاصر، غير أن فعاليته تبقى مرتبطة بسلامة إجراءات جمعه وحفظه وتحليله، وبمدى توفر الكفاءات التقنية والقانونية اللازمة للتعامل معه. كما خلصت الدراسة إلى ضرورة تطوير التشريعات الوطنية وتعزيز التعاون الدولي وتدعيم الخبرة الفنية الرقمية لمواجهة التطور المستمر للجرائم السيبرانية وضمان تحقيق العدالة الجنائية في البيئة الرقمية.

الكلمات المفتاحية:

الجرائم السيبرانية، الإثبات القضائي، الدليل الإلكتروني، الأدلة الرقمية، الخبرة الفنية الرقمية، التحقيق الإلكتروني، العدالة الجنائية الرقمية.

This dissertation examines judicial evidence in cybercrimes and its evaluation, as one of the most significant contemporary legal issues resulting from the rapid development of information and communication technologies. The study aims to highlight the specific nature of cybercrimes and assess the effectiveness of judicial evidence in detecting and proving such crimes, with particular emphasis on electronic evidence as the primary means of proof in the digital environment.

The research adopts an analytical approach through the examination of legal texts governing digital evidence, in addition to a descriptive approach to explain concepts related to cybercrime and digital evidence. The study addresses the legal value of electronic evidence, procedures for collecting and analyzing digital evidence, the role of judicial authorities and digital forensic experts in cybercrime investigations, as well as the practical challenges facing criminal proof in cyberspace.

The study concludes that electronic evidence has become a fundamental component of modern criminal proof. However, its effectiveness depends on the legality of its collection, preservation, and analysis, as well as the availability of technical and legal expertise. The

research also emphasizes the need to update national legislation, strengthen international cooperation, and enhance digital forensic capabilities to effectively combat cybercrime and ensure the proper administration of justice in the digital age.

Keywords:

Cybercrime, Judicial Evidence, Electronic Evidence, Digital Evidence, Digital Forensics, Cyber Investigation, Digital Criminal Justice.