قانون جنائي

النظرية العامة
للقانون الجنائي المعلوماتي

دروس في مقرر قانون مكافحة الجرائم الإلكترونية اللبيي
رقم (05 لسنة 2022م)

.. {الأحكام الموضوعية والإجرائية} ..

إعداد

المستشار الدكتور مسعود مجمد خليفة شلندي

كلية القانون صرمان – قسم القانون الجنائي

جامعة صبراتة

مدينة صرمان [2026/03/25م]

العام الجامعي .. 2025 /2026 م..

. . بسم الله الرحمن الرحيم . .

الحمدُ للهِ العدلِ في مُلكه، الذي أقام القسطَ أساسًا للحكم والتكليف، وجعل العلمَ مناطَ التمييز والإدراك؛ إذ قال الله ﷻ: ﴿وَعَلَّمَ آدَمَ الْأَسْمَاءَ كُلَّهَا﴾ [البقرة: 31]، دلالةً على أن المعرفة أصلُ المسؤولية وأساسُ المساءلة، والصلاةُ والسلامُ على رسول الله "محمدٍ ﷺ"، وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين...

- **ثم أما بعد:**

فإن تأصيلَ النظرية العامة للقانون الجنائي المعلوماتي يستند – في بعده القيمي والمعرفي– إلى دلالة قول الله ﷻ: ﴿وَعَلَّمَ آدَمَ الْأَسْمَاءَ كُلَّهَا﴾ [البقرة: 31]، بما يُقرّر أن العلمَ أساسُ الإدراك، وأن الإدراكَ مناطُ المسؤولية، ومن ثمّ، فإن قيام المسؤولية الجنائية، في صورتها التقليدية أو الرقمية، يُفترض توافر العلم بالفعل وإرادة ارتكابه، اتساقًا مع مقتضيات القصد الجنائي.

ولا يخرج القانون الجنائي المعلوماتي، رغم خصوصية مجاله، عن أصول النظرية العامة للجريمة، بل يُعيد تكييفها في ضوء البيئة الرقمية؛ حيث يغدو العلم بطبيعة النظم والبيانات، والإدراك لمخاطر السلوك الإلكتروني، عنصرًا لازمًا لقيام الركن المعنوي، وبذلك تتكامل المرجعية الشرعية مع البناء القانوني في تقرير قاعدة مفادها: "لا مسؤولية جنائية دون علمٍ مُعتبر وإرادةٍ آثمة"، تحقيقًا للتوازن بين حماية النظام المعلوماتي وضمان الشرعية الجنائية.

ويأتي هذا المؤلف في إطار الجهود العلمية الرامية إلى تأصيل هذه النظرية، عبر استحضار الأسس التقليدية للجريمة وإعادة بنائها في ضوء التحولات الرقمية المعاصرة، وقد عالجتُ الموضوع بمنهج تحليلي تأصيلي، يقوم على بيان المبادئ الحاكمة لفلسفة التجريم والعقاب بوصفها قواعد عامة تنسحب على مختلف الأنماط الإجرامية، بما فيها الجرائم الإلكترونية في إطار الأحكام الموضوعية والإجرائية التي نصَّ عليها قانون مكافحة الجرائم الإلكترونية الليبي رقم (05 لسنة 2022م).

.. المؤلف..

- **مقدمــة:**

حقيقة الواقع الإنساني المعاش هي أن الحاسوب وتكنولوجيا الاتصالات ونُظُم المعلومات قد أضحت اليوم من المقومات الأساسية التي لا غنى عنها في مختلف مجالات الحياة الإنسانية، سواء على الصعيد الفردي أم الجماعي، إذ أصبحت ركيزة جوهرية في دعم الأنشطة الاقتصادية والاجتماعية والعلمية والصناعية والزراعية وغيرها من أوجه النشاط البشري، بما أسهم في إحداث نقلة نوعية في مسارات التنمية والتطور.

وقد ترتب على هذا الانتشار المتسارع لاستخدام التقنيات المعلوماتية بروز أنماط مستحدثة من السلوك الإجرامي، عُرفت بالإجرام المعلوماتي، بوصفه نتيجة طبيعية لكل تقدم تقني. ذلك أن الحاسوب قد يكون أداة لارتكاب الجريمة، أو محلاً للاعتداء، أو بيئة رقمية تُرتكب فيها الأفعال الإجرامية.

ويتميز العصر الراهن بكونه عصر التكنولوجيا الرقمية، حيث غدت تكنولوجيا المعلومات والاتصالات الإطار الذي يتحرك فيه الأفراد والجماعات، وقد واكب هذا التحول ظهور صور متطورة من الإجرام، تمثلت فيما يُعرف بالجريمة الإلكترونية. فقد امتدت شبكات المعلومات لتغطي أرجاء العالم، وتوغلت تطبيقاتها في أدق تفاصيل الحياة اليومية، مما أسهم في تعزيز التواصل الحضاري والثقافي، وظهور ما يمكن تسميته بـ"الجوار الإلكتروني" الذي تجاوز حدود الجوار الجغرافي التقليدي، وعزز التفاعل الإنساني بين الشعوب، وكسر حواجز العزلة.

غير أن هذا التقدم التقني، وعلى الرغم من آثاره الإيجابية، قد أفرز في المقابل بيئة خصبة لانتشار أنماط جديدة من الإجرام، سواء في صورته التقليدية أم في صوره المستحدثة المرتبطة بنُظُم المعلومات، الأمر الذي أدى إلى بروز ظاهرة عولمة الجريمة، حيث لم تعد الجريمة مقيدة بإقليم الدولة، بل أصبحت عابرة للحدود، مستفيدة من الطبيعة اللامركزية للشبكات الرقمية.

ويكشف التأمل في شبكة الإنترنت – على وجه الخصوص– عن دورها البارز في تيسير ارتكاب الأنشطة الإجرامية، سواء على المستوى الفردي أو في إطار الجريمة المنظمة، بما جعل الأمن الفردي والجماعي، الاجتماعي والاقتصادي، عرضة لتهديدات متزايدة في مختلف دول العالم، دون استثناء، نتيجة لظهور أنماط من الجرائم الذكية التي تتسم بالسرعة والتعقيد وصعوبة التتبع.

وأمام هذه التحديات، بات لزامًا على المشرّع الجنائي، في التشريعات المقارنة وكذلك في ليبيا، أن يتدخل بوضع إطار قانوني خاص لمكافحة هذه الظاهرة الإجرامية المستحدثة، من خلال سن

نصوص تواكب طبيعتها التقنية، وتستجيب لخصوصيتها من حيث التجريم والإجراءات، مع الأخذ في الاعتبار تنوع هذه الجرائم وتطورها المستمر، وما تطرحه من صعوبات عملية أمام جهات الضبط والتحقيق والقضاء في كشفها وتتبع مرتكبيها.

وتتميز الجرائم في نطاق القانون الجنائي المعلوماتي بخصائص مغايرة للجرائم التقليدية، إذ إن محل الاعتداء فيها ينصرف في الغالب إلى كيانات غير مادية، كالمعطيات الرقمية ونُظُم المعلومات، الأمر الذي يثير إشكاليات قانونية دقيقة، من أبرزها مدى الاعتراف بالحماية الجنائية للمال المعنوي، وإعادة النظر في المفاهيم التقليدية لمحل الجريمة.

وفي هذا السياق، شهدت مفاهيم قانونية عدة تحولات جوهرية، حيث انتقل مفهوم النقود من صورتها المادية إلى التحويلات الإلكترونية التي تمثل قيمة مالية في شكل بيانات رقمية، كما تطور مفهوم المحرر من صورته الورقية إلى المحرر الإلكتروني، وكذلك التوقيع من شكله التقليدي إلى التوقيع الإلكتروني، وهو ما انعكس بدوره على طبيعة محل الجريمة، الذي أصبح ذا طابع معنوي غير ملموس، بما استتبع تغيرًا في كيفية ارتكاب الفعل الإجرامي وآلياته، وتحول مفهوم المجني عليه أو الضحية من شخص عاقل يقع عليه الاعتداء إلى ما يمكن أن يسمى بالعقل الالكتروني أو النظام المعلوماتي كما في – جرائم الاحتيال المالي– فيسلم للجاني متحصلات الجريمة.

كما أن هذه الجرائم تتسم بدرجة عالية من الخطورة، نظرًا لتعدد أغراضها، وضخامة الخسائر الناجمة عنها مقارنة بالجرائم التقليدية، فضلًا عن صعوبة التنبؤ بمرتكبيها، الذين ينتمون إلى فئات متنوعة، كما تنطوي على أنماط سلوكية غير مألوفة في إطار القواعد العامة لقانون العقوبات التقليدي.

كما أن إجراءات البحث والتحري والتحقيق والمحاكمة في هذا النوع من الجرائم تثير العديد من الإشكاليات القانونية والإدارية والإجرائية، لاسيما فيما يتعلق بجمع الأدلة الرقمية، وتحديد القانون الواجب التطبيق، وإجراءات الضبط والتفتيش، ومتطلبات الإثبات والشهادة، الأمر الذي يفرض تحديات حقيقية على المستوى القضائي والتطبيقي، ومما قدمنا تنبع أهمية الدراسة.

- **أهمية موضوع الدراسة:**

تكتسب دراسة القانون الجنائي المعلوماتي أهميتها من خطورة الجرائم الإلكترونية وتناميها كماً ونوعاً، وما تثيره من تحدٍّ حقيقي لفعالية القواعد التقليدية للنظرية العامة للجريمة، التي لم تعد – في كثير من صورها– كافية لاستيعاب خصوصية السلوك الإجرامي في البيئة الرقمية، ومن ثمّ، فإن

الحاجة تبرز إلى تأصيلٍ حديث يعيد بناء المفاهيم الجنائية في ضوء التحول المعلوماتي، ومن هذا المنطلق؛ تتجلى أهمية هذه الدراسة في بُعدين متكاملين:

- **أولًا: الأهمية النظرية (التأصيلية):**

تتمثل في السعي إلى إرساء ملامح نظرية عامة للقانون الجنائي المعلوماتي، عبر ضبط مفهوم الجريمة المعلوماتية، وتحديد أركانها وتمييزها عن نظيرتها التقليدية، وبيان مدى ملاءمة النصوص الجنائية – العامة والخاصة– لمواكبة التطورات التكنولوجية. كما تنصرف إلى تحليل الخصوصية القانونية لهذا النمط الإجرامي، في ضوء الاتجاهات الفقهية المقارنة، بما يُسهم في تطوير البناء النظري للقانون الجنائي.

- **ثانيًا: الأهمية العملية (التطبيقية):**

تتجسد في اختبار كفاية الإطار التشريعي الليبي، وعلى رأسه قانون مكافحة الجرائم الإلكترونية الليبي رقم (5 لسنة 2022م)، من حيث قدرته على تحقيق الحماية الجنائية الفعالة للأنظمة المعلوماتية، ومواجهة صور الاعتداء المستحدثة. كما تمتد إلى تحليل آليات التطبيق القضائي، وفعالية إجراءات المكافحة والإثبات، وصولًا إلى تقديم حلول عملية تسهم في تعزيز الردع الجنائي والوقاية من الجريمة المعلوماتية.

وإذ أفرد المشرّع هذا النوع من الجرائم بتنظيم خاص، فإن ذلك يعكس اعترافًا بخصوصيتها، سواء من حيث طبيعة محل الجريمة "البيانات والمعلومات"، أو وسيلتها، أو آثارها العابرة للحدود. الأمر الذي يقتضي مقاربةً تحليليةً مقارنة، تستحضر التجارب الدولية، وتُقيّم مدى نجاعة التشريع الوطني في ملاحقة هذا النمط الإجرامي.

وعليه، فإن هذه الدراسة تستهدف تحقيق غاية مزدوجة: تأصيلًا علميًا للنظرية العامة للقانون الجنائي المعلوماتي، وتقويمًا عمليًا لمدى كفاية النصوص والتطبيقات في مواجهة الجرائم الإلكترونية، بما يكفل تعظيم الاستفادة من الثورة الرقمية، والحدّ من مخاطرها على الأفراد والمجتمع.

- **أهداف الدراسة:**

إن الهدف من وضع هذا المقرر الدراسي يتمثل في رصد وتحليل الظاهرة المعلوماتية الإجرامية بدقة علمية، مع التركيز على عناصر الجريمة المعلوماتية وآليات مكافحتها وفق مبادئ النظرية العامة

للقانون الجنائي المعلوماتي والإجراءات الجنائية ذات الصلة، وخاصة فيما يتعلق ببيان الإطار التنظيمي لمسألة الملاحقة في الفضاء الإلكتروني، مع معالجة الإشكالات العملية الناشئة عند اتخاذ إجراءات الاستدلال والتحقيق، وحالات التتبع المرتبطة بالتشابك الإلكتروني بين الأجهزة على المستويين الوطني والدولي، وذلك في نطاق تحليل النصوص القانونية الليبية والمقارنة مع تشريعات أجنبية مماثلة، بهدف استخلاص نتائج عملية تُسهم في تطوير الأحكام الموضوعية والإجرائية المتعلقة بمكافحة الجرائم المعلوماتية وتعزيز فعاليتها.

- **إشكالية الدراسة:**

إن تطور المعلوماتية والتحولات التكنولوجية المعاصرة حولت العالم إلى فضاء مفتوح بلا حدود، ما أفرز نشوء جرائم معلوماتية متقدمة تقنيًا تفوقت على قدرات الدولة الرقابية التقليدية، مهددة الأمن والاستقرار والاقتصاد الوطني، وفي ظل قصور النصوص القانونية الليبية، الموضوعية والإجرائية، عن الإحاطة بكل جوانب هذه الجرائم، واجهت الأجهزة المكلفة بمكافحتها تحديات عملية وإشكالات في تعريفها وضبط عناصرها وأنواعها وكشف مرتكبيها ومعاقبتهم.

من هنا، تتركز إشكالية الدراسة في السؤال القانوني التالي:

ما مدى تأثير تطور المعلوماتية على النظام القانوني الجنائي الليبي، موضوعيًا وإجرائيًا، في ضبط الجرائم المعلوماتية ومعاقبة مرتكبيها وفق القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية (المعلوماتية) ؟.

وانطلاقًا مما تثيره الإشكالية أعلاه، تنبثق الأسئلة التالية:

1. ما مفهوم الجريمة المعلوماتية، وما تعريفها القانوني، وأركانها وأنواعها؟.
2. كيف يتم قمع الجريمة المعلوماتية، وما الإجراءات القانونية للضبط، والتحقيق، والتنفيذ والمحاكمة؟.
3. هل النصوص الجنائية التقليدية، موضوعيًا وإجرائيًا، كافية لمواجهة الجريمة المعلوماتية، أم أن الأمر يستلزم تدخلًا تشريعيًا جديدًا لضمان عدم إفلات الجناة من العقاب؟.

- **منهج الدراسة:**

تأسيسًا على الطبيعة القانونية المركبة لموضوع النظرية العامة للقانون الجنائي المعلوماتي، وأهميته العلمية والعملية، وارتباطه بإشكالية دقيقة تستهدف تأصيل المفاهيم القانونية المستحدثة، وبيان الخصائص الفنية والقانونية للجرائم المعلوماتية، اعتمدت الدراسة على المنهج التحليلي بوصفه منهجًا رئيسًا، وذلك من خلال تحليل نصوص القانون رقم (05 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، في جانبيه الموضوعي والإجرائي، وبيان مدى كفايته في مواجهة هذا النمط المستحدث من الإجرام المعلوماتي.

كما تم توظيف المنهج الوصفي، من خلال الرجوع إلى الدراسات والبحوث الفقهية المتخصصة كمصدر أساس، مع الاستفادة من المصادر الحديثة، بما في ذلك المنصات والمواقع المتخصصة في رصد وتتبع الجرائم المعلوماتية، وذلك بهدف الإحاطة بالتطورات التقنية والعملية المرتبطة بهذه الظاهرة.

وإلى جانب ذلك، اعتمدت الدراسة المنهج المقارن، من خلال مقابلة التشريع الليبي بنظائره في بعض التشريعات المتقدمة في مجال مكافحة الجرائم المعلوماتية، بغية الوقوف على أوجه الاتفاق والاختلاف، واستخلاص أفضل الممارسات التشريعية التي تسهم في تعزيز فعالية السياسة الجنائية المعلوماتية، وتطوير آليات المواجهة القانونية لهذا النوع من الجرائم.

- **خطة الدراسة:**

من أجل وضع دراسة في النظرية العامة للقانون الجنائي المعلوماتي والإجابة على إشكاليتها والتساؤلات المقترحة عنها، استدعى الأمر تقسيم الدراسة إلى جزئين: يُعنى الأول بتحديد ماهية الأحكام الموضوعية للجرائم المعلوماتية، ويتطرق الثاني إلى دراسة وتحليل الأحكام الإجرائية والتعاون في مكافحة الجرائم المعلوماتية. ذلك بعد التمهيد لها بمدخل يتعلق بماهية تقنية المعلومات من الناحيتين التقنية والجنائية؛ ويشتمل هذا المقرر الدراسي على الآتي:

- **الجزء الأول: أثر الجريمة المعلوماتية على قانون العقوبات.**
- **الجزء الثاني: أثر الجريمة المعلوماتية على قانون الإجراءات الجنائية.**

• الجزء الأول:

أثر الجريمة المعلوماتية على قانون العقوبات.

أصبح الحاسوب وتقنيات المعلومات والاتصالات في العصر الحديث من الركائز الأساسية للحياة المعاصرة، وأداةً لا غنى عنها في إدارة مختلف الأنشطة الاقتصادية والإدارية والعلمية والاجتماعية. وقد صاحب هذا التطور التقني المتسارع ظهور أنماط جديدة من السلوك الإجرامي ارتبطت بالبيئة الرقمية، سواء باتخاذ الأنظمة المعلوماتية وسيلة لارتكاب الجريمة أو باعتبارها محلًا للاعتداء، الأمر الذي أدى إلى نشوء ما يُعرف بالجريمة المعلوماتية أو الإلكترونية.

ومع التوسع الهائل في استخدام شبكة المعلومات الدولية وتزايد الاعتماد على الخدمات الرقمية في مختلف المعاملات، لم تعد الجريمة محصورة في إطارها التقليدي القائم على الاعتداء المادي المباشر، بل انتقلت إلى فضاء افتراضي يتسم بالسرعة والتعقيد والعالمية، بحيث بات من الممكن ارتكاب الفعل الإجرامي عن بُعد، وتجاوز الحدود الجغرافية للدول، واستهداف مصالح وأشخاص وأنظمة معلوماتية في أماكن متعددة في الوقت ذاته.

وقد كشفت هذه التحولات عن تحديات جوهرية أمام قانون العقوبات التقليدي، إذ أفرزت الجريمة المعلوماتية صورًا مستحدثة للاعتداء على مصالح قانونية لم تكن معروفة بالقدر ذاته في البيئة التقليدية، كسلامة البيانات وسريتها وأمن الأنظمة المعلوماتية والثقة في المعاملات الإلكترونية. كما فرضت إعادة النظر في العديد من المفاهيم الجنائية المستقرة، ولا سيما تلك المتعلقة بمحل الجريمة، وطبيعة السلوك الإجرامي، والنتيجة الجنائية، والاختصاص المكاني، فضلاً عن مدى كفاية النصوص العقابية التقليدية لاستيعاب هذه الأفعال المستحدثة.

ولم يقتصر أثر الجريمة المعلوماتية على استحداث صور جديدة من الجرائم، بل امتد إلى التأثير في فلسفة التجريم ذاتها، من خلال توسيع نطاق الحماية الجنائية ليشمل البيئة الرقمية ومكوناتها المختلفة، وإضفاء الحماية القانونية على المصالح المعلوماتية بوصفها مصالح جديرة بالحماية المستقلة. كما دفع التشريعات الحديثة إلى استحداث نصوص خاصة لمواجهة الأفعال التي يصعب إخضاعها للقواعد التقليدية أو التي تتطلب تنظيمًا جنائيًا يتلاءم مع طبيعتها التقنية.

ومن ثم، فإن دراسة أثر الجريمة المعلوماتية على قانون العقوبات لا تقتصر على بيان الجرائم المستحدثة التي أفرزها التطور التكنولوجي، وإنما تمتد إلى بحث مدى تأثير هذا النمط الإجرامي في

البنيان الموضوعي للقانون الجنائي، وفي مفاهيمه الأساسية ونطاق حمايته وأدواته التشريعية، بما يكشف عن حجم التحول الذي فرضته البيئة الرقمية على الفكر الجنائي المعاصر.

وعلى هذا الأساس، يتناول هذا الجزء الأحكام الموضوعية للجريمة المعلوماتية وما أحدثته من تأثير في القواعد التقليدية لقانون العقوبات في **(الفصل الأول)**، ثم نعرض لصور الجريمة المعلوماتية وتطبيقاتها الجنائية لأهم أنواعها وتطبيقاتها العملية في ضوء التشريع الجنائي الليبي في **(الفصل الثاني)**.

• الفصل الأول:
الأحكام الموضوعية للجريمة المعلوماتية.

يشكل الوقوف على الأحكام الموضوعية للجريمة المعلوماتية مدخلًا أساسيًا لفهم طبيعتها القانونية وتمييزها عن أنماط الإجرام التقليدي، ذلك أن التطور المتسارع في تقنيات المعلومات والاتصالات لم يقتصر أثره على استحداث صور جديدة من السلوك الإجرامي، بل امتد ليُحدث تحولًا جوهريًا في البنيان القانوني للجريمة ذاتها وفي خصائص مرتكبيها. فقد أفرزت البيئة الرقمية جرائم تتسم بخصوصية موضوعية تتعلق بطبيعة محل الاعتداء ووسائل ارتكابه وآثاره، كما أوجدت نمطًا متميزًا من الجناة يتمتع بقدرات تقنية ومعرفية تجعل من الصعب إخضاعه للمعايير التقليدية التي استقرت عليها الدراسات الجنائية.

ومن ثم، فإن دراسة الجريمة المعلوماتية لا تكتمل بالوقوف عند عناصرها القانونية المجردة، وإنما تقتضي تحليل الخصائص الموضوعية التي تميزها عن غيرها من الجرائم، إلى جانب بحث الخصوصية الشخصية للمجرم المعلوماتي وما يرتبط بها من سمات فنية وسلوكية تؤثر في تكوين الظاهرة الإجرامية الرقمية وأساليب مكافحتها. وعلى هذا الأساس، سيتم تناول الأحكام الموضوعية للجريمة المعلوماتية من خلال بيان خصوصيتها الموضوعية، ثم الوقوف على الخصوصية الشخصية للمجرم المعلوماتي في ضوء أحكام القانون الجنائي المعلوماتي ومقتضيات السياسة الجنائية المعاصرة.

• المبحث الأول: الخصوصية الموضوعية للجريمة المعلوماتية.

أدت التطورات المتسارعة في مجال تقنية المعلومات والاتصالات إلى ظهور أنماط جديدة من الجرائم اتسمت بخصائص موضوعية مغايرة لتلك التي تميز الجرائم التقليدية، سواء من حيث محل الاعتداء أو وسيلة ارتكاب الجريمة أو طبيعة آثارها. وقد أضفت هذه الخصائص على الجريمة

المعلوماتية طابعًا خاصًا استدعى إعادة النظر في كثير من المفاهيم الجنائية التقليدية لمواكبة متطلبات البيئة الرقمية.

وعليه، تقتضي دراسة الجريمة المعلوماتية الوقوف على خصوصيتها الموضوعية وبيان أهم السمات التي تميزها عن غيرها من الجرائم، وما يترتب على ذلك من آثار قانونية في مجال التجريم والمساءلة الجنائية **(المطلب الأول)**، ثم نتناول خصوصية محل الجريمة المعلوماتية وأدلتها في **(المطلب الثاني)**.

- **المطلب الأول: مفهوم الجريمة المعلوماتية وأساسها القانوني.**

أدى التطور المتسارع في تقنيات المعلومات والاتصالات إلى ظهور نمط إجرامي جديد تجاوز الإطار التقليدي للجريمة، بحيث أصبحت البيئة الرقمية مجالًا لارتكاب أفعال تمس البيانات والأنظمة والمصالح المحمية قانونًا، وقد فرض هذا التحول إعادة النظر في المفاهيم الجنائية التقليدية، سواء من حيث تحديد مفهوم الجريمة المعلوماتية أو بيان خصائصها الموضوعية التي تميزها عن الجرائم المألوفة.

وعليه، فإن دراسة هذا النوع المستحدث من الإجرام تقتضي بيان مدلوله القانوني والفقهي، ثم الوقوف على خصوصيته من حيث طبيعة محل الاعتداء ووسائل ارتكابه وبنيانه المادي، يتطلب تناول تعريف الجريمة المعلوماتية في **(الفرع الأول)**، ومن ثم تناول خصوصية الجريمة المعلوماتية من الناحية الموضوعية في **(الفرع الثاني)**.

- **الفرع الأول: تعريف الجريمة المعلوماتية.**

تمثل الجريمة المعلوماتية صورة مستحدثة من صور الإجرام فرضتها التطورات التقنية والتحول الرقمي، حيث انتقل السلوك الإجرامي من المجال المادي التقليدي إلى البيئة الرقمية، فأصبحت البيانات والأنظمة المعلوماتية محلًا للحماية الجنائية أو وسيلة لارتكاب الفعل الإجرامي. ومن ثم، فإن تحديد مفهومها يقتضي بيان أساسها الجنائي والفقهي والتشريعي وخصوصيتها الموضوعية.

- **أولا: التعريف الجنائي والفقهي للجريمة المعلوماتية.**

يقوم مفهوم الجريمة في إطار القانون الجنائي على أساس أنها فعل غير مشروع صادر عن إرادة جنائية، يقرر له المشرع جزاءً جنائيًا تحقيقًا لمبدأ الشرعية الجنائية الذي يقضي بعدم جواز التجريم أو العقاب إلا بناءً على نص قانوني سابق. ومن ثم فإن وصف الفعل بأنه جريمة لا يستند إلى مجرد

مخالفته للقواعد الأخلاقية أو الاجتماعية، وإنما إلى تدخل المشرع بتحديد السلوك المحظور والجزاء المقرر له.

وانطلاقًا من هذه القواعد، ظهرت الجريمة المعلوماتية بوصفها صورة حديثة من صور الإجرام ارتبطت بالتطور التقني، حيث انتقل السلوك الإجرامي من المجال المادي التقليدي إلى المجال الرقمي. ويمكن تعريفها بأنها:"كل سلوك غير مشروع معاقب عليه قانونًا، يتم باستخدام الأنظمة المعلوماتية أو يستهدفها، وينصب على البيانات أو البرامج أو الأنظمة الإلكترونية بما يؤدي إلى الاعتداء على مصلحة قانونية يحميها القانون"، ويتميز هذا التعريف بأنه يجمع بين عناصر أساسية تتمثل في:

1. البيئة الرقمية التي يقع فيها النشاط الإجرامي، سواء من خلال الحاسب الآلي أو شبكات الاتصال أو غيرها من الوسائل التقنية.
2. محل الاعتداء، الذي يتمثل في البيانات والمعلومات والبرامج والأنظمة المعلوماتية، باعتبارها كيانات غير مادية تختلف عن محل الجريمة التقليدية.
3. الوسيلة التقنية المستخدمة في ارتكاب الفعل أو تسهيله أو إخفاء آثاره.

وقد تعددت الاتجاهات الفقهية في تعريف الجريمة المعلوماتية؛ فذهب اتجاه ضيق إلى قصرها على الجرائم التي لا يمكن تصور وقوعها إلا في البيئة الرقمية، مثل اختراق الأنظمة المعلوماتية، بينما اتجه اتجاه واسع إلى اعتبارها كل سلوك إجرامي تستخدم فيه التقنية كوسيلة أو تكون محلًا للاعتداء. أما الاتجاه الشمولي فينظر إليها باعتبارها كل اعتداء غير مشروع يرتبط بالمعالجة الإلكترونية للبيانات أو الأنظمة المعلوماتية.

وعليه، فإن جوهر الجريمة المعلوماتية يتمثل في الاعتداء على المعلومة أو النظام المعلوماتي، سواء اتخذت التقنية محلًا للجريمة أو وسيلة لارتكابها.

- **ثانيا: التعريف التشريعي للجريمة المعلوماتية في القانون الليبي:**

اعتمد المشرع الليبي في القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية مفهومًا واسعًا للجريمة الإلكترونية، إذ نص في المادة (1) على أنها:"كل فعل يُرتكب من خلال استخدام أنظمة الحاسب الآلي أو شبكة المعلومات الدولية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون"، ويستخلص من هذا التعريف أن المشرع أقام الجريمة المعلوماتية على ثلاثة عناصر رئيسية:

1. **السلوك الإجرامي:** حيث استخدم المشرع عبارة "كل فعل" بما يشمل صور السلوك الإيجابي، كالاختراق أو التعديل أو النشر، وقد يمتد إلى الامتناع متى رتب القانون عليه مسؤولية جنائية.
2. **وسيلة ارتكاب الجريمة:** وتتمثل في أنظمة الحاسب الآلي أو شبكة الإنترنت أو أي وسيلة تقنية معلومات أخرى.
3. **عدم المشروعية:** بمعنى أن الفعل لا يكتسب وصف الجريمة إلا إذا كان مخالفًا لأحكام القانون، تطبيقًا لمبدأ الشرعية الجنائية.

ومن خلال استقراء أحكام القانون، يتضح أن المشرع الليبي تبنى نموذجًا موسعًا للتجريم يقوم على حماية البيئة الرقمية من خلال:

1. تجريم الأفعال المستقلة المرتبطة بالأنظمة المعلوماتية.
2. وتجريم استخدام الوسائل الإلكترونية في ارتكاب جرائم تقليدية.

وقد أكد هذا الاتجاه من خلال تقرير إمكانية تطبيق أحكام قانون العقوبات العام متى استُخدمت الوسائل الإلكترونية في ارتكاب الجريمة.

وبذلك يمكن استخلاص مفهوم تشريعي جامع للجريمة المعلوماتية باعتبارها:"كل سلوك غير مشروع يُرتكب باستخدام الوسائل التقنية أو يستهدفها، ويترتب عليه الاعتداء على البيانات أو الأنظمة المعلوماتية أو المصالح القانونية المرتبطة بها".

- **ثالثا: عناصر الخصوصية الموضوعية للجريمة المعلوماتية:**

تستمد الجريمة المعلوماتية خصوصيتها الموضوعية من طبيعة البيئة الرقمية التي ترتكب فيها، إذ تختلف عن الجرائم التقليدية من حيث محل الاعتداء ووسائل ارتكاب الفعل الإجرامي والآثار المترتبة عليه. فمحل الجريمة قد ينصب على عناصر غير مادية تتمثل في البيانات والبرامج والأنظمة المعلوماتية، كما تعتمد في تنفيذها على وسائل تقنية متطورة تجعلها أكثر تعقيدًا من حيث الاكتشاف والإثبات والملاحقة الجنائية.

ومن ثم، فإن خصوصية الجريمة المعلوماتية لا ترتبط بمجرد استخدام التقنية، وإنما بطبيعة الاعتداء الرقمي ذاته وما يترتب عليه من تحديات قانونية تستوجب تطوير قواعد الحماية الجنائية بما يتلاءم مع خصائص الإجرام الإلكتروني، وذلك في الآتي:

1. خصوصية محل الجريمة ووسيلة ارتكابها:

تختلف الجريمة المعلوماتية عن الجريمة التقليدية من حيث محل الاعتداء، إذ ينصب غالبًا على عناصر غير مادية تتمثل في البيانات والبرامج وقواعد المعلومات والأنظمة الإلكترونية. وهذه الطبيعة غير المادية تجعل الاعتداء عليها مختلفًا عن الاعتداء على الأموال أو الأشياء المادية.

فالبيانات الرقمية تمثل قيمة قانونية واقتصادية مستقلة، وقد يكون الاعتداء عليها في صورة الوصول غير المشروع أو التعديل أو الإتلاف أو النسخ أو الاستيلاء عليها.

كما تتميز وسيلة ارتكاب الجريمة المعلوماتية بكونها عنصرًا جوهريًا في تكوينها، إذ تعتمد على استخدام تقنيات وبرمجيات وشبكات إلكترونية، ولا تكون التقنية مجرد وسيلة عارضة وإنما جزء من البناء القانوني للجريمة.

ومن ثم، يخرج عن نطاق الجريمة المعلوماتية الاعتداء على المكونات المادية للأجهزة الإلكترونية متى كان محلها مالًا ماديًا، إذ تخضع هذه الأفعال للقواعد التقليدية في قانون العقوبات.

2. خصوصية آثار الجريمة المعلوماتية وتمييزها عن الجريمة التقليدية:

تتميز الجريمة المعلوماتية بخصائص تجعلها تختلف عن الجرائم التقليدية، فهي غالبًا ما تكون عابرة للحدود، وسريعة التنفيذ، وصعبة الاكتشاف، قابلة لإخفاء آثارها أو تغييرها. كما أن الضرر الناتج عنها قد لا يكون ماديًا مباشرًا، بل قد يتمثل في المساس بسرية المعلومات أو سلامة الأنظمة أو الثقة في البيئة الرقمية.

ولهذا اتجهت التشريعات الحديثة، ومنها التشريع الليبي، إلى بناء حماية جنائية خاصة للفضاء المعلوماتي، تقوم على حماية الأمن المعلوماتي باعتباره مصلحة قانونية مستقلة، وبهذا، فإن الجريمة المعلوماتية تمثل نموذجًا حديثًا للجريمة، فرض إعادة تطوير المفاهيم التقليدية للقانون الجنائي بما يتلاءم مع طبيعة المجتمع الرقمي.

- **الفرع الثاني:**

خصوصية الجريمة المعلوماتية من الناحية الموضوعية.

تمثل الجريمة المعلوماتية تحولًا جوهريًا في البناء التقليدي للجريمة، فرضته التطورات المتلاحقة في مجال تقنية المعلومات والاتصالات، حيث انتقل السلوك الإجرامي من نطاقه المادي المحسوس

إلى بيئة رقمية تتسم بالتعقيد والسرعة والخفاء. فلم يعد الاعتداء الجنائي مقصورًا على الأشخاص أو الأموال المادية، وإنما امتد ليشمل البيانات والأنظمة المعلوماتية باعتبارها مصالح قانونية جديرة بالحماية.

وقد استجاب المشرع الليبي لهذا التطور من خلال إصدار القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، الذي وضع إطارًا قانونيًا خاصًا لمواجهة الاعتداءات المرتبطة بالبيئة الرقمية، وإن لم يضع تعريفًا تفصيليًا جامعًا للجريمة المعلوماتية، وإنما ربطها باستخدام أنظمة الحاسب الآلي أو شبكات المعلومات أو غيرها من الوسائل التقنية.

وتظهر خصوصية الجريمة المعلوماتية من الناحية الموضوعية في اختلاف بنيانها القانوني عن الجريمة التقليدية، خاصة من حيث طبيعة الركن المادي، وطبيعة السلوك الإجرامي، ومحل الحماية الجنائية، إضافة إلى طابعها العابر للحدود، وتبيان ذلك الآتي:

- **أولًا: خصوصية الركن المادي في الجريمة المعلوماتية:**

يمثل الركن المادي المظهر الخارجي للجريمة، فلا تقوم المسؤولية الجنائية بمجرد وجود الإرادة الإجرامية، وإنما يلزم أن تتجسد هذه الإرادة في نشاط خارجي يعتد به القانون، ويقصد به النشاط الذي يصدر عن الجاني ويؤدي إلى نتيجة إجرامية ترتبط به بعلاقة سببية.

غير أن الركن المادي في الجريمة المعلوماتية يختلف عن صورته التقليدية؛ إذ لم يعد يرتبط بفعل مادي ظاهر يمكن إدراكه بالحواس، وإنما يظهر غالبًا في صورة نشاط تقني يتم داخل البيئة الرقمية من خلال الأنظمة والبرامج وقواعد البيانات.

فالسلوك الإجرامي المعلوماتي قد يتمثل في:

1. إصدار أوامر إلكترونية للنظام المعلوماتي.
2. معالجة أو نقل البيانات بصورة غير مشروعة.
3. تجاوز وسائل الحماية الإلكترونية.
4. إدخال أو تعديل أو حذف المعلومات.
5. استخدام برامج أو وسائل تقنية للإضرار بالنظام.

وعليه، فإن الركن المادي في الجريمة المعلوماتية يقوم على التفاعل بين الإرادة البشرية والوسيلة التقنية، حيث يصدر الجاني أوامر رقمية يقوم النظام بتنفيذها، فتتحقق النتيجة الإجرامية من خلال معالجة البيانات أو التأثير على النظام المعلوماتي.

- **ثانيًا: الطبيعة اللامادية للفعل الإجرامي المعلوماتي:**

تتمثل أهم خصوصيات الفعل الإجرامي المعلوماتي في طابعه غير المادي، إذ لا يظهر غالبًا في صورة حركة جسدية أو اعتداء مباشر، وإنما يتحقق من خلال عمليات تقنية غير مرئية.

فالفعل الإجرامي قد يكون عبارة عن:

1. كتابة شيفرة ضارة.
2. إرسال بيانات أو أوامر إلكترونية غير مشروعة.
3. تعديل محتوى قاعدة بيانات.
4. تجاوز أنظمة الحماية.

ومن ثم فإن النشاط الإجرامي المعلوماتي لا يعتمد على القوة المادية، وإنما على المعرفة التقنية والمهارة الفنية، وهو ما يفسر صعوبة اكتشافه وإثباته مقارنة بالجرائم التقليدية.

كما أن محل الاعتداء غالبًا ما يكون غير مادي، مثل البيانات والمعلومات والبرامج، الأمر الذي يجعل آثاره تظهر في صورة سجلات إلكترونية أو آثار رقمية تحتاج إلى وسائل فنية متخصصة للكشف عنها وتحليلها.

- **ثالثًا: الطبيعة اللا إقليمية للجريمة المعلوماتية:**

تتميز الجريمة المعلوماتية بأنها جريمة عابرة للحدود، إذ تحررت من الارتباط بالمكان الجغرافي المحدد الذي يميز الجرائم التقليدية، وبحيث قد يقع الفعل في دولة، وتتحقق النتيجة في دولة أخرى، بينما توجد البيانات أو الخوادم في دولة ثالثة.

وينتج عن ذلك عدة إشكالات قانونية أهمها:

1. صعوبة تحديد مكان ارتكاب الجريمة.
2. تعدد الاختصاصات القضائية.
3. تحديد القانون الواجب التطبيق.

وقد ظهرت في هذا المجال بعض النظريات لمعالجة مشكلة الاختصاص، ومنها:

1. **نظرية الإصدار**: وتقوم على تطبيق قانون الدولة التي صدر منها النشاط الإجرامي.
2. **نظرية التقبل:** وتعتمد على تطبيق قانون الدولة التي تحققت فيها النتيجة أو وقع فيها الضرر.

إلا أن الطبيعة العالمية للجريمة المعلوماتية تجعل مواجهتها تتطلب التعاون الدولي وتطوير قواعد الاختصاص الجنائي بما يتلاءم مع طبيعتها الرقمية.

- **رابعًا: خصائص الجريمة المعلوماتية في ضوء التشريع الليبي:**

يستخلص من القانون رقم (5 لسنة 2022م) أن الجريمة المعلوماتية تتميز بمجموعة من الخصائص الموضوعية، أهمها:

1. **الطابع التقني:** حيث ترتكب باستخدام الحاسب الآلي أو الشبكات أو الأنظمة الرقمية.
2. **ازدواجية محل الجريمة:** فقد تكون التقنية وسيلة لارتكاب الجريمة، كما في الاحتيال الإلكتروني، وقد تكون محلًا للاعتداء كما في اختراق الأنظمة أو إتلاف البيانات.
3. **الطبيعة غير المادية للمحل:** إذ تنصب الحماية الجنائية على البيانات والمعلومات والهوية الرقمية والأنظمة الإلكترونية.
4. **الطابع العابر للحدود:** حيث يمكن أن تمتد آثار الجريمة خارج إقليم الدولة، وهو ما يستوجب التعاون القضائي الدولي.
5. **تنوع صور السلوك الإجرامي:** فقد شمل التشريع الليبي صورًا متعددة وفقا لما نص عليه القانون رقم (05 لسنة 2022م) بشأن مكافحة الجرائم الالكترونية، منها:
   أ. الدخول غير المشروع إلى الأنظمة طبقا لنص المادة (11، 12، 18).
   ب. اعتراض البيانات والاتصالات طبقا لنص المادة (13، 47).
   ت. الاعتداء على المعلومات طبقا لنص المادتين (15، 16).
   ث. الجرائم المتعلقة بالخصوصية والهوية الرقمية طبقا لنص المادتين (04، 05، 10، 22).
   ج. الجرائم الاقتصادية الإلكترونية طبقا لنص المواد (17، 24، 25، 26، 28، 44، 46).
   ح. الجرائم المتعلقة بتداول الأشياء الأفعال المحظورة طبقا لنص المواد (19، 20، 21، 23، 27، 29، 30، 31، 32، 33، 38، 40، 44، 43).
   خ. الجرائم الماسة بأمن الدولة والمصلحة العامة طبقا لنص المواد (34، 35،36، 37، 42، 45).

د. الجرائم المتعلقة بالملكية الأدبية أو الفكرية أو العملية أو الصناعة طبقا لنص المواد (06، 07، 24، 25، 26، 39).

وبذلك تظهر الجريمة المعلوماتية باعتبارها نموذجًا إجراميًا حديثًا يتميز ببناء موضوعي خاص، فرض إعادة تطوير المفاهيم التقليدية للقانون الجنائي بما يحقق التوازن بين فعالية الحماية الجنائية ومتطلبات البيئة الرقمية.

• المطلب الثاني:

خصوصية محل الجريمة المعلوماتية وأدلتها.

تختلف الجريمة المعلوماتية عن الجريمة التقليدية من حيث طبيعة محل الاعتداء ووسائل إثباته؛ فبينما تنصب الجرائم التقليدية في الغالب على أشياء أو مصالح مادية يمكن إدراكها بالحواس، تتجه الجريمة المعلوماتية إلى عناصر رقمية غير ملموسة تتمثل في البيانات والمعلومات والأنظمة الإلكترونية. كما أن إثبات هذا النوع من الجرائم لا يعتمد على الأدلة التقليدية وحدها، بل يرتكز بصورة أساسية على الأدلة الرقمية المستخرجة من البيئة المعلوماتية، ولذلك فإن فهم البناء القانوني للجريمة المعلوماتية يقتضي الوقوف على طبيعة البيانات المعلوماتية باعتبارها محلًا للحماية الجنائية في **(الفرع الأول)**، ثم دراسة الدليل الجنائي الرقمي بوصفه الوسيلة الأساسية للكشف عن الجريمة وإثباتها في **(الفرع الثاني)**.

• الفرع الأول:

البيانات المعلوماتية محلًا للحماية الجنائية.

تمثل البيانات المعلوماتية الركيزة الأساسية التي تقوم عليها البيئة الرقمية، إذ تشكل المادة الأولية التي تعتمد عليها الأنظمة المعلوماتية في عمليات الإدخال والتخزين والمعالجة واسترجاع المعلومات، ومع التطور المتسارع لتكنولوجيا المعلومات والاتصالات، أصبحت البيانات تتمتع بقيمة اقتصادية وأمنية وشخصية متزايدة، الأمر الذي استوجب إحاطتها بحماية جنائية خاصة، سواء باعتبارها محلًا مباشرًا للاعتداء أو وسيلة لارتكاب الجريمة المعلوماتية.

ويقصد بالبيانات المعلوماتية كل تمثيل رقمي للوقائع أو المعلومات يتم إنشاؤه أو إدخاله أو تخزينه أو معالجته داخل نظام معلوماتي على هيئة إشارات أو نبضات إلكترونية قابلة للمعالجة بواسطة البرامج والتطبيقات الحاسوبية بهدف إنتاج معنى أو نتيجة قابلة للفهم والاستخدام. كما يمكن تعريفها

بأنها مجموعة من الإشارات أو النبضات الإلكترونية المشفرة التي يعالجها الحاسوب لتحويلها إلى معلومات ذات دلالة ومعنى.

ويتضح من ذلك أن مفهوم البيانات المعلوماتية لا يقتصر على الأرقام أو الرموز المجردة، وإنما يمتد ليشمل مختلف أشكال المحتوى الرقمي، كالنصوص المكتوبة والصور والتسجيلات الصوتية والمرئية والأرقام السرية والملفات الإلكترونية وقواعد البيانات وغيرها من العناصر التي يمكن للنظام المعلوماتي تخزينها أو معالجتها أو تداولها.

وتتميز البيانات المعلوماتية بطبيعة تقنية خاصة تجعلها تختلف عن الأشياء المادية التقليدية؛ فهي تُخزن داخل الأنظمة الإلكترونية في صورة ثنائية تعتمد على النبضات الرقمية (0 و1)، ولا تكتسب قيمتها أو مدلولها العملي إلا من خلال البرامج والتطبيقات القادرة على تفسيرها ومعالجتها وتحويلها إلى معلومات قابلة للفهم والاستعمال. ومن ثم فإن البيانات تمثل المادة الخام للمعلومات، بحيث تؤدي معالجتها بواسطة البرمجيات إلى إنتاج المعرفة أو النتائج المطلوبة، وهو ما يمكن التعبير عنه بالمعادلة الآتية: "البيانات + البرامج = معلومات قابلة للفهم والمعالجة"[1].

وتبرز الأهمية الجنائية للبيانات المعلوماتية في كونها قد تكون محلًا مباشرًا للاعتداء الإجرامي، كما قد تمثل أداة لتنفيذ الجريمة أو مصدرًا للكشف عنها وإثباتها. فقد يستهدف الجاني سرقة البيانات أو نسخها أو تعديلها أو إتلافها أو تعطيل الوصول إليها أو استخدامها دون وجه حق، كما قد تشكل البيانات ذاتها دليلًا يكشف عن النشاط الإجرامي من خلال ما تتركه من آثار رقمية داخل الأنظمة المعلوماتية.

كما تتسم البيانات المعلوماتية بخصائص تميزها عن الأموال والأشياء المادية التقليدية، فهي غير ملموسة بطبيعتها، وسهلة النسخ والنقل والتداول، وقابلة للتعديل أو الإتلاف في فترات زمنية وجيزة، ولا يمكن إدراك قيمتها أو محتواها إلا من خلال الوسيط التقني القادر على قراءتها ومعالجتها، ومن ثم

---

[1] **البيانات المعلوماتية**: تعرف بأنها:"تمثيلات رقمية للوقائع أو المعلومات، تُخزن أو تُعالج داخل النظام المعلوماتي على شكل إشارات أو نبضات إلكترونية، قابلة للمعالجة بواسطة البرامج لإنتاج معنى أو نتيجة"، وتعريف البيانات المعلوماتية بأنها:"مجموعة من النبضات أو الإشارات الإلكترونية المشفرة التي يعالجها الحاسوب لإنتاج معلومات ذات معنى:، وللتوضيح: البيانات ليست مجرد أرقام، بل قد تكون نصوصًا، أو صورًا، أو أرقامًا سرية، بحيث تُخزن في صورة (0 و1)، ولا تكتسب معناها إلا عبر البرامج، وبالتالي البيانات + البرنامج = معلومات قابلة للفهم.

فإن حمايتها تقتضي تبني قواعد قانونية خاصة تراعي طبيعتها الرقمية وتكفل مواجهة صور الاعتداء المستحدثة التي قد ترد عليها.

وعليه، فإن خصوصية البيانات المعلوماتية لا تنبع من كونها مجرد وعاء للمعلومات، وإنما من كونها تمثل عنصرًا جوهريًا في البنيان القانوني والتقني للجريمة المعلوماتية؛ فهي قد تكون محل الاعتداء، وموضوع الحماية الجنائية، ومصدر الدليل في آن واحد، ولذلك أصبحت حمايتها وتنظيم التعامل معها من أهم مقتضيات السياسة الجنائية الحديثة في مواجهة الجرائم الإلكترونية، وبما يضمن حماية المصالح الفردية والمؤسسية المرتبطة بالبيئة الرقمية.

- **الفرع الثاني:**

الدليل الجنائي الرقمي وحجيته في الإثبات.

تُعد الأدلة الجنائية الركيزة الأساسية التي تقوم عليها عملية الإثبات في المجال الجنائي، غير أن التطور التقني الذي صاحب ظهور الجرائم المعلوماتية أدى إلى بروز نمط جديد من الأدلة يختلف في طبيعته ومصدره عن الأدلة التقليدية، وهو ما يعرف بالدليل الجنائي الرقمي أو الدليل الإلكتروني. فإذا كانت البيانات المعلوماتية تمثل محل الاعتداء في الجريمة الإلكترونية، فإن الدليل الجنائي الرقمي يمثل الوسيلة الرئيسة للكشف عن الجريمة وإثباتها ونسبتها إلى مرتكبها.

- **أولًا: مفهوم الدليل الجنائي الرقمي:**

يقصد بالدليل الجنائي الرقمي كل بيانات أو معلومات ذات قيمة إثباتية يتم إنشاؤها أو تخزينها أو نقلها أو معالجتها بواسطة نظام معلوماتي، ويُمكن الاستناد إليها في إثبات وقوع الجريمة أو الكشف عن مرتكبها أو بيان ظروف ارتكابها. كما يمكن تعريفه بأنه كل أثر رقمي ناتج عن تفاعل المستخدم والبرامج والأنظمة المعلوماتية والبيانات الإلكترونية، يكون قابلاً للاستخلاص والفحص والتحليل الفني بما يسمح باستخدامه في مجال الإثبات الجنائي.

ويتميز الدليل الرقمي عن الدليل التقليدي بأن وجوده لا يرتبط بأثر مادي محسوس يمكن إدراكه بالحواس مباشرة، وإنما يتمثل في آثار إلكترونية تنشأ داخل البيئة الرقمية نتيجة تشغيل الأنظمة والبرامج ومعالجة البيانات. فكل عملية دخول إلى نظام معلوماتي، أو إرسال رسالة إلكترونية، أو تعديل ملف رقمي، أو نقل بيانات عبر الشبكات، تؤدي إلى إنشاء سجلات إلكترونية وآثار رقمية تحفظها الأنظمة بصورة تلقائية، وتشكل فيما بعد مصدرًا مهمًا للإثبات الجنائي.

وفي الجرائم المعلوماتية يغيب في الغالب الدليل المادي التقليدي، لتحل محله الأدلة الرقمية التي تتخذ شكل سجلات إلكترونية أو بيانات وصفية أو معلومات مخزنة داخل الأنظمة والشبكات. ونظرًا لما تتميز به هذه الأدلة من قابلية للمحو أو الإخفاء أو التعديل، فقد اتجه المشرّع الليبي إلى توفير الحماية الجنائية لها من خلال تجريم إتلافها أو إخفائها أو العبث بها، فضلاً عن تجريم الوسائل والأدوات المستخدمة في الاعتداء غير المشروع على الأنظمة والبيانات المعلوماتية.

- **ثانيًا: خصائص الدليل الإلكتروني:**

يتميز الدليل الجنائي الرقمي[2] بمجموعة من الخصائص التي تمنحه طبيعة قانونية وفنية متميزة عن الأدلة التقليدية، ومن أبرز هذه الخصائص:

1. **الطابع اللامادي للدليل:** فهو لا يتمثل في شيء مادي محسوس، وإنما في بيانات وسجلات وآثار رقمية لا يمكن إدراكها إلا من خلال وسائل تقنية متخصصة.
2. **الطبيعة الديناميكية والمتغيرة:** إذ يمكن تعديل الدليل الرقمي أو محوه أو نقله خلال فترة زمنية قصيرة، الأمر الذي يجعله أكثر هشاشة من الدليل التقليدي.
3. **كونه ناتجًا عن معالجة آلية:** فغالبية الأدلة الرقمية لا تنشأ بفعل بشري مباشر، وإنما تنتج تلقائيًا عن عمل الأنظمة والبرامج، كملفات الأحداث وسجلات الاستخدام وتواريخ العمليات الإلكترونية.
4. **اعتماده على الوسيط التقني:** فلا يمكن قراءة الدليل أو تفسيره أو الاستفادة منه إلا من خلال أجهزة وبرامج متخصصة قادرة على استخلاصه وتحليله.
5. **القابلية للنسخ دون فقدان المحتوى:** إذ يمكن استنساخ الدليل الرقمي مرات متعددة مع الاحتفاظ بالمحتوى ذاته، وهو ما يثير إشكالات قانونية تتعلق بحجية النسخ الإلكترونية ومدى مطابقتها للأصل.

وتتجلى هذه الخصائص بصورة واضحة عند وقوع جريمة اختراق إلكتروني؛ فالجاني قد لا يترك أي أثر مادي ظاهر، إلا أن النظام يحتفظ تلقائيًا ببيانات تتعلق بوقت الدخول، وعنوان الجهاز المستخدم، ونوع العمليات المنفذة، وهي بيانات تشكل أساسًا للاستدلال والإثبات.

[2]

- **ثالثًا: حجية الدليل الرقمي في الإثبات الجنائي:**

أصبحت الأدلة الرقمية تحتل مكانة متزايدة في الإثبات الجنائي المعاصر، لاسيما في الجرائم المعلوماتية التي يصعب إثباتها بالوسائل التقليدية. غير أن حجية الدليل الرقمي لا تقوم بمجرد وجود البيانات أو السجلات الإلكترونية، وإنما ترتبط بمدى سلامة الإجراءات التي تم اتباعها في جمع الدليل واستخراجه وحفظه وتحليله.

فالقيمة القانونية للدليل الرقمي تتوقف على توافر عدد من الضمانات الأساسية، من أهمها سلامة عملية الاستخراج، والمحافظة على الدليل من أي تعديل أو عبث، وتوثيق إجراءات الضبط والفحص الفني، وإمكانية التحقق من مصدر البيانات وصحتها. كما تزداد قوة الدليل كلما أمكن إخضاعه للفحص الفني بواسطة خبراء مختصين، وإثبات سلامة السلسلة الإجرائية التي مر بها منذ ضبطه وحتى تقديمه أمام القضاء.

ويختلف الدليل الرقمي عن الدليل التقليدي في أن حجيته تعتمد بدرجة كبيرة على الوسائل التقنية المستخدمة في التحقق من صحته، مثل السجلات الإلكترونية، والبيانات الوصفية (Metadata)، وملفات الأحداث (Logs)، وآليات التحقق الرقمي التي تضمن عدم تغيير محتواه بعد استخراجه.

- **رابعًا: التحديات القانونية والفنية المرتبطة بالأدلة الرقمية:**

يثير الدليل الرقمي مجموعة من الإشكالات القانونية والفنية التي تجعل التعامل معه أكثر تعقيدًا من الأدلة التقليدية. فمن الناحية الفنية، يتميز بسهولة المحو أو التعديل أو التشفير، الأمر الذي قد يؤدي إلى ضياعه أو التأثير في قيمته الإثباتية إذا لم يتم التعامل معه وفق إجراءات علمية دقيقة.

أما من الناحية القانونية، فتبرز إشكالات تتعلق بمدى مشروعية الحصول على الدليل الرقمي، وضمان احترام الخصوصية والحقوق الأساسية للأفراد، بالإضافة إلى الصعوبات المرتبطة بإثبات نسبة الدليل إلى شخص معين في ظل إمكانية استخدام الهويات الرقمية المستعارة أو وسائل إخفاء الهوية.

كما تزداد هذه التحديات تعقيدًا بسبب الطبيعة العابرة للحدود للجرائم المعلوماتية، إذ قد يوجد الجاني في دولة، وتكون البيانات مخزنة في دولة ثانية، بينما تتحقق النتيجة الإجرامية في دولة ثالثة، الأمر الذي يثير إشكالات الاختصاص القضائي وتنازع القوانين والتعاون الدولي في مجال جمع الأدلة الرقمية ونقلها.

ونخلص إلى القول، بإن الدليل الجنائي الرقمي لا يمثل مجرد وسيلة حديثة للإثبات، بل يعكس تحولًا جوهريًا في مفهوم الدليل الجنائي ذاته؛ حيث انتقل الإثبات من الاعتماد على الآثار المادية المحسوسة إلى الاعتماد على الآثار الرقمية الناتجة عن التفاعل التقني داخل الأنظمة المعلوماتية، ومن ثم فإن فعالية مكافحة الجرائم الإلكترونية تقتضي تطوير قواعد الإثبات الجنائي، وتعزيز دور الخبرة الفنية المتخصصة، ووضع ضمانات قانونية وتقنية تكفل المحافظة على سلامة الدليل الرقمي وحجيته أمام القضاء.

- **ملخص: الدليل الإلكتروني:**
- **تعريف الدليل الرقمي.**

في الجريمة المعلوماتية يُعد غياب الدليل المادي سمة جوهرية، وإنما هو مجرد نغمات الكترونية، ونظرًا لإمكانية محو الأدلة الرقمية بسهولة وسرعة، وهذا دفع المشرّع الليبي إلى تجريم إتلاف أو إخفاء الأدلة الإلكترونية، وتجريم أدوات الاختراق والتأثير غير المشروع على الأنظمة والبيانات.

ويعرف الدليل الإلكتروني على أه هو "كل أثر رقمي ناتج عن تفاعل الأنظمة والبرامج مع البيانات، يتم توليده أو تخزينه أو نقله داخل بيئة معلوماتية، ويكون قابلاً للاستخلاص والتحليل الفني بما يسمح باستخدامه في الإثبات الجنائي".

والدليل الرقمي وفق مفهوم القانون الليبي، هو:"كل بيانات أو معلومات ذات قيمة إثباتية يتم إنشاؤها أو تخزينها أو نقلها عبر نظام معلوماتي"، وعلى ذلك يتميز هذا الدليل بـ:

أ. الهشاشة وسهولة المحو.
ب. القابلية للتعديل دون أثر ظاهر.
ت. الحاجة لوسائل فنية لاستخراجه.

وللتوضيح العميق، وهو جوهر الإضافة. فالدليل الإلكتروني ليس شيئًا ثابتًا بذاته مثل السكين أو البصمة، بل هو نتيجة تفاعل (Interaction) بين:

1. **المستخدم** (الجاني)
2. **البرنامج** (Software)
3. **النظام** (System)
4. **البيانات** (Data)

- **بمعنى أدق:** عندما يقوم الجاني بـ:
  1. تسجيل الدخول
  2. إرسال رسالة
  3. تعديل ملف
- **فإن النظام يقوم تلقائيًا** بـ:
  1. تسجيل العملية (Log)
  2. حفظ الوقت والتاريخ
  3. تحديد عنوان الجهاز (IP)
  4. تخزين الأثر في قاعدة بيانات

وهذه النتائج هي التي يقصد تحديدا "الدليل الإلكتروني".

- **مثال توضيحي:** عند اختراق بريد إلكتروني: الجاني لا يترك أثرًا ماديًا،
- **لكن النظام يسجل :**
  1. وقت الدخول،
  2. الجهاز المستخدم،
  3. العمليات المنفذة.

وهذه السجلات ليست "أشياء"، بل ناتج معالجة برمجية.

- **خصائص الدليل الإلكتروني** (مع تفسير):

1. **غير مادي:** ← لا يُدرك بالحواس، بل عبر برامج تحليل.
2. **ديناميكي** (متغير): ← يمكن تعديله أو محوه بسهولة.
3. **ناتج عن معالجة آلية:** ← لا يُنشأ يدويًا دائمًا، بل عبر النظام تلقائيًا.
4. **يعتمد على الوسيط التقني:** ← لا قيمة له دون جهاز أو برنامج يقرأه.

ويمكن استخلاص الفروق الجوهرية على النحو التالي:

1. **من حيث الطبيعة:**

أ. **الدليل التقليدي** = أثر مادي.

ب. **الدليل الإلكتروني** = ناتج تفاعل برمجي.

وهذا هو **الفارق الجوهري:** وهو أن **الدليل الإلكتروني** ليس "**شيئًا**"، بل "**نتيجة عملية تقنية**".

2. **من حيث الإثبات:**

أ. **الدليل التقليدي** يعتمد على الإدراك الحسي.

ب. **الدليل الإلكتروني** يعتمد على التحليل الفني.

مما يفرض إدخال الخبرة التقنية كعنصر أساسي في الإثبات.

3. **من حيث الخطورة:**

أ. **الدليل التقليدي** يصعب إخفاؤه،

ب. **الدليل الإلكتروني** يمكن :

1. محوه
2. تعديله
3. تشفيره

مما يجعله – الدليل الالكتروني– أكثر هشاشة وأكثر تعقيدًا.

4. **من حيث الامتداد:**

أ. **الدليل التقليدي** محلي،

ب. **الدليل الإلكتروني** عابر للحدود، وهذا **يخلق إشكال:**

1. الاختصاص القضائي، أي قضاء يكون مختصا.
2. تنازع القوانين، أي قانون يطبق.

5. **من حيث الحجية:**

أ. **الدليل التقليدي:** حجية مستقرة.

ب. **الدليل الإلكتروني:** حجية مشروطة بـ :

1. سلامة الاستخراج،
2. عدم التلاعب،
3. توثيق الإجراءات.

ونخلص بأن الدليل الإلكتروني لا يمثل مجرد تطور في وسائل الإثبات، بل يُحدث تحولًا بنيويًا في مفهوم الدليل الجنائي، حيث:

1. يتحول الدليل من أثر مادي إلى أثر رقمي تحليلي،

2. ويتحول الإثبات من معاينة حسية إلى تحليل تقني متخصص،
3. وتنتقل الجريمة من الواقع المادي إلى الفضاء الرقمي.

- **وهو ما يستوجب:**

1. تطوير قواعد الإثبات الجنائي،
2. إدماج الخبرة التقنية،
3. وضع ضمانات لحماية الدليل الرقمي.

- **مقارنة بين الدليل الإلكتروني والدليل التقليدي** (تحليل جدولي):

معيار المقارنة	الدليل التقليدي	الدليل الإلكتروني	التحليل القانوني
التعريف	كل أثر مادي محسوس ناتج عن الجريمة يمكن إدراكه بالحواس	كل أثر رقمي ناتج عن تفاعل الأنظمة والبرامج مع البيانات داخل بيئة معلوماتية	الاختلاف الجوهري أن التقليدي مادي، بينما الإلكتروني ناتج عن معالجة تقنية
الطبيعة	مادي ملموس (سلاح، بصمة، مستند)	غير مادي (بيانات، سجلات، ملفات رقمية)	يفرض الدليل الإلكتروني أدوات إثبات فنية وليس حسية
طريقة النشأة	نتيجة مباشرة لفعل مادي	نتيجة تفاعل (User + System + Software + Data)	الدليل الإلكتروني "مُنشأ آليًا" غالبًا وليس بفعل بشري مباشر
إمكانية الإدراك	يُدرك بالحواس مباشرة	لا يُدرك إلا عبر أجهزة وبرمجيات	يحتاج خبرة تقنية لفهمه وتحليله
الثبات	ثابت نسبيًا	متغير (ديناميكي) وقابل للتعديل	يثير إشكالية سلامة الدليل
قابلية المحو	صعبة نسبيًا	سهلة وسريعة جدًا	خطر فقدان الدليل أعلى في البيئة الرقمية
القوة الإثباتية	مستقرة تقليديًا في القضاء	محل تقدير فني وقضائي	تعتمد على سلامة الاستخراج والتحليل
وسيلة الحصول عليه	تفتيش مادي، معاينة	فحص تقني، تحليل رقمي، استخلاص بيانات	يتطلب إجراءات خاصة وخبراء
الوسيط الحامل	أشياء مادية (ورق، أدوات)	وسائط رقمية (أقراص، خوادم، سحابة)	الوسيط قد يكون بعيدًا عن مكان الجريمة

الزمن	مرتبط بزمن وقوع الجريمة	يسجل الزمن بدقة (Logs – timestamps)	الدليل الإلكتروني أدق زمنياً
نطاق الانتشار	محدود جغرافيًا	عابر للحدود	يعقد مسألة الاختصاص القضائي
إمكانية التكرار	لا يمكن نسخه بسهولة	يمكن نسخه بلا حدود دون فقد الجودة	يثير مسألة حجية النسخ
التحقق من الصحة	عبر الفحص المادي والشهود	عبر تقنيات (Hash – Logs – Metadata)	يعتمد على أدوات تقنية متخصصة
درجة الخفاء	ظاهر غالبًا	خفي وغير مرئي	يتطلب خبرة لاكتشافه
التلاعب	صعب نسبيًا	ممكن بمهارة تقنية	يستوجب ضمانات تقنية وقانونية
الاعتماد القضائي	تقليدي ومستقر	حديث ومتطور	يتطلب تكيفًا تشريعيًا وقضائيًا

يتضح مما تقدم أن البيانات المعلوماتية والدليل الجنائي الرقمي يمثلان ركيزتين أساسيتين في البناء القانوني للجريمة المعلوماتية؛ فالبيانات المعلوماتية تُعد محلًا رئيسًا للاعتداء ومناطًا للحماية الجنائية، بينما يشكل الدليل الجنائي الرقمي الأداة الرئيسة لإثبات الأفعال الإجرامية المرتكبة داخل البيئة الإلكترونية.

ويكشف ذلك عن التحول الذي أحدثته التكنولوجيا في المفاهيم الجنائية التقليدية، حيث انتقل محل الحماية من الأشياء المادية إلى الكيانات الرقمية، كما انتقلت وسائل الإثبات من الأدلة المادية المحسوسة إلى الآثار الرقمية المستخرجة بواسطة الوسائل الفنية المتخصصة. ومن ثم أصبح تحقيق الفعالية في مكافحة الجرائم المعلوماتية مرهونًا بمدى قدرة التشريعات الجنائية على استيعاب الطبيعة الخاصة للبيانات الرقمية، وبمدى كفاءة آليات جمع الأدلة الإلكترونية والمحافظة على حجيتها أمام جهات التحقيق والقضاء.

- **المبحث الثاني: الخصوصية الشخصية للمجرم المعلوماتي.**

أفرز التطور التقني المتسارع نمطًا جديدًا من الإجرام اتسم بخصائص مغايرة لما استقر عليه الفكر الجنائي التقليدي، فلم تعد الجريمة ترتبط بالضرورة بمسرح مادي ملموس أو بوسائل تقليدية، بل

أصبحت البيئة المعلوماتية مجالًا خصبًا لارتكاب أفعال إجرامية تستهدف البيانات والأنظمة والشبكات الإلكترونية. وقد ترتب على ذلك ظهور فئة خاصة من الجناة يتميزون بقدرات تقنية ومعارف متخصصة تمكنهم من استغلال الثغرات الرقمية، بما يثير تساؤلات جوهرية حول مدى كفاية القواعد الجنائية التقليدية في مواجهتهم.

وتتجلى خصوصية الجريمة المعلوماتية ليس فقط في طبيعة محل الاعتداء ووسائل ارتكابه، وإنما كذلك في شخصية مرتكبها وطبيعة مسؤوليته الجنائية؛ إذ يختلف المجرم المعلوماتي عن المجرم التقليدي من حيث أسلوب التنفيذ، والقدرة على التخفي، وصعوبة تحديد هويته وإثبات صلته بالفعل الإجرامي، الأمر الذي يفرض إعادة النظر في الآليات الموضوعية والإجرائية التي تحكم مساءلته.

وعليه، يقتضي بحث هذه الخصوصية الوقوف على السمات المميزة للمجرم المعلوماتي من جهة، وبيان الأساس القانوني للمسؤولية الجنائية الناشئة عن الجرائم المعلوماتية من جهة أخرى، وذلك من خلال تناول خصوصية المجرم المعلوماتي في **(المطلب الأول)**، ثم بحث المسؤولية الجنائية عن الجريمة المعلوماتية في **(المطلب الثاني)**.

- **المطلب الأول: خصوصية المجرم المعلوماتي.**

تُعدّ شخصية المجرم المعلوماتي من أكثر الشخصيات الإجرامية تميزًا في الفقه الجنائي المعاصر، إذ تختلف اختلافًا جوهريًا عن المجرم التقليدي، سواء من حيث التكوين النفسي أو الأسلوب الإجرامي أو الوسيلة المستخدمة. فالجريمة لم تعد فعلًا ماديًا يُرتكب في الواقع المحسوس، بل أصبحت نشاطًا ذهنيًا وتقنيًا يُنفذ داخل بيئة رقمية غير مرئية.

كما أن شخصية مرتكب الجريمة المعلوماتية – المجرم المعلوماتي– تتصف بالغموض، وهو ما أضفى عليه بعض الخصوصية حيث جعلت منه مجرما من نوع خاص يتميز عن غيره من المجرمين العاديين سواء كفاعل أصلي (أولا) أو كشريك (ثانيا).

- **أولًا: المجرم المعلوماتي كفاعل أصلي.**

أدى التطور المتسارع في مجال تكنولوجيا المعلومات والاتصالات إلى ظهور نمط جديد من الجناة يختلف في خصائصه وطريقة ارتكابه للفعل الإجرامي عن الصورة التقليدية للمجرم، إذ لم يعد ارتكاب الجريمة مرتبطًا بالوجود المادي في مسرح الجريمة أو باستخدام الوسائل التقليدية، وإنما أصبح الفضاء

السيبراني مجالًا لارتكاب أفعال غير مشروعة تعتمد على المعرفة التقنية والقدرة على التعامل مع الأنظمة والبيانات الرقمية.

ويقصد بالمجرم المعلوماتي بوجه عام هو:"الشخص الذي يمتلك قدرًا من المعرفة والمهارة التقنية، ويستخدم الوسائط والأنظمة المعلوماتية لارتكاب سلوك مجرّم قانونًا، دون حاجة إلى تدخل مادي مباشر أو وجود فعلي في مكان وقوع الضرر. فهو جاني يعتمد على الفكر والمعرفة التقنية أكثر من اعتماده على القوة المادية، ويستبدل الوسائل التقليدية بأدوات رقمية كالبرمجيات والشبكات وقواعد البيانات.

وتتميز شخصية الفاعل الأصلي في الجريمة المعلوماتية بخصوصية واضحة؛ فهو غالبًا شخص يمتلك قدرات فنية متقدمة في مجالات البرمجة أو أمن المعلومات أو إدارة الأنظمة الإلكترونية، تمكنه من استغلال نقاط الضعف التقنية لتحقيق أغراض غير مشروعة. فقد يقوم باختراق نظام معلوماتي، أو الاستيلاء على بيانات، أو تغيير محتوى رقمي، أو تعطيل خدمة إلكترونية، دون أن يترك أثرًا ماديًا ظاهرًا كما هو الحال في الجرائم التقليدية.

ولا تقتصر المسؤولية الجنائية في البيئة الرقمية على الفاعل المادي الذي ينفذ السلوك الإجرامي مباشرة، بل قد تمتد إلى أشخاص آخرين يرتبط دورهم بالمنظومة التقنية التي مكنت من وقوع الجريمة، ومن بينهم مقدمو الخدمات المعلوماتية، متى توافرت شروط المسؤولية التي يحددها القانون، ويُقصد بمقدم الخدمة كل شخص طبيعي أو معنوي يساهم في إتاحة أو تشغيل خدمات الاتصالات ذات القيمة المضافة أو توفير البنية التقنية اللازمة لاستخدام الشبكات.

وتبرز أهمية تحديد مسؤولية مقدمي الخدمات بالنظر إلى الدور المحوري الذي يؤدونه في البيئة الرقمية، باعتبارهم القائمين على إدارة أو استضافة أو تمكين المستخدمين من الوصول إلى المحتوى الإلكتروني. فقد تستغل هذه الخدمات كوسيلة لارتكاب الجرائم المعلوماتية، الأمر الذي يفرض تحقيق التوازن بين ضرورة ضمان حرية استخدام التكنولوجيا من جهة، وفرض التزامات قانونية تضمن عدم تحول البيئة الرقمية إلى مجال للإفلات من المسؤولية من جهة أخرى.

وفي هذا الإطار، قد يتحمل مقدم الخدمة مسؤولية قانونية متى ثبت إخلاله بالواجبات المفروضة عليه، خاصة فيما يتعلق بالرقابة على المحتوى أو اتخاذ التدابير اللازمة لمنع استغلال الخدمة في ارتكاب أفعال غير مشروعة، وذلك وفقًا للقواعد التي تنظم مسؤولية الناشر أو المسؤول عن المحتوى في التشريعات ذات الصلة.

ومن الناحية السلوكية، يتميز المجرم المعلوماتي بعدة خصائص تميزه عن المجرم التقليدي، أهمها الاعتماد على الذكاء والمهارة التقنية، وعدم اللجوء غالبًا إلى العنف المادي، والقدرة على التخفي خلف الوسائط الإلكترونية. كما أنه قد يكون شخصًا مندمجًا اجتماعيًا يبدو في ظاهره شخصًا عاديًا، كطالب أو موظف أو متخصص تقني، وهو ما يزيد من صعوبة اكتشافه وتعقب نشاطه الإجرامي.

كما يتسم المجرم المعلوماتي بالتخصص؛ إذ قد يركز نشاطه على نمط محدد من الجرائم، كاختراق الأنظمة، أو الاستيلاء على البيانات، أو الاحتيال الإلكتروني، أو الاعتداء على الأنظمة المالية. وقد يتكرر نشاطه الإجرامي بهدف تطوير قدراته التقنية وتجنب وسائل الكشف، مما يجعل الخبرة السابقة عنصرًا مساعدًا في ارتكاب جرائم أكثر تعقيدًا.

وتتعدد صور المجرمين المعلوماتيين بحسب طبيعة الدور والدافع، فمنهم من يرتكب الفعل بدافع الفضول أو التحدي التقني، ومنهم من يستغل صلاحياته الوظيفية للوصول غير المشروع إلى المعلومات، ومنهم من يستخدم المعرفة التقنية لتحقيق مكاسب مالية أو تنفيذ أنشطة منظمة، كما قد تظهر صور أكثر خطورة كالجريمة المعلوماتية المنظمة أو التجسس الإلكتروني أو الإرهاب المعلوماتي.

وترتبط هذه الأنماط المختلفة بدوافع متعددة، أبرزها تحقيق الربح المالي، أو الانتقام، أو الرغبة في إثبات القدرة التقنية، أو الشعور بالتفوق على الأنظمة الأمنية، أو خدمة أهداف سياسية أو أيديولوجية. وقد يكون من أسباب السلوك الإجرامي كذلك ضعف الإدراك بخطورة الفعل أو الاعتقاد الخاطئ بأن النشاط الرقمي لا يشكل جريمة طالما لم ينتج عنه ضرر مادي مباشر.

ومن ثم، فإن خصوصية المجرم المعلوماتي لا تنبع فقط من الوسيلة التي يستخدمها، وإنما من طبيعة شخصيته الإجرامية ودوره في البيئة الرقمية؛ فهو جاني يمتلك أدوات غير مادية، ويرتكب فعلًا قد يكون غير مرئي، ويترك آثارًا رقمية تحتاج إلى وسائل إثبات متخصصة. الأمر الذي يفرض تطوير السياسة الجنائية لتستوعب هذه التحولات، وهو ما اتجه إليه المشرّع الليبي من خلال القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، بهدف توسيع نطاق الحماية الجنائية ومواجهة صور الإجرام المستحدثة بما يحقق حماية المجتمع ومواكبة التطور التقني.

- **ملخص:**

المجرم المعلوماتي كفاعل أصلي:

- تعريف تفسيري: يمكن تعريف المجرم المعلوماتي بأنه:"شخص يمتلك معرفة تقنية متقدمة، يستخدمها عبر الوسائط الرقمية لارتكاب سلوك غير مشروع، دون حاجة إلى تدخل مادي مباشر في مسرح الجريمة".
- **توضيح مبسّط:**
- **أ): هو مجرم:**
    1. يفكر أكثر مما يتحرك،
    2. يستخدم لوحة المفاتيح بدل السلاح،
    3. يعتمد على المعرفة بدل القوة.
- **مـثال:** شخص يخترق نظام مصرفي من منزله ويحوّل أموالًا إلى حسابه دون أن يلتقي بأي موظف أو يدخل البنك فعليًا.
- **ب): السمات المميزة للمجرم المعلوماتي:**
    1. الاعتماد على الذكاء والمهارة التقنية،
    2. لا يستخدم العنف،
    3. بل يوظف قدراته في البرمجة واختراق الأنظمة.
- **مثال:** اختراق نظام شركة عبر ثغرة برمجية دون إحداث أي كسر مادي.
- **ج): الاندماج الاجتماعي:**
    1. غالبًا ما يبدو شخصًا عاديًا،
    2. وقد يكون طالبًا،
    3. أو موظفًا محترمًا.

وهذا **ما يجعل اكتشافه** – المجرم المعلوماتي– أكثر **صعوبة مقارنة** بالمجرم التقليدي.

- **د): التخصص الدقيق:** يركز نشاطه الإجرامي في مجال محدد (اختراق – تزوير رقمي – سرقة بيانات).
    - **مثال:** شخص متخصص فقط في سرقة الحسابات البنكية.
- هـ): **العود الإجرامي** (التكرار): **يعود لارتكاب الجريمة** بهدف تحسين مهاراته وتفادي الكشف، أي أن الفشل السابق يتحول إلى خبرة لاحقة.
- **و): أنماط المجرمين المعلوماتيين** (بتفسير مبسّط):

1. **الهواة** (Hackers) تعريفهم هم أشخاص يخترقون الأنظمة بدافع الفضول أو التحدي.

مثال: طالب يخترق موقع مدرسة لإثبات قدرته التقنية.

2. **النخبة التقنية**(Insiders) تعريفهم هم أفراد لديهم صلاحيات مشروعة داخل المؤسسات يستغلونها بشكل غير مشروع.

مثال: موظف بنك ينسخ بيانات العملاء ويبيعها.

3. **الكراكرز** (Crackers) تعريفهم هم مجرمون يستخدمون وسائل تخريبية لتحقيق مكاسب غير مشروعة.

مثال: زرع فيروس لتعطيل نظام شركة وابتزازها.

4. **الجريمة المنظمة المعلوماتية**

- تعريف :جماعات تستخدم التقنية لتنفيذ جرائم مالية أو احتيالية بشكل منظم.

مثال: شبكة دولية لسرقة بطاقات الائتمان.

5. **الجواسيس المعلوماتيون**

تعريف :أشخاص يستهدفون سرقة معلومات سرية لأغراض سياسية أو اقتصادية.

مثال: اختراق شركة للحصول على أسرار صناعية.

6. **الإرهاب المعلوماتي**

تعريف :استخدام الفضاء الرقمي لنشر الرعب أو التخريب أو الدعاية المتطرفة.

مثال: تعطيل مواقع حكومية أو نشر محتوى تحريضي.

- **ز): الدوافع الإجرامية** (بتفسير سلوكي):
- **تعريف:** هي "العوامل النفسية أو المادية التي تدفع الجاني إلى ارتكاب الجريمة في البيئة الرقمية".
- **أهم هذه الدوافع:**

1. **الربح المالي:** مثل سرقة الحسابات البنكية .
2. **الانتقام الوظيفي:** مثل موظف مفصول يخترق نظام شركته السابقة .
3. **التحدي التقني:** الرغبة في إثبات القدرة على الاختراق .
4. **الشعور بالنخبوية:** اعتقاد الجاني أنه أذكى من النظام والقانون .
5. **التجسس أو الإرهاب:** لخدمة أهداف سياسية أو أيديولوجية .

6. **ضعف الوعي بعدم المشروعية:** البعض لا يرى الاختراق جريمة إذا لم يسبب ضررًا مباشرًا .
7. **شيوع السلوك داخل المؤسسات:** استخدام غير مشروع للأنظمة يصبح سلوكًا عاديًا.

- **ثانيًا: المجرم المعلوماتي كشريك في الجريمة:**

لا تقتصر المساهمة في ارتكاب الجريمة المعلوماتية على الشخص الذي يقوم بالتنفيذ المباشر للفعل الإجرامي، وإنما قد تمتد لتشمل كل من يقدم دعمًا أو عونًا أو مساهمة يكون لها أثر فعّال في تحقيق النتيجة الإجرامية، وهو ما يثير مسألة تحديد نطاق المسؤولية الجنائية للشريك في البيئة الرقمية.

فوفقًا للقواعد العامة في قانون العقوبات، يُعد شريكًا في الجريمة كل من ساهم في ارتكابها عن طريق التحريض أو الاتفاق أو المساعدة متى توافرت علاقة سببية بين نشاطه والنتيجة الإجرامية المتحققة. وقد استند المشرّع الليبي إلى هذا الأصل العام في تنظيم أحكام الاشتراك، حيث تقرر المسؤولية الجنائية للشريك متى ثبت أن تدخله كان عنصرًا مؤثرًا في وقوع الجريمة.

غير أن تطبيق هذه القواعد في المجال المعلوماتي يكتسب خصوصية متميزة؛ إذ لم تعد المساهمة الإجرامية بالضرورة ذات طبيعة مادية محسوسة، بل أصبحت تأخذ صورة مساهمة رقمية أو تقنية، تتمثل في تقديم الوسائل أو البيانات أو الخبرات التي تمكّن الفاعل الأصلي من تنفيذ الجريمة، ومن ثم يُقصد بالشريك المعلوماتي كل شخص يقدم دعمًا تقنيًا أو معلوماتيًا يسهم في ارتكاب الجريمة الإلكترونية، دون أن يكون هو المنفذ المباشر للسلوك الإجرامي.

وتظهر صور هذه المساهمة في البيئة الرقمية من خلال العديد من الأفعال، كإرسال أدوات أو برامج مخصصة للاختراق، أو تزويد الجاني بكلمات مرور أو بيانات دخول، أو إرشاده إلى الوسائل الفنية اللازمة لتنفيذ الاعتداء، أو توفير خوادم أو بنية تقنية تُستخدم كوسيلة لارتكاب الفعل الإجرامي. فالشخص الذي لا يقوم باختراق النظام بنفسه، وإنما يزوّد غيره بأداة الاختراق مع علمه بالغرض الإجرامي منها، قد تتوافر في حقه صفة الشريك متى ثبت ارتباط فعله بالجريمة.

ويتمثل المعيار الأساسي لقيام مسؤولية الشريك في المجال المعلوماتي في وجود إسهام تقني فعّال يرتبط سببيًا بالفعل الإجرامي؛ إذ لا يكفي مجرد المعرفة أو التواجد العرضي، وإنما يجب أن يكون النشاط المقدم قد ساعد بصورة مؤثرة في وقوع الجريمة أو تسهيل ارتكابها.

وقد أكد المشرّع الليبي امتداد القواعد العامة للاشتراك إلى نطاق الجرائم المعلوماتية، وذلك من خلال تطبيق أحكام المادة (100) من قانون العقوبات الليبي، إلى جانب ما قرره القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، حيث أكد في المادة (49) سريان الأحكام العامة للمسؤولية الجنائية على الجرائم الواردة فيه.

وتتجلى خصوصية الشريك في الجريمة المعلوماتية في عدة مظاهر، أهمها أن المساهمة الإجرامية أصبحت ذات طابع غير مادي، فقد تكون محلها برامج أو بيانات أو رموز دخول، كما قد تتم عن بُعد من خلال وسائل الاتصال الحديثة، سواء في صورة تحريض إلكتروني أو اتفاق يتم عبر الشبكات الرقمية. كذلك قد تتحول بعض الأفعال التقنية ذاتها إلى صور من السلوك المجرّم، كحيازة أدوات الاختراق أو اعتراض البيانات أو الدخول غير المشروع إلى الأنظمة المعلوماتية.

كما تتميز الجرائم المعلوماتية غالبًا بالطابع الجماعي والتنظيمي، حيث قد تتوزع الأدوار بين عدة أشخاص؛ فيتولى أحدهم تطوير الأدوات التقنية، ويقوم آخر بالتنفيذ، بينما يساهم غيرهما بالتمويل أو الاستفادة من العائد الإجرامي، الأمر الذي يجعل تحديد المسؤوليات الجنائية أكثر تعقيدًا، سواء من ناحية إثبات الأفعال أو تحديد درجة مساهمة كل متدخل في المشروع الإجرامي.

ومن ثم، فإن خصوصية الجريمة المعلوماتية لا تكمن فقط في اختلاف الوسيلة المستخدمة، وإنما تمتد إلى طبيعة البناء الإجرامي ذاته؛ فالفعل الإجرامي قد يكون عملية تقنية غير ملموسة، والدليل الجنائي يتمثل في أثر رقمي كالسجلات والبيانات الإلكترونية، والجاني غالبًا ما يكون شخصًا ذا معرفة تقنية متخصصة، كما أن نطاق النشاط الإجرامي قد يتجاوز الحدود الإقليمية للدول.

وعليه، فإن فهم المسؤولية الجنائية في المجال المعلوماتي لا يمكن أن يقوم على التحليل القانوني المجرد وحده، بل يتطلب تكاملًا بين المعرفة القانونية والفهم التقني لطبيعة البيئة الرقمية، بما يحقق قدرة فعالة على مواجهة هذا النمط الحديث من الإجرام، وهو ما يعكس توجه المشرّع الليبي نحو تبني سياسة جنائية أكثر مرونة من خلال القانون رقم (5 لسنة 2022م)، تقوم على توسيع نطاق التجريم واستيعاب الوسائل التقنية الحديثة وتحقيق التوازن بين حماية المجتمع وضمان مواكبة التطور التكنولوجي.

- **ملخص:**

في المجرم المعلوماتي كشريك في الجريمة.

يمكن تعريف الشريك كتأصيل قانوني وفقًا للقواعد العامة:"هو كل من ساهم في ارتكاب الجريمة بطريق التحريض أو الاتفاق أو المساعدة مع قيام علاقة سببية". أما التعريف في البيئة المعلوماتية، فهو "كل من يقدم دعمًا تقنيًا أو معلوماتيًا يُسهم في وقوع الجريمة المعلوماتية دون أن يكون منفذًا مباشرًا لها".

- **التوضيح التقني:** المساهمة **لا تكون مادية، بل رقمية،** مثل:
  1. إرسال برنامج اختراق،
  2. تزويد بكلمة مرور،
  3. شرح طريقة تنفيذ الجريمة،
  4. توفير خوادم أو أدوات تقنية.
- **مثال:** شخص لا يخترق بنفسه، لكنه يرسل أداة اختراق لصديقه الذي ينفذ الجريمة.
- **أساس المسؤولية الجنائية:**

1. تقوم على المادة (100) من قانون العقوبات الليبي
2. وأكدها القانون رقم (5 لسنة 2022م) بسريانها على الجرائم المعلوماتية في المادة (49).

- **المعيار الحاسم:** للقول بالشريك في المجال الالكتروني، يتمثل في وجود إسهام تقني فعّال مرتبط سببيًا بالجريمة.
- **مظاهر خصوصية الشريك في البيئة الرقمية:** وتتمثل في الآتي:

1. **الطابع غير المادي للمساهمة،** وتتمثل في (برمجيات – بيانات – كلمات مرور).
2. **تنوع صور الاشتراك عن بُعد،** (تحريض إلكتروني – اتفاق عبر الإنترنت).
3. **تجريم أفعال تقنية بذاتها:** من مثل: حيازة أدوات الاختراق، أو اعتراض البيانات، أو الدخول غير المشروع، أو الطابع الجماعي والتنظيمي.
4. **توزيع الأدوار بين عدة أشخاص:** مبرمج، منفذ، ممول، مستفيد.

وهذ؛ يؤدي إلى صعوبة الإثبات، وصعوبة تحديد المسؤوليات، وذلك لكثرة المتدخلين في الفعل الاجرامي الرقمي. أي أن خصوصية الجريمة المعلوماتية لا تقتصر على اختلاف الوسيلة، بل تمتد إلى طبيعة الجريمة ذاتها:

1. الفعل الإجرامي =عملية تقنية،
2. الدليل الجنائي = أثر رقمي (بيانات – سجلات)،
3. الجاني = عقل تقني متخصص،

4. النطاق = عابر للحدود.

وبالتالي لا يمكن فهم الجريمة المعلوماتية بالتحليل القانوني وحده، بل يتطلب الأمر دمجًا حقيقيًا بين: التحليل القانوني، والفهم التقني، وفيما يتعلق بخصوصية الجريمة والمجرم. فهنا تُبرز الجريمة المعلوماتية تحولًا عميقًا في البناء التقليدي للجريمة، سواء من حيث:

1. **الركن المادي** (لامادي وغير مرئي)
2. **شخصية الجاني** (تقنية ومتخصصة)
3. **صور الاشتراك** (غير تقليدية)

وهذا ما يبرر توجه المشرّع الليبي، من خلال القانون رقم (5 لسنة 2022م)، إلى تبني مقاربة مرنة تقوم على توسيع نطاق التجريم، واستيعاب الوسائل التقنية، وضمان فعالية المواجهة الجنائية، وبما يحقق التوازن بين حماية المجتمع ومواكبة التطور التكنولوجي.

- **المطلب الثاني:**

المسؤولية الجنائية عن الجريمة المعلوماتية.

تُثير الجريمة المعلوماتية إشكاليات قانونية معقّدة على مستوى تحديد المسؤولية الجنائية، نظرًا لخصوصية الفضاء الرقمي الذي تتداخل فيه الأدوار وتتعدد فيه مراكز التأثير والسيطرة على الفعل الإجرامي. فلم يعد السلوك الإجرامي وليد فعل فردي بسيط، بل أصبح نتيجة تفاعل تقني تشاركي يشمل الفاعل المباشر، والمتدخلين في البنية التقنية، والجهات التي تتيح أو تدير أو تراقب تدفق المعلومات.

وفي هذا الإطار، تجاوز المشرّع الليبي المفهوم التقليدي للمسؤولية الجنائية، ليقرّ بنطاق أوسع يشمل إلى جانب الشخص الطبيعي، الشخص المعنوي، وكذلك مزودي خدمات الاتصالات وتقنية المعلومات، كلٌ بحسب دوره ومدى إسهامه في وقوع الجريمة. وقد تجسّد هذا التوجه في أحكام القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، مدعومًا بالقواعد العامة في قانون العقوبات، لاسيما المادة (64) المتعلقة بالمسؤولية عن النشر.

وعليه، فإن تحديد المسؤولية الجنائية في مجال الجرائم المعلوماتية يقتضي التمييز بين الفاعل الأصلي (أولا)، ومسؤولية الشخص المعنوي (ثانيا)، ودور مزودي الخدمات (ثالثا)، وهو ما سيتم بيانه تباعًا على النحو التالي:

- **أولًا: المجرم المعلوماتي كفاعل أصلي ومسؤولية المتدخلين في الفضاء المعلوماتي:**

يتميّز الفضاء المعلوماتي بطبيعة تقنية معقدة تفرز تعددًا في مراكز المسؤولية الجنائية، بحيث لم يعد الفاعل الأصلي وحده هو المسؤول عن الفعل الإجرامي، بل تتسع دائرة التجريم لتشمل مختلف المتدخلين في هذا الفضاء، سواء كانوا أشخاصًا طبيعيين أو معنويين.

فالأصل أن الفاعل الأصلي هو كل شخص طبيعي يرتكب السلوك الإجرامي المكوّن للجريمة الإلكترونية بنفسه، كالدخول غير المشروع إلى الأنظمة المعلوماتية أو التعدي على البيانات أو نشر محتوى غير مشروع، وفقًا للأفعال المجرّمة بموجب نصوص القانون رقم (5 لسنة 2022م). غير أن خصوصية البيئة الرقمية تجعل هذا الفعل غالبًا مرتبطًا ببنية تقنية تتيح لغيره التدخل أو التمكين أو التسهيل، وهم أشخاص غير الشريك، وهو ما يبرر مساءلة أطراف أخرى.

وفي هذا السياق، يبرز مؤدو خدمات الاتصالات وتقنية المعلومات بوصفهم فاعلين محتملين أو مساهمين في الجريمة، نظرًا للدور الجوهري الذي يضطلعون به في تمكين المستخدمين من الوصول إلى الشبكة أو تخزين المحتوى أو تداوله، ويُقصد بهم كل شخص معنوي، عامًا كان أو خاصًا، مرخص له بتقديم خدمات الاتصالات أو الخدمات ذات القيمة المضافة المرتبطة بها.

ورغم أن التشريع الليبي لم يضع تصنيفًا دقيقًا لهؤلاء من حيث وظائفهم "كمزودي دخول أو مزودي إيواء أو منصات نشر"، إلا أن مسؤوليتهم الجنائية تقوم متى توافر أحد صور الإسهام الجنائي، خاصة إذا كان نشاطهم يتيح أو يسهل ارتكاب الجريمة أو الامتناع عن منعها رغم القدرة على ذلك.

- **ثانيًا: مسؤولية الشخص المعنوي في ضوء القانون رقم (5 لسنة 2022م):**

كرّس المشرّع الليبي صراحة مسؤولية الشخص المعنوي عن الجرائم الإلكترونية، حيث نصت المادة (48) من القانون رقم (5 لسنة 2022م) على مساءلة المسؤول عن الإدارة الفعلية للشخص المعنوي إذا ارتكبت الجريمة باسم هذا الشخص ولصالحه، وكان ذلك نتيجة إخلاله بواجبات الإشراف أو الرقابة.

- **ويُستفاد من هذا النص أن:**

1. المسؤولية لا تقوم على الشخص **المعنوي** في **ذاته** بشكل **مجرد**، بل تمتد إلى الشخص الطبيعي الذي يتولى إدارته الفعلية.
2. يشترط لقيام المسؤولية أن تُرتكب الجريمة باسم الشخص المعنوي ولصالحه.
3. تقوم المسؤولية على أساس الخطأ المفترض في الإشراف أو الرقابة.

4. يجوز للمحكمة أن تقضي بحل الشخص المعنوي إذا ثبت أن إنشائه كان غطاءً لارتكاب الجرائم الإلكترونية.

وبذلك، يتجه المشرّع إلى إقرار نوع من المسؤولية الجنائية غير المباشرة التي تستند إلى فكرة الرقابة والالتزام القانوني بمنع الانحراف في استخدام الوسائل التقنية.

- **ثالثًا: مسؤولية مزودي الخدمات في ضوء المادة (64- ق.ع.ل):**

بالنظر إلى غياب تنظيم تفصيلي دقيق لمسؤولية مزودي الخدمات من حيث محتوى النشر الإلكتروني، يمكن الرجوع إلى القواعد العامة، وعلى رأسها المادة (64) من قانون العقوبات الليبي، التي نظمت المسؤولية عن الجرائم المرتكبة بواسطة وسائل النشر.

وتأسيسًا على القياس الوظيفي بين النشر التقليدي والنشر الإلكتروني، فإن:

1. مدير الخدمة أو المسؤول عن المحتوى يعد في مركز قانوني مماثل لمدير التحرير في الصحافة.
2. تقوم مسؤوليته الجنائية إذا لم يتخذ التدابير اللازمة لمنع نشر محتوى غير مشروع، متى كان ذلك ممكنًا ولم توجد قوة قاهرة أو سبب أجنبي يمنع التدخل.
3. تمتد المسؤولية تدريجيًا بحسب ترتيب الأشخاص (المؤلف – الناشر – الطابع) وفقًا للحالات التي يكون فيها الفاعل الأصلي مجهولًا أو غير قابل للمساءلة.

وبتطبيق ذلك على البيئة الرقمية، فإن مزود الخدمة – سواء كان مزود دخول أو إيواء– يُسأل جنائيًا إذا:

1. علم بالمحتوى غير المشروع ولم يتخذ إجراءً لإزالته أو منعه.
2. أو أخلّ بواجب الرقابة المفروضة عليه بحكم نشاطه.

- **رابعًا: خلاصة تحديد المسؤولية:**

يتضح مما تقدم أن تحديد المسؤولية في الجرائم الإلكترونية يقوم على أساس تعدد الفاعلين، وذلك وفقًا لما يلي:

1. **الشخص الطبيعي:** يسأل كفاعل أصلي أو شريك متى ارتكب أو ساهم في الفعل الإجرامي.

2. **الشخص المعنوي:** تقوم مسؤوليته من خلال ممثليه، خاصة المسؤول عن الإدارة الفعلية، وفقًا لشروط المادة (48) من قانون الجرائم الإلكترونية.
3. **مزودو الخدمات:** يسألون جنائيًا متى ثبت تقصيرهم في الرقابة أو الامتناع عن منع المحتوى غير المشروع، استنادًا إلى القواعد العامة، لاسيما المادة (64) من قانون العقوبات.

وبذلك، يتجه التنظيم القانوني الليبي إلى إرساء نظام مسؤولية متكامل يواكب خصوصية الفضاء المعلوماتي، قائم على توزيع الأدوار وربط المسؤولية بمدى السيطرة التقنية والقدرة على المنع أو التوجيه.

- **ملخص تفاعلي:**

المسؤولية الجنائية عن الجريمة المعلوماتية

- **الفكرة الرئيسة:**

تتميز الجريمة المعلوماتية بأنها تُرتكب داخل بيئة رقمية معقدة تتعدد فيها الأطراف ومراكز السيطرة، لذلك لم تعد المسؤولية الجنائية مقصورة على الفاعل المباشر وحده، بل قد تمتد إلى كل من أسهم في ارتكاب الجريمة أو سهّل وقوعها أو امتنع عن منعها رغم قدرته على ذلك.

ومن ثم تبنّى المشرّع الليبي في القانون رقم (5 لسنة 2022م) مفهومًا موسعًا للمسؤولية الجنائية يتلاءم مع طبيعة الفضاء المعلوماتي، نوجزه في الآتي:

- **أولًا: من يسأل جنائيًا عن الجريمة المعلوماتية؟**

يمكن حصر أطراف المسؤولية الجنائية في ثلاثة مراكز رئيسة:

1. **الشخص الطبيعي** "الفاعل المباشر أو المساهم"، وهو كل من يرتكب بنفسه السلوك الإجرامي المعلوماتي، كاختراق الأنظمة، أو التعدي على البيانات، أو نشر المحتوى غير المشروع.
- سؤال تطبيقي: هل تقتصر المسؤولية على المخترق فقط؟
- الجواب: لا، فقد تمتد إلى كل من ساهم في تمكين الجريمة أو تسهيلها متى توافرت شروط المسؤولية الجنائية.
2. **الشخص المعنوي**، أقر المشرّع الليبي مسؤوليته بصورة غير مباشرة من خلال مساءلة المسؤول عن الإدارة الفعلية، وتقوم هذه المسؤولية إذا: ارتُكبت الجريمة باسم الشخص المعنوي، أو كانت لمصلحته، أو نتجت عن إخلال بواجبات الإشراف أو الرقابة.

- **الأساس القانوني للمسؤولية:** الخطأ في الرقابة أو الإشراف.
- **النتيجة القانونية:** قد تصل العقوبة إلى حل الشخص المعنوي إذا ثبت أنه استُخدم ستارًا أو أداة لارتكاب الجرائم المعلوماتية.

3. **مزودو خدمات الاتصالات وتقنية المعلومات،** كالشركات التي تقدم خدمات النفاذ إلى الإنترنت أو الإيواء أو إدارة المنصات الرقمية.

ولا تقوم مسؤوليتهم لمجرد وجود الخدمة، وإنما إذا ثبت: علمهم بالمحتوى أو النشاط غير المشروع، وقدرتهم على منعه أو إزالته، وامتناعهم عن اتخاذ الإجراءات اللازمة.

- **القاعدة الحاكمة:** "لا مسؤولية دون علم، ولا مسؤولية مع انعدام القدرة على التدخل".

- **ثانيًا: ما الأساس الذي تقوم عليه المسؤولية؟**

يقوم نظام المسؤولية في الجرائم المعلوماتية على ثلاثة معايير مترابطة:

1. **السيطرة التقنية:** أي مدى قدرة الشخص على التحكم في النظام أو المنصة أو المحتوى.
2. **العلم بالنشاط غير المشروع:** فلا يكفي مجرد الوجود في البيئة الرقمية، بل يجب ثبوت العلم بالفعل الإجرامي أو إمكانية العلم به.
3. **القدرة على المنع أو التدخل:** وهو المعيار الأكثر أهمية، إذ ترتبط المسؤولية غالبًا بإمكانية منع الجريمة أو الحد من آثارها وعدم القيام بذلك.

- **ثالثًا: خصوصية المسؤولية في البيئة الرقمية:**

على خلاف الجرائم التقليدية التي يبرز فيها الفاعل بصورة واضحة، فإن الجريمة المعلوماتية قد تتوزع فيها الأدوار بين: من يرتكب الفعل، ومن يوفر البنية التقنية، ومن يدير المنصة أو النظام، ومن يملك سلطة الرقابة أو الإشراف.

ومن هنا انتقل مفهوم المسؤولية من مجرد تنفيذ الفعل الإجرامي إلى مساءلة كل من كانت له سيطرة فعلية أو قدرة قانونية وتقنية على التوجيه أو المنع.

وبالتالي فإن نظام المسؤولية الجنائية في الجرائم المعلوماتية يقوم على مبدأ جوهري مفاده أن المسؤولية تتبع العلم والسيطرة والقدرة على التدخل؛ لذلك يسأل:

1. الشخص الطبيعي بوصفه فاعلًا أو مساهمًا في الجريمة[3].
2. والشخص المعنوي من خلال إدارته الفعلية عند الإخلال بواجبات الرقابة.
3. ومزود الخدمة متى علم بالنشاط غير المشروع وكان قادرًا على منعه أو إزالته.

وبذلك يكرّس المشرّع الليبي نموذجًا حديثًا للمسؤولية الجنائية يتجاوز المفهوم التقليدي للفاعل، ويربط المساءلة بمدى السيطرة التقنية والقدرة على الحماية داخل الفضاء المعلوماتي.

• الفصل الثاني:

صور الجريمة المعلوماتية وتطبيقاتها الجنائية.

أفرز المخترع الرقمي وما صاحبه من تطور متسارع في تقنيات المعلومات والاتصالات أنماطًا جديدة من السلوك الإجرامي تجاوزت في طبيعتها وحدودها المفاهيم التقليدية للجريمة، حيث أصبحت البيئة الإلكترونية فضاءً خصبًا لممارسة صور متعددة من الاعتداءات التي تستهدف الأفراد والمؤسسات والدول على حد سواء، وقد أدى ذلك إلى ظهور ما يُعرف بالجريمة المعلوماتية بوصفها أحد أخطر التحديات الجنائية المعاصرة، نظرًا لما تتميز به من طابع تقني معقد، وسرعة في التنفيذ، واتساع في نطاق الأثر، وصعوبة في الاكتشاف والإثبات.

وإذا كانت الجرائم المعلوماتية تتخذ صورًا وأشكالًا متعددة تبعًا لطبيعة المصلحة المعتدى عليها أو الوسيلة المستخدمة في ارتكابها، فإن بعض هذه الجرائم قد تجاوز حدود الاعتداء على البيانات والأنظمة المعلوماتية لتصبح أداة فعالة في خدمة أغراض إجرامية أكثر خطورة، وفي مقدمتها الإرهاب، وبحيث أتاح الفضاء السيبراني للتنظيمات الإرهابية وسائل غير مسبوقة للتواصل والتجنيد والتمويل والتخطيط والتنفيذ والتأثير الإعلامي، الأمر الذي أدى إلى نشوء نمط خاص من الجرائم المعلوماتية ذات الصبغة

---

[3] تنص المادة (99) في (الفاعل وعقوبته) على أنه:"يعد فاعلاً للجريمة:

- أولاً: من يرتكبها وحده أو مع غيره.
- ثانياً: من يدخل في ارتكابها إذا كانت تتكون من جملة أعمال فيأتي عمداً عملاً من الأعمال المكونة لها.

وتنطبق على كل فاعل العقوبة المقررة للجريمة المقترفة.

ومع ذلك إذا وجدت أحوال خاصة بأحد الفاعلين تقتضي تغيير وصف الجريمة أو العقوبة بالنسبة له فلا يتعدى أثرها إلى غيره منهم إذا كان غير عالم بتلك الأحوال، وكذلك إذا تغير الوصف باعتبار قصد مرتكب الجريمة أو كيفية علمه بها".

الإرهابية، والتي تمثل التقاءً بين الجريمة المعلوماتية والجريمة الإرهابية في إطار إجرامي مركب يهدد الأمن الوطني والدولي.

ومن ثم، يقتضي الأمر الوقوف على أنواع الجرائم المعلوماتية المختلفة، وبيان خصائصها وتمييزها عن غيرها من الجرائم التقليدية في **(المبحث الأول)**، وذلك تمهيدًا لدراسة البنيان الموضوعي للجريمة المعلوماتية ذات الصبغة الإرهابية من خلال تحليل أركانها وعناصرها القانونية، وبيان خصوصيتها في ضوء أحكام التشريع الليبي في **(المبحث الثاني)**.

• المبحث الأول: في أنواع الجرائم المعلوماتية.

أفرز التطور التكنولوجي المعاصر واقعًا إجراميًا مستحدثًا، اتسم بارتباط وثيق بين استخدام الحاسب الآلي وارتكاب الأفعال غير المشروعة، بحيث غدت التقنية المعلوماتية إما محلًا للاعتداء أو أداة لاقترافه، وقد واكب المشرّع الليبي هذا التحول بإصدار القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، الذي بسط الحماية الجنائية على مختلف صور الاعتداء التي تمس الأنظمة المعلوماتية والبيانات والخدمات الرقمية.

ولم يُعد الخطر مقتصرًا على الاعتداء المادي التقليدي، بل امتد ليشمل ما يُعرف بالأموال المعلوماتية، المتمثلة في الأجهزة والبرامج والبيانات، وهي عناصر ذات طبيعة غير مادية تفرض إشكاليات قانونية خاصة، سواء من حيث التكييف أو الإثبات أو تحديد نطاق الحماية الجنائية، وقد أسهم الانتشار الواسع والمتسارع لتقنيات المعلومات، في ظل ثورة رقمية عابرة للحدود، في توسيع دائرة هذه الجرائم وتعقيد أنماطها، بما أوجد صورًا إجرامية ذات طابع تقني متميز.

وعليه، فإن الجرائم المعلوماتية تمثل نمطًا حديثًا من الإجرام، يقوم على توظيف الوسائل التقنية في الاعتداء على المصالح المحمية قانونًا، الأمر الذي استوجب تدخلًا تشريعيًا خاصًا يراعي خصوصيتها ويستجيب لتحدياتها المستجدة.

• تعريف الجريمة المعلوماتية

هي "كل سلوك إجرامي يتم باستخدام الحاسوب أو الأنظمة المعلوماتية كوسيلة أو محل للاعتداء"، وعلى ذلك يمكن أن تكون المعلوماتية بأنظمتها ومعطياتها محل اعتداء، فإنها بالمثل يمكن أن تكون سبباً في تسهيل ارتكاب الجريمة، فنتحدث في الصورة الأولى عن جرائم الاعتداء على سرية وسلامة وجاهزية المعطيات والأنظمة المعلوماتية في مرحلة أولى، وعن التزوير والتدليس المعلوماتي في مرحلة

ثانية، وهذه هي الجريمة المعلوماتية في مفهومها الضيق (أ)، ونتعرض في الصورة الثانية لمسألة الجرائم المتعلقة بالمحتوى (ب). وهذا هو التقسيم الذي استقر عليه الرأي دولياً ووطنياً.

• المطلب الأول: جرائم الاعتداء على المعلوماتية.

تقوم جرائم الاعتداء على المعلوماتية – في جوهرها – على المساس غير المشروع بسلامة نظم المعالجة الآلية للبيانات أو بوظائفها أو بمحتواها المعلوماتي، وذلك في أي مرحلة من مراحل تشغيلها. فالأصل في هذا النمط الإجرامي أنه ينصرف إلى الإخلال بوحدة النظام المعلوماتي أو تعطيل سيره أو إتلاف البيانات المخزنة أو المعالجة داخله.

وقد كرّس المشرّع الليبي هذا المفهوم في القانون رقم (5 لسنة 2022م)، من خلال تجريم كل سلوك ينال من الأنظمة المعلوماتية أو البيانات الإلكترونية، سواء تعلّق الأمر بالدخول غير المشروع أو البقاء دون سند قانوني (م11)، أو بالاعتداء على البيانات حذفًا أو تعديلًا أو إتلافًا أو نسخًا، أو بتعطيل النظام أو عرقلة أدائه (م15).

ولا يُعتد في قيام الجريمة بكون النظام متصلًا بشبكة من عدمه، أو بكون البيانات داخل الحاسب أو خارجه، متى كانت محمية في إطار تقني معلوماتي. كما يمتد نطاق التجريم ليشمل كل صور التلاعب أو التدليس في السندات الإلكترونية، باعتبارها جزءًا من البنية المعلوماتية محل الحماية الجنائية.

وعليه، فإن جوهر الجريمة المعلوماتية يتمثل في كل اعتداء ينصب على النظام المعلوماتي أو مكوناته أو مخرجاته، سواء وقع هذا الاعتداء على الكيان التقني ذاته أو على المعطيات التي يحتويها، بما يخل بوظيفته أو يمس سلامته أو يعرّضه للاستغلال غير المشروع.

– أولا: لاعتداء على الأنظمة والمعلومات:

يُقصد بالاعتداء على الأنظمة والمعطيات المعلوماتية كل سلوك إجرامي ينال من سرية البيانات وسلامتها وتوافرها، وهو ما أحاطه المشرّع الليبي بحماية جنائية صريحة بموجب القانون رقم (5 لسنة 2022م)، من خلال نصوص متكاملة تُجرّم مختلف صور هذا الاعتداء.

ففيما يتعلق بـ النفاذ أو الدخول غير المشروع، فقد نص على تجريم الدخول العمدي إلى نظام معلوماتي أو البقاء فيه دون وجه حق، سواء كان هذا النظام مؤمّنًا أو غير مؤمّن، وسواء كان مستقلًا أو مرتبطًا بشبكة، متى توافر القصد في الحصول على بيانات أو إحداث ضرر.

أما بشأن الاعتراض أو الالتقاط غير المشروع للبيانات، فقد جرّم المشرّع – في إطار حماية سرية الاتصالات والبيانات – الأفعال التي تنصب على التقاط أو اعتراض البيانات الإلكترونية أثناء انتقالها عبر الشبكات، بما في ذلك الإشارات أو الإرساليات الكهرومغناطيسية، وذلك، دون اشتراط تحقق ضرر فعلي.

وفيما يخص الاعتداء على سلامة المعطيات المعلوماتية، فقد نصّ كذلك على تجريم كل فعل عمدي من شأنه إتلاف البيانات أو حذفها أو تعديلها أو نسخها أو نشرها دون مسوغ قانوني، باعتبار ذلك مساسًا مباشرًا بسلامة المحتوى المعلوماتي.

كما عالج المشرّع صور الاعتداء على سلامة النظام المعلوماتي، حيث نصّ على تجريم الأفعال التي تؤدي إلى تعطيل النظام أو عرقلة عمله أو إضعاف كفاءته، سواء تم ذلك عن طريق إدخال بيانات أو نقلها أو إتلافها أو التلاعب بها، بما يشمل الهجمات التقنية التي تستهدف شلّ عمل الأنظمة.

وعليه، يتضح أن المشرّع الليبي قد أقام حماية جنائية متكاملة تشمل: سرية الأنظمة، وسرية وسلامة البيانات، وجاهزية وتوافر الأنظمة، وبما يعكس تصورًا تشريعيًا حديثًا يحيط بكافة عناصر البيئة المعلوماتية، ويجرّم كل اعتداء يقع عليها، سواء من حيث النفاذ أو الاعتراض أو الإتلاف أو التعطيل.

- **ثانيا: أفعال التدليس والتزوير المعلوماتي:**

يُقصد بـ التدليس المعلوماتي كل سلوك عمدي ينصب على إنشاء أو إدخال أو تعديل أو حذف المعطيات الإلكترونية على نحو يغيّر من حقيقتها، بقصد استعمالها في مواجهة الغير على أنها صحيحة، بما من شأنه الإضرار بمصالحه، وهو في جوهره انحراف بالحقيقة الرقمية عبر التلاعب بالمحتوى المعلوماتي.

أما التزوير المعلوماتي فينصرف إلى صور الاعتداء الأوسع نطاقًا التي تستهدف البيانات أو النظام المعلوماتي ذاته، من خلال أفعال عمدية غير مشروعة، كإتلاف المعطيات أو تعديلها أو إدخال بيانات مصطنعة أو محوها، بقصد تحقيق منفعة غير مشروعة أو إلحاق ضرر مادي بالغير، وهو ما يُقارب في بنيانه التزوير التقليدي، مع اختلاف الوسيط ليصبح رقميًا.

وقد عالج المشرّع الليبي هذه الأفعال ضمن إطار حماية الثقة في المعاملات الإلكترونية، حيث نصّ القانون رقم (5 لسنة 2022م) على تجريم استخدام وسائل تقنية المعلومات في تغيير الحقيقة بقصد الاستيلاء على مال الغير أو تحقيق منفعة غير مشروعة، وهو ما يشمل صور التدليس والتزوير المعلوماتي متى اقترنت بالقصد الاحتيالي.

كما تمتد الحماية الجنائية – وفقًا لنصوص القانون– إلى تجريم الأفعال التمهيدية المرتبطة بهذه الجرائم، إذ يُعاقب على إنتاج أو حيازة أو تداول الأدوات أو البرامج المعلوماتية المعدّة لارتكاب الجرائم المعلوماتية، متى توافرت نية استخدامها في ذلك، وهو ما يستفاد من نطاق التجريم الوارد في القانون التي تُجرّم إساءة استخدام وسائل تقنية المعلومات لتحقيق أغراض غير مشروعة.

وعليه، يتضح أن المشرّع الليبي لم يقف عند حد تجريم الفعل النهائي للتدليس أو التزوير، بل بسط نطاق الحماية ليشمل كذلك الوسائل والأدوات الممكّنة له، بما يعكس توجّهًا تشريعيًا وقائيًا يهدف إلى تجفيف منابع الجريمة المعلوماتية قبل اكتمال صورتها التنفيذية.

• المطلب الثاني: الجرائم المتعلقة بالمحتوى المعلوماتي.

تتميّز الجرائم المرتبطة بالمحتوى المعلوماتي بأن محلّ الاعتداء فيها لا ينصب على النظام المعلوماتي أو البيانات في ذاتها، وإنما تُستَخدم الوسائل التقنية كأداة لارتكاب أفعال غير مشروعة تمس حقوقًا ومصالح محمية قانونًا، ومن ثمّ، فإنها تمثّل صورة من صور الإجرام المعلوماتي بالوسيلة لا بالمحل.

وقد أحاط المشرّع الليبي هذه الأفعال بالتجريم في القانون رقم (5 لسنة 2022م)، من خلال نصوص تعالج إساءة استخدام وسائل تقنية المعلومات، حيث نصّ على تجريم استعمال هذه الوسائل في التهديد أو الابتزاز أو نشر ما من شأنه الإضرار بالغير، بما يشمل الاعتداء على الحياة الخاصة وانتهاك البيانات الشخصية.

كما تمتد الحماية الجنائية – في إطار ذات القانون– إلى الأفعال التي تقع عبر الوسائط الإلكترونية وتمس الملكية الفكرية أو تنطوي على نشر محتوى غير مشروع أو مضلل، متى توافرت أركان التجريم، باعتبار أن هذه السلوكيات تُشكل اعتداءً على حقوق مالية أو أدبية يقرّها القانون.

وتشمل هذه الجرائم كذلك ما يقع في نطاق النشر الإلكتروني ووسائل الإعلام الرقمية، من تجاوزات وتمس السمعة أو الشرف أو تخالف الضوابط القانونية المنظمة، فضلًا عن الأفعال التي تنال من

حقوق المستهلك عبر الفضاء الرقمي، كالتضليل أو عرض خدمات أو منتجات على نحو ينطوي على غش أو خداع.

وعليه، يتضح أن المشرّع الليبي قد تبنّى مفهومًا واسعًا للجرائم المرتبطة بالمحتوى المعلوماتي، قوامه تجريم كل استخدام غير مشروع لوسائل التقنية من شأنه المساس بالحقوق الشخصية أو المالية أو الاعتبارية، بما يضمن حماية فعّالة لمختلف المصالح القانونية في البيئة الرقمية.

- **أولا: الاعتداء على الحياة الخاصة والبيانات الشخصية:**

تُعد حماية الحياة الخاصة والبيانات الشخصية من أبرز التحديات التي أفرزها التطور التكنولوجي، إذ باتت المعالجة الآلية للبيانات في البيئة الرقمية تمثل أحد أهم مصادر المساس بخصوصية الأفراد، نظرًا لما توفره من إمكانيات واسعة في جمع المعلومات وتخزينها واسترجاعها وربطها عبر شبكات الاتصال.

وقد ازدادت هذه الإشكالية تعقيدًا في الفضاء المعلوماتي المفتوح، حيث أصبح من اليسير النفاذ إلى البيانات الشخصية أو معالجتها أو تداولها دون إذن أصحابها، بما يشكل تهديدًا مباشرًا للحق في الخصوصية، وهو ما استدعى تدخّل المشرّع الليبي في إطار القانون رقم (5 لسنة 2022م)، لتوفير حماية جنائية فعّالة لهذا الحق.

وفي هذا السياق، جرّم المشرّع كل استعمال غير مشروع لوسائل تقنية المعلومات من شأنه المساس بالحياة الخاصة أو نشر بيانات أو معلومات شخصية أو استخدامها أو إفشائها دون سند قانوني، بما يحقق الاعتداء على حرمة الحياة الخاصة للأفراد.

وتتخذ صور هذا الاعتداء أشكالًا متعددة، من بينها جمع البيانات الشخصية أو معالجتها أو نشرها أو تداولها بغير رضا صاحبها، أو استخدامها في أغراض غير مشروعة، وهو ما يعكس الطبيعة المركبة لهذا النوع من الجرائم التي تقوم على استغلال البيئة الرقمية في انتهاك الخصوصية.

كما يقوم النظام القانوني لحماية البيانات الشخصية على جملة من المبادئ المستقرة، التي يمكن استلهامها في إطار التطبيق، ومن أبرزها: مبدأ الإشعار المسبق[4]، والموافقة الصريحة، والشرعية في

[4] **مبدأ الموافقة المسبقة:** يقوم مبدأ الموافقة المسبقة على عدم جواز معالجة البيانات الشخصية المتصلة بالحياة الخاصة إلا بعد الحصول على رضا صريح ومسبق من صاحب البيانات في جميع مراحل المعالجة، بما في ذلك الجمع، والتخزين، والبحث، والتنظيم، والتوزيع، واستغلال قواعد البيانات، وذلك مع استثناء الحالات التي يجيزها القانون

المعالجة، والشفافية والاطلاع، وصحة البيانات وتحديثها، فضلًا عن مبدأ جبر الضرر عن كل اعتداء يقع على الحياة الخاصة.

وعليه، يتضح أن المشرّع الليبي قد تبنّى في القانون رقم (5 لسنة 2022م) اتجاهًا حمائيًا واضحًا، يهدف إلى تحقيق التوازن بين تطور استخدامات التقنية من جهة، وصون الحياة الخاصة والبيانات الشخصية من جهة أخرى، عبر تجريم كل سلوك يمس هذا الحق في البيئة الرقمية.

- **ثانيا: الاعتداء على قواعد النشر والصحافة:**

الحقيقة أن المعالجة الإلكترونية وخاصة في فضائها المفتوح أي توزيع المحتوى عبر الشبكات المفتوحة، ليست وسيلة من وسائل الاتصال أو خدمة من الخدمات السمعية البصرية فقط بل هي خدمة من خدمات الصحافة والنشر.

ومن ثم فإنه من الممكن استعمال الشبكات المفتوحة لارتكاب جميع الجرائم ذات الصلة. فالثلب والشتم من الجرائم البسيطة التي يمكن ارتكابها سواء عبر مواقع الويب أو عن طريق مجموعات الأخبار، ويستثنى من ذلك البريد الإلكتروني باعتبار أنه يتميز بخصوصيته.

- **ثالثا: الاعتداء على الملكية الفكرية:**

يشمل الاعتداء على الملكية الفكرية في البيئة المعلوماتية صورتين رئيسيتين: الملكية الأدبية والملكية الصناعية، وكلاهما يخضع لحماية جنائية في إطار القانون رقم (5 لسنة 2022م) بشأن

صراحة. ولا يعتد قانونًا بموافقة القاصر، إذ يتعين الحصول على موافقة الولي أو الممثل القانوني، باعتبار أن الأطفال فئة تستوجب حماية خاصة في مجال تداول البيانات.

كما يشمل هذا المبدأ مرحلة جمع البيانات الشخصية، حيث لا يجوز للمواقع الإلكترونية، خاصة التجارية منها، جمع أي بيانات تتعلق بالمستخدم مثل الاسم أو العنوان أو البيانات البنكية إلا بناءً على موافقة صريحة ومسبقة، ويُعد الضغط على خانة القبول بعد الاطلاع على الشروط بمثابة تعبير عن الرضا القانوني.

ويمتد المبدأ كذلك إلى عمليات نشر البيانات وتوزيعها أو المتاجرة فيها، حيث لا يجوز إتاحة أو تداول المعلومات الشخصية أو استخدامها لأغراض إعلانية أو تجارية دون موافقة صاحبها، باستثناء ما يتعلق بالتحقيقات القضائية أو ما يجيزه القانون.

كما يقرّ النظام إمكان تمكين المستعمل من حق الاعتراض المسبق أو اللاحق على معالجة بياناته أو استخدامها لأغراض تسويقية، عبر آليات تقنية مثل ((opt–out، بما يضمن خضوع تداول البيانات لموافقة واعية ومستمرة من صاحبها.

مكافحة الجرائم الإلكترونية، الذي جرّم كل استعمال غير مشروع لوسائل تقنية المعلومات يمس الحقوق المحمية أو يخل بها طبقا للمادة (6)[5].

أ. **الاعتداء على الملكية الأدبية:**

يُعد حق المؤلف حقًا استئثاريًا في استغلال المصنف أو الترخيص للغير باستغلاله بأي وسيلة، بما في ذلك النشر والإتاحة الرقمية، وفي البيئة المعلوماتية، يمثل الإنترنت مجالًا خصبًا للاعتداء على هذا الحق، لاسيما عبر عرض المصنفات أو نسخها أو إعادة نشرها دون إذن صاحب الحق، ويظهر الاعتداء على الملكية الأدبية في مستويين:

- **المستوى الأول: استغلال المحتوى:** من خلال عرض المصنف أو تحميله أو إعادة توزيعه دون ترخيص، وهو ما يشكل اعتداءً مباشرًا على حق المؤلف.
- **أما المستوى الثاني: إنتاج المحتوى الرقمي:** عبر رقمنة المصنفات أو إعادة نشرها أو إدماجها في مواقع إلكترونية، بما قد يثير إشكاليات حول مدى اعتبار الرقمنة عملاً مشروعًا أو تعديًا على حق النقل والاستغلال.

وتُعد الرقمنة في ذاتها صورة من صور النقل للمصنف، لا يجوز القيام بها إلا بإذن صاحب الحق، كما أن عرض المصنفات عبر الإنترنت يُكيف كإتاحة عامة تستوجب الترخيص المسبق، باعتبار أن الشبكة وسيلة اتصال عامة تتيح الوصول غير المحدود للمحتوى.

كما تثير تقنيات الربط التشعبي إشكاليات قانونية دقيقة، إذ إن مجرد الإحالة لا يُعد اعتداءً في الأصل، غير أن بعض صور الربط العميق أو الإطار أو الربط الآلي قد تؤدي إلى إعادة عرض غير مباشر للمصنف أو استخراج غير مشروع لمحتواه، بما قد يندرج ضمن صور الاعتداء على حقوق المؤلف أو قواعد البيانات المحمية.

كذلك، قد تسهم هذه التقنيات في الإخلال بقواعد المنافسة المشروعة، خاصة عند إعادة عرض محتوى المواقع دون واجهتها الأصلية أو الإشهارية، بما يضر بالمراكز الاقتصادية لأصحابها.

---

[5] تنص المادة (6) في (الأعمال الأدبية أو الفنية أو العملية) على أنه :"كل عمل أدبي أوفني أو علمي ينشر عبر شبكة المعلومات الدولية أو أي نظام تقني أخر ملك لصاحبه، لا يجوز تقليده أو نسخه أو إعادة نشره إلا بتصريح مكتوب أو إلكتروني من مالكه، ويعد في حكم التقليد الاستيلاء على أنظمة المعلومات أو البرمجيات أو نسخها في غير الأحوال المسموح بها في القانون".

وعليه، فإن استخدام تقنيات الإنترنت والربط التشعبي قد يتحول – في بعض تطبيقاته – إلى وسيلة للاعتداء على حقوق الملكية الفكرية، رغم أن الأصل في الاستعمال هو الإباحة المشروطة بعدم الإضرار أو الاعتداء.

ب. الاعتداء على الملكية الصناعية:

تتجسد الملكية الصناعية في الفضاء المعلوماتي أساسًا في أسماء الكيانات الصناعية التي تخضع لنظام التسجيل القائم على مبدأ الأولوية في الحجز، حيث يثبت الحق لمن يبادر بالتسجيل.

غير أن سهولة التسجيل وضعف آليات الرقابة المسبقة أتاحا إمكانية استغلال هذه الأسماء بطرق غير مشروعة، بما في ذلك تسجيل أسماء تجارية أو علامات صناعية مملوكة للغير، سواء بسوء نية أو حتى بحسن نية، بما يؤدي إلى التعدي على حقوق الغير أو الإضرار بمصالحهم التجارية.

وقد ترتب على ذلك تحول أسماء النطاقات إلى محل نزاع ومجال للاستغلال غير المشروع، لارتباطها المباشر بالقيمة التجارية للمؤسسات والعلامات، وهو ما يندرج ضمن صور الاعتداء التي تستوجب الحماية وفقًا لأحكام القانون رقم (5 لسنة 2022م)، بوصفه اعتداءً يتم عبر الوسائط الإلكترونية على حقوق ملكية محمية قانونًا.

ونخلص الى القول: أن التطور التقني، رغم ما أتاحه من إمكانيات واسعة، قد أفرز صورًا متعددة من الاعتداء على الملكية الفكرية، سواء الأدبية أو الصناعية، مما استوجب تدخل المشرّع الليبي لتجريم كل استعمال غير مشروع للوسائط الإلكترونية يمس هذه الحقوق أو يخل بحمايتها.

- **رابعا: الاعتداء على حقوق المستهلك:**

تُعد التجارة الإلكترونية والإشهار الرقمي من أبرز مظاهر النشاط الاقتصادي عبر الشبكات المعلوماتية، حيث أصبح الإشهار التجاري أداة رئيسية للتأثير في إرادة المستهلك وتوجيه قراره، مستفيدًا من الإمكانيات التقنية الحديثة، وعلى رأسها الروابط الإلكترونية ومحركات البحث وما توفره من تصنيف للمحتوى وجمع للبيانات.

وقد أتاح هذا التطور بروز أنماط جديدة من التسويق الرقمي، عبر الإعلانات المدمجة في المواقع، أو من خلال التبادل الإعلاني بين التجار، أو عبر ما يُعرف بحلقات الويب، إضافة إلى خدمات البريد الإلكتروني الإعلاني غير المرغوب فيه، الذي يُعد من أكثر الوسائل انتشارًا في الإشهار المباشر.

غير أن هذا الاستخدام الواسع للتقنيات الرقمية قد أفرز مخاطر جدية على حقوق المستهلك، الأمر الذي تدخّل بشأنه المشرّع الليبي في القانون رقم (5 لسنة 2022م)، من خلال تجريم كل استعمال غير مشروع لوسائل تقنية المعلومات من شأنه التضليل أو الإضرار بالغير أو انتهاك حقوقه، بما يشمل صور الإشهار الإلكتروني المضلل أو غير المشروع.

ويُعد من صور الاعتداء على حقوق المستهلك في البيئة الرقمية:

أ. الإعلانات الكاذبة أو المضللة التي تنطوي على خداع أو تضليل .

ب. المقارنات غير الصحيحة بين المنتجات أو الخدمات .

ت. الإشهارات المحظورة المتعلقة بسلع أو خدمات غير مشروعة أو مقيدة قانونًا .

ث. الإعلانات غير المرغوب فيها عبر البريد الإلكتروني دون موافقة مسبقة.

وفي المقابل، استقر الاتجاه التنظيمي على ضرورة احترام مبدأ الموافقة المسبقة أو حق الاعتراض، بما يضمن للمستهلك حق التحكم في تلقي الإعلانات أو رفضها، في إطار حماية خصوصيته وبياناته الشخصية.

كما ظهرت آليات تقنية وقانونية لضبط الإشهار الرقمي، من بينها اعتماد أنظمة المصادقة على المواقع الإعلانية، ووضع معايير للمحتوى الإشهاري المسموح به، بهدف تعزيز الثقة في المعاملات الإلكترونية وحماية المستهلك من التضليل والاستغلال.

وعليه، فإن المشرّع الليبي – من خلال القانون رقم (5 لسنة 2022م)– قد وسّع نطاق الحماية الجنائية ليشمل البيئة الاستهلاكية الرقمية، عبر تجريم كل سلوك إلكتروني من شأنه الإضرار بحقوق المستهلك أو تضليله أو التأثير غير المشروع على إرادته في الفضاء الرقمي.

- **خامسا: الاعتداء على الأمن والأخلاق الحميدة والأشخاص:**

يُقر الفقه الجنائي التقليدي تقسيم الجرائم إلى جرائم تمس الأمن العام، وأخرى تمس الأموال، وثالثة تمس الأخلاق والآداب العامة، غير أن البيئة المعلوماتية قد أفرزت نمطًا جديدًا من الإجرام يتسم بالسهولة والسرعة واتساع نطاق الانتشار، بحيث أصبح من الممكن ارتكاب مختلف صور الجرائم عبر الشبكات المفتوحة بوسائل تقنية متطورة وفي زمن وجيز، مع صعوبة ضبط آثارها أو الحد من امتدادها.

وقد أدرك المشرّع الليبي هذه الخصوصية، فنصّ في القانون رقم (5 لسنة 2022م) على تجريم كل استعمال غير مشروع لوسائل تقنية المعلومات من شأنه المساس بالأمن أو النظام العام أو القيم

الاجتماعية أو حقوق الأشخاص، وذلك في إطار ما قرره من تجريم الأفعال الإلكترونية الضارة أو المهددة أو المحرضة على الإضرار بالغير.

وتتجلى صور هذا الاعتداء في عدة مظاهر، من أبرزها:

أ. المساس بشرف الأشخاص وسمعتهم عبر التشهير أو القدح أو الذم الإلكتروني.

ب. نشر خطاب الكراهية أو التمييز العنصري أو الطائفي عبر الوسائط الرقمية.

ت. التحريض على العنف أو الإرهاب أو ارتكاب الجرائم.

ث. استخدام الشبكات في أعمال التجسس أو جمع المعلومات غير المشروعة.

كما تمثل الشبكات المفتوحة بيئة خصبة لارتكاب الجرائم الجنسية، ولا سيما تلك التي تستهدف الأطفال، سواء عبر استغلالهم أو إتاحة محتوى إباحي أو الترويج له، وهو ما يُعد من أخطر صور الاعتداء على القيم الأخلاقية والمجتمعية، وقد حظي بتجريم صارم في التشريعات الوطنية والدولية، لما ينطوي عليه من انتهاك جسيم للكرامة الإنسانية.

ويمتد نطاق الإجرام المعلوماتي كذلك إلى نشر الأخبار الزائفة، والدعوة إلى الانتحار أو القتل، وإنشاء منصات للمقامرة أو السمسرة غير المشروعة، أو استغلال الفضاء الرقمي في أنشطة تمس الأمن الاقتصادي والاجتماعي للدولة.

وعليه، يتضح أن المشرّع الليبي – من خلال القانون رقم (5 لسنة 2022م)– قد وسّع نطاق الحماية الجنائية ليشمل الفضاء الرقمي بكافة امتداداته، باعتباره بيئة قد تمكّن من ارتكاب نفس الأفعال الإجرامية التقليدية ولكن بوسائل أكثر خطورة وانتشارًا وتأثيرًا، بما يؤكد أن ما يمكن القيام به في العالم المادي يمكن – بل وبصورة أشد– أن يُرتكب في العالم الافتراضي.

ونخلص مما تقدم، أن الجريمة المعلوماتية في مفهومها الدقيق تنصرف إلى كل اعتداء يقع على البيانات أو الأنظمة المعلوماتية، سواء كانت مستقلة أو مرتبطة بالشبكات أو مدمجة ضمن سندات إلكترونية، حيث تكون هذه الأنظمة والمعطيات هي محل الحماية الجنائية والمجني عليها في نهاية الأمر، وهو ما كرسه المشرّع الليبي في القانون رقم (5 لسنة 2022م) من خلال تجريم الأفعال الماسة بسرية وسلامة وتوافر الأنظمة والبيانات.

أما إذا استُخدمت الوسائل المعلوماتية كأداة لارتكاب اعتداءات تمس الغير دون أن تكون هي محل الاعتداء، فإنها لا تُعد محل الجريمة، وإنما تتحول إلى مجرد وسيلة تقنية حديثة ضمن وسائل الإجرام،

وعندئذ يُنظر إلى الفعل بوصفه إجرامًا معلوماتيًا بالوسيلة لا بالمحل، وبذلك يتضح أن المشرّع قد ميّز بين صورتين أساسيتين:

- **الصورة الأولى:** جريمة معلوماتية يكون محلها النظام أو البيانات المعلوماتية .
- **الصورة الثانية:** جريمة يُستخدم فيها النظام المعلوماتي كأداة لارتكاب اعتداء على الغير.

وهو تمييز جوهري يحدد نطاق التطبيق والتكييف القانوني في إطار القانون رقم (5 لسنة 2022م).

• المبحث الثاني:

البناء القانوني للجريمة المعلوماتية ذات الطابع الإرهابي.

(قراءة تحليلية في ضوء النظرية العامة للجريمة المعلوماتية وأحكام القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية).

تمثل الجريمة المعلوماتية ذات الطابع الإرهابي أحد أبرز مظاهر تطور السياسة الجنائية المعاصرة في مواجهة المخاطر الناشئة عن استغلال الفضاء الإلكتروني في خدمة الأنشطة الإرهابية، وقد جسد المشرع الليبي هذا التوجه من خلال المادة (45) من القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، والتي لم تقتصر على تجريم الأفعال الإرهابية التقليدية، وإنما امتدت إلى تجريم الوسائط الرقمية والبنى الإلكترونية التي يمكن أن تُستخدم في دعم التنظيمات الإرهابية أو الترويج لأفكارها أو تسهيل أنشطتها.

ويكشف هذا الاتجاه التشريعي عن انتقال مفهوم التجريم من مواجهة الفعل الإرهابي في صورته النهائية إلى التصدي للمخاطر الرقمية السابقة على وقوعه، بما يعكس تبني المشرع لسياسة جنائية وقائية تستهدف حماية الأمن القومي والأمن الرقمي من التهديدات المستحدثة.

• المطلب الأول:

التأصيل القانوني للجريمة المعلوماتية ذات الطابع الإرهابي وطبيعتها القانونية.

تنص المادة (45) من القانون رقم (5 لسنة 2022م) على معاقبة كل من أنشأ موقعًا إلكترونيًا أو نشر معلومات عبر شبكة المعلومات الدولية أو أي وسيلة إلكترونية لصالح جماعة إرهابية، ولو اتخذت تلك الجماعة مسميات تمويهية، متى كان الغرض من ذلك تسهيل الاتصال بقياداتها أو

أعضائها، أو الترويج لأفكارها، أو تمويلها، أو نشر وسائل تصنيع الأجهزة الحارقة أو المتفجرة أو غيرها من الأدوات المستخدمة في الأعمال المحظورة.

وبتحليل النص يتبين أنه يقوم على مجموعة من العناصر الجوهرية تتمثل في:

- **أولاً: تعدد صور السلوك الإجرامي:**

إذ لم يحصر المشرع النشاط الإجرامي في صورة واحدة، وإنما وسع نطاق التجريم ليشمل إنشاء المواقع الإلكترونية، ونشر المعلومات والبيانات، واستخدام الوسائل الإلكترونية المختلفة في خدمة الأهداف الإرهابية.

- **ثانياً: الارتباط التنظيمي بجماعة إرهابية:**

حيث اشترط النص وجود صلة بين النشاط الإلكتروني والجماعة الإرهابية، سواء تم ذلك بصورة مباشرة أو من خلال استخدام أسماء أو واجهات أو مسميات تمويهية.

- **ثالثاً: تعدد الأغراض الإجرامية:**

ويتمثل ذلك في تسهيل الاتصالات التنظيمية، أو الترويج للفكر الإرهابي، أو تقديم الدعم المالي، أو نشر الخبرات الفنية المتعلقة بصناعة الأدوات المستخدمة في الأعمال الإرهابية.

أما من حيث التكييف القانوني، فإن الجريمة المنصوص عليها في المادة (45) تعد:

1. جريمة خطر مجرد لا يشترط لقيامها تحقق نتيجة إجرامية مادية.
2. جريمة متعددة السلوك تقوم بأي صورة من الصور التي حددها المشرع.
3. جريمة عمدية ذات قصد خاص يتجاوز مجرد العلم والإرادة إلى ضرورة توافر الغرض الإرهابي.

- **المطلب الثاني:**

أركان الجريمة المعلوماتية ذات الطابع الإرهابي وتطبيقاتها العملية.

بالنظر إلى طبيعة الأفعال الإرهابية التقليدية، لذا تُعد الجريمة المعلوماتية ذات الطابع الإرهابي من أخطر صور الإجرام المعاصر، لما تنطوي عليه من استغلال للفضاء الإلكتروني في خدمة الأهداف الإرهابية وتوفير بيئة رقمية داعمة لأنشطتها.

وقد واكب المشرع هذا التطور من خلال توسيع نطاق التجريم ليشمل الأفعال والوسائط الإلكترونية التي تُسهم في دعم التنظيمات الإرهابية أو الترويج لأفكارها أو تسهيل أنشطتها، دون الاقتصار على الأفعال الإرهابية التقليدية أو النتائج الضارة المترتبة عليها، ويعكس هذا التوجه تبني سياسة جنائية وقائية تستهدف مواجهة الخطر في مراحله المبكرة قبل تحوله إلى اعتداء فعلي يهدد كيان الدولة.

ولما كانت المادة (45) من القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية تجسد هذا الاتجاه التشريعي، فإن الوقوف على أحكامها يقتضي بحث الأساس القانوني الذي تقوم عليه الجريمة المعلوماتية ذات الطابع الإرهابي، وبيان طبيعتها القانونية وموقعها ضمن النظرية العامة للجريمة المعلوماتية، فضلًا عن تحليل أركانها القانونية وعناصرها المكونة لها، وتحديد نطاق الحماية الجنائية التي استهدفها المشرع من خلال هذا التجريم، بما يسمح بإبراز خصوصية هذا النموذج الإجرامي وتكييفه القانوني في ضوء التطبيقات العملية المعاصرة، وذلك على النحو التالي:

- **أولاً: الركن المادي للجريمة:**

يقوم الركن المادي في هذه الجريمة على عدد من الصور السلوكية المستقلة، من أهمها:

- **أ): السلوك الإنشائي:** ويتمثل في إنشاء موقع إلكتروني أو منصة رقمية تخدم أهداف الجماعات الإرهابية، ويُعد هذا السلوك من أخطر صور النشاط الإجرامي لكونه يؤسس بنية إلكترونية دائمة قابلة للاستغلال المستمر.
- **ب): السلوك النشري:** ويتمثل في نشر المعلومات أو البيانات التي من شأنها خدمة النشاط الإرهابي أو دعم أهدافه، ولو بصورة غير مباشرة.
- **ج): السلوك الاتصالي:** ويتحقق من خلال تسهيل الاتصالات بين عناصر التنظيم الإرهابي أو قياداته، بما يمثل صورة مستحدثة من صور المساهمة الجنائية الرقمية.
- **د): السلوك التدريبي:** ويتمثل في نشر أو تداول المعلومات المتعلقة بكيفية تصنيع الأجهزة الحارقة أو المتفجرة أو غيرها من الوسائل المستخدمة في الأعمال الإرهابية، وهو ما يعد صورة من صور نقل الخبرة الإجرامية عبر الوسائط الرقمية.

أما النتيجة الإجرامية، فلا يشترط المشرع تحقق ضرر فعلي أو وقوع عمل إرهابي محدد، وإنما يكتفي بتعريض المجتمع والأمن العام لخطر محتمل، الأمر الذي يؤكد الطبيعة الوقائية للجريمة.

وفيما يتعلق بعلاقة السببية، فإنها تُفترض تشريعياً في هذا النموذج التجريمي، تأسيساً على افتراض المشرع أن كل دعم أو تسهيل إلكتروني للنشاط الإرهابي يمثل بطبيعته تعزيزاً محتملاً لهذا النشاط.

- **ثانياً: الركن المعنوي للجريمة:** تتطلب الجريمة توافر القصد الجنائي بشقيه:

1. **القصد الجنائي العام،** المتمثل في علم الجاني بطبيعة النشاط الذي يمارسه وبعلاقته بجماعة إرهابية، واتجاه إرادته إلى مباشرة ذلك النشاط.
2. **القصد الجنائي الخاص،** ويتمثل في انصراف إرادة الجاني إلى تحقيق غاية إرهابية معينة، كالترويج أو التمويل أو الدعم أو تسهيل الاتصال أو التدريب.

ومن ثم فإن مشروعية السلوك في ظاهره لا تحول دون قيام الجريمة متى ثبت اقترانه بهذا القصد الخاص.

- **ثالثاً: محل الجريمة والمصلحة محل الحماية:**

يستهدف المشرع من خلال هذا النص حماية مجموعة من المصالح الجوهرية، تتمثل في:

1. الأمن الرقمي وسلامة الفضاء الإلكتروني.
2. الأمن الفكري ومنع انتشار الفكر المتطرف.
3. الأمن القومي وحماية الدولة من التهديدات الإرهابية المستحدثة.

وهي مصالح جماعية عليا تتجاوز نطاق الحماية الفردية لتتصل بحماية كيان الدولة واستقرار المجتمع.

- **رابعاً: التكييف القانوني والتطبيقات العملية:**

في إطار النظرية العامة للجريمة يمكن تكييف الجريمة المنصوص عليها في المادة (45) باعتبارها جريمة تامة بمجرد ارتكاب السلوك المجرم، وجريمة مستقلة قائمة بذاتها وليست مجرد صورة من صور الاشتراك الجنائي، فضلاً عن كونها جريمة وقائية تستهدف مكافحة الخطر قبل تحوله إلى ضرر فعلي.

وتطبيقاً لذلك:

1. إذا أنشأ شخص موقعاً إلكترونياً باسم مستعار لنشر الفكر المتطرف، قامت الجريمة تامة بمجرد تحقق السلوك المجرم.
2. وإذا أعاد شخص نشر محتوى إرهابي دون علم بطبيعته أو مضمونه، انتفت مسؤوليته الجنائية لانتفاء القصد الجنائي، بينما تقوم المسؤولية متى ثبت العلم والإرادة.

3. وإذا قام مبرمج بتصميم منصة إلكترونية استُخدمت لاحقاً من قبل جماعة إرهابية، فإن مساءلته الجنائية تظل رهينة بثبوت علمه بالغرض غير المشروع أو تواطئه مع القائمين على النشاط الإرهابي.

- **ملخص:**

الجريمة المعلوماتية ذات الطابع الإرهابي:

لم يعد الخطر الإرهابي مرتبطًا بالفعل المادي التقليدي، بل أصبح يتشكل في الفضاء الإلكتروني قبل أن يتحقق في الواقع، ومن ثم، فإن النص محل الدراسة لا يُعاقب على النتيجة فقط، بل يُجرّم البنية التحتية الرقمية للإرهاب، وعلى ضوئه يمكن ملاحظة الآتي:

- **أولاً: التحليل المفاهيمي للنص محل الدراسة** (المادة 45):

- **تنص المادة (45) على أن:**

" يعاقب بالسجن كل من أنشأ موقع أو نشر معلومات على شبكة المعلومات الدولية أو إحدى الوسائل الإلكترونية لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقيادتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة، أو أية أدوات تستخدم في أعمال محظورة".

- **ويمكن تفكيك النص والتحليل البنيوي له كالآتي:** حيث نجده يتضمن نص المادة (45) عدة عناصر جوهرية:

1. **تعدد صور السلوك الإجرامي:**"إنشاء موقع، نشر معلومات، استخدام وسائل إلكترونية".
2. **ارتباط السلوك بجماعة إرهابية:**"بشكل مباشر أو تحت مسميات تمويهية".
3. **تعدد الأغراض الإجرامية:**"تسهيل الاتصال، الترويج، التمويل، التدريب ويتمثل في نشر طرق التصنيع".

- **الطبيعة القانونية لنص المادة (45) تمثل:**

أي ما نصت عليه من أفعال تكيف على النحو التالي:

1. جريمة خطر مجرد، وبحيث لا يشترط تحقق نتيجة مادية.
2. جريمة سلوك متعدد بحيث تتحقق بأي فعل من الأفعال المذكورة.
3. جريمة ذات قصد خاص، وبحيث يتطلب ارتباطها بغرض إرهابي.

- **ثانياً: الركن المادي في ضوء المادة** (45):

- **أ): السلوك الإجرامي:**

السلوك في هذا النص يتسم باتساع غير مسبوق، ويمكن تحليله إلى:

1. **السلوك الإنشائي،** ويتمثل في إنشاء موقع إلكتروني، وبالتحليل نجد هذا السلوك يمثل مرحلة تأسيس البنية الرقمية للإرهاب، وهو أخطر من الفعل اللاحق لأنه يخلق منصة دائمة.
2. **السلوك النشري،** أي نشر معلومات وعند التحليل. فلا يشترط أن تكون المعلومات سرية، أو مباشرة. بل يكفي مجرد أن تؤدي إلى خدمة الأهداف الإرهابية ولو بشكل غير مباشر.
3. **السلوك الاتصالي،** ويتمثل في تسهيل الاتصال بين العناصر الإرهابية، وعند التحليل نجده هنا يتحول الفعل إلى وساطة جنائية رقمية، وهو شكل مستحدث من المساهمة الجنائية.
4. **السلوك التدريبي،** ومناطه نشر كيفية تصنيع أدوات خطرة، وبتحليله نجده التحليل يمثل في نقل الخبرة الإجرامية، وهو ما يعادل في الفقه التقليدي "التحريض الفني".

- **ب): النتيجة الإجرامية:**

يلاحظ عليها من الناحية الجوهرية أن النص لا يشترط وقوع تفجير، أو تنفيذ عمل إرهابي بل يكتفي بتعريض المجتمع للخطر، وهذا يؤكد أن الجريمة؛ جريمة خطر لا ضرر، وهي جريمة وقائية.

- **ج): العلاقة السببية:**

في هذا النموذج التجريمي نجد أن العلاقة السببية مفترضة تشريعيًا، ولا تحتاج إلى إثبات مباشر لأن المشرع يفترض أن أي دعم رقمي هو تعزيز محتمل للنشاط الإرهابي.

- **ثالثاً: الركن المعنوي:**

في ضوء القراءة لنص المادة (45) نستخلص الآتي:

1. القصد الجنائي العام، وهو يتطلب العلم بطبيعة النشاط، والعلم بارتباطه بجماعة إرهابية.
2. القصد الخاص، وهو العنصر الحاسم بحيث يتجلى في نية الترويج أو الدعم أو التمويل.

- **نقطة دقيقة:**

حتى لو كان السلوك في ظاهره مشروعًا "مثل إنشاء موقع"، فإن القصد الخاص يُضفي عليه الصفة الإجرامية.

- **رابعاً: محل الجريمة:**

ويقصد به المصلحة التي أراد المشرع حمايتها، وهي تتمثل في التالي:

1. **الأمن الرقمي**، وسلامة الفضاء الإلكتروني.
2. **الأمن الفكري**، ومنع انتشار الفكر المتطرف.
3. **الأمن القومي**، وحماية الدولة من التهديدات غير التقليدية.

- **بالتدقيق في المصلحة محل الحماية:**

يتبين أنها مصلحة ليست فردية، بل مصلحة جماعية عليا تتعلق ببقاء الدولة.

- **خامساً: التكييف القانوني للنص في إطار النظرية العامة**

يمكن تكييف الجريمة وفقًا للمادة (45) على أنها:

1. جريمة تامة بمجرد الفعل لا حاجة لنتيجة.
2. جريمة مستقلة وليست مجرد اشتراك.
3. جريمة ذات طبيعة وقائية.

- **إشكالية فقهية:**

هل تعد هذه الجريمة صورة من صور الاشتراك؟ أم جريمة قائمة بذاتها؟ الرأي الذي نرجحه هي أنها جريمة مستقلة لأن المشرع جرم السلوك ذاته.

- **التطبيقات العملية:**

- **الحالة الأولى:** شخص أنشأ موقعًا باسم مستعار لنشر أفكار متطرفة.
  - **التكييف:** جريمة تامة وفق المادة (45).
- **الحالة الثانية:** شخص أعاد نشر محتوى إرهابي دون قصد.
  - **التكييف:** تنتفي المسؤولية إذا انعدم القصد، تقوم إذا ثبت العلم.
- **الحالة الثالثة:** مبرمج صمم منصة استخدمت لاحقًا من جماعة إرهابية.
  - **الإشكال:** هل يسأل؟ **الجواب:** يسأل إذا ثبت: العلم أو التواطؤ.

- **خاتمة الجزء الأول من المقرر:**

وفي ختام هذه المرحلة من دراستنا للنظرية العامة للقانون الجنائي المعلوماتي، يتبين لنا أن الجريمة المعلوماتية لم تعد مجرد صورة عابرة من صور الإجرام التقليدي، وإنما أصبحت تمثل نموذجًا إجراميًا مستقلاً له خصوصيته القانونية والفنية والتقنية، سواء من حيث محل الحماية الجنائية، أو طبيعة السلوك الإجرامي، أو خصائص الجاني، أو الوسائل المستعملة في ارتكاب الفعل المجرَّم، وقد كشف التطور الرقمي المعاصر عن تحوّل جوهري في مفهوم الجريمة ذاتها، إذ لم يعد الاعتداء مقصورًا على الأموال أو الأشخاص في صورتهم المادية، بل امتد ليشمل البيانات والمعطيات والأنظمة المعلوماتية بوصفها محالًا قانونية جديرة بالحماية الجنائية.

وقد حاول المشرّع الليبي، من خلال سن القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، أن يواكب هذا التحول، فتبنى تصورًا تشريعيًا حديثًا يقوم على حماية مزدوجة: حماية البنية التقنية للمعلوماتية ذاتها، وحماية الحقوق والمصالح التي قد تكون التقنية وسيلة للاعتداء عليها، ومن ثمّ، ظهر التمييز الجوهري بين الجريمة المعلوماتية التي يكون محلها النظام أو البيانات، وبين الجريمة التي تُرتكب بواسطة الوسائط الإلكترونية دون أن تكون المعلوماتية هي محل الاعتداء المباشر.

كما تبيّن لنا أن خصوصية الجريمة المعلوماتية لا تقف عند حدود طبيعتها الفنية، بل تمتد إلى خصوصية المجرم الإلكتروني ذاته، الذي يتميز – في الغالب– بامتلاكه خبرة تقنية وقدرة على استغلال الثغرات الرقمية، والعمل في بيئة افتراضية تتسم بالسرعة والعالمية وصعوبة التتبع، الأمر الذي يجعل من اكتشاف الجريمة وإثباتها وتعقب مرتكبيها أكثر تعقيدًا مقارنة بالجريمة التقليدية، وقد أدى ذلك إلى إعادة النظر في كثير من المفاهيم التقليدية المرتبطة بالمساهمة الجنائية، والفاعل الأصلي، والمسؤولية الجنائية، لتشمل – إلى جانب الشخص الطبيعي– الشخص المعنوي ومزودي خدمات الاتصالات وتقنية المعلومات، كل بحسب دوره ومدى سيطرته التقنية وقدرته على المنع أو الرقابة.

ومن خلال استعراض صور الجرائم المعلوماتية، اتضح أن هذا النمط الإجرامي يتسم بالتنوع والتطور المستمر، فيشمل جرائم الاعتداء على الأنظمة والبيانات، والتدليس والتزوير المعلوماتي، والاعتداء على الخصوصية والبيانات الشخصية، والملكية الفكرية، وحقوق المستهلك، فضلًا عن الجرائم الماسة بالأمن العام وتعطيل أعمال الحكومة والإضرار بالقيم الاجتماعية والأخلاقية، وهو ما يعكس اتساع نطاق الحماية الجنائية في البيئة الرقمية، وتحول الفضاء المعلوماتي إلى مجال قد تُرتكب فيه ذات الجرائم التقليدية ولكن بوسائل أكثر خطورة وتأثيرًا وانتشارًا.

وعليه، فإن التأصيل الموضوعي للجريمة المعلوماتية يقودنا بالضرورة إلى نتيجة مفادها أن القواعد التقليدية في قانون العقوبات – رغم أهميتها– لم تعد وحدها كافية لاستيعاب هذا النوع من الإجرام، بما يفرض ضرورة تطوير قواعد إجرائية خاصة تتلاءم مع طبيعة الدليل الرقمي، وخصوصية التفتيش والضبط والتحقيق والإثبات في البيئة الإلكترونية، فضلًا عن مشكلات الاختصاص القضائي والتعاون الدولي.

ومن هنا، فإن المرحلة القادمة من دراستنا ستنتقل من الجانب الموضوعي للجريمة المعلوماتية إلى جانبها الإجرائي، لنبحث خصوصية الإجراءات الجنائية في مواجهة هذا النوع من الجرائم، من حيث وسائل التحري الرقمي، وضبط الأدلة الإلكترونية[6]، والتفتيش المعلوماتي، وحجية الدليل الرقمي، وصعوبات الإثبات، ودور الجهات الفنية والقضائية في مكافحة الجرائم الإلكترونية، وذلك في ضوء أحكام القانون رقم (5 لسنة 2022م)، والقواعد العامة في قانون الإجراءات الجنائية الليبي، وصولًا إلى بناء تصور متكامل للنظام الجنائي المعلوماتي بشقيه الموضوعي والإجرائي.

الدليل الجنائي الرقمي:

يقصد بالدليل الجنائي الرقمي النتائج الفنية المستخلصة من تحليل البيانات والمعلومات المستمدة من أنظمة الحاسوب، وشبكات الاتصال، ووسائط التخزين الإلكترونية بمختلف أنواعها، بما يُسهم في كشف الحقيقة وإثبات الواقعة الإجرامية ونسبتها إلى مرتكبها.

وتبرز أهمية هذا الدليل في نطاق الجريمة المعلوماتية بالنظر إلى الطبيعة اللامادية التي تتسم بها هذه الجرائم، حيث ترتكب الأفعال الإجرامية عبر إشارات ونبضات إلكترونية غير مرئية، وفي مدد زمنية وجيزة قد لا تتجاوز أجزاء من الثانية، الأمر الذي يجعل آثارها بعيدة عن الإدراك الحسي المباشر، ويصعّب اكتشافها أو تتبعها بالوسائل التقليدية. كما تتفاقم خطورة هذا النوع من الجرائم بقدرة الجاني – بما يمتلكه من خبرة تقنية– على محو الأدلة الرقمية أو تعديلها أو إتلافها خلال وقت قصير، بما يعرقل الوصول إلى الحقيقة أو تحديد المسؤول عن الفعل الإجرامي.

[6] نصت المادة الأولى من القانون رقم (05 لسنة 2026م) على أن :"**الدليل الجنائي الرقمي**: هو نتائج تحليل البيانات من أنظمة الحاسوب أو شبكات الاتصال أو أجهزة التخزين الرقمية بمختلف أنواعها".

وقد أدرك المشرّع الليبي هذه الخصوصية، فنصّ في المادة (36)[7] من القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية على تجريم إتلاف الأدلة القضائية المعلوماتية أو إخفائها أو العبث بها بأي صورة كانت، بما يعكس اعترافاً تشريعياً بالطبيعة الهشة للدليل الرقمي وسهولة التأثير فيه مقارنة بالأدلة الجنائية التقليدية.

ويقصد بالدليل في المجال الجنائي الوسيلة التي يعتمد عليها القاضي في تكوين اقتناعه بثبوت الواقعة الإجرامية أو نفيها، وصولاً إلى الحقيقة القضائية التي يؤسس عليها حكمه، إذ يقوم الإثبات الجنائي على إقامة الدليل المشروع على وقوع الفعل المجرّم قانوناً، وتحديد عناصره، وإسناده إلى شخص معين بوصفه فاعلاً أو مساهماً فيه، تمهيداً لتحريك الدعوى الجنائية وتوقيع الجزاء المقرر قانوناً[8].

• الجزء الثاني:

أثر الجريمة المعلوماتية على قانون الإجراءات الجنائية

(خصوصية الجريمة المعلوماتية من الناحية الإجرائية)

تُعدّ الجريمة المعلوماتية من أخطر الظواهر الجنائية المستحدثة التي أفرزتها الثورة التقنية المعاصرة والتطور المتسارع في وسائل الاتصال ونظم المعلومات، إذ لم تعد الجريمة في مفهومها التقليدي مرتبطة بالمكان المادي أو الأثر المحسوس، وإنما تجاوزت ذلك إلى فضاء رقمي مفتوح تتشابك فيه شبكات الاتصال وقواعد البيانات والأنظمة الإلكترونية، بما أوجد صوراً إجرامية جديدة اتسمت بالتعقيد الفني والخطورة البالغة، وأصبحت تشكل تهديداً مباشراً للأمن المعلوماتي والاقتصادي والاجتماعي للدول والأفراد على السواء، ومن ثم، غدت الجريمة المعلوماتية أحد أبرز التحديات التي تواجه السياسة

---

[7] تنص المادة (36) من القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية في (إتلاف الأدلة القضائية الرقمية) على أنه :"يعاقب بالسجن مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن (10.000) عشرة آلاف دينار ولا تزيد على (100.000) مائة ألف دينار كل من قام بإتلاف أدلة قضائية معلوماتية أو بإخفائها أو التعديل فيها أو محوها أو العبث بها بأي شكل من الأشكال".

[8] ومن المبادئ المستقرة في الإثبات الجنائي أن الأصل في الإنسان البراءة، وأن عبء الإثبات يقع على عاتق سلطة الاتهام، باعتبار أن الادعاء بارتكاب الجريمة يمثل خروجاً على أصل البراءة المفترض قانوناً، ومن ثم فلا يجوز المساس بحرية الفرد أو إدانته إلا بناءً على دليل مشروع يقيني تتوافر فيه عناصر المشروعية والكفاية والإقناع القضائي.

الجنائية الحديثة، لما تنطوي عليه من اعتداءات تمس سلامة البيانات والمعلومات والأنظمة الإلكترونية، نتيجة الاستخدام غير المشروع لتقنيات الحاسوب ووسائل الاتصال الرقمية.

وتتميّز هذه الجريمة بخصوصية فنية وإجرائية تميزها عن غيرها من الجرائم التقليدية، فهي جريمة ترتكب في بيئة افتراضية خفية، يغلب عليها الطابع التقني الدقيق، وغالباً ما تصدر عن فاعل يمتلك قدراً عالياً من المعرفة الرقمية والخبرة الفنية في مجال البرمجيات وتقنيات الاتصال ونظم المعلومات. فالمجرم المعلوماتي لا يمثل – في الغالب– الصورة التقليدية للمجرم، وإنما هو شخص متمكن من أدوات التقنية الحديثة، يحيط علماً بالثغرات الأمنية وأساليب الاختراق وطرق تجاوز أنظمة الحماية، الأمر الذي يمكنه من توظيف هذه المعارف بصورة غير مشروعة للاعتداء على البيانات أو الأنظمة الإلكترونية، سواء بالتلاعب أو الإتلاف أو التعطيل أو الاستيلاء أو تحقيق منفعة غير مشروعة.

ولما كانت الجريمة المعلوماتية قد اتخذت طابعاً متطوراً ومتسارعاً من حيث الوسائل والأساليب، فقد أصبح من الضروري إرساء تشريعات وطنية ودولية متخصصة تتولى تنظيم هذا النمط المستحدث من الإجرام، من خلال بناء سياسة جنائية معلوماتية متكاملة تقوم على تحديد مفهوم الجريمة الإلكترونية وضبط أركانها وعناصرها الفنية والقانونية، إلى جانب تنظيم الأحكام الموضوعية والإجرائية اللازمة لمواجهتها، بما يحقق التوازن بين متطلبات حماية الأمن المعلوماتي وضمان الحقوق والحريات الرقمية.

وفي هذا السياق، اتجه المشرّع الليبي إلى إصدار القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية بوصفه إطاراً تشريعياً خاصاً يهدف إلى حماية الفضاء الرقمي الوطني، وتجريم الأفعال الواقعة على نظم المعلومات والبيانات والشبكات الإلكترونية، فضلاً عن وضع قواعد للحماية الجنائية الموضوعية والإجرائية المتعلقة بالمعاملات الإلكترونية والأدلة الرقمية، وقد تبنى هذا القانون سياسة جنائية حديثة ترمي إلى تعزيز الثقة في البيئة الرقمية، وتوفير الحماية القانونية للأنظمة المعلوماتية، ومواجهة صور الاعتداء الإلكتروني التي تستهدف أمن المجتمع واستقراره.

ومن المقرر فقهاً وتشريعاً أن نجاح السياسة الجنائية لا يقاس بمجرد سنّ النصوص العقابية أو تشديد الجزاءات، وإنما يقاس بمدى قدرتها على تحقيق الغاية التي شرعت من أجلها بفاعلية وكفاءة، وفي إطار من التوازن بين مقتضيات الردع وضمانات الحقوق والحريات. فالتشريع الجنائي الناجح هو الذي يحقق الحماية القانونية بأقل قدر ممكن من التعقيد الإجرائي والكلفة العملية، دون أن يفضي تطبيقه إلى نتائج سلبية تتجاوز مقاصده التشريعية.

وفي مجال مكافحة الجريمة المعلوماتية، يتجلى معيار النجاح في قدرة المنظومة القانونية على الحد من صور الاعتداء الإلكتروني، وضبط مرتكبيها في بيئة تقنية معقدة، مع تجنب الآثار السلبية التي قد تمس الخصوصية الرقمية أو حرية تداول المعلومات أو سلامة المعاملات الإلكترونية، لاسيما في ظل اتساع نطاق وسائل المراقبة والتحري الرقمي.

وإذا كان الاهتمام الدولي بمواجهة الجريمة المعلوماتية قد شهد تطوراً ملحوظاً من حيث التنظيم التشريعي والتعاون الفني والقضائي، فإن الجهود الإقليمية العربية – على أهميتها– ما تزال في كثير من الأحيان تعاني قصوراً في بناء رؤية علمية وتقنية متكاملة لمواجهة هذا النوع من الجرائم، إذ انصبت أغلب الدراسات والمؤتمرات المتخصصة على الجوانب الموضوعية المتعلقة بالتجريم والعقاب والتكييف القانوني، في حين لم تحظَ الجوانب الإجرائية بالعناية الكافية، رغم أنها تمثل الركيزة الأساسية لتحقيق الفعالية العملية للحماية الجنائية المعلوماتية.

ومن ثم، فإن مواجهة الظاهرة الإجرامية المعلوماتية لا تتحقق بمجرد وضع قواعد التجريم والعقاب، وإنما تقتضي – بالضرورة– بناء منظومة إجرائية جنائية دقيقة تضبط وسائل البحث والتحري والتحقيق والمحاكمة في البيئة الرقمية؛ إذ لا يكفي أن يقرر المشرّع الحماية الموضوعية للحق، ما لم يضع الوسائل الإجرائية الكفيلة بصيانته وضمان تنفيذه عملياً أمام القضاء الجنائي.

ولذلك، اتجهت غالبية الدراسات القانونية العربية إلى بحث موضوعات الحماية الجنائية للمعلومات، والتكييف القانوني للبيانات الإلكترونية، وحجية المستخرجات الرقمية أمام القضاء، ومسؤولية مستخدمي نظم الحاسب الآلي، ومدى ملاءمة التشريعات التقليدية لمواجهة الجرائم المرتكبة عبر البيئة الرقمية، فضلاً عن دراسة العلاقة بين القواعد الجنائية التقليدية والتشريعات المنظمة لتداول المعلومات عبر شبكات الاتصال الحديثة.

ومن زاوية الاستخدام الإجرامي لتقنيات الحاسوب والاتصال، يمكن القول إن لهذه الوسائط ثلاثة أدوار رئيسة في النشاط الإجرامي المعاصر؛ فهي أولاً تمثل وسيلة تقنية متطورة لارتكاب الجرائم التقليدية بصورة أكثر سرعة وفاعلية، كما في جرائم الاحتيال الإلكتروني والتزوير الرقمي والنصب عبر الشبكات المعلوماتية، وهي ثانياً تمثل محلاً مباشراً للاعتداء الإجرامي عندما تستهدف الجريمة الأنظمة المعلوماتية أو البيانات أو البرامج ذاتها، من خلال الاختراق غير المشروع أو الاستيلاء على البيانات أو اعتراضها أو تعطيلها أو إتلافها باستخدام البرمجيات الخبيثة والفيروسات الإلكترونية، وهي صور جرمها المشرّع الليبي صراحة ضمن أحكام القانون رقم (5 لسنة 2022م).

أما الدور الثالث، فيتمثل في كون البيئة الرقمية أصبحت فضاءً خصباً لاحتضان الأنشطة غير المشروعة وتسهيل ارتكاب الجرائم العابرة للحدود، كالاتجار بالمخدرات والمؤثرات العقلية، والاتجار بالبشر، ونشر المواد الإباحية، والتحريض على الإرهاب أو العنف، وغسل الأموال الإلكتروني، وغيرها من صور الإجرام السيبراني المنظم، وهي جرائم أفرد لها المشرّع الليبي تنظيماً خاصاً وعقوبات مشددة بالنظر إلى خطورتها على أمن المجتمع والدولة.

وتبرز الإشكاليات الإجرائية بوصفها من أكثر التحديات تعقيداً في مجال الجريمة المعلوماتية، إذ تواجه سلطات الضبط والتحقيق والقضاء صعوبات فنية وقانونية تتعلق بعمليات التحري الرقمي، والتفتيش الإلكتروني، وضبط الأدلة الجنائية الرقمية، ومراقبة الاتصالات، فضلاً عن إشكالات الاختصاص القضائي والقانون الواجب التطبيق، خاصة في ظل الطبيعة العابرة للحدود التي تتسم بها الجرائم الإلكترونية، حيث قد يرتكب السلوك الإجرامي في دولة، بينما تتحقق نتيجته في دولة أخرى، أو تكون البيانات والخوادم محل الجريمة موزعة عبر نطاقات قانونية متعددة، الأمر الذي يثير تنازعاً بين الاختصاصات القضائية الوطنية.

كما تتميز الجريمة المعلوماتية بصعوبة إثباتها من الناحية العملية، لكونها لا تخلّف – في الغالب– آثاراً مادية ظاهرة كالتي تخلفها الجرائم التقليدية، إذ تقع على بيانات وأنظمة افتراضية قد تُمحى أو تُعدل في لحظات معدودة دون أن تترك أثراً مادياً محسوساً، مما يجعلها جريمة صامتة ترتكب في الخفاء ويصعب اكتشافها أو تتبعها بوسائل الإثبات التقليدية.

ويزداد الأمر تعقيداً بالنظر إلى أن هذا النوع من الجرائم يُرتكب غالباً عن بُعد، بحيث لا يكون الجاني موجوداً في مسرح الجريمة بالمعنى التقليدي، وإنما قد يمارس نشاطه الإجرامي من دولة أخرى مستفيداً من الطبيعة اللامركزية لشبكات الاتصال الدولية، وهو ما يضاعف من صعوبة تعقبه وإخضاعه للولاية القضائية الوطنية.

ويضاف إلى ذلك ما يُعرف في الفقه الجنائي بـ"الرقم الأسود للجريمة المعلوماتية"، والمتمثل في امتناع كثير من الضحايا عن الإبلاغ عن الجرائم الإلكترونية التي يتعرضون لها، إما لعدم اكتشافها ابتداءً، أو خشية المساس بسمعتهم التجارية أو بسرية بياناتهم أو بمراكزهم المالية، الأمر الذي يؤدي إلى انخفاض معدلات الكشف الرسمي عن هذه الجرائم، ويؤثر سلباً في فعالية السياسة الجنائية والإحصاءات المتعلقة بها.

كما تثير مرحلة المحاكمة بدورها إشكالات قانونية معقدة تتعلق بتنازع الاختصاص القضائي والقانون الواجب التطبيق، لاسيما وأن الجريمة المعلوماتية قد تمس في وقت واحد عدة أنظمة قانونية وسيادية، وهو ما استدعى من المشرّع الليبي التوسع في نطاق السريان المكاني للقانون، بإخضاع الجرائم الإلكترونية لأحكامه متى ارتكبت كلها أو بعضها داخل الدولة، أو امتدت آثارها إلى الداخل الليبي ولو ارتكبت خارج الإقليم الوطني.

وتقتضي خصوصية هذا النوع من الجرائم الاعتماد على وسائل فنية متخصصة في جمع الأدلة الرقمية وتحليلها وحفظها، وتتمثل أهم الإجراءات الجنائية ذات الصلة في المعاينة الرقمية، والضبط الإلكتروني، والتفتيش المعلوماتي، ومراقبة الاتصالات والمحادثات الإلكترونية، والاستجواب، والمواجهة، وسماع الشهود، وندب الخبراء الفنيين المختصين بتحليل الأنظمة والبيانات الرقمية.

ومن المبادئ المستقرة في قانون الإجراءات الجنائية أن سلطة التحقيق لا تلتزم باتباع ترتيب معين في مباشرة إجراءات التحقيق، كما أنها غير ملزمة باتخاذ جميع الإجراءات المنصوص عليها، وإنما تباشر منها ما تقتضيه مصلحة التحقيق وظروف الدعوى وخصوصية الواقعة محل البحث، ويكتسب هذا المبدأ أهمية خاصة في نطاق الجرائم المعلوماتية بالنظر إلى طبيعتها التقنية المتغيرة وسرعة اندثار أدلتها الرقمية، الأمر الذي يفرض على سلطات التحقيق قدراً واسعاً من المرونة الفنية والإجرائية في مباشرة أعمال البحث والتحري والكشف عن الحقيقة الجنائية.

- **الفصل الأول:**

الأحكام الإجرائية للجريمة المعلوماتية.

(الخصوصية الإجرائية للجريمة المعلوماتية)

لما كانت الجريمة المعلوماتية تُعد من الجرائم ذات الطبيعة الخاصة، بما تنفرد به من خصائص فنية وتقنية معقدة، وبما تتسم به من طابع غير مادي وعابر للحدود الوطنية، فإنها تثير إشكاليات قانونية وإجرائية تختلف في جوهرها عن تلك التي تثيرها الجرائم التقليدية.

فهي لا تُرتكب في الغالب بوسائل مادية محسوسة، وإنما تقع عبر نبضات وإشارات إلكترونية غير مرئية، تستهدف البيانات والأنظمة والشبكات المعلوماتية داخل فضاء رقمي مفتوح، الأمر الذي يجعل من وسائل الإثبات التقليدية وإجراءات البحث والتحقيق المنصوص عليها في قانون الإجراءات الجنائية

التقليدي عاجزة – في كثير من الأحيان– عن الإحاطة بهذا النمط المستحدث من الإجرام المعلوماتي أو مواكبة خصوصية الأدلة الإلكترونية المرتبطة به.

ومن ثم، أضحى من الضروري إرساء منظومة إجرائية جنائية خاصة تتلاءم مع الطبيعة اللامادية للجريمة المعلوماتية، وتستجيب لخصوصيتها التقنية والإقليمية، بما يكفل فعالية البحث والتحري والتحقيق والمحاكمة في هذا المجال، ويحقق التوازن بين مقتضيات مكافحة الإجرام المعلوماتي وضمانات الشرعية الإجرائية وحماية الحقوق والحريات الرقمية.

وعليه، سوف نتناول قصور القواعد الإجرائية التقليدية في مواجهة الأدلة الإلكترونية والاعتداءات غير المادية في **(المبحث الأول)**، ثم نبين ملامح القواعد الإجرائية الجنائية الخاصة الملائمة لطبيعة الجريمة المعلوماتية في **(المبحث الثاني)**.

- **المبحث الأول:**

محدودية قواعد الإجراءات التقليدية في مجابهة الجريمة المعلوماتية.

أفرزت الجريمة المعلوماتية تحديات إجرائية غير مسبوقة، كشفت عن محدودية القواعد التقليدية الواردة في قانون الإجراءات الجنائية في استيعاب الخصوصية الفنية والتقنية لهذا النمط المستحدث من الإجرام. فالقواعد الإجرائية التقليدية قد وُضعت أساساً لمواجهة جرائم مادية تقع في نطاق مكاني محسوس وتترك آثاراً مادية ظاهرة يمكن إدراكها ومعاينتها وضبطها بوسائل الإثبات التقليدية، في حين أن الجريمة المعلوماتية تقوم – في الغالب– على الاعتداء على البيانات والأنظمة الرقمية داخل بيئة افتراضية تتسم بالخفاء والسرعة والطابع العابر للحدود، الأمر الذي يجعل وسائل الاستدلال والبحث والتحري والإثبات التقليدية عاجزة، في كثير من الأحيان، عن ملاحقة هذا النوع من الجرائم المعلوماتية بكفاءة وفعالية.

وعلى الرغم من أن المشرّع الليبي قد تدخل بموجب القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية لوضع إطار موضوعي لتجريم الأفعال الواقعة على الأنظمة والشبكات المعلوماتية وتقرير الحماية الجنائية لها، إلا أن هذا التدخل لم يصاحبه – بالقدر ذاته– تطوير موازٍ لقواعد الإجراءات الجنائية بما يتلاءم مع خصوصية الجريمة المعلوماتية وطبيعة الدليل الرقمي، الأمر الذي أوجد فراغاً إجرائياً يثير العديد من الصعوبات العملية في مرحلة الاستدلال والتحقيق والإثبات الجنائي، ومن ثم، تقتضي الدراسة بيان أوجه القصور التي تعتري القواعد الإجرائية التقليدية في مواجهة الجريمة المعلوماتية، وذلك من خلال تناول صعوبة معاينة مسرح الجريمة المعلوماتية في **(المطلب الأول)**، ثم

بيان قصور إجراءات الاستدلال والتحقيق التقليدية عن إثبات الجريمة المعلوماتية، أو إشكاليات الإجراءات الجنائية في مجال الجريمة الإلكترونية في **(المطلب الثاني)**.

- **المطلب الأول:**

صعوبة معاينة مسرح الجريمة المعلوماتية.

تُعدّ مُعاينة مسرح الجريمة من أهم الإجراءات الأولية في الدعوى الجنائية، لما تمثله من وسيلة جوهرية في الكشف عن الحقيقة وجمع الأدلة والمحافظة على الآثار المادية المرتبطة بالفعل الإجرامي. غير أن هذا الإجراء يواجه صعوبات استثنائية في نطاق الجريمة المعلوماتية، بالنظر إلى الطبيعة اللامادية واللااقليمية لهذا النوع من الجرائم، إذ لا يقع الاعتداء في مسرح مادي تقليدي يمكن تطويقه أو معاينته بالوسائل المعتادة، وإنما يتم داخل بيئة رقمية افتراضية تتداخل فيها الأنظمة والشبكات والبيانات الإلكترونية، وقد تمتد عناصرها عبر عدة نطاقات جغرافية في وقت واحد.

وتزداد خطورة هذه الصعوبة بالنظر إلى قابلية الدليل الرقمي للمحو أو التعديل أو الإخفاء في لحظات معدودة، فضلاً عن افتقار الآثار الإلكترونية إلى الطابع المادي الظاهر الذي تستند إليه إجراءات المعاينة التقليدية، ومن ثم، فإن معاينة مسرح الجريمة المعلوماتية **(الفرع الثاني)** تقتضي خبرة فنية متخصصة ووسائل تقنية دقيقة تتجاوز المفهوم التقليدي للمعاينة الجنائية **(الفرع الأول)**، بما يكفل الحفاظ على سلامة الدليل الرقمي وضمان حجيته في الإثبات الجنائي.

- **الفرع الأول:**

مدى مواءمة المُعاينة التقليدية لطبيعة مسرح الجريمة المعلوماتية.

تكشف نصوص قانون الإجراءات الجنائية الليبي، ولا سيما المواد (11)، و(14)، و(21)[9]، و(74)[10]إجراءات، عن أن المشرّع قد بنى قواعد المعاينة والاستدلال والتحقيق الجنائي على أساس

---

[9] تنص المادة (21) في (الانتقال إلى محل الواقعة) على أنه :"يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى محل الواقعة ويعاين الآثار المادية للجريمة ويحافظ عليها ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، ويسمع أقوال من كان حاضراً أو من يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبها، ويجب عليه أن يخطر النيابة العامة فوراً بانتقاله. ويجب على النيابة العامة بمجرد إخطارها بجناية متلبس بها الانتقال فورا إلى محل الواقعة".

[10] تنص المادة (74) في (انتقال المحقق) على أنه :"ينتقل المحقق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة مادياً وكل ما يلزم إثبات حالته".

الجرائم التقليدية ذات الطبيعة المادية، التي تقع في نطاق مكاني محسوس وتخلّف آثاراً ظاهرة يمكن إدراكها بالحواس وضبطها بالوسائل الفنية المعتادة، وبحيث خولت هذه النصوص مأموري الضبط القضائي وسلطات التحقيق صلاحية الانتقال إلى محل الواقعة، ومعاينة الآثار المادية للجريمة، وإثبات حالة الأماكن والأشخاص والأشياء، واتخاذ التدابير التحفظية اللازمة للمحافظة على أدلة الجريمة، وهي إجراءات تقوم – في جوهرها– على وجود مسرح جريمة مادي ثابت يمكن السيطرة عليه ومعاينته بصورة مباشرة[11].

غير أن هذا التصور الإجرائي التقليدي يثير إشكالات جوهرية عند تطبيقه على الجريمة المعلوماتية، بالنظر إلى الطبيعة الخاصة التي تتسم بها هذه الجرائم، فهي ترتكب داخل بيئة رقمية افتراضية لا تخضع للمفهوم التقليدي للمكان، ولا تخلّف – في الغالب– آثاراً مادية محسوسة بالمعنى المقصود في قواعد المعاينة التقليدية.

فمسرح الجريمة المعلوماتية قد يمتد عبر أجهزة وخوادم وشبكات معلوماتية موزعة في أكثر من نطاق جغرافي، كما أن محل الاعتداء ذاته يتمثل في بيانات أو نظم إلكترونية غير مرئية، الأمر الذي يجعل الانتقال المادي إلى "محل الواقعة" وفق المفهوم التقليدي الوارد بالمادة (21) إجراءات، غير كافٍ للإحاطة بكافة عناصر الجريمة الإلكترونية أو ضبط آثارها الفنية.

كما أن اشتراط معاينة "الآثار المادية للجريمة" يثير صعوبة عملية في نطاق الجرائم المعلوماتية، ذلك أن الدليل الرقمي يتميز بطبيعته اللامادية، وقابليته السريعة للمحو أو التعديل أو الإخفاء، وقد يوجد في صورة إشارات إلكترونية أو ملفات مشفرة أو بيانات مخزنة عن بعد، وهو ما يقتضي الاستعانة بوسائل تقنية متخصصة وخبرات فنية دقيقة تختلف بطبيعتها عن إجراءات المعاينة التقليدية المقررة للجرائم العادية.

ورغم أن المادة (14)[12]إجراءات، قد منحت رجال الضبط القضائي سلطة اتخاذ "جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة"، وهي عبارة تتسم بقدر من العمومية يسمح – من

---

[11] .. تنص المادة (11) في (سلطات رجال الضبط القضائي) على أنه :"يقوم مأمورو الضبط القضائي بالبحث عن الجرائم ومرتكبيها، وجمع الاستدلالات التي تلزم للتحقيق والدعوى".

[12] تنص المادة (14) في فقرتها الثانية، على أنه :"ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على جميع الإيضاحات، ويجروا المعاينات اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم، أو التي يعلنون بها بأية كيفية كانت. وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة".

الناحية التفسيرية– بامتدادها إلى الأدلة الرقمية، إلا أن المشرّع لم يضع تنظيماً إجرائياً دقيقاً يبين كيفية جمع الدليل الجنائي الإلكتروني أو حفظه أو فحصه أو ضمان سلامة حجيته الفنية والقانونية، الأمر الذي يكشف عن قصور تشريعي واضح في مواكبة خصوصية الجريمة المعلوماتية ومتطلبات الإثبات الجنائي الرقمي.

ويزداد هذا القصور وضوحاً عند مقارنة أحكام قانون الإجراءات الجنائية بأحكام القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، الذي توسع في تجريم صور متعددة من الاعتداءات الواقعة على البيانات والأنظمة والشبكات الإلكترونية، وأقر مفاهيم حديثة كالدليل الجنائي الرقمي، والاختراق غير المشروع، واعتراض البيانات[13]، وإتلاف الأدلة المعلوماتية[14]، دون أن يقابل ذلك بتنظيم إجرائي متكامل يحدد ضوابط المعاينة الرقمية، وآليات التفتيش الإلكتروني، وكيفية ضبط الأدلة الجنائية المعلوماتية وحفظها بما يتلاءم مع طبيعتها التقنية الخاصة[15].

ومن ثم، يتبين أن القواعد الإجرائية التقليدية، وإن كانت تشكل أساساً عاماً لإجراءات الاستدلال والتحقيق؛ إلا أنها تظل محدودة الفاعلية في مواجهة الجريمة المعلوماتية، ما لم تُدعّم بمنظومة إجرائية متخصصة تستجيب لخصوصية البيئة الرقمية، وتواكب التطور التقني المتسارع في وسائل ارتكاب الجرائم الإلكترونية وأساليب إثباتها.

---

[13] **يلاحظ**: أن اعتراض البيانات في نطاق الجرائم المعلوماتية، فيقصد به التقاط أو مراقبة أو الحصول – بغير وجه حق– على البيانات أو المعلومات المتداولة عبر الأنظمة المعلوماتية أو شبكات الاتصال أثناء انتقالها أو بثها أو استقبالها، سواء تم ذلك بصورة مباشرة عبر النفاذ إلى النظام المعلوماتي، أو بصورة غير مباشرة عن طريق التنصت الإلكتروني أو وسائل الالتقاط التقنية، وقد أخذت بهذا المفهوم التشريعات المقارنة والاتفاقيات الدولية، ولا سيما اتفاقية بودابست بشأن الجرائم الإلكترونية التي جرّمت الاعتراض غير المشروع للبيانات المتبادلة عبر الأنظمة والشبكات المعلوماتية، باعتباره اعتداءً على سرية الاتصالات والبيانات الرقمية.

[14] تنص المادة (36) من القانون رقم (05 لسنة 2022م) في (إتلاف الأدلة القضائية الرقمية) على أنه :"يعاقب بالسجن مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن (10.000) عشرة آلاف دينار ولا تزيد على (100.000) مائة ألف دينار كل من قام بإتلاف أدلة قضائية معلوماتية أو بإخفائها أو التعديل فيها أو محوها أو العبث بها بأي شكل من الأشكال".

[15] تنص المادة من القانون رقم (05 لسنة 2022م) على أن :"**الاختراق**: هو القدرة على الوصول إلى أي وسيلة تقنية المعلومات بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة". كما نصت على أن :"**الالتقاط أو الاعتراض** : مشاهدة البيانات أو المعلومات أو الحصول عليها".

- **الفرع الثاني:**

رؤية فقهية في مُعاينة مسرح الجريمة المعلوماتية.

لم يضع المشرّع تعريفاً محدداً للمعاينة الجنائية، الأمر الذي ترك للفقه مهمة تحديد مفهومها وبيان نطاقها، وقد استقر الفقه الجنائي على تعريف المعاينة بأنها مشاهدة أو فحص يباشره القائم بالتحقيق لمكان أو شخص أو شيء، بقصد إثبات حالته وضبط كل ما يفيد في كشف الحقيقة وإظهار الدليل، وتستلزم المعاينة – بهذا المعنى– الانتقال إلى محل الواقعة أو ما يعرف بمسرح الجريمة، وهو المكان الذي وقعت فيه الأفعال الإجرامية وخلفت آثاراً مادية يمكن الاستدلال بها على الجريمة ومرتكبها.

ولأهمية هذا الإجراء، اتجهت بعض التشريعات الإجرائية المقارنة إلى تجريم كل تغيير أو عبث بمسرح الجريمة قبل مباشرة سلطات الاستدلال والتحقيق للمعاينة الأولية، حمايةً للأدلة والمحافظة على سلامتها، مع استثناء الحالات التي يقتضيها الحفاظ على الأمن العام أو المصلحة العامة.

إلا أن فكرة "مسرح الجريمة" في نطاق الجريمة المعلوماتية تختلف بصورة جوهرية عن مفهومها التقليدي، إذ يتضاءل دور المُعاينة المادية في الكشف عن الحقائق والأدلة، ويرجع ذلك إلى سببين رئيسين: **أولهما:** أن الجريمة المعلوماتية قلّما تخلّف آثاراً مادية محسوسة، باعتبار أن محل الاعتداء فيها ينصب – في الغالب– على البيانات والبرامج والأنظمة المعلوماتية، وهي عناصر ذات طبيعة رقمية غير مرئية، **وثانيهما:** أن الفترة الزمنية الفاصلة بين وقوع الجريمة واكتشافها تكون – في كثير من الأحيان– طويلة نسبياً، بما يسمح بتعدد الأشخاص المترددين على مسرح الجريمة، ويمنح الجاني أو شركاءه فرصة العبث بالأدلة أو تعديلها أو إتلافها، إن وجدت.

ولذلك، ذهب جانب من الفقه الجنائي المعلوماتي إلى ضرورة مراعاة مجموعة من الضوابط الفنية والإجرائية عند معاينة مسرح الجريمة المعلوماتية، يُمكن إجمالها فيما يأتي:

1. ضرورة تحديد أجهزة الحاسب الآلي والأنظمة المعلوماتية الموجودة بمكان المعاينة، وتحديد مواقعها بصورة دقيقة وفي أسرع وقت ممكن، مع البحث عن خوادم الشبكات عند وجود اتصال شبكي، وذلك بغرض تعطيل الاتصالات ومنع محو الأدلة أو العبث بها. كما ينبغي تصوير الأجهزة، لاسيما أجزاؤها الخلفية والتوصيلات المتصلة بها، مع إثبات تاريخ وزمان ومكان التقاط الصور.
2. فرض حراسة كافية على مسرح الجريمة المعلوماتية، ومراقبة الحركة داخله، ورصد الاتصالات الواردة والصادرة منه، مع تعطيل أجهزة الاتصال أو الهواتف المحمولة التي قد تستخدم –

بوسائل تقنية معينة– في إتلاف الأدلة الرقمية أو محو البيانات المخزنة على الأجهزة محل المعاينة.

3. ملاحظة الكيفية الفنية التي أُعد بها النظام المعلوماتي، والآثار الإلكترونية التي يخلّفها، وفحص السجلات الرقمية الخاصة بالشبكات لمعرفة مواقع الاتصال ونوعية الأجهزة المستخدمة، والاستفادة من بروتوكولات الاتصال عبر الإنترنت وعناوين[16] (IP Address) في تتبع النشاط الإجرامي والكشف عن مصدر الاتصال، إذ إن مستخدم شبكة الإنترنت يترك – غالباً– آثاراً رقمية أثناء تنقله بين المواقع، يُمكن الاستفادة منها في عملية التتبع والتحليل الجنائي الرقمي.
4. إثبات حالة التوصيلات والكابلات والملحقات المرتبطة بمكونات النظام المعلوماتي، حتى يتسنى تحليل البيانات لاحقاً ومقارنتها واستخلاص الدليل الفني منها عند عرض النزاع أمام قاضي الموضوع.
5. عدم التسرع في نقل الأجهزة أو الوسائط المعلوماتية خارج مسرح الجريمة قبل التأكد من خلو البيئة المحيطة من المجالات المغناطيسية أو المؤثرات التقنية التي قد تؤدي إلى إتلاف البيانات أو محوها، وهو أمر لا يتحقق إلا بالاستعانة بخبراء متخصصين في مجال الحاسوب وتقنيات المعلومات.
6. التحفظ على محتويات سلة المهملات، وما قد تتضمنه من أوراق ممزقة أو أقراص أو وسائط ممغنطة تالفة أو محطمة، مع رفع البصمات عنها متى أمكن ذلك، بالإضافة إلى التحفظ على مستندات الإدخال والمخرجات الورقية والوثائق ذات الصلة بالنظام المعلوماتي محل الجريمة.
7. قصر إجراءات المعاينة الرقمية على الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال المعلوماتية وتحليل الأنظمة واسترجاع البيانات، بالنظر إلى الطبيعة التقنية الدقيقة لهذا النوع من الجرائم.

وتكشف هذه الضوابط عن أن معاينة مسرح الجريمة المعلوماتية تقتضي قدراً كبيراً من التأهيل الفني والخبرة التقنية، إلى جانب توافر وسائل بحث وتحقيق متطورة تتلاءم مع طبيعة الأدلة الرقمية،

---

[16] عنوان بروتوكول الإنترنت :(IP Address) هو معرّف رقمي يُخصَّص لكل جهاز متصل بشبكة معلوماتية، ويُستخدم لتمييزه وتحديد موقعه المنطقي على الشبكة بما يتيح تبادل البيانات وتوجيه الاتصالات الإلكترونية بين الأجهزة، ويكتسب أهمية خاصة في مجال التحقيق الجنائي المعلوماتي باعتباره أحد الآثار الرقمية التي يمكن الاستناد إليها في تتبع مصدر النشاط الإلكتروني وربط بعض الأفعال الإجرامية بجهاز أو اتصال معين، مما يجعله من الوسائل الفنية المساعدة في جمع الأدلة الرقمية والكشف عن مرتكبي الجرائم المعلوماتية.

وهو ما يبرز قصور قانون الإجراءات الجنائية التقليدي عن استيعاب هذه المتطلبات الفنية المتخصصة، فضلاً عن محدودية الخبرة المعلوماتية لدى كثير من مأموري الضبط القضائي، وقصور الوسائل التقنية المتاحة لهم في مجال مكافحة الجرائم الإلكترونية.

- **المطلب الثاني:**

إشكاليات الإجراءات الجنائية في مجال الجريمة الإلكترونية.

أفرز التطور المتسارع في تقنيات المعلومات والاتصالات، وما صاحبه من توسع غير مسبوق في استخدام الوسائط الرقمية وشبكات الإنترنت، أنماطًا مستحدثة من السلوك الإجرامي تجاوزت في طبيعتها وحدودها المفهوم التقليدي للجريمة، الأمر الذي أدى إلى بروز ما يُعرف بالجريمة الإلكترونية بوصفها أحد أخطر التحديات التي تواجه السياسة الجنائية المعاصرة. فقد اتسمت هذه الجرائم بخصائص تقنية معقدة، من أبرزها سهولة ارتكابها، وسرعة انتشار آثارها، وعابريتها للحدود، فضلًا عن صعوبة اكتشاف مرتكبيها وإثبات أفعالهم بالوسائل التقليدية للإثبات الجنائي.

ولم يعد من الكافي مواجهة هذا النمط الإجرامي المستحدث من خلال القواعد الموضوعية التي تقتصر على التجريم والعقاب، وإنما يقتضي الأمر تدخل المشرع الليبي لوضع إطار إجرائي خاص يواكب الطبيعة الفنية والتقنية للجريمة الإلكترونية كما هو حال التشريعات الحديثة، وبما يكفل تحقيق التوازن بين مقتضيات حماية المجتمع من مخاطر الإجرام المعلوماتي، وبين ضمان احترام الحقوق والحريات الفردية المكفولة دستوريًا، ولاسيما الحق في الخصوصية وسرية البيانات والمراسلات الإلكترونية.

وانطلاقًا من خصوصية الدليل الرقمي ومتطلبات البحث عنه وضبطه[17]، تبرز الحاجة إلى تقييم مدى كفاية الإجراءات الجنائية التقليدية لاستيعاب هذا النمط المستحدث من الأدلة، وما يثيره استحداث إجراءات خاصة بالتحري والتحقيق الإلكتروني من نقاش فقهي وقانوني بشأن مشروعيتها وضماناتها. لذلك، نتناول في (الفرع الأول) قصور الإجراءات التقليدية في تحصيل الدليل الرقمي، وفي (الفرع الثاني) الجدل الفقهي المتعلق بمشروعية إجراءات التحري والتحقيق في الجرائم الإلكترونية.

[17] يقصد بخصوصية الدليل الرقمي ومتطلبات البحث عنه وضبطه أن الدليل المستمد من البيئة الإلكترونية يتميز بطبيعته غير المادية وسهولة تعديله أو محوه وانتشاره عبر الأنظمة والشبكات، مما يقتضي اتباع إجراءات فنية وقانونية خاصة في البحث عنه وجمعه وضبطه وحفظه بما يضمن سلامته وحجيته في الإثبات الجنائي.

- **الفرع الأول:**

قصور الإجراءات الجنائية التقليدية في تحصيل الدليل الرقمي.

لا شك إن مرحلة البحث عن الدليل الجنائي وتحصيله من أخطر مراحل الدعوى الجنائية، لما لها من أثر مباشر في كشف الحقيقة وإثبات الجريمة ونسبتها إلى مرتكبها، وقد استقر قانون الإجراءات الجنائية التقليدي على مجموعة من الوسائل الإجرائية التقليدية، وفي مقدمتها التفتيش، والضبط، والاستعانة بالخبرة الفنية، باعتبارها أدوات قانونية تهدف إلى جمع الأدلة المادية المتعلقة بالجريمة وضبط الأشياء المتحصلة عنها أو المستخدمة في ارتكابها.

غير أن هذه الوسائل، وإن كانت كافية في نطاق الجرائم التقليدية ذات الطابع المادي، فإنها تواجه قصوراً بيّناً عند تطبيقها على الجريمة المعلوماتية[18]، بالنظر إلى الطبيعة الخاصة للدليل الرقمي وما يتسم به من طابع غير مادي وقابلية فائقة للمحو أو التعديل أو الإخفاء، فضلاً عن كونه يوجد غالباً في صورة بيانات أو إشارات إلكترونية مخزنة داخل أنظمة معلوماتية أو متداولة سابحة عبر شبكات الاتصال الرقمية.

كما أن تحصيل الدليل الرقمي يقتضي إجراءات فنية متخصصة تختلف في طبيعتها عن وسائل البحث التقليدية، إذ لم يُعد التفتيش مقتصراً على الأماكن والأشياء المادية، بل امتد ليشمل الأنظمة الإلكترونية والبيانات الرقمية وقواعد المعلومات، ولم يُعد الضبط ينصب فقط على الأشياء المحسوسة، وإنما أصبح يتناول البيانات والبرامج والوسائط الإلكترونية، في حين غدت الخبرة الفنية المعلوماتية عنصراً جوهرياً لا غنى عنه في تحليل الأدلة الرقمية واستخلاص مدلولها الفني والقانوني.

---

[18] **تتسم الجريمة الإلكترونية بطبيعة غير مادية**، إذ تُرتكب داخل بيئة رقمية افتراضية تعتمد على البيانات والإشارات الإلكترونية، بما يجعل آثارها الفنية سريعة الزوال وقابلة للمحو أو التعديل في لحظات وجيزة، الأمر الذي ينعكس بصورة مباشرة على صعوبة اكتشافها وإثباتها. كما أن هذا النوع من الجرائم لا يخلّف – في الغالب– أدلة مادية تقليدية أو آثارًا محسوسة يمكن معاينتها بالوسائل المعتادة، وإنما يرتبط بدليل رقمي ذي طبيعة تقنية خاصة، يتطلب وسائل فنية متطورة وخبرة تقنية متخصصة لاستخلاصه وتحليله والمحافظة عليه من العبث أو التلف، ويزداد الأمر تعقيدًا بالنظر إلى اعتماد الجاني على مهارات تقنية عالية تمكّنه من إخفاء نشاطه الإجرامي أو طمس معالمه الإلكترونية، فضلًا عن ارتكاب الجريمة بأساليب هادئة وغير ظاهرة، خلافًا لما هو مألوف في الجرائم التقليدية التي تقترن غالبًا بمظاهر مادية أو عنف محسوس، وهو ما يفسر أن اكتشاف العديد من الجرائم الإلكترونية يتم في كثير من الأحيان بطريق المصادفة أو نتيجة تتبع فني دقيق.

ومن ثم، فإن قصور الإجراءات الجنائية التقليدية في مجال تحصيل الدليل الرقمي يبرز بوضوح عند مباشرة إجراءات التفتيش الإلكتروني، وضبط الوسائط والبيانات الرقمية، والاستعانة بالخبرة الفنية المعلوماتية، وهو ما يقتضي بيان أوجه هذا القصور من خلال دراسة: إجراء التفتيش(أ)، إجراء الضبط للأشياء(ب)، ندب الخبير الفني(ج).

- **أ): إجراء التفتيش:**

لم يحدد المشرع المقصود من التفتيش إلا أنه يمكن تعريفه بأنه "إجراء من إجراءات التحقيق يقوم به موظف مختص طبق الإجراءات المقررة قانوناً في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم"[19].

والتفتيش ليس غاية في حد ذاته[20]، لكن غايته البحث عن دليل يتعلق بالجريمة التي وقعت ولذلك قد يتعلق بالأشخاص أو الأماكن كما قررت المواد (75، 78) إجراءات، أو أيا كانت طبيعة المكان مسكن أو حديقة أو غيرها من الأماكن الملحقة، هل يمكن تطبيق قواعد التفتيش التقليدية على الجرائم المعلوماتية أم أن الأمر في حاجة إلى تدخل تشريعي لسن قواعد إجرائية خاصة؟.

ان القواعد التي تنظم التفتيش سواء أكانت أماكن أو اشخاص لا يمكن اعتمادها بالنسبة لهذه النوعية من الجرائم ذلك أن المادة (75) إجراءات؛ التي تقضي في تفتيش الأماكن، بأن:"تفتيش المنازل عمل من أعمال التحقيق، ولا يجوز الالتجاء إليه إلا في تحقيق مفتوح وبناء على تهمة موجهة إلى شخص مقيم في المنزل المراد تفتيشه، بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها أو إذا وجدت قرائن على أنه حائز لأشياء تتعلق بالجريمة.

وللمحقق أن يفتش أي مكان ويضبط فيه الأوراق والأسلحة والآلات وكل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج عنها أو وقعت عليه وكل ما يفيد في كشف الحقيقة".

---

[19] تنص المادة (74) في (انتقال المحقق) على أنه :"ينتقل المحقق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة مادياً وكل ما يلزم إثبات حالته".

[20] تنص المادة (11) في (سلطات رجال الضبط القضائي) على أنه :"يقوم مأمورو الضبط القضائي بالبحث عن الجرائم ومرتكبيها، وجمع الاستدلالات التي تلزم للتحقيق والدعوى".

وكذلك المادة (78) إجراءات؛ التي تقضي في شأن تفتيش الأشخاص؛ أن :"لقاضي التحقيق أن يفتش المتهم، وله أن يفتش غير المتهم إذا اتضح من أمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة، ويراعى في التفتيش حكم الفقرة الثانية من المادة 35[21]".

وإذا علمنا أن إجراءات التفتيش في الغالب تأخذ وقت وتتم في وقت محدد قد يكون ظرف الليل مثلا يستبعد اجرؤه فيه في محلات السكنى وتوابعها لا يمكن أن يقع قبل الساعة السادسة صباحا وبعد الساعة الثامنة ليلا، وإذا ما علمنا أن الجريمة المعلوماتية ترتكب في فترة زمنية قصيرة وأن آثارها قد تضمحل بمجرد وقوعها. فانه في صورة ارتكاب الجريمة المعلوماتية ليلا فانه يتعين على مأموري الضبط القضائي ومساعدوهم أو سلطة التحقيق انتظار اليوم المقبل لإجراء التفتيشات اللازمة لإثباتها وقد يكون ذلك بعد فوات الأوان.

فضلا عن أن المواد (40[22]، 76[23]، 77[24]) إجراءات[25]، تنصان على حضور صاحب المنزل، وإخطار النيابة بالانتقال للتفتيش، وأوجبت المادة (74) إجراءات؛ بأنه :"لا يجوز الالتجاء إليه إلا في تحقيق مفتوح وبناء على تهمة موجهة إلى شخص مقيم في المنزل المراد تفتيشه، بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها أو إذا وجدت قرائن على أنه حائز لأشياء تتعلق بالجريمة"، أو التي من

---

[21] تنص المادة (35) في (تفتيش المقبوض عليهم) على أنه :"في الأحوال التي يجوز فيها القبض قانوناً على المتهم يجوز لمأمور الضبط القضائي أن يفتشه. وإذا كان المتهم أنثى، وجب أن يكون التفتيش بمعرفة أنثى يندبها لذلك مأمور الضبط القضائي".

[22] تنص المادة(40) في (إجراءات التفتيش) على أنه :"يحصل التفتيش بحصول المتهم أو من ينيبه عنه كلما أمكن ذلك، ويجب أن يكون بحضور شاهدين، ويكون هذان الشاهدان بقدر الامكان من أقاربه البالغين أو من القاطنين معه بالمنزل أو من الجيران، ويثبت ذلك في المحضر".

[23] تنص المادة (76) في (حضور صاحب المنزل) على أن :"يحصل التفتيش بحضور المتهم أو من ينيبه عنه إن أمكن ذلك. وإذا حصل التفتيش في منزل غير المتهم يدعى صاحبه للحضور بنفسه وبواسطة من ينيبه عنه إن أمكن ذلك".

[24] تنص المادة (77) في (إخطار النيابة بالانتقال للتفتيش) بأنه :"على قاضي التحقيق كلما رأى ضرورة للانتقال للأمكنة أو للتفتيش أن يخطر بذلك النيابة العامة".

[25] تنص المادة (76) في (حضور صاحب المنزل) على أنه :"يحصل التفتيش بحضور المتهم أو من ينيبه عنه إن أمكن ذلك. وإذا حصل التفتيش في منزل غير المتهم يدعى صاحبه للحضور بنفسه وبواسطة من ينيبه عنه إن أمكن ذلك". وتنص المادة (77) في (إخطار النيابة بالانتقال للتفتيش) بأنه :"على قاضي التحقيق كلما رأى ضرورة للانتقال للأمكنة أو للتفتيش أن يخطر بذلك النيابة العامة".

شأنها الإعانة على كشف الحقيقة و أن يحجزها ولكنه تحدث عن الأشياء المادية فحسب الأمر الذي يستبعد الحديث عن الأشياء اللامادية.

ومن ناحية أخرى أجازت المادة (79) إجراءات[26]، لقاضي التحقيق أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب التلغرافات كافة البرقيات، كما يجوز له مراقبة المحادثات التليفونية متى كان لذلك فائدة في ظهور الحقيقة، والمقصود بذلك هي المراسلات العادية وبذلك لا يمكن أن تنطبق هذه الإجراءات على التقاط المراسلات الالكترونية.

وفي المقابل، نجد في التشريعات المقارنة حيث كرس المشرّع الفرنسي مبدأ سرية المراسلات الإلكترونية بموجب القانون رقم (646 لسنة 1991م) المؤرخ في (1 يوليو 1991م)، غير أنه لم يسبغ على هذه السرية طابعاً مطلقاً، بل أجاز المساس بها استثناءً متى اقتضت ذلك اعتبارات المصلحة العامة، وفي الحدود التي رسمها القانون، وقد ميّز التنظيم الفرنسي بين مقتضيات البحث القضائي ومتطلبات الأمن العام؛ ففي المجال القضائي خول لقاضي التحقيق سلطة الإذن بالتقاط المراسلات الإلكترونية أو تسجيلها في الجرائم المعاقب عليها بالسجن لمدة تزيد على سنتين، بينما منح الوزير الأول – بصفة استثنائية– صلاحية الترخيص بأعمال الالتقاط لأغراض حماية الأمن العام، وصون المصالح الأساسية للدولة، ومكافحة الإرهاب والجريمة المنظمة.

كما استحدث المشرّع الفرنسي هيئة إدارية مستقلة تمثلت في "اللجنة القومية لمراقبة أعمال الالتقاط"، وأسند إليها الرقابة على الأذون الصادرة، مع منحها سلطة الأمر بوقفها عند مخالفة القانون، ولم يقف التطور التشريعي الفرنسي عند هذا الحد، بل تعاقبت تعديلات لاحقة عززت الحماية الجنائية والإجرائية، حيث جرم قانون سنة (1992م) إفشاء أعمال الالتقاط، ثم اعتبر قانون سنة (2000م) الامتناع عن إنهائها مخالفة قانونية، لاسيما من جانب مزودي الخدمات ومشغلي الشبكات، إلى أن ألزم قانون سنة (2001م) مزودي خدمات التشغيل بالكشف عن الأرقام السرية المعتمدة، ورتب المسؤولية القانونية على الامتناع عن ذلك.

---

[26] تنص المادة (79) في (ضبط الخطابات والرسائل) على أن :"لقاضي التحقيق أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب التلغرافات كافة البرقيات، كما يجوز له مراقبة المحادثات التليفونية متى كان لذلك فائدة في ظهور الحقيقة".

أما فيما يتعلق بالتفتيش بحثا عن بيانات الحاسب الآلي، تكمن المشكلة في الصعوبات العملية التي تعيق عملية خضوع البيانات المخزنة آليا لقواعد التفتيش التقليدية المنصوص عليها حسب القواعد العامة للإجراءات الجزائية، وتلخص هذه الصعوبات في الآتي:

1. في حالة وجود النظام المعلوماتي داخل إحدى المساكن مع وجود النهاية الطرفية في مكان آخر، مما يعطي للجاني فرصة سانحة للتخلص من البيانات التي يستهدفها التفتيش، الأمر الذي يتطلب من الشخص المخول بالتنفيذ السلطة الكاملة كي يوصل إلى النهاية الطرفية وتسجيل ما تحويه من بيانات دون التقيد بالحصول على إذن القاضي الجزئي طبقا لنص المادة (79) إجراءات.
2. وفيما يتعلق بإذن التفتيش، فتبدو الصعوبة في هذا الصدد في اشتراط أن يكون الإذن محدداً فيما يخص محله والأشياء التي يهدف التفتيش إلى ضبطها طبقا للمادة (75) إجراءات، وهي بيانات جوهرية يجب توافرها في إذن التفتيش حسب القواعد العامة، وهذا الشرط يتطلب أن يقوم مصدر الإذن بتحديد الأشياء المراد ضبطها بطريقة فنية الأمر الذي لا يمكن له القيام به لأنه يتجاوز اختصاصه وثقافته المحدودة في المجال المعلوماتي.
3. إن التفتيش عن البيانات المخزنة أليا يتطلب القيام بعملية ولوج إلى الأنظمة المعلوماتية التي تحويها لضبط ما يُعد صالحاً من هذه البيانات كدليل أو قرينة لارتكاب جريمة ما، وهذا الأمر يتطلب مسبقاً معرفة معقولة من قبل الشخص القائم بالتفتيش بكيفية التعامل مع برامج وملفات البيانات المخزنة بالحاسب وكذلك كلمة السر والمرور اللازمتين للدخول إلى النظام.

فالمتهم لا يمكن إجباره على تقديم دليل إدانته حسب القواعد العامة للإجراءات الجنائية حيث أنه لن يجبر على البوح بالرقم السري الذي يمكن من النفاذ إلى ملفات البيانات أو على كشف طبيعة البيانات المخزنة وغير ذلك من الأمور التي من شأنها أن تؤدي إلى إدانته.

وبالنظر إلى القصور التشريعي الذي يواجه إمكانية تفتيش النظم المعلوماتية لجأ المشروع في دول عديدة إلى تقرير بعض القواعد الإجرائية الخاصة بهدف التغلب على الصعوبات العملية ومن هذه الدول هولندا، وكندا، ونعرض في هذا الخصوص نعرض لتجربتين على النحو التالي:

- **تجربة هولندا الإجرائية:**

بالنسبة للصعوبة التي تتعلق بوجود النهاية الطرفية للنظام المعلوماتي في منزل آخر – غير منزل المتهم– أجاز مشروع قانون جريمة الحاسب الآلي الهولندي في المادة (25) منه إمكانية امتداد تفتيش

المساكن إلى "تفتيش نظام آلي"... موجود في مكان آخر بغية التوصل إلى بيانات يُمكن أن تفيد بشكل معقول... في كشف الحقيقة وإذا ما وجدت هذه البيانات يجب تسليمها، وذلك دون التقييد بالحصول على إذن مسبق من قاضي التحقيق، ولكن هذه السلطة ليست مطلقة[27]، وإنما يرد عليها قيود ثلاثة هي:

1. ألا تكون النهاية الطرفية المتصل بها الحاسب الآلي موجودة ضمن إقليم دولة أخرى حتى لا يؤدي الاتصال بها إلى انتهاك السيادة الإقليمية للدولة إذا ما أخذنا بعين الاعتبار أن القانون الجنائي يمثل مظهرا من مظاهر سيادة الدولة وذلك اتساقا مع مبدأ الشرعية الجنائية الذي أصلت له المادة الرابعة عقوبات ليبي:"تسري أحكام هذا القانون على كل ليبي أو أجنبي يرتكب في الأراضي الليبية جريمة من الجرائم المنصوص عليها فيه ...".
2. أن تحتوي النهاية الطرفية المتصل بها الحاسب الآلي على بيانات ضرورية لظهور الحقيقة، حتى يكون هناك هدفا أو غرضا للتفتيش وهو ضبط هذه المعلومات.
3. أن يحل قاضي التحقيق محل الشخص صاحب المكان الذي يجب تفتيشه بصورة مؤقتة، لأن ذلك الشخص يعد من قبيل؛ غير المتهم، ووجود قاضي التحقيق أثناء مباشرة إجراء التفتيش يُعد ضمانة لحقوقه.

- **تجربة كندا الإجرائية:**

فيما يتعلق بصعوبة تحديد إذن التفتيش والأشياء التي يهدف إلى حجزها، فيمكن الاعتماد في ذلك على صيغة إذن التفتيش الذي اعتمدته الشرطة التابعة للإدارة الأمنية لمركز المعلوماتية الكندي والذي استخلصته من واقع خبرتها العملية، وتتضمن هذه الصيغة الضوابط الآتية:

1. البحث عن ضبط البرنامج أو كيان الحاسب المنطقي والتي يدخل فيها برنامج التطبيق ونظم التشغيل وما يتفرع عنها من نظم.
2. البحث عن البيانات المستخدمة بواسطة برنامج الحاسب أو كيانه المنطقي.
3. البحث عن السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

[27] في هولندا لقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة".

وبالتالي فإن مثل هذه الصيغة تمكن القائم بالتفتيش من العثور على أدلة لارتكاب الجرائم المعلوماتية والقيام بحجزها.

وبالنبآء على ما تقدم يتبين؛ أن هذه القوانين وغيرها ومنها القانون الإجرائي الليبي تبين أن الأحكام التقليدية في التفتيش لا يمكن أن تشمل ما أحدثه التقدم التكنولوجي من تغييرات، لذلك يرى البعض أنه يتعين إدخال وإقرار تشريعات وتعديلات إجرائية جنائية على وسائل البحث التقليدية وتخويل إمكانية التفتيش في أي لحظة دون ارتباط بعامل الزمن.

ويكون عبر نفس الوسيلة التي استعملها الجاني أي أن يتولى مأمور الضبط القضائي أو النيابة العامة بحسب الأحوال القيام بعملية التفتيش عبر جهاز الحاسوب المرتبط بشبكة الإنترنت الموجود بمكتبه الشخصي بقطع النظر عن مكان ارتكاب الجريمة أي داخل البلاد أو خارجها؛ إلا أن هذا الإجراء يتضمن الانخراط في اتفاقيات دولية، وأن تكون لمأموري الضبط القضائي وأعضاء النيابة العامة وقاضي التحقيق الدراية اللازمة لإجراء تلك الأعمال عبر أجهزة الاتصال الحديثة أو تكون مكاتبهم مجهزة بالآليات اللازمة للقيام بضبط وحجز تلك الأدلة الرقمية.

- **ب): إجراء الضبط للأشياء:**

الضبط كما نصت المادة (2/75) إجراءات، أو الحجز في معظم الأحوال هو الغرض من التفتيش، وهو لا يخرج عن كونه وضع اليد على أشياء تتصل بجريمة وقعت وتفيد في كشف الحقيقة عنها وعن مرتكبيها أي الأشياء التي تعد في ذاتها دليلا على الجريمة، أو يمكن استخراج هذا الدليل منها، وهذه الأشياء قد تكون هي ما استعمل في ارتكاب الجريمة، وقد تكون ما نتج عن ارتكابها، وقد تكون الموضوع الذي وقعت عليه الجريمة، وقد تمكن المشروع عن طريق إجراء الحجز من صيانة هذه الأشياء من العبث والمحافظة عليها باعتبارها دليل إثبات ضد المتهم أو لمصلحته.

أما بالنسبة للجرائم المعلوماتية، فإن عملية الضبط أو الحجز قد تثير صعوبات عديدة بالنظر لطبيعة محل الجريمة المعلوماتية ذاته فيما إذا كان يتعلق محلها ببرنامج الحاسب الآلي، أو بيانات هذا الحاسب، وذلك كالتالي:

- **أولا: ضبط برنامج الحاسب الآلي:**

ليس هناك صعوبة في ضبط أدلة الجريمة المعلوماتية حين يكون محلها سرقة الدعامة المادية للبرنامج المعلوماتي أو الوسائل المادية المستخدمة في نسخه بصورة غير مشروعة أو إتلافه بوسائل

تقليدية، من ذلك البرنامج المطبوع على (C.d) أو (F.d) وحاليا ما يطلق عليه "فلاش ممري" Flash Memory لكن تبدو الصعوبة في حالة استخدام وسائل فنية لإتلاف البرنامج عن طريق الفيروسات، وذلك نتيجة لضعف خبرة مأموري الضبط القضائي في المجال المعلوماتي الأمر الذي يترتب عليه فشلها في جمع الأدلة في هذا الميدان الإلكتروني[28].

ويزيد الأمر تعقيداً إذا كانت عملية الضبط لهذه الوسائل التقنية تتم في الشبكات الكبيرة حيث يصادف ضبط الأشياء وبصورة مؤكدة الصعوبتين الآتيتين:

1. عملية الضبط قد تؤدي إلى عزل النظام المعلوماتي بالكامل عن دائرته لمدة زمنية قد تطول أو تقصر الأمر الذي قد يترتب عنه أضرارا بالجهة مستخدمة النظام طالما أنها تعتمد على النظام المعلوماتي في تسيير خدماتها وأعمالها.
2. عدم إبداء مستخدمي الأنظمة المعلوماتية الاستعداد للتعاون الكامل والفعال مع سلطات التحقيق لما يعنيه لها الضبط للأشياء في هذا الإطار من مساس بحقوق الغير.

- **ثانيا: ضبط بيانات الحاسب الآلي:**

تعترض مأموري الضبط القضائي أو سلطة التحقيق الابتدائي عوائق مختلفة عند ضبط البيانات[29] تتلخص في الآتي:

1. غياب الآثار المادية للجرائم التي يكون محلها بيانات الحاسب الآلي التي يمكن الاستدلال بها عليها، ويتجلى ذلك بصورة واضحة في جرائم الاختلاس والتزوير التي يستخدم فيها الحاسب الآلي.
2. ضخامة البيانات التي يجب فحصها من قبل قاضي التحقيق أو مأموري الضبط القضائي، فضلا عن تطلب قدر كبير من الخبرة الفنية لتحديد البيانات التي تصلح كأداة من عدمه، الأمر الذي يعوق الوصول إليها في الكثير من الأحيان، ومما يزيد الأمر صعوبة عدم معرفة

---

[28] د. عبد الفتاح حجازي، مباديء الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، مصر، (2007م)، (ص – 209).

[29] يلاحظ: أنه؛ يقصد ببيانات الحاسب الآلي كل معلومات أو معطيات أو أوامر أو برامج تُنشأ أو تُعالج أو تُخزن أو تُرسل أو تُستقبل بواسطة نظام معلوماتي أو جهاز حاسب آلي، متى كانت قابلة للإدراك أو المعالجة إلكترونياً، سواء ظهرت في صورة نصوص أو أرقام أو رموز أو إشارات أو صور أو أصوات أو غير ذلك من المخرجات الرقمية.

القائم بالتفتيش لكلمات السر أو شِفرات ترميز البيانات الأمر يقتضي تعاون مستخدم النظام معه أو الاستعانة بالغير من ذوي الخبرة في هذا المجال.

- **ج): في ندب الخبير:**

تكشف المادة (69) إجراءات[30]؛ عن تبني المشرّع الليبي لفكرة الاستعانة بالخبرة الفنية كلما تعلّق الأمر بمسائل ذات طبيعة تقنية أو علمية تخرج عن نطاق المعرفة القانونية للقاضي أو سلطة التحقيق، إذ خولت لقاضي التحقيق ندب الخبراء لإثبات الحالة والكشف عن الوقائع الفنية المرتبطة بالجريمة، ويُفهم من النص أن المشرّع أقام الخبرة الجنائية على مبدأ الرقابة القضائية المباشرة، فأوجب – كأصل عام– حضور قاضي التحقيق أثناء مباشرة الخبير لمهمته، ضماناً لسلامة الإجراءات وتحقيقاً لمبدأ الشرعية الإجرائية، مع جواز الاستثناء من ذلك متى اقتضت طبيعة الأعمال الفنية القيام بتحضيرات تقنية أو تجارب متكررة أو إجراءات تستلزم استقلال الخبير في مباشرة مأموريته.

ورغم أن هذا النص وُضع أساساً لمواجهة الجرائم التقليدية، إلا أنه يكتسب أهمية خاصة في نطاق الجرائم المعلوماتية، بالنظر إلى الطبيعة الفنية البحتة للدليل الرقمي، وتعقيد الأنظمة المعلوماتية، واعتماد إثبات الجريمة الإلكترونية – في الغالب– على التحليل التقني للأجهزة والبيانات والشبكات الإلكترونية. فالجريمة المعلوماتية من الجرائم التي يتعذر – عملياً– كشف حقيقتها أو تحليل أدلتها دون الاستعانة بخبراء متخصصين في تقنيات الحاسوب والشبكات وتحليل البيانات الرقمية واسترجاعها.

---

[30] في ندب الخبير تنص المادة (69) في (ندب الخبراء) على أنه :"إذا استلزم إثبات الحالة الاستعانة بطبيب أو غيره من الخبراء، يجب على قاضي التحقيق الحضور وقت العمل وملاحظته. وإذا اقتضى الأمر إثبات الحالة بدون حضور القاضي نظراً إلى ضرورة القيام ببعض أعمال تحضيرية أو تجارب متكررة أو لأي سبب آخر يجب على القاضي أن يصدر أمراً يبين فيه أنواع التحقيقات وما يراد إثبات حالته. ويجوز في جميع الأحوال أن يؤدي الخبير مأموريته بغير حضور الخصوم". كما تنص المادة (70) في (يمين الخبراء) على أنه :"يجب على الخبراء أن يحلفوا أمام المحقق يميناً على أن يبدوا رأيهم بالأمانة والصدق وعليهم أن يقدموا تقريرهم كتابة". ونصت المادة (71) في (ميعاد تقديم التقرير) على أنه :"يحدد المحقق ميعاداً للخبير ليقدم تقريره فيه، وله أن يستبدل به خبيراً آخر إذا لم يقدم التقرير في الميعاد المحدد". ونصت المادة (72) في (الخبراء الاستشاريون) على أنه :"للمتهم أن يستعين بخبير استشاري ويطلب تمكينه من الاطلاع على الأوراق وسائر ما سبق تقديمه للخبير المعين من قبل القاضي، على ألا يترتب على ذلك تأخير السير في الدعوى". كما نصت المادة (73) في (رد الخبراء) على أنه :"للخصوم رد الخبير إذا وجدت أسباب قوية تدعو لذلك، ويقدم طلب الرد إلى المحقق للفصل فيه، ويجب أن تبين فيه أسباب الرد، وعلى المحقق الفصل فيه في مدة ثلاثة أيام من يوم تقديمه. ويترتب على هذا الطلب عدم استمرار الخبير في عمله إلا في حالة الاستعجال بأمر من القاضي".

غير أن اتساق نص المادة (69) إجراءات؛ مع خصوصية الجرائم المعلوماتية يظل اتساقاً جزئياً ومحدوداً؛ ذلك أن الخبرة المعلوماتية تختلف في طبيعتها عن الخبرة التقليدية، لأنها لا تقتصر على مجرد إثبات حالة مادية ظاهرة، وإنما تمتد إلى تحليل نظم رقمية معقدة، وتتبع آثار إلكترونية خفية، وفحص بيانات قد تكون مشفرة أو ممحوة أو مخزنة عن بُعد.

كما أن اشتراط حضور قاضي التحقيق أثناء مباشرة أعمال الخبرة يبدو – في كثير من صور الجرائم الإلكترونية– أمراً عسير التطبيق من الناحية العملية، نظراً للطابع الفني الدقيق والمعقد للعمليات التقنية التي تستغرق وقتاً طويلاً وتتطلب بيئة تقنية متخصصة.

ويؤخذ على النص كذلك أنه لم يضع تنظيماً إجرائياً خاصاً بالخبرة الرقمية، ولم يحدد الضوابط الفنية المتعلقة بكيفية جمع الأدلة الإلكترونية أو حفظها أو فحصها أو ضمان سلامة سلسلة حيازتها الرقمية، كما خلا من النص على شروط تأهيل الخبراء المعلوماتيين أو اعتماد المختبرات الجنائية الرقمية، الأمر الذي يكشف عن قصور تشريعي في مواكبة التطور التقني المتسارع الذي أفرزته الجرائم الإلكترونية.

ومن ثم، فإن المادة (69) إجراءات، وإن كانت تصلح أساساً عاماً للاستعانة بالخبرة الفنية، إلا أنها تظل قاصرة عن استيعاب خصوصية الجريمة المعلوماتية، الأمر الذي يقتضي تدخلاً تشريعياً يقر نظاماً خاصاً للخبرة الجنائية الرقمية، يتلاءم مع طبيعة الدليل الإلكتروني ومتطلبات الإثبات في البيئة الرقمية الحديثة.

وتبرز أهمية الخبرة في الجرائم المعلوماتية بصورة خاصة، بالنظر إلى تعدد أنظمة الحاسوب وشبكات الاتصال وتنوع نماذجها وتقنياتها، فضلاً عن الطابع الفني الدقيق والمتخصص للعلوم المرتبطة بها، وما تشهده من تطور تقني متسارع ومتلاحق قد يتعذر – أحياناً– حتى على المتخصصين الإحاطة الكاملة به أو مواكبة مستجداته.

ويتعين في خبراء الحاسب الآلي المنتدبين للتحقيق أن يتوافر لديهم القدرة الفنية والإمكانيات العلمية في المسألة موضوع ندب الخبرة طبقا للمادة (69) إجراءات، ولا يكفي حصول الخبير على شهادة علمية، بل يجب مراعاة الخبرة العملية لأنها تحقق الكفاءة الفنية، ولذلك يمكن القول بصفة عامة بأنه لا يوجد حتى الآن خبير معلوماتي لديه المعرفة المتعمقة في سائر أنواع الحاسبات وشبكاتها، وكذلك لا يوجد خبير معلوماتي قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو بواسطتها.

ونظرا لأن الجريمة المعلوماتية لها خصوصيتها فان الخبير المعلوماتي قد يكون من أولئك الجناة الذين سبق لهم ارتكاب مثل هذه الجرائم وتم احتوائهم داخل المؤسسات الالكترونية للاستفادة ايجابيا من قدراتهم، فضلا عن تأهيلهم كمواطنين صالحين، وإن كان ذلك يجوز أن يكون سبباً للقدح في الخبير المعني في الدعوى من قبل أصحاب المصلحة في ذلك طبقا للماد (73) إجراءات؛ في شأن رد الخبراء[31].

ولكن يبقى الرجوع إلى الخبراء في ميدان الجرائم المعلوماتية أمرا ضرورياً دون أن يكون ملزماً لقاضي التحقيق. لكن في صورة اختيار خبير فإنه لا بد وفق القواعد العامة من تحديد مهمته على وجه الدقة والتاريخ الذي يجب عليه تقديم فيه تقريره طبقا للمادة (69) إجراءات[32]، مما يستوجب تأهيل مأموري الضبط القضائي وأعضاء سلطة التحقيق في الجرائم المعلوماتية لنجاح تحقيق مثل هذه الجرائم، ودرءاً لما ينادي به البعض من أنه يمكن للخبير نفسه أن يحدد إطار مهمته، إذ أن ذلك سوف يقوض دور الباحث والقاضي في الدعوى الجنائية في مثل هذه الجرائم.

ويمكن إجمال المسائل التي يحتاج قاضي التحقيق في وصفها إلى خبير معلوماتي، كما يلي:

1. وصف تركيب الحاسب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها، بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشغيل.
2. وصف الموضوع المحتمل لأدلة الإثباتات والشكل أو الهيئة التي تكون عليها.
3. القيام عند الاقتضاء بعزل النظام المعلوماتي دون إطلاق الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.
4. نقل أدلة الإثبات إلى أوعية ملائمة دون أن يصيبها التلف.

---

[31] تنص المادة (73) في (رد الخبراء) على أنه :"للخصوم رد الخبير إذا وجدت أسباب قوية تدعو لذلك، ويقدم طلب الرد إلى المحقق للفصل فيه، ويجب أن تبين فيه أسباب الرد، وعلى المحقق الفصل فيه في مدة ثلاثة أيام من يوم تقديمه. ويترتب على هذا الطلب عدم استمرار الخبير في عمله إلا في حالة الاستعجال بأمر من القاضي".

[32] تنص المادة (69) في (ندب الخبراء) على أنه :"إذا استلزم إثبات الحالة الاستعانة بطبيب أو غيره من الخبراء، يجب على قاضي التحقيق الحضور وقت العمل وملاحظته. وإذا اقتضى الأمر إثبات الحالة بدون حضور القاضي نظراً إلى ضرورة القيام ببعض أعمال تحضيرية أو تجارب متكررة أو لأي سبب آخر يجب على القاضي أن يصدر أمراً يبين فيه أنواع التحقيقات وما يراد إثبات حالته. ويجوز في جميع الأحوال أن يؤدي الخبير مأموريته بغير حضور الخصوم.

5. تجسيد الأدلة في صورة مادية يتلقاها إذا أمكن إلى أوعية ورقية بحيث يتاح للقاضي الاطلاع عليها وفهمها مع إثبات أن المسطر على الورق مطابق لذلك المسجل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة.

يمكن لقاضي التحقيق سماع الشهود واستجواب المتهمين أو سؤالهم في حضور الخبير المعلوماتي، والذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب وذلك وفق كيفية يتم الاتفاق عليها.

ومن المفضل أن يكتب الخبير السؤال الفرعي على ورقة يضعها أمام قاضي التحقيق حتى يحدد الوقت الذي يوجه فيه ذلك السؤال، كذلك يمكن إتاحة الفرصة للخبير بعد انتهاء قاضي التحقيق من استجواب المتهمين.

كل هذه الإجراءات والاحتياطيات الواجب اتخاذها لإنجاح البحث والتحقيق في جرائم المعلوماتية لا أثر لها في النصوص الإجرائية العامة مما يسهل الأمر على مجرمي المعلوماتية ارتكاب ما يحلو لهم من جرائم دون الخوف من التتبع أو المحاكمة، وفي ظل هذا القصور الإجرائي الخطير أصبحت الضرورة ملحة لإرساء قواعد إجرائية جنائية مستحدثة خاصة لمجابه الجريمة المعلوماتية.

- **الفرع الثاني:**

مشروعية إجراءات التحري والتحقيق في الجريمة المعلوماتية.

أفرزت خصوصية الجريمة المعلوماتية وما تتسم به من تعقيد تقني وخفاء في ارتكابها اتجاهًا تشريعيًا حديثًا نحو تبني إجراءات تحرٍ وتحقيق ذات طبيعة خاصة، تستهدف تمكين السلطات المختصة من تعقب الأنشطة الإجرامية الرقمية وضبط أدلتها الفنية والكشف عن مرتكبيها، وذلك تحت إشراف السلطة القضائية ووفق الضوابط القانونية المقررة، ويُقصد بهذه الإجراءات الوسائل الفنية والاستثنائية التي تُستخدم في البحث والتحري عن الجرائم الإلكترونية وجمع أدلتها، ومن أبرزها التفتيش الإلكتروني، واعتراض أو مراقبة الاتصالات والبيانات الرقمية، والتسرب الإلكتروني.

ولم يُنظم المشرع الليبي الأحكام الإجرائية بموجب قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م)، وذلك استجابةً لمقتضيات مكافحة الإجرام المعلوماتي وملاحقة مرتكبيه، غير أن إقرار هذه الوسائل الاستثنائية في التشريعات المقارنة أثار جدلًا فقهيًا وقانونيًا بشأن مدى مشروعيتها وحدود توافقها مع الضمانات الدستورية، لاسيما ما يتعلق بحماية الخصوصية وحرمة الحياة الخاصة وسرية الاتصالات والبيانات الإلكترونية، وانقسم الفقه تبعًا لذلك بين اتجاه معارض يرى في هذه الإجراءات

مساسًا بالحقوق والحريات الفردية (أولا)، واتجاه مؤيد يبرر مشروعيتها بضرورة مواجهة الخطورة الإجرامية المتنامية للجريمة الإلكترونية وتحقيق الفعالية الإجرائية في كشفها وإثباتها (ثانيا).

- **أولا: الاتجاه الرافض لمشروعية الإجراءات الخاصة في الجريمة المعلوماتية:**

ذهب اتجاه فقهي إلى رفض التوسع في إجراءات التحري والتحقيق الخاصة بالجريمة المعلوماتية، استنادًا إلى اعتبارات فنية وقانونية تتصل بطبيعة الجريمة المعلوماتية ذاتها، باعتبارها كل فعل يُرتكب باستخدام أنظمة الحاسب الآلي أو شبكات المعلومات أو غيرها من وسائل تقنية المعلومات بالمخالفة لأحكام قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م).

فمن الناحية الفنية، يرى هذا الاتجاه أن الدليل الجنائي الرقمي – والمتمثل في نتائج تحليل البيانات المستخرجة من أنظمة الحاسوب أو شبكات الاتصال أو وسائط التخزين الرقمية– يظل بطبيعته الفنية عرضة للتعديل أو الحذف أو الاصطناع، بما قد يؤثر في سلامته وقيمته الإثباتية ويثير الشك بشأن مدى تعبيره عن الحقيقة الواقعية.

أما من الناحية القانونية، فيذهب هذا الاتجاه إلى أن بعض إجراءات التحري الإلكتروني، كالمراقبة واعتراض الاتصالات والتفتيش الرقمي، قد تشكل مساسًا بحرمة الحياة الخاصة وسرية المراسلات والاتصالات، وهي حقوق كفلتها القواعد الدستورية لإعلان (2011م) في الباب الثاني "الحقوق والحُريات العامة" في المادة (7) منه[33]، وأحاطتها التشريعات الجنائية بالحماية، الأمر الذي يثير التخوف من تحول هذه الإجراءات الاستثنائية إلى وسيلة للتوسع في تقييد الحقوق والحريات الفردية خارج الحدود التي تقتضيها الضرورة الإجرائية.

- **ثانيا: الاتجاه المؤيد لمشروعية الإجراءات الخاصة في الجريمة المعلوماتية:**

ذهب اتجاه فقهي وقانوني مؤيد إلى إقرار مشروعية استخدام إجراءات التحري والتحقيق الخاصة في مجال الجريمة المعلوماتية، تأسيسًا على اعتبارات تتصل بمتطلبات المصلحة العامة وفعالية السياسة الجنائية الحديثة، التي لم يعد يكفي معها الاعتماد على الوسائل التقليدية في مواجهة أنماط إجرامية

[33] تنص المادة (7) من الإعلان الدستوري (2011م) والتعديلات اللاحقة له على أن :"تصون الدولة حقوق الإنسان وحرياته الأساسية، وتسعى إلى الانضمام للإعلانات والمواثيق الدولية والإقليمية التي تحمي هذه الحقوق والحريات، وتعمل على إصدار مواثيق جديدة تكرم الإنسان كخليفة الله في الأرض".

متطورة تتسم بالسرعة والمرونة والتقنية العالية. فالجريمة المعلوماتية، باعتبارها أحد صور الإجرام المعاصر، قد أفرزت واقعًا جديدًا يقتضي تطوير أدوات المواجهة الإجرائية بما يتلاءم مع طبيعتها غير المادية واللاإقليمية، وتعقيد وسائل ارتكابها.

ويستند هذا الاتجاه إلى أن المجرم المعلوماتي ذاته قد طوّر أساليبه ووسائله في تنفيذ نشاطه الإجرامي، مستعينًا بالتطبيقات الحديثة وشبكات التواصل وتقنيات الاتصال المشفر، وهو ما يجعل من غير المنطقي تقييد سلطات العدالة الجنائية بالوسائل التقليدية في التحري والإثبات، وإلا فقدت فعاليتها في الكشف عن هذا النوع من الجرائم.

ومن ثم فإن إخضاع بعض وسائل الاتصال والمراقبة الفنية لرقابة قانونية وقضائية يُعد ضرورة لملاحقة الجرائم الخطيرة، لا سيما تلك التي تستهدف أمن الدولة واستقرارها، بما في ذلك الجرائم المنظمة والإرهابية التي تعتمد على الفضاء الرقمي في التجنيد والتنسيق والتنفيذ وتحريك الأموال.

وفي هذا السياق، اتجهت التشريعات المقارنة، والتي يجب أن يكون من بينها التشريع الليبي وفي إطار قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م)، وبحكم الضرورة إلى تبني هذا المنحى الإصلاحي، من خلال إقرار جملة من الإجراءات الجنائية الخاصة التي تراعي خصوصية الدليل الرقمي وتواكب التطور المتسارع في تقنيات المعلومات والاتصال، وذلك في إطار السعي إلى تحقيق متطلبات الفعالية في مكافحة الجريمة المعلوماتية.

وخاصة في ظل خصوصية الدليل الجنائي الرقمي الذي يُعد من أهم المستجدات التي أفرزها التطور التقني في مجال الإثبات الجنائي، إذ إنه لا يقوم على معطيات مادية محسوسة بالمعنى التقليدي، وإنما يتجسد في كونه نتاجًا لعملية تحليل فني للبيانات المستخلصة من أنظمة الحاسوب أو شبكات الاتصال أو أجهزة التخزين الرقمية بمختلف أنواعها طبقا للمادة الأولى من القانون محل الدراسة، وبذلك فإن هذا الدليل لا يُدرك مباشرة بالحواس، وإنما يُستخرج عبر إجراءات تقنية دقيقة تقوم على جمع البيانات الرقمية ومعالجتها وتفسيرها باستخدام أدوات وبرمجيات متخصصة.

وتكمن خصوصية هذا الدليل في كونه دليلاً غير مباشر ذو طبيعة تقنية محضة، حيث يمر بعدة مراحل تبدأ بمرحلة الاستخراج الرقمي للبيانات من مصادرها الأصلية، ثم مرحلة الفحص والتحليل الفني، وصولًا إلى مرحلة التفسير القانوني للنتائج المستخلصة، وهذا التسلسل يجعل من الدليل الرقمي دليلاً مركبًا، يعتمد في جوهره على الكفاءة الفنية والخبرة التقنية للجهات المختصة أكثر من اعتماده على الإدراك الحسي المباشر.

كما تتجلى خصوصيته في كونه دليلاً هشًّا بطبيعته، إذ يمكن أن يتعرض للتعديل أو الحذف أو التلاعب دون ترك أثر مادي ظاهر، الأمر الذي يفرض ضرورة إحاطته بضمانات فنية وقانونية صارمة تضمن سلامة مصادره وسلسلة حيازته، حتى يظل محتفظًا بقيمته الإثباتية أمام القضاء، ومن هنا فإن الدليل الرقمي لا يكتسب حجّيته من شكله الظاهري، وإنما من سلامة الإجراءات الفنية التي مر بها منذ لحظة استخراجه وحتى تقديمه في الدعوى.

ويُضاف إلى ذلك أن هذا الدليل يتميز بطابع افتراضي ومتشعب المصادر، إذ قد يستمد من أنظمة متعددة مترابطة كالحواسيب، وشبكات الإنترنت، وخوادم البيانات، وأجهزة التخزين السحابية، وهو ما يجعله عابرًا للحدود في كثير من الأحيان، ويثير إشكالات قانونية تتعلق بالاختصاص المكاني وصعوبة ضبط مكان ارتكاب الفعل أو مصدر الدليل.

وبناءً على ذلك، فإن الدليل الجنائي الرقمي يُمثل تحولًا نوعيًا في نظرية الإثبات الجنائي، إذ لم يعد مجرد أثر مادي للجريمة، بل أصبح عملية تحليلية مركبة للبيانات الرقمية، تتطلب تكييفًا قانونيًا خاصًا يوازن بين متطلبات الفاعلية في كشف الحقيقة وضمانات المشروعية الإجرائية وحماية الحقوق والحريات، وهذا يستدعي من حيث المنطق القانوني والضرورة الإجرائية إلى إرساء قواعد إجرائية خاصة تعطي فاعلية تطبيقية للقواعد الموضوعية التي أقرها القانون رقم (5 لسنة 2022م).

- **المبحث الثاني:**

ضرورة إرساء قواعد إجرائية خاصة لمجابهة الجريمة المعلوماتية.

أفرزت الجريمة المعلوماتية، بما تتسم به من طابع عابر للحدود وسرعة في التنفيذ واعتمادها على بيئة رقمية معقدة، عجزًا واضحًا في القواعد الإجرائية التقليدية عن مواكبة متطلبات البحث والتحري وجمع أدلة الإثبات. الأمر الذي استوجب إعادة النظر في المنظومة الإجرائية الجنائية، بما يضمن إرساء قواعد خاصة تتلاءم مع طبيعة الدليل الرقمي وخصوصية هذا النمط المستحدث من الإجرام.

وقد اتجهت التشريعات المقارنة إلى تطوير إجراءات خاصة أو تعديل قوانينها الإجرائية بما يحقق الفاعلية في الملاحقة الجنائية، مع السعي إلى تحقيق التوازن بين متطلبات مكافحة الجريمة المعلوماتية وضمانات الشرعية الإجرائية، ويُؤمل أن يواكب المشرع الليبي هذا الاتجاه من خلال تبني إطار قانوني متكامل يسترشد بالحلول التشريعية المقارنة والمعايير الدولية ذات الصلة، بما يُسهم في تجاوز صعوبات الإثبات المعلوماتي، وعلى هذا الأساس، سنتناول في **(المطلب الأول)** القواعد الإجرائية الخاصة بالجريمة المعلوماتية، بينما يعالج **(المطلب الثاني)** الإجراءات المستحدثة لمكافحتها في القانون الدولي.

- **المطلب الأول:**

القواعد الإجرائية الخاصة بالجريمة المعلوماتية.

يُقرر المشرع، في إطار تنظيم الجريمة المعلوماتية، قواعد إجرائية خاصة تطال فئات معينة من هذه الجرائم، لا سيما تلك المتعلقة بالاتصالات، والاعتداء على البيانات الشخصية، والتجارة الإلكترونية، والمساس بالملكية الفكرية والأدبية، والتحويل الإلكتروني للأموال، فضلاً عن جرائم القذف والسب عبر الوسائط الإلكترونية، وتتجلى خصوصية هذه القواعد في مستويين رئيسيين: (أولاً)، تكليف مأموري ضبط قضائي متخصصين بمعاينة هذه الجرائم، (وثانياً)، تخصيص هياكل معنية بإثارة الدعوى الجنائية.

- **أولاً: تكليف أفراد متخصصين بمعاينة الجريمة المعلوماتية:**

تقتضي خصوصية الجريمة المعلوماتية، وما يرتبط بها من تعقيدات تقنية وطبيعة رقمية للدليل الجنائي، إسناد مهمة المعاينة والتحري إلى أشخاص يتمتعون بالكفاءة الفنية والخبرة التقنية اللازمة للتعامل مع الأنظمة المعلوماتية ووسائط التخزين الرقمية.

كما تستوجب هذه الخصوصية إخضاع إجراءات الضبط والمعاينة لضمانات شكلية دقيقة، في مقدمتها تحرير محاضر رسمية تثبت الإجراءات المتخذة وتحافظ على سلامة الدليل الرقمي وحجيته في الإثبات الجنائي، وانطلاقًا من ذلك، سيتم تناول مأموري الضبط القضائي المختصين بالجرائم المعلوماتية (1)، ثم بيان الأحكام المتعلقة بتحرير محاضر الضبط الخاصة بها (2).

1. **مأموري الضبط القضائي:**

تُسند في التشريعات المقارنة[34] سلطة معاينة الجرائم المعلوماتية وما يتصل بها من مخالفات إلى فئات متعددة من مأموري الضبط القضائي، وذلك في حدود الاختصاصات المخولة لهم قانونًا، بالنظر إلى الطبيعة التقنية الخاصة لهذا النوع من الجرائم. كما يجوز للجهات الإدارية المختصة بقطاع الاتصالات الاستعانة بخبراء ومتخصصين يتم اختيارهم وفق معيار الكفاءة والخبرة الفنية في مجال تقنيات الاتصال والمعلومات، للمشاركة في أعمال البحث والتحري والكشف عن الجرائم المعلوماتية.

[34] كما نص الفصل (79) من مجلة الاتصالات التونسية، والفصل (10) من مجلة الإجراءات الجزائية.

ويجوز للجهات المختصة[35]، في إطار المهام المسندة إليها، مباشرة أعمال التحري والاستدلال والمعاينة الفنية، والاطلاع على الوثائق والبيانات اللازمة لكشف وقائع الجريمة المعلوماتية، فضلًا عن اتخاذ الإجراءات التحفظية المتعلقة بوسائل التشفير أو الأنظمة التي قد تُشكل خطرًا على شبكات الاتصال أو أمن المعلومات[36]. كما تمتد سلطة المعاينة إلى بعض المجالات المرتبطة بالنشاط الرقمي، كالتجارة الإلكترونية وحماية البيانات الشخصية[37] وحقوق الملكية الفكرية، حيث تُمنح صلاحيات الضبط والمعاينة لموظفين مختصين أو خبراء معتمدين إلى جانب مأموري الضبط القضائي[38].

ويكشف هذا الاتجاه عن حرص المشرع على إسناد مهمة المعاينة إلى عناصر تتمتع بالتأهيل الفني والقدرة التقنية اللازمة للتعامل مع خصوصية الجريمة المعلوماتية والدليل الرقمي. غير أن هذا التوسع في الجهات المختصة، رغم أهميته العملية، لا يُغني عن الحاجة إلى إنشاء جهاز متخصص لمكافحة جرائم المعلوماتية والاتصالات ضمن البنية التنظيمية لوزارة الداخلية، يضم مأموري ضبط قضائي وخبراء فنيين، بما يكفل تحقيق التكامل بين الجانبين الإجرائي والتقني في مواجهة هذا النوع من الجرائم.

2. **اشتراط تحرير محضر ضبط:**

ومن مقتضيات تعزيز الضمانات الإجرائية في هذا المجال، ضرورة إخضاع أعمال المعاينة والتحريز لرقابة قانونية دقيقة، من خلال اشتراط تحرير المحاضر بواسطة أكثر من مختص، وتنظيم التعاون بين الخبراء الفنيين ومأموري الضبط القضائي ضمن إطار إجرائي واضح. كما يتعين على المشرع تحديد القوة الثبوتية لهذه المحاضر بنص خاص، بحيث تكون حجة إلى أن يثبت عكسها، باعتبارها تقوم على قرينة قانونية بسيطة قابلة لإثبات العكس بكافة طرق الإثبات[39].

---

[35] بحسب الفصل (43) من القانون عدد (83 لسنة 2000م) المتعلق بالمبادلات والتجارة الالكترونية.

[36] بحسب ما نص الفصل (19) من الأمر عدد (2726 لسنة 2001م) المؤرخ في (2001/11/20م)، نشر في الرائد الرسمي للجمهورية التونسية المؤرخ في (2001/11/27م) عدد (59)، (ص – 4701).

[37] كما أجاز المشرع التونسي في الفصل (77) من القانون عدد (63 لسنة 2004م) المؤرخ في (2004/07/27م) المتعلق بحماية المعطيات الشخصية.

[38] بحسب الفصل (10) من مجلة الإجراءات الجزائية التونسية، والفصل (54) من قانون (1954م) المؤرخ في (1954/02/24م) المتعلق بحماية الملكية الأدبية والفنية التونسي.

[39] بحسب الفصل (202) من مجلة الديوانية التونسية، والفصل (154) من مجلة الإجراءات الجزائية التونسية.

وتبرز خصوصية أخرى لهذه المحاضر في كونها لا تُحال مباشرة إلى النيابة العامة في بعض الحالات، وإنما تُرفع ابتداءً إلى الجهة الإدارية المختصة لتقدير ما يلزم بشأنها، وهو ما يُضفي على إجراءات تحريك الدعوى العمومية في الجرائم المعلوماتية طابعًا إجرائيًا متميزًا يختلف عن القواعد التقليدية في الإجراءات الجنائية[40].

- **ثانياً: الهياكل المختصة في إثارة الدعوى الجنائية:**

على الرغم من أن النيابة العامة تمثل السلطة الأصلية في إثارة الدعوى العمومية، إلا أنها ليست السلطة الوحيدة المخولة قانوناً بذلك[41]، إذ يمنح القانون الجنائي الاقتصادي للإدارة سلطات واسعة ودوراً مهماً في هذا المجال، وفي إطار جرائم المعلوماتية، إذ وجب أن يجيز المشرع لبعض الإدارات والهيئات المتخصصة إثارة الدعوى الجنائية، ومن أبرزها.

1. **السلطة الإدارية المكلفة بالاتصالات:**

وجب أن تنص الأحكام الخاصة على أن المحاضر الناتجة عن معاينة جرائم الاتصالات تُرسل إلى السلطة المكلف بالاتصالات، التي تدرسها وتتخذ قراراً بشأنها، متمتعةً بسلطة ملائمة الملاحقة ذاتها المخولة للنيابة العامة، إذ لها إما إحالة الملف إلى النيابة العامة المختصة مكانياً، أو اللجوء إلى إجراء الصلح مع المخالف وفقاً للشروط التي يقررها القانون، ويُعتبر هذا التنظيم تطوراً مقارنة بالنظم السابقة التي كانت تكتفي بإرسال نسخ من المحاضر إلى عدة جهات دون منحها سلطة تقديرية، وقد يرتئي المشرع، انطلاقاً من خصوصية هذا النوع من الجرائم وطابعها الفني، أن تكون إحالة هذه الملفات من اختصاص السلطة الإدارية المكلفة بالاتصالات، لكونها وحدها القادرة على فهم المصطلحات التقنية وتكييف الجرائم وإنارة سبيل النيابة العامة في قرارات الإحالة.

غير أنه في إطار سلطة ملائمة التتبع والملاحقة، يجوز للإدارة أن تعدل عن إحالة الملف إلى القضاء الجنائي، ولكن القانون يحصر ذلك في حالات معينة كالمخالفات المتعلقة بالإضرار بوسائل الاتصالات، حيث يمكن للإدارة المختصة إجراء الصلح، وهو ما يؤدي إلى انقضاء الدعوى الجنائية مع حفظ الحقوق المدنية للمتضررين، مع الإشارة إلى أن السلطة الإدارية المذكورة لا تملك ممارسة الادعاء الجنائي مباشرة أمام المحكمة المختصة، بل لا يمكنها الوصول إلى النزاع القضائي

---

[40] ينظر: منية بن ترادايت غمارسة: خصوصية الجريمة المعلوماتية، المجلة الجزائية (9 – 2013/12/10م).

[41] وهو ما يتوافق مع نص المادتين: الأولى، والثانية من قانون الإجراءات الجنائية الليبي.

إلا عن طريق النيابة العامة، التي تبقى الهيكل الوحيد القائم بممارسة الدعوى الجنائية، وعليه، تعتبر السلطة الإدارية طرفاً منظماً في هذه الممارسة، ويتم تمثيلها أمام الجلسات بواسطة أحد أعضاء إدارة قضايا الدولة الذي لا يملك سوى طلب تسليط العقوبات المادية والحجز للمضبوطات.

2 . الهيئة الوطنية لحماية البيانات الشخصية:

وجب أن تُنشأ بقانون هيئة وطنية مكلفة بحماية البيانات الشخصية، تتمتع بالشخصية المعنوية والاستقلال المالي، ويتمثل دورها في تلقي التصريحات المتعلقة بمعالجة البيانات الشخصية، وضبط الضمانات الواجب احترامها، وتلقي الشكاوى والبلاغات من الأفراد حول المساس ببياناتهم، والبحث فيها، وتُوجب عليها إعلام النيابة العامة المختصة مكانياً بالجرائم المعلوماتية التي تبلغ إلى علمها، ولا تحتج بالسر المهني كعائق.

وتمنح هذه الهيئة سلطة إجراء الصلح بالوساطة في بعض الجرائم، مما يُثبت أنها تتمتع بسلطة ملائمة التتبع نفسها المخولة للنيابة العامة، فهي التي تقرر إحالة المحاضر إلى النيابة العامة أو إجراء الصلح بالوساطة في الجرائم المحددة قانوناً كتعديل وجهة البيانات الشخصية لتحقيق منفعة شخصية أو للغير، أو إحداث ضرر بالمعني بالأمر، أو مواصلة المعالجة رغم اعتراضه.

كما يُمكن للهيئة، بعد سماع المسؤول عن المعالجة أو المناول، أن تقرر سحب الترخيص أو منع المعالجة إذا ثبت عدم احترام الواجبات القانونية، وتكون قرارات الهيئة معللة وتُبلغ إلى المعنيين بوساطة محضر منفذ، ويجوز الطعن فيها أمام محكمة الاستئناف المختصة خلال شهر من تاريخ الإعلام، ويُبت في الطعن وفق قواعد قانون المرافعات.

وتُنفذ القرارات بقطع النظر عن الطعن فيها، مع إمكانية وقف تنفيذها بأمر من رئيس محكمة الاستئناف إذا ترتب على تنفيذها ضرر لا يمكن تداركه، وتلتزم المحكمة المتعهدة بالبت في الطعن خلال ثلاثة أشهر، وتقبل أحكامها الطعن بالتعقيب.

3 . منظمات الدفاع عن حقوق الإنسان:

إذا كان السب أو القذف المرتكب بواسطة الصحافة أو أي وسيلة أخرى، بما فيها الوسائل الإلكترونية، موجهاً إلى فئة من الأشخاص على أساس أصلهم أو عرقهم أو دينهم، وكان الهدف منه التحريض على الكراهية أو التمييز، فيجوز لكل جمعية ثبت تأسيسها قبل سنة من تاريخ ارتكاب الفعل، وكان نظامها الأساسي يؤهلها للدفاع عن حقوق الإنسان ومناهضة التمييز، أن تثير الدعوى العمومية.

أما إذا كانت الجريمة موجهة ضد أشخاص معينين، فلا يجوز لهذه الجمعيات مباشرة الدعوى إلا بموافقة كتابية وصريحة من الأشخاص المعنيين.

تلك هي الإجراءات التي يجب أن تتخذ من المشرع الليبي على مستوى القانون الوطني حتى يصبح القانون رقم (5 لسنة 2022م) نافذ إجرائيا. فما هي الإجراءات المستحدثة على المستوى الدولي لمجابهة الجريمة المعلوماتية؟.

- **المطلب الثاني:**

الإجراءات المستحدثة للتصدي للجريمة المعلوماتية في القانون الدولي.

تُشكل اتفاقية بودابست بشأن الجريمة المعلوماتية المرجع الدولي الأبرز في مجال مكافحة هذا النوع من الجرائم، إذ أرست مجموعة من القواعد والأحكام التي يمكن الاستناد إليها على مستويين متكاملين: أولهما على صعيد التشريعات الوطنية للدول من خلال تطوير الأطر الموضوعية والإجرائية المنظمة للجريمة المعلوماتية **(الفرع الأول)**، وثانيهما على مستوى التعاون الدولي عبر تعزيز آليات التنسيق والمساعدة القانونية المتبادلة في مواجهة الجرائم ذات الطابع العابر للحدود **(الفرع الثاني)**.

- **الفرع الأول:**

الإجراءات الممكن اعتمادها على المستوى الوطني للدول.

نظرًا لخصوصية الجريمة المعلوماتية وما تثيره من صعوبات تقنية وإجرائية في مجال البحث والتحقيق والإثبات، اتجهت التشريعات الحديثة والاتفاقيات الدولية إلى إقرار تدابير إجرائية خاصة تكفل فعالية الملاحقة الجنائية وحماية الدليل الرقمي من الضياع أو العبث، وفي هذا الإطار، أوصت اتفاقية بودابست بشأن الجريمة السيبرانية بجملة من الوسائل الإجرائية القابلة للاعتماد على مستوى القانون الوطني، بهدف تنظيم قواعد البحث والتحري وإثبات الجريمة المعلوماتية بما يتلاءم مع طبيعتها التقنية والعابرة للحدود.

1. **حفظ البيانات والكشف عنها من قبل مزود الخدمة:**

اتجهت اتفاقية بودابست بشأن الجريمة السيبرانية إلى إقرار مجموعة من التدابير الإجرائية الخاصة الرامية إلى ضمان فعالية البحث والتحقيق في الجرائم المعلوماتية، ومن أبرزها نظام حفظ البيانات الرقمية والكشف عنها من قبل مزودي الخدمات، وقد ميزت الاتفاقية في هذا الإطار بين صورتين

أساسيتين، تتمثل الأولى في حفظ البيانات المخزنة والكشف عنها، بينما تتعلق الثانية بالحفظ والكشف السريع لبيانات النشاط أو حركة الاتصالات.

ويقصد بحفظ البيانات المخزنة اتخاذ الإجراءات الفنية والقانونية الكفيلة بضمان سلامة البيانات الرقمية وحمايتها من التعديل أو الإتلاف أو المحو[42]، مع الإبقاء على طبيعتها الأصلية وإمكانية الرجوع إليها عند الاقتضاء، وهو ما يختلف عن مجرد الأرشفة التي لا تتجاوز وظيفة التخزين، وفي هذا السياق، ألزمت الاتفاقية مزودي الخدمة بالاحتفاظ بالبيانات المخزنة لديهم لفترة زمنية محددة، مع تمكين سلطات البحث والتحقيق من الوصول إليها أو الكشف عنها متى اقتضت ضرورات التحقيق ذلك، على أن يلتزم مزود الخدمة خلال مدة الحفظ باتخاذ التدابير اللازمة للحفاظ على سلامة البيانات وسريتها، وعدم إشعار الشخص المعني بالإجراء المتخذ بحقه، ضمانًا لفعالية التحريات وعدم التأثير على سيرها.

أما فيما يتعلق بالحفظ والكشف السريع عن بيانات النشاط، فإن المقصود بها البيانات المرتبطة بحركة الاتصال الإلكتروني، كبيانات المصدر والوجهة والمسار والتوقيت ونوع الخدمة المستعملة، وهي بيانات تكتسي أهمية بالغة في تحديد هوية المستخدمين ومزودي الخدمة ومسار انتقال المعلومات ومكان تواجد المشتبه فيه، ونظرًا للطبيعة المتشعبة لشبكات الاتصال وتعدد المتدخلين في نقل البيانات، أوصت الاتفاقية بإلزام مختلف مزودي الخدمات الذين ساهموا في تمرير أو معالجة البيانات بحفظها والكشف عنها بناءً على طلب السلطات المختصة، مع ترك تنظيم الإجراءات التفصيلية المتعلقة بالحفظ والكشف للتشريعات الوطنية.

وقد أخذت بعض التشريعات المقارنة بهذا الاتجاه، من خلال فرض التزامات قانونية على مزودي خدمات الإنترنت والاتصالات بحفظ محتوى البيانات أو سجلات النشاط الإلكتروني لفترات محددة، وتمكين السلطات المختصة من الاطلاع عليها عند الضرورة، بما يحقق التوازن بين مقتضيات مكافحة الجريمة المعلوماتية وضمان احترام الخصوصية وحماية البيانات الشخصية.

---

[42] حفظ البيانات والكشف عنها من قبل مزود الخدمة: يقصد به التزام مزود خدمات الاتصالات أو الإنترنت أو الاستضافة بالاحتفاظ بالبيانات والسجلات الإلكترونية المرتبطة باستخدام الشبكات أو الأنظمة المعلوماتية لمدة معينة، وتمكين السلطات المختصة من الوصول إليها أو الإفصاح عنها بناءً على أمر قانوني، متى كانت لازمة لأغراض التحري أو التحقيق أو الإثبات في الجرائم المعلوماتية، بما يضمن المحافظة على الأدلة الرقمية وعدم ضياعها أو العبث بها.

ولا يترتب على التزام مزودي الخدمة بالحفظ والكشف تحملهم مسؤولية صحة البيانات أو مضمونها، باعتبار أن دورهم يقتصر على الحفظ الفني وتوفير البيانات المتاحة لديهم، دون أن يمتد إلى التحقق من هوية المستخدمين أو صحة المعلومات المتداولة عبر الشبكات الرقمية.

2. إجراءات التفتيش والحجز على المعطيات المعلوماتية المخزنة:

نظراً لخصوصية المعطيات غير الورقية، أوجبت الاتفاقية على الدول تكييف قواعد التفتيش والضبط أو الحجز التقليدية – المطبقة على السندات الورقية– لتشمل السندات الإلكترونية كأداة إثبات في اطار الإثبات الرقمي، شريطة أن يتم الضبط وفق الإجراءات القانونية السليمة، وتُبقي الاتفاقية على القواعد الإجرائية التقليدية لتحديد السلطات المؤهلة قانوناً، مع ضرورة مراعاة خصوصية السندات غير الورقية داخل الأنظمة الإلكترونية، والاستعانة بذوي الخبرة الفنية في النظام المعلوماتي المعني.

3. الجمع الآني في الوقت الفعلي للمعطيات الإلكترونية:

تناولت الاتفاقية إمكانية الجمع الآني لبيانات النشاط المعلوماتي واعتراض بيانات المحتوى، تحقيقاً لمبدأ السرعة قبل إتلاف هذه المعطيات أو تغييرها من قبل مزود الخدمة، ويهدف هذا الإجراء إلى تسجيل المعطيات المتداولة لحظة بلحظة، وليس المخزنة مسبقاً.

غير أن هذا الإجراء يمس بحرمة الحياة الخاصة[43]، لذلك لا تلجأ إليه معظم الدول إلا في الجرائم الخطيرة والمنظمة، ولا سيما الإرهابية، وعلى الرغم من معارضة بعض الدول له لما فيه من مساس بحرية الفرد، فإنه يظل أكثر الوسائل نجاعة لإثبات الأفعال الإجرامية.

يُشبه هذا الإجراء التنصت الهاتفي في الشبكات التقليدية، إلا أن التنظيم الداخلي وحده لا يكفي، لأن الجرائم المعلوماتية لا تعترف بالحدود الجغرافية، مما يستلزم استحداث آليات تعاون دولي لجمع وسائل الإثبات المتفرقة بين دول متعددة، وهو ما أوصت به الاتفاقية.

---

[43] **حرمة الحياة الخاصة**: يقصد بها حماية حق الإنسان في عدم التدخل غير المشروع في شؤونه الشخصية أو أسراره أو بياناته أو مراسلاته، بما يكفل احترام كرامته وحريته الفردية. وقد أكدت الصكوك والاتفاقيات الدولية هذا الحق باعتباره من الحقوق الأساسية للإنسان، كما قررته الشريعة الإسلامية من خلال حماية الخصوصية وصيانة الأسرار والنهي عن التجسس وتتبع عورات الآخرين، بما يحقق التوازن بين حماية الفرد ومتطلبات المجتمع، وتستند إلى جملة من المبادئ الشرعية التي تحظر الاعتداء على خصوصية الإنسان أو كشف أسراره، ومن أبرزها قوله تعالى: ﴿وَلَا تَجَسَّسُوا﴾ [الحجرات: 12]، بما يؤكد صيانة الحياة الخاصة وحماية الفرد من التدخل غير المشروع في شؤونه.

- **الفرع الثاني:**

التدابير القابلة للاعتماد على مستوى التعاون الدولي.

تعد اتفاقية بودابست[44] أول معاهدة تناولت التعاون الدولي في مكافحة الجرائم المعلوماتية بشكل مباشر، وأرسَت قواعد عامة وخاصة في هذا الشأن.

1. **المبادئ العامة للتعاون الدولي:**

وهي ثلاثة مباديء تتعلق بالسرعة، والتجريم، والاعلام التلقائي، ومؤداها كالآتي:

- أ)**: مبدأ السرعة:** نظراً لسرعة انتقال المعلومات الإلكترونية وتعديلها أو زوالها، توصي الاتفاقية باستخدام وسائل الاتصال الحديثة من مثل تقنية البريد الإلكتروني والفاكس؛ بدلاً من الوسائل التقليدية، والمتمثلة في البريد والطرق الدبلوماسية.
- ب)**: مبدأ تجريم الفعل الثنائي أو "ازدواجية التجريم"**: يجب أن يكون الفعل المسند إلى المتهم معاقباً عليه في كل من الدولة الطالبة والدولة المطلوب إليها التعاون، حتى ولو اختلف التكييف القانوني للفعل بينهما.
- ج)**: مبدأ واجب الإعلام التلقائي:** إذا توصلت دولة إلى وسائل إثبات تتعلق بجرائم موضوع النظر، فيجب عليها إعلام الدول المعنية بذلك تلقائياً، حتى دون طلب مسبق.

2. **المبادئ الخاصة للتعاون الدولي:**

أوصت الاتفاقية بإنشاء شبكة اتصالات معلوماتية بين الدول الأعضاء لضمان السرعة في تبادل المعلومات والتشاور المباشر، على غرار شبكة مجموعة الثمانية، ويُشترط على كل دولة توفير نقطة اتصال دائمة خلال الأربع والعشرين ساعة على مدار أيام الأسبوع، وذلك لتقديم المساعدة الآنية في البحث عن وسائل الإثبات، وتشمل المساعدة:

أ. الإرشاد الآني إلى أماكن التخزين،
ب. وتقديم النصائح الفنية والقانونية،
ت. والمبادرة المباشرة لإنهاء الأعمال الاستقرائية والتحفظية عند الضرورة،

---

[44] **اتفاقية بودابست بشأن الجرائم المعلوماتية**: هي أول اتفاقية دولية متخصصة في مكافحة الجرائم الإلكترونية، اعتمدها مجلس أوروبا عام 2001، وتهدف إلى توحيد التجريم المتعلق بالأفعال المعلوماتية، ووضع قواعد إجرائية لجمع وضبط الأدلة الرقمية، وتعزيز التعاون الدولي في مواجهة الجرائم التي تتم عبر الأنظمة والشبكات الإلكترونية. وتُعد إطارًا مرجعيًا مهمًا في تطوير التشريعات الجنائية المعلوماتية الحديثة.

ث. وتسهيل حفظ المعطيات واستلام وسائل الإثبات بشكل إلكتروني وسريعة.

وتعود لكل دولة حرية تحديد موقع هذه الشبكة وإسناد المهمة إلى هيكل مستقل مزود بوسائل تكنولوجية متطورة وكفاءات ذات خبرة لضمان النجاعة.

ورغم سعي الاتفاقية إلى تحقيق النجاعة في إثبات الجريمة المعلوماتية من خلال آليات بحث جنائي حديثة تختلف عن الطرق التقليدية، فإن التطبيقات العملية لهذه التقنيات قد تمس بحقوق الإنسان والحريات الأساسية؛ لذا، أكدت ديباجة الاتفاقية على ضرورة احترام الاتفاقيات السابقة، لا سيما الاتفاقية الأوروبية لحقوق الإنسان العام (1950م)، والعهد الدولي الخاص بالحقوق المدنية والسياسية العام (1966م)، وشددت الاتفاقية على أن تكون الإجراءات المتخذة مناسبة لجسامة الجريمة، وذلك بإخضاع الإجراء إلى مبدأ النسبية أو الملائمة.

ونتخلص إلى إن تخصيص الجريمة المعلوماتية بتنظيم دولي خاص يُجسد الطبيعة العابرة للحدود التي تميز هذا النمط المستحدث من الإجرام، ويكشف في الوقت ذاته عن محدودية القواعد الوطنية التقليدية في مواجهته، الأمر الذي فرض ضرورة تعزيز التعاون الدولي وتوحيد الجهود التشريعية والأمنية والقضائية للتصدي لمخاطره المتنامية.

وفي هذا الإطار، اضطلعت العديد من المنظمات والهيئات الدولية بدور مهم في مكافحة الجرائم المعلوماتية، وفي مقدمتها المنظمة الدولية للشرطة الجنائية "الإنتربول"، التي أنشأت هياكل متخصصة تُعنى بتنسيق الجهود بين أجهزة مكافحة الجرائم المعلوماتية في مختلف الدول، من خلال تبادل المعلومات والخبرات، وتنظيم الدورات التدريبية المتعلقة بآليات الكشف عن الجرائم المعلوماتية وسبل تعزيز الأمن السيبراني.

ورغم التطور الذي شهدته بعض التشريعات المقارنة في هذا المجال، فإن مواجهة الجريمة المعلوماتية لا تزال تقتضي مزيدًا من الإصلاح التشريعي والإجرائي، خاصة فيما يتعلق بإرساء قواعد خاصة للتحري والتحقيق والإثبات تتلاءم مع خصوصية الدليل الرقمي والطابع التقني لهذه الجرائم. كما أن تشتت النصوص القانونية وغياب التنظيم الإجرائي المتكامل قد يؤدي إلى إضعاف فعالية العدالة الجنائية في ملاحقة مرتكبي الجرائم المعلوماتية وتحقيق الردع القانوني اللازم.

ومن ثم، تبدو الحاجة ملحة إلى تبني سياسة جنائية معلوماتية متكاملة تقوم على عدة مرتكزات أساسية، من أهمها: وضع إطار قانوني موحد للجرائم المعلوماتية من الناحيتين الموضوعية والإجرائية،

وإنشاء وحدات أمنية متخصصة في مكافحة الجرائم الإلكترونية، وتأهيل أعضاء السلطة القضائية ومأموري الضبط القضائي فنيًا وتقنيًا للتعامل مع الدليل الرقمي، فضلًا عن تعزيز التعاون الدولي في مجال تبادل المعلومات والمساعدة القضائية، بالنظر إلى ما تمثله الجرائم المعلوماتية من تهديد حقيقي لأمن الدول واستقرارها ومصالحها الحيوية، ويضمن تحقيق فاعلية متقنة لإثبات الجريمة المعلوماتية.

• الفصل الثاني: إثبات الجريمة المعلوماتية.

يتميز العصر الرقمي المعاصر بأنه مرحلة متقدمة من تطور النظم التقنية، حيث أضحت تكنولوجيا المعلومات والاتصالات الإطار الحاكم لمختلف المعاملات والأنشطة الإنسانية، وهو ما رافقه ظهور أنماط إجرامية مستحدثة عُرفت بالجرائم المعلوماتية، التي تتسم بطابع تقني معقد ووسائل ارتكاب غير مادية تعتمد على النظم الحاسوبية وشبكات الاتصال والفضاء الإلكتروني.

وتُعرّف الجريمة المعلوماتية بأنها كل فعل أو امتناع يتم التخطيط له أو تنفيذه باستخدام الحاسب الآلي أو شبكات المعلومات أو الإنترنت أو وسائل التواصل الاجتماعي، بقصد تسهيل ارتكاب جريمة أو الإخلال بالنظام القانوني، سواء استهدف هذا الفعل الأنظمة المعلوماتية ذاتها عبر الاختراق أو التعطيل أو التعديل أو الحذف أو استهدف البيانات والبرامج المخزنة فيها، وتشمل هذه الجرائم صورًا متعددة، من بينها الاعتداء على سلامة وسرية نظم المعلومات، وانتهاك الحياة الخاصة للأفراد، والجرائم المالية المرتبطة بالاحتيال والتزوير المعلوماتي.

ومتى كانت الجريمة المعلوماتية قائمة على معطيات رقمية غير مادية، فإن إثباتها يُعد محورًا جوهريًا في الدعوى الجنائية، إذ لا قيمة للحق محل الحماية القضائية ما لم يقم الدليل على الواقعة المنشئة له، الأمر الذي يفرض تطوير وسائل الإثبات بما يتلاءم مع الطبيعة الخاصة للدليل الرقمي، ويستجيب للتحديات التقنية التي تفرضها هذه الجرائم، وعلى هذا الأساس، نتناول في اطار تحليلي وسائل إثبات الجرائم المعلوماتية في **(المبحث الأول)**، ثم نعرض لمعوقات إثباتها في ضوء خصوصية البيئة الرقمية وتعقيداتها الفنية في **(المبحث الثاني)**.

• المبحث الأول: وسائل إثبات الجرائم المعلوماتية.

يُعد إثبات الجريمة المعلوماتية من أكثر المسائل تعقيدًا في نطاق القانون الجنائي المعلوماتي، بالنظر إلى الطبيعة التقنية لهذا النوع من الجرائم واعتمادها على بيئة رقمية تختلف عن البيئة التقليدية

لارتكاب الجرائم، ومع ذلك، فإن قواعد الإثبات الجنائي لا تنفصل كليةً عن الأصول العامة، إذ يمكن الاستناد إلى بعض وسائل الإثبات التقليدية متى أمكن تكييفها مع خصوصية الجريمة الإلكترونية.

غير أن التطور المتسارع في تقنيات المعلومات والاتصالات أفرز في المقابل وسائل إثبات مستحدثة تتلاءم مع طبيعة الدليل الرقمي والآثار الإلكترونية التي تخلّفها الجريمة المعلوماتية، الأمر الذي استدعى تطوير آليات البحث والتحقيق والإثبات بما يحقق الفعالية في كشف الحقيقة الجنائية.

وعلى هذا الأساس، سيتم تناول وسائل إثبات الجرائم المعلوماتية من خلال **(المطلب الأول)**؛ يُخصص لوسائل الإثبات التقليدية، بينما يتناول **(المطلب الثاني)** وسائل الإثبات الحديثة المرتبطة بالدليل الرقمي.

- **المطلب الأول: وسائل الإثبات التقليدية.**

على الرغم من خصوصية الجريمة المعلوماتية وطبيعتها التقنية، فإن وسائل الإثبات التقليدية لا تزال تحتفظ بقيمتها في مجال الإثبات الجنائي المعلوماتي، متى أمكن تكييفها مع البيئة الرقمية وطبيعة الدليل الإلكتروني. فالإقرار والشهادة والمعاينة والتفتيش والضبط أو الحجز والخبرة تظل من الوسائل الإجرائية المعتمدة في الكشف عن الحقيقة، غير أن فعاليتها في الجرائم المعلوماتية تتوقف على مدى قدرة سلطات البحث والتحقيق على توظيفها بما يتلاءم مع خصوصية الأنظمة المعلوماتية والدليل الجنائي الرقمي، وسنتناولها تباعا على النحو التالي:

- **أولا: الاعتراف في الجريمة المعلوماتية:**

والاعتراف يُقصد به الإقرار، أي: اعتراف المتهم على نفسه بارتكاب الوقائع المكوِّنة للجريمة، سواء تعلق ذلك بكامل الأفعال المنسوبة إليه أو ببعض عناصرها الجوهرية. ويُعد الاعتراف من وسائل الإثبات التقليدية المعترف بها في المادة الجنائية، لما قد يتضمنه من كشف مباشر للحقيقة متى صدر بصورة صحيحة ومطابقة للواقع.

ولا يختلف الاعتراف في نطاق الجريمة المعلوماتية، الخاضعة لأحكام قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م)، عن الاعتراف في الجرائم التقليدية من حيث طبيعته القانونية أو حجيته في الإثبات، إذ يظل خاضعًا للسلطة التقديرية لقاضي الموضوع، الذي يملك تقدير قيمته ومدى انسجامه مع باقي أدلة الدعوى وظروفها. كما يبقى الأخذ به مرهونًا بتكوين القناعة الوجدانية للمحكمة وفقًا للقواعد العامة المقررة في قانون الإجراءات الجنائية، ولاسيما ما تقضي به المادة (275) إجراءات بشأن حرية القاضي الجنائي في تكوين اقتناعه من الأدلة المطروحة أمامه.

- **ثانيا: الشهادة في الجريمة المعلوماتية:**

تُعد الشهادة من وسائل الإثبات التقليدية المعترف بها في الإجراءات الجنائية، وتتحقق من خلال سماع أقوال شخص أدرك الواقعة الإجرامية بإحدى حواسه، سواء بالمشاهدة أو السماع أو غير ذلك من وسائل الإدراك المباشر، بقصد الاستدلال بها على حقيقة الواقعة محل التحقيق، ولا تختلف الشهادة، في نطاق الجريمة المعلوماتية الخاضعة لأحكام قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م)، من حيث طبيعتها القانونية عن الشهادة في الجرائم التقليدية التي نظمتها المواد (93 – 104) إجراءات، غير أن خصوصية البيئة الرقمية أفرزت نوعًا متميزًا من الشهود يُعرف اصطلاحًا بـ"الشاهد المعلوماتي".

ويقصد بالشاهد المعلوماتي الشخص الفني المتخصص في تقنيات الحاسب الآلي ونظم المعلومات والاتصالات، والذي تتوافر لديه معلومات فنية أو تقنية جوهرية تتعلق بالنظام المعلوماتي محل الجريمة أو بآليات المعالجة الآلية للبيانات، متى كانت مصلحة التحقيق تقتضي الاستعانة بمعرفته الفنية للكشف عن الحقيقة، ويتميز هذا الشاهد عن الشاهد التقليدي بأن شهادته تقوم، في جانب كبير منها، على المعرفة التقنية والخبرة المتخصصة المرتبطة بالبنية المعلوماتية والبرمجية محل الفحص.

ويشمل الشاهد المعلوماتي عدة فئات فنية متخصصة، من أبرزها:

1. **مشغلو الحاسب الآلي** :وهم الأشخاص المسؤولون عن تشغيل أجهزة الحاسب والأنظمة المرتبطة بها، والذين يمتلكون خبرة عملية في إدخال البيانات ومعالجتها وتشغيل البرامج ونقل المعلومات إلى وسائط التخزين المختلفة .
2. **المحللون** :وهم المختصون بتحليل النظم وتجميع البيانات المتعلقة بها، ودراسة بنيتها الوظيفية وتقسيمها إلى وحدات مترابطة للكشف عن العلاقات الفنية بين عناصر النظام المعلوماتي .
3. **المبرمجون وخبراء البرمجة** :وهم المختصون بإعداد البرامج والأوامر البرمجية، وينقسمون إلى :

أ. **مخططي برامج التطبيقات**، الذين يتولون تحويل متطلبات النظام إلى برامج دقيقة تحقق الوظائف المطلوبة.

ب. **مخططي برامج النظم**، الذين يختصون بتطوير برامج التشغيل وإدخال التعديلات الفنية عليها وصيانتها.

4. **مهندسو الصيانة والاتصالات** :وهم المسؤولون عن صيانة مكونات الحاسب الآلي وشبكات الاتصال المرتبطة به وضمان سلامتها الفنية.
5. **مديرو النظم المعلوماتية** :وهم القائمون على إدارة وتشغيل النظم المعلوماتية والإشراف على بنيتها التقنية وتأمينها.

وتخضع الشهادة التي يدلي بها هؤلاء، شأنها شأن غيرها من أدلة الإثبات، للسلطة التقديرية لقاضي الموضوع، الذي يملك تقدير مدى حجيتها وقيمتها في الإثبات وفقًا لما يستخلصه من ظروف الدعوى وملابساتها.

وتثير الشهادة في الجريمة المعلوماتية إشكالًا تقنيًا يتعلق بكيفية حفظها وتداولها في الوسائط الإلكترونية، إذ قد تُحفظ في صورة ملفات رقمية داخل أجهزة الحاسب الآلي، أو على وسائط تخزين مادية كأجهزة USB أو البطاقات الذكية، وقد تأخذ شكل "شهادة برنامج" يتم تحميلها داخل النظام المعلوماتي، أو تُحفظ عبر وسائل تقنية تتطلب برامج تشغيل أو قارئات إلكترونية خاصة، بما يفرض ضرورة توفير ضمانات فنية تكفل سلامة هذه الشهادات الرقمية وصحة نسبتها وعدم التلاعب بها.

كما يلتزم الشاهد المعلوماتي، متى كانت المعلومات المتوافرة لديه لازمة لكشف الحقيقة، بالتعاون مع سلطات البحث والتحقيق، وتقديم البيانات الفنية الجوهرية المرتبطة بالجريمة، وذلك في الحدود التي يجيزها القانون، ويشمل ذلك تمكين جهات التحقيق من الاطلاع على البيانات المخزنة، والإفصاح عن وسائل الدخول الفنية ككلمات المرور أو الشفرات اللازمة لتشغيل البرامج أو قراءة البيانات، متى كان ذلك ضروريًا لكشف الحقيقة الجنائية، ودون إخلال بالضمانات القانونية المقررة لحماية الحقوق والحريات.

- **ثالثا: المعاينة في الجريمة المعلوماتية:**

يقصد بالمعاينة، في نطاق الإجراءات الجنائية، انتقال سلطة التحقيق أو مأموري الضبط القضائي إلى المكان الذي وقعت فيه الجريمة، لإثبات حالة الأشخاص والأماكن والأشياء، وكل ما من شأنه الإسهام في كشف الحقيقة وتحديد مرتكب الجريمة. المواد (2/14، 21، 74، 77) إجراءات.

وتكتسب المعاينة أهمية خاصة باعتبارها وسيلة مباشرة للوقوف على الآثار المادية للجريمة وضبط ما يتصل بها من أدلة وقرائن، الأمر الذي يقتضي مباشرتها على وجه السرعة حتى لا تمتد الفترة

الزمنية بين وقوع الجريمة وإجراء المعاينة، بما يسمح للجاني بمحو الآثار أو تغيير معالمها بما يؤثر في سلامة الدليل الجنائي.

غير أن المعاينة في مجال الجريمة المعلوماتية تختلف في طبيعتها ونطاقها عن المعاينة في الجرائم التقليدية، ذلك أن هذه الأخيرة غالباً ما تترك مسرحاً مادياً ظاهراً يمكن من خلاله الوقوف على آثار الجريمة وضبط الأدوات المستعملة فيها، بينما تقع الجريمة المعلوماتية في بيئة رقمية أو افتراضية يكون محلها أنظمة الحاسب الآلي أو الشبكات أو قواعد البيانات أو التطبيقات الإلكترونية، الأمر الذي يجعل مسرح الجريمة ذا طبيعة تقنية غير مرئية في أغلب الأحيان، وتتمثل عناصره في الأجهزة والبرمجيات وقواعد البيانات ووسائط التخزين والاتصالات الرقمية.

وفي ضوء خصوصية الجرائم المنصوص عليها في القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، فإن المعاينة الفنية للجريمة المعلوماتية تستوجب مراعاة جملة من الضوابط الإجرائية والتقنية، من أهمها سرعة الانتقال إلى محل الجريمة الرقمية، والسيطرة على البيئة المعلوماتية محل الفحص، ومنع أي تدخل قد يؤدي إلى تغيير البيانات أو إتلافها، فضلاً عن ضرورة توثيق حالة الأجهزة والأنظمة والاتصالات القائمة وقت المعاينة توثيقاً دقيقاً.

كما تقتضي المعاينة تحديد أجهزة الحاسب الآلي ووسائط التخزين والشبكات المتصلة بها، والتحقق من وجود خوادم أو أنظمة اتصال فعّالة قد تسمح بمحو الأدلة أو العبث بها عن بُعد، مع اتخاذ التدابير الفنية اللازمة لتعطيل الاتصال عند الاقتضاء، ويجب كذلك ملاحظة طبيعة النظام المعلوماتي محل الجريمة، وآثار الدخول أو الاستخدام غير المشروع، والسجلات الإلكترونية وبيانات الاتصال المرتبطة به، بما في ذلك عناوين بروتوكول الإنترنت (IP) والملفات والسجلات الرقمية التي قد تُسهم في تحديد مصدر النشاط الإجرامي.

ومن مقتضيات سلامة المعاينة أيضاً، التحفظ على جميع المكونات والوسائط ذات الصلة بالجريمة، بما في ذلك الأقراص والشرائط والملفات المحذوفة أو التالفة، وسلة المهملات الرقمية، والمستندات الورقية أو الإلكترونية المرتبطة بالنظام محل الفحص، مع مراعاة عدم نقل الأجهزة أو الوسائط المعلوماتية إلا وفق إجراءات فنية دقيقة تحول دون تلف البيانات أو فقدانها نتيجة المؤثرات المغناطيسية أو التقنية.

كما تفرض خصوصية الدليل الرقمي قصر إجراءات المعاينة على مأموري الضبط القضائي والخبراء المختصين في مجال تقنية المعلومات، ممن تتوافر لديهم الكفاءة الفنية اللازمة للتعامل مع الأنظمة الرقمية واستخراج البيانات وتحليلها واسترجاعها وفق الأصول العلمية والقانونية المقررة.

وتذهب التشريعات المقارنة في هذا الاتجاه إلى إسناد مهام المعاينة والتحقيق في الجرائم المعلوماتية إلى وحدات متخصصة تتبع الجهات الأمنية المختصة، مع تمكينها من الاستعانة بالخبراء والفنيين المؤهلين قانوناً، ضماناً لسلامة الإجراءات وحجية الدليل الرقمي أمام القضاء.

- **رابعا: الضبط والتفتيش في الجريمة المعلوماتية:**

من المعلوم الآن أن الحاسوب ينكوّن من مكونات مادية **(Hardware)**، ومكونات منطقية أو نظامية **(Software)**. كما يمكن أن يكون متصلا بشبكة اتصالات سلكية أو لا سلكية، سواء كان ذلك على المستوى المحلي أو المستوى الدولي:

1. **التفتيش في المجال المعلوماتي:**

ويُقصد بالتفتيش، في نطاق الإجراءات الجنائية، البحث عن الأشياء أو البيانات أو الآثار المتصلة بجريمة وقعت بالفعل، والتي من شأنها الإسهام في كشف الحقيقة وتحديد مرتكبها، وإذا كان التفتيش في الجرائم التقليدية يرد غالباً على الأشخاص أو المساكن أو الأشياء المادية، فإن محل التفتيش في الجريمة المعلوماتية يمتد إلى جميع مكونات النظام المعلوماتي، سواء كانت مادية أو رقمية، بما في ذلك الشبكات والبرامج والبيانات ووسائط التخزين والأشخاص المستخدمين للنظام محل التفتيش.

وقد ثار خلاف فقهي بشأن مدى صلاحية البيانات الرقمية لأن تكون محلاً للتفتيش وفق النصوص الإجرائية التقليدية، باعتبار أن هذه البيانات ذات طبيعة غير مادية. غير أن التطور التشريعي المقارن اتجه إلى إقرار مشروعية التفتيش الإلكتروني، من خلال النص صراحة على جواز تفتيش الأنظمة المعلوماتية وضبط البيانات والرسائل الإلكترونية والبريد الإلكتروني والحسابات الرقمية والمواقع الإلكترونية متى اتصلت بالجريمة محل التحقيق.

وتخضع إجراءات التفتيش المعلوماتي لجملة من الضوابط الموضوعية والشكلية:

فمن **الناحية الموضوعية**، يشترط أن يكون هناك فعل مجرّم أو شبهة جدية بارتكاب جريمة معلوماتية، وأن يكون التفتيش لازماً للكشف عن أدوات الجريمة أو عائداتها أو الأدلة الرقمية المرتبطة

بها. كما يجب أن ينصب التفتيش على الأنظمة أو الأشخاص أو الوسائط التي يُحتمل اتصالها بالفعل الإجرامي.

أما من **الناحية الشكلية**، فيتعين أن يجري التفتيش بواسطة جهة مختصة قانوناً، مع مراعاة الضمانات المقررة قانوناً بشأن حضور ذوي الشأن أو من يمثلهم متى أمكن ذلك، واحترام الأوقات والإجراءات المحددة قانوناً، واتخاذ التدابير الكفيلة بالمحافظة على سرية البيانات والمعلومات التي يفرض القانون حمايتها، لاسيما إذا تعلق الأمر ببيانات مهنية أو معلومات مشمولة بالسر المهني أو الخصوصية الرقمية.

يقصد بالتفتيش في المجال المعلوماتي دخول سلطات البحث أو التحقيق إلى الأنظمة المعلوماتية أو نظم المعالجة الآلية للبيانات، بما تتضمنه من مدخلات ومخرجات ووسائط تخزين وقواعد بيانات، بقصد البحث عن الأدلة أو الآثار المرتبطة بالجريمة المعلوماتية والكشف عن مرتكبيها، ويُعد هذا الإجراء من أخطر إجراءات التحقيق الجنائي لما ينطوي عليه من مساس بحرمة الحياة الخاصة وسرية البيانات والاتصالات، الأمر الذي يقتضي ممارسته في حدود الضوابط القانونية المقررة ووفق ضمانات تكفل التوازن بين مقتضيات الكشف عن الحقيقة وحماية الحقوق والحريات الفردية .

وفي إطار القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، يكتسب التفتيش المعلوماتي خصوصية متميزة بالنظر إلى الطبيعة التقنية للبيئة الرقمية وما تتسم به الأدلة الإلكترونية من قابلية للمحو أو التعديل أو النقل عبر الشبكات المعلوماتية، ومن ثم، فإن التفتيش في هذا المجال لا يقتصر على البحث في الأماكن المادية التقليدية، وإنما يمتد إلى النظم المعلوماتية ومكوناتها المادية والمنطقية، وكذلك شبكات الاتصال المرتبطة بها، وعلى النحو التالي:

- **أ): تفتيش أنظمة الحاسب الآلي:**

يشمل التفتيش في هذه الحالة المكونات المادية للحاسب الآلي، كالأجهزة والملحقات الإلكترونية الملموسة، ومن بينها وحدات المعالجة، والذاكرة، ولوحات التحكم، ولوحات المفاتيح، ووسائط التخزين المختلفة، ولا يثير تفتيش هذه المكونات صعوبات جوهرية من الناحية الإجرائية، باعتبارها أشياء مادية يجوز ضبطها والعثور عليها في مسكن المتهم أو محل عمله أو أي مكان آخر، ويخضع تفتيشها للقواعد العامة المقررة في قانون الإجراءات الجنائية بشأن تفتيش الأشخاص والمساكن.

كما يمتد التفتيش إلى المكونات المعنوية أو المنطقية للنظام المعلوماتي، والمتمثلة في البرامج والتطبيقات وقواعد البيانات وأنظمة التشغيل والتعليمات الإلكترونية اللازمة لمعالجة البيانات وتشغيل الحاسب الآلي، وتنقسم هذه البرامج إلى نظم أساسية تتولى تشغيل النظام المعلوماتي، وبرامج تطبيقية تمكن المستخدم من تنفيذ وظائف وأعمال محددة، وقد تشكل هذه العناصر محلاً للجريمة أو وسيلة لارتكابها أو دليلاً عليها.

- ب): **تفتيش شبكات الحاسب الآلي:**

قد يرد التفتيش على الشبكات المعلوماتية المتصلة بالحاسب الآلي محل الجريمة، لاسيما إذا كان النظام المعلوماتي مرتبطاً بشبكات داخلية أو خارجية تتيح انتقال البيانات أو تخزينها عن بُعد، وفي هذا الإطار، يثور التمييز بين حالتين:

- **الحالة الأولى:** اتصال النظام المعلوماتي بأجهزة أو شبكات داخل إقليم الدولة، وفي هذه الصورة يجوز لسلطات التحقيق توسيع نطاق التفتيش ليشمل الأنظمة أو البيانات المتصلة بالحاسب محل التفتيش متى كان ذلك لازماً لإظهار الحقيقة والكشف عن الجريمة.
- **أما الحالة الثانية:** فتتعلق باتصال النظام المعلوماتي بأنظمة أو خوادم موجودة خارج إقليم الدولة، وهي من أكثر الصور تعقيداً في الجرائم المعلوماتية، إذ يلجأ بعض الجناة إلى تخزين البيانات أو إدارة الأنشطة الإجرامية عبر خوادم أجنبية بقصد عرقلة إجراءات التحقيق والحيلولة دون ضبط الأدلة الرقمية.

ومن ثم، فإن مباشرة التفتيش العابر للحدود تقتضي وجود تعاون قضائي دولي أو اتفاقيات ثنائية أو متعددة الأطراف تنظم تبادل المساعدة القانونية والإجراءات المتعلقة بالحصول على الأدلة الإلكترونية.

2. **الضبط في المجال المعلوماتي:**

يقصد بالضبط أو الحجز، في نطاق الإجراءات الجنائية، وضع اليد على الأشياء أو الوسائط المرتبطة بالجريمة متى كان من شأنها الإسهام في كشف الحقيقة أو الاستدلال على مرتكبها، ويُعد الضبط من أهم الإجراءات التحفظية التي تباشرها سلطات التحقيق أو مأمورو الضبط القضائي، لما يترتب عليه من المحافظة على الأدلة ومنع العبث بها أو إخفائها. غير أن خصوصية الجريمة

المعلوماتية وما يرتبط بها من أدلة رقمية تفرض مفهوماً متميزاً للضبط يختلف عن صور الضبط التقليدية المعروفة في الجرائم العادية.

ففي مجال الجرائم المعلوماتي المنصوص عليها في القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية، قد يرد الضبط على المكونات المادية للأنظمة المعلوماتية، كما قد يمتد إلى البيانات والمعلومات الرقمية المخزنة أو المتداولة عبر تلك الأنظمة، باعتبارها تمثل محلاً للجريمة أو وسيلة لارتكابها أو دليلاً على وقوعها.

ويشمل ذلك أجهزة الحاسب الآلي وملحقاتها المختلفة، كوحدة المعالجة المركزية، ولوحة المفاتيح، والشاشات، والفأرة، وأجهزة الاتصال بالشبكات، ووسائط التخزين الإلكترونية، والأقراص الصلبة، والأقراص المدمجة، والأشرطة والبطاقات الممغنطة، فضلاً عن أجهزة الربط والاتصال عبر شبكة الإنترنت، كأجهزة المودم والموجهات الإلكترونية.

ولا يقتضي الضبط في الجرائم المعلوماتية التحفظ على كامل المنظومة الإلكترونية دائماً، بل قد تكتفي جهة التحقيق بنسخ البيانات أو المعطيات محل البحث، أو نسخ البرامج والسجلات اللازمة لفهم محتوى الدليل الرقمي وتحليله، مع حفظها على دعائم تخزين إلكترونية مؤمنة وقابلة للضبط، ضماناً لسلامة البيانات واستمرارية عمل النظام المعلوماتي متى اقتضت الضرورة ذلك.

وتتعدد صور الأدلة المادية القابلة للضبط في الجرائم المعلوماتية، ومن أبرزها الأوراق والمستندات المرتبطة بالنشاط الإجرامي، كالمخططات والبيانات التحضيرية المكتوبة بخط اليد، أو النسخ المطبوعة للمستندات الإلكترونية، أو الأوراق التالفة والممزقة التي قد تتضمن آثاراً تفيد التحقيق، إضافة إلى الوثائق الأصلية أو الحسابات أو السجلات التي تم العبث بها أو تزويرها بواسطة الوسائط المعلوماتية.

كما يشمل الضبط أجهزة الحاسب الآلي وملحقاتها المختلفة متى ثبت اتصالها بالجريمة أو بمرتكبها، باعتبارها الوسيلة الفنية التي استُخدمت في ارتكاب الفعل الإجرامي أو تخزين بياناته، ويمتد ذلك أيضاً إلى وسائط التخزين الرقمية، كالأقراص الصلبة الخارجية والمرنة والأقراص الضوئية، لما قد تحتويه من ملفات أو بيانات أو برامج تمثل دليلاً فنياً على الجريمة. كذلك تُعد البطاقات الممغنطة والبطاقات الذكية وما يرتبط بها من أدوات وبرامج ومواد تقنية من بين الوسائط التي يجوز ضبطها متى اتصلت بالفعل الإجرامي، لاسيما في جرائم التزوير الإلكتروني والاعتداء على نظم الدفع والتحويلات المالية.

ويقتضي الضبط في المجال المعلوماتي مراعاة الأصول الفنية اللازمة للحفاظ على سلامة الدليل الرقمي، من خلال اتخاذ التدابير التقنية الكفيلة بمنع محو البيانات أو تعديلها أثناء إجراءات الضبط أو النقل أو الفحص، وهو ما يستوجب مباشرة هذا الإجراء بواسطة مأموري ضبط قضائي وخبراء فنيين تتوافر لديهم الكفاءة التقنية اللازمة للتعامل مع الأنظمة والوسائط الإلكترونية وفق الضوابط القانونية المقررة.

ويُلاحظ أن التقليد أو النسخ في البيئة الرقمية لا يُعد في ذاته فعلاً مجرّماً، باعتباره صورة من صور المحاكاة التقنية، غير أنه يكتسب وصفه غير المشروع متى انطوى على اعتداء على حق يحميه القانون، كما هو الشأن في تقليد البرامج أو البيانات أو المصنفات الرقمية أو التعدي على حقوق الملكية الفكرية المحمية قانوناً.

- **خامسا: ندب الخبير في الجريمة المعلوماتية:**

تُعد الجريمة المعلوماتية من الجرائم ذات الطبيعة التقنية المعقدة، الأمر الذي يجعل مواجهتها وكشف حقيقتها متوقفاً بدرجة كبيرة على الاستعانة بالخبرة الفنية المتخصصة. فالدليل الرقمي لا يمكن إدراكه أو تحليله بالوسائل التقليدية المعتادة، وإنما يتطلب معرفة دقيقة بالأنظمة المعلوماتية وبرامج الحاسب الآلي ووسائط التخزين والشبكات الإلكترونية وأساليب المعالجة الرقمية للبيانات.

ومن ثم، فإن نجاح إجراءات البحث والتحقيق في الجرائم المنصوص عليها في القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية يرتبط ارتباطاً وثيقاً بكفاءة الخبراء والفنيين القائمين على فحص وتحليل الأدلة الرقمية واستخلاص مدلولها الفني والقانوني.

ويقصد بالخبير المعلوماتي الشخص المتخصص فنياً في مجال تقنيات المعلومات والاتصالات، ممن تتوافر لديه المعرفة العلمية والخبرة العملية التي تمكنه من فحص الأنظمة المعلوماتية وتحليل البيانات الرقمية واستخراج الأدلة الفنية المرتبطة بالجريمة.

وتبرز أهمية الاستعانة بالخبير في كونه يُعين سلطة التحقيق والقضاء على فهم الجوانب التقنية المعقدة للقضية، ويُسهم في تفسير الأدلة الرقمية وربطها بعناصر الجريمة وأركانها القانونية، بما يكفل الوصول إلى الحقيقة وتحقيق العدالة الجنائية.

ولا يكفي في الخبير المنتدب مجرد التأهيل الأكاديمي أو الحصول على مؤهل علمي متخصص، بل يجب أن يقترن ذلك بخبرة عملية وفنية في مجال الأنظمة المعلوماتية وجرائم التقنية الحديثة، بالنظر

إلى التطور المستمر في أساليب ارتكاب الجرائم الإلكترونية وتنوع وسائلها التقنية؛ ذلك أنه لا يوجد – من الناحية العملية– خبير يحيط بجميع أنواع الحواسيب والبرمجيات والشبكات وأساليب الاختراق والجرائم الرقمية المتجددة، مما يفرض ضرورة التخصص الدقيق والتحديث المستمر للخبرات الفنية.

كما يتعين على جهات التحقيق تحديد نطاق مهمة الخبير بدقة، وبيان المسائل الفنية المطلوب فحصها، حتى يؤدي دوره في حدود الاختصاص الفني دون تجاوز إلى المسائل القانونية التي تبقى من صميم اختصاص سلطة التحقيق والمحكمة.

ويقتضي ذلك وجود تنسيق فعّال بين الخبير المعلوماتي وجهات التحقيق، من خلال إحاطة الخبير بطبيعة الواقعة محل التحقيق وأبعادها القانونية، مع ربط النتائج الفنية المستخلصة بعناصر الجريمة المادية والمعنوية.

ويستلزم أداء الخبير لمهامه في مجال الجرائم المعلوماتية الإلمام بجملة من الجوانب الفنية والتقنية، من أبرزها المعرفة الدقيقة بتركيب الحاسب الآلي وطرازه ونظم تشغيله الرئيسية والفرعية، والأجهزة والوسائط الملحقة به، وكلمات المرور وأنظمة التشفير والحماية الإلكترونية، فضلاً عن الإحاطة بطبيعة البيئة المعلوماتية محل الفحص، سواء كانت مركزية أو موزعة، وبوسائل الاتصال المستخدمة فيها، وأماكن تخزين البيانات وكيفية الوصول إليها.

كما يجب أن يكون الخبير قادراً على تحديد مواضع الأدلة الرقمية المحتملة وأشكالها الفنية، واتخاذ التدابير التقنية اللازمة لعزل النظام المعلوماتي عند الحاجة دون إتلاف البيانات أو تغييرها، مع إمكانية نسخ الأدلة الرقمية ونقلها إلى دعائم أخرى بصورة تحافظ على سلامتها وحجيتها القانونية، ويقتضي الأمر كذلك القدرة على تحويل البيانات الرقمية والرموز التقنية إلى أدلة مقروءة ومفهومة يمكن عرضها على جهة التحقيق أو المحكمة بصورة واضحة ومقنعة.

وتتأكد أهمية الخبرة الفنية في الجرائم المعلوماتية بالنظر إلى ما قد يترتب على نقص التأهيل أو الخطأ في التعامل مع الأنظمة الرقمية من إتلاف الأدلة أو ضياعها أو المساس بحجيتها، وهو ما قد يؤدي في النهاية إلى تعذر إثبات الجريمة وإفلات الجاني من العقاب.

ومن ثم، فإن فعالية السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية لا تتوقف على وجود نصوص موضوعية تجرم هذه الأفعال فحسب، وإنما تقتضي أيضاً إرساء قواعد إجرائية متخصصة، وتوفير كوادر فنية مؤهلة، وتعزيز التعاون بين سلطات التحقيق والخبراء الفنيين، فضلاً عن دعم آليات

التعاون الدولي لمواجهة ما تثيره الجرائم المعلوماتية من إشكالات تتعلق بالاختصاص وجمع الأدلة العابرة للحدود.

وإذا كانت وسائل الإثبات التقليدية قد تكفي في كثير من الأحيان لإثبات الجرائم التقليدية، فإن خصوصية الجريمة المعلوماتية وتعقيد الدليل الرقمي يفرضان الاعتماد على وسائل إثبات فنية وتقنية حديثة، يكون للخبرة المعلوماتية فيها الدور المحوري والأساس في كشف الحقيقة الجنائية.

- **المطلب الثاني: وسائل الإثبات الحديثة.**

لقد أفرز التطور التكنولوجي في مجال الجريمة المعلوماتية تحولات جوهرية في منظومة الإثبات الجنائي، إذ لم تعد الوسائل التقليدية كافية وحدها لاستيعاب الطبيعة التقنية والمعقدة للأدلة الرقمية، الأمر الذي استوجب استحداث وسائل إثبات حديثة تتسم بالمرونة والدقة والقدرة على التعامل مع المعطيات الإلكترونية.

وتنقسم هذه الوسائل المستحدثة في مجال الإثبات إلى قسمين متكاملين: وسائل مادية حديثة تتمثل في التقنيات والأدوات الفنية التي تُمكّن من جمع الدليل الرقمي وحفظه وتحليله **(الفرع الأول)**، وإجراءات إجرائية متطورة تتعلق بالأساليب المعتمدة في مباشرة أعمال التحري والتحقيق، سواء ما كان منها ثابتاً ومقنناً أو متغيراً تبعاً لطبيعة الواقعة الإجرامية (الفرع الثاني).

- **الفرع الأول:**

الوسائل المادية الحديثة في الإثبات الجنائي المعلوماتي.

يقصد بالوسائل المادية الحديثة تلك الأدوات والتقنيات الفنية ذات الطبيعة التقنية التي تُستخدم داخل بيئات نظم المعلومات، والتي تستهدف كشف وقوع الجريمة المعلوماتية وتحديد مرتكبيها، من خلال جمع الأدلة الجنائية الرقمية وتحليلها وربطها بالواقعة الإجرامية.

وتتمثل هذه الوسائل في أدوات أو برمجيات متخصصة ذات طابع تقني، غايتها تمكين سلطات البحث والتحقيق من الوصول إلى الدليل الرقمي وتفسيره على نحو يكشف ملابسات الجريمة الإلكترونية

ويحدد هوية الفاعل، ومن أبرزها: بروتوكول IP/TCP، وتقنية البروكسي Proxy[45]، وملفات تعريف الارتباط Cookies، وبرامج التتبع وكشف الاختراق، والأمر فيها كالتالي:

- **أولاً: استخدام بروتوكول** (IP/TCP):

يُعد بروتوكول TCP/IP من أهم البروتوكولات المستخدمة في شبكة الإنترنت، بل يمثل البنية الأساسية لعملها، إذ يتولى بروتوكول TCP مسؤولية تقسيم البيانات إلى حزم معلوماتية وإعادة تجميعها، في حين يقوم بروتوكول IP بتوجيه هذه الحزم عبر الشبكة إلى وجهتها الصحيحة، ويتكون عنوان IP من بيانات تعريفية تشير إلى عدة عناصر، من بينها المنطقة الجغرافية، ومزود الخدمة، والشبكة الفرعية، والجهاز النهائي المتصل بالشبكة.

ويُستخدم عنوان IP في المجال التحقيقي كوسيلة لتتبع مصدر الاتصال وتحديد الجهاز المستخدم في ارتكاب الفعل الإجرامي، بالاستناد إلى البيانات التي يحتفظ بها مزودو خدمات الإنترنت. غير أن الاعتماد على هذا العنوان يثير إشكالات عملية، لكونه يُعرّف الجهاز أكثر من تعريفه للشخص الفاعل، الأمر الذي يطرح صعوبة في نسبة الفعل الإجرامي إلى مرتكبه بشكل مباشر. ومع ذلك، فإنه يُعد قرينة فنية يمكن الاستناد إليها ضد حائز الجهاز أو مستخدمه إلى حين إثبات العكس، كما تزداد صعوبة الإثبات في ظل إمكانية استخدام عناوين IP مزيفة أو برامج إخفاء الهوية لإعاقة التتبع وإخفاء المسارات الرقمية.

- **ثانياً: استخدام ملفات تعريف الارتباط** (Cookies)

تُعد ملفات Cookies ملفات نصية صغيرة تُنشئها المواقع الإلكترونية عند زيارة المستخدم لها، وتُخزن على القرص الصلب بهدف تسجيل بيانات التصفح وتحسين تجربة الاستخدام. وتحتوي هذه الملفات على معلومات ذات قيمة تحقيقية، مثل تواريخ الدخول إلى المواقع، وسجل التعديلات أو التفاعل داخل الموقع، إضافة إلى حفظ كلمات المرور وبيانات الدخول في بعض الحالات.

---

[45] **تقنية البروكسي** :(Proxy) هي خادم وسيط يعمل بين المستخدم وشبكة الإنترنت، حيث تمر الاتصالات والبيانات من خلاله قبل وصولها إلى الوجهة النهائية، ويُستخدم لإخفاء عنوان المستخدم الحقيقي ((IP Address، أو تنظيم حركة البيانات، أو تعزيز الخصوصية والأمن الشبكي. وفي المجال الجنائي المعلوماتي قد تُستخدم هذه التقنية لإخفاء مصدر الاتصال أو صعوبة تتبع مرتكب النشاط الإلكتروني.

وتكمن أهميتها في كونها تُشكل مصدراً مهماً لاستعادة النشاط الرقمي للمستخدم، بما يسمح لسلطات التحقيق بإعادة بناء السلوك الإلكتروني للمتهم وربط نشاطه بالواقعة محل البحث.

- **ثالثاً: استخدام تقنية البروكسي** (Proxy):

تُعد تقنية البروكسي من التقنيات الأمنية المستخدمة كوسيط بين المستخدم وشبكة الإنترنت، حيث تقوم بإعادة توجيه الطلبات والبيانات عبر خادم وسيط قبل وصولها إلى وجهتها النهائية. وتتميز هذه التقنية بوظائف أمنية وتنظيمية متعددة، من بينها التحكم في عمليات الاتصال، وتحديد المستخدمين المصرح لهم، وضبط أوقات الاستخدام، وتصفية المواقع والخدمات المسموح بالوصول إليها.

وتُسجل مزودات البروكسي مختلف عمليات الاتصال في قواعد بيانات خاصة، وهو ما يجعلها ذات أهمية كبيرة في مجال الإثبات الجنائي الرقمي، حيث يمكن الرجوع إلى هذه السجلات لتتبع نشاط المستخدم وتحديد ارتباطه بالواقعة الإجرامية. غير أن هذه التقنية قد تُشكل في الوقت ذاته عائقاً للتحقيق في بعض الحالات، من خلال حجب الوصول إلى بعض البيانات أو تقديم نسخ غير مكتملة من السجلات، دون أن ينفي ذلك قيمتها كوسيلة إثبات فنية مهمة.

- **رابعاً: برامج التتبع وكشف الاختراق:**

تتمثل هذه البرامج في أدوات تقنية متخصصة تهدف إلى رصد محاولات الاختراق والهجمات الإلكترونية، وتتبع مصدرها، وتحديد هوية الجهة المنفذة لها، مع إشعار النظام أو الجهة المتضررة عند وقوع الاعتداء. ومن أمثلتها برنامجHack Tracker V1.2 ، الذي يعمل على رصد محاولات الاختراق بشكل فوري، ثم إغلاق منافذ الدخول غير المصرح بها، مع تتبع مصدر الهجوم وصولاً إلى الجهاز أو الشبكة التي انطلق منها.

كما يوفر هذا النوع من البرامج بيانات تقنية دقيقة، من بينها عنوان IP الخاص بالمهاجم، وتوقيت الهجوم باليوم والساعة، إضافة إلى معلومات مزود الخدمة، وهو ما يجعلها أداة ذات قيمة عالية في مجال الإثبات الجنائي الرقمي وتحديد المسؤولية المعلوماتية.

وبذلك يتضح أن الوسائل المادية الحديثة تمثل ركيزة أساسية في منظومة الإثبات في الجرائم المعلوماتية، لما توفره من إمكانيات تقنية متقدمة في كشف الجريمة وتحديد مرتكبيها، في إطار ما قرره القانون رقم (5 لسنة 2022م) بشأن مكافحة الجرائم الإلكترونية.

- **الفرع الثاني:**

الوسائل الإجرائية الحديثة في الإثبات الجنائي المعلوماتي.

تُعد الوسائل الإجرائية في مجال الإثبات المعلوماتي مجموعة من الإجراءات والأساليب القانونية والفنية المحددة بنصوص التشريع، والتي تُتخذ أثناء مباشرة سلطات البحث والتحقيق لطرق الإثبات الثابتة أو المتغيرة، بهدف كشف واقعة الجريمة المعلوماتية وتحديد هوية مرتكبها، وذلك عبر توظيف تقنيات وبرامج إلكترونية متخصصة تواكب طبيعة هذا النوع من الجرائم.

وتتمثل أبرز هذه الوسائل الإجرائية في اعتراض الاتصالات والمراقبة الإلكترونية، باعتبارهما من أهم الإجراءات المستحدثة ذات الفاعلية في جمع الأدلة الرقمية، ونتناولهما على النحو التالي:

- **أولاً: اعتراض الاتصالات:**

يُعد اعتراض الاتصالات من أخطر وأهم الإجراءات التقنية في مجال الإثبات الجنائي المعلوماتي، لما له من دور محوري في جمع الأدلة الرقمية وتوثيقها، ويُقصد به اعتراض أو تسجيل أو نسخ محتوى الاتصالات التي تتم عبر وسائل الاتصال السلكية أو اللاسلكية، باعتبارها بيانات قابلة للإنتاج والتخزين والاسترجاع والعرض.

وقد اتجهت التشريعات المقارنة، وخاصة القانونين المتعلقة بمكافحة جرائم أنظمة المعلومات والاتصالات، إلى إسناد سلطة الأمر بالاعتراض إلى قاضي التحقيق، بحيث يأذن بالاعتراض الفوري على محتوى الاتصالات وتسجيلها أو نسخها، على ألا تتجاوز مدة الاعتراض ثلاثة أشهر من تاريخ البدء الفعلي في التنفيذ، مع جواز تمديدها مرة واحدة بموجب قرار قضائي معلل صادر عن قاضي التحقيق المختص.

وينصب هذا الإجراء في الغالب على وسائل الاتصال الإلكتروني، ولا سيما رسائل البريد الإلكتروني (E-mail)، التي تتضمن بيانات متعددة ذات أهمية تحقيقية، من بينها تاريخ إنشاء الرسالة وإرسالها واستقبالها، وعنوان المرسل والمرسل إليه. غير أن الأهمية القانونية الأكبر تتركز فيما يُعرف بـ رأس الرسالة **(E-mail Header)**[46]، الذي يحتوي على بيانات تقنية دقيقة، أهمها عنوان بروتوكول

[46] رأس الرسالة الإلكترونية (E-mail Header): هو مجموعة من البيانات التقنية المصاحبة للرسالة الإلكترونية، تتضمن معلومات مثل عنوان المرسل والمستقبل، وتاريخ الإرسال، ومسار انتقال الرسالة عبر خوادم البريد، وعناوين

الإنترنت (IP)، والذي يُمكّن من تحديد الجهاز المستخدم في الإرسال، والموقع التقريبي للاتصال، ومزود خدمة الإنترنت، بما يُسهم في تتبع المصدر الرقمي للواقعة الإجرامية.

- **ثانياً: المراقبة الإلكترونية:**

تُعرف المراقبة الإلكترونية بأنها إجراء أمني ذو طابع معلوماتي، يتمثل في متابعة ورصد النشاط الاتصالي عبر الأنظمة الإلكترونية وشبكات الإنترنت، باستخدام وسائل تقنية متطورة، بهدف جمع البيانات وتحليلها وإفراغ نتائجها في تقارير رقمية تُدرج ضمن ملف التحقيق.

وتتجلى أهمية هذا الإجراء في كونه يُمكّن سلطات التحقيق من تتبع السلوك الإلكتروني للفاعل، ورصد أنماط الاتصال والحركة الرقمية ذات الصلة بالجريمة، بما يُسهم في بناء الدليل الفني.

وقد نصت بعض القوانين المقارنة، وخاصة منها المتعلقة بمكافحة جرائم أنظمة المعلومات والاتصال، على منح كل من النيابة العامة وقاضي التحقيق ومأموري الضبط القضائي المأذون لهم قانوناً، سلطة الإذن بجمع أو تسجيل بيانات حركة الاتصالات بالوسائل الفنية المناسبة، مع إمكانية الاستعانة بمزودي خدمات الاتصالات كل بحسب نطاق الخدمة التي يقدمها، وذلك في إطار احترام الضوابط القانونية المنظمة لهذا الإجراء.

وبذلك، يتبين أن الوسائل الإجرائية الحديثة تمثل امتداداً تطورياً لوسائل الإثبات التقليدية، لكنها تتسم بخصوصية تقنية وقانونية تجعلها أكثر ملاءمة لطبيعة الجريمة المعلوماتية، رغم ما قد يعتري تطبيقها من صعوبات عملية تتعلق بمدى تعقيد البيئة الرقمية وتشابك بياناتها.

- **المبحث الثاني: معوقات إثبات الجريمة المعلوماتية.**

يثير إثبات الجريمة المعلوماتية جملة من الصعوبات العملية والقانونية الناجمة عن خصوصية البيئة الرقمية وطبيعة الدليل الإلكتروني، الأمر الذي يجعل من الوصول إلى الحقيقة الجنائية في هذا النوع من الجرائم مسألة بالغة التعقيد مقارنة بالجرائم التقليدية.

الاتصال (.(IP Addressويُعد من الأدلة الرقمية المهمة في التحقيق الجنائي المعلوماتي؛ إذ يساعد على تتبع مصدر الرسالة والتحقق من مسارها وتحديد الجهات أو الأجهزة المرتبطة بها.

فالجريمة المعلوماتية ترتكب في فضاء افتراضي سريع التغير، يعتمد على وسائل تقنية متطورة تتيح إخفاء الآثار الرقمية أو محوها أو نقلها عبر حدود متعددة، بما ينعكس مباشرة على فعالية إجراءات البحث والتحقيق والإثبات.

وتتخذ معوقات الإثبات في هذا المجال صورتين أساسيتين؛ تتمثل الأولى في المعوقات الموضوعية أو المادية المرتبطة بطبيعة الدليل الرقمي ذاته، وصعوبة الحصول عليه، وما يتصل بالآثار الفنية للجريمة المعلوماتية وإمكانية محوها أو التلاعب بها. أما الصورة الثانية فتتمثل في المعوقات الإجرائية، والمتعلقة بصعوبة الإبلاغ عن الجرائم المعلوماتية، وضعف الخبرة الفنية لدى بعض جهات البحث والتحقيق، فضلًا عن الإشكالات التي يثيرها التعاون الدولي في الجرائم ذات الطابع العابر للحدود.

وعلى هذا الأساس، سنتناول في **(المطلب الأول)** المعوقات الموضوعية لإثبات الجريمة المعلوماتية، بينما يُخصص **(المطلب الثاني)** للمعوقات الإجرائية المرتبطة بعمليات البحث والتحقيق والتعاون الدولي.

- **المطلب الأول:**

المعوقات الموضوعية لإثبات الجريمة المعلوماتية.

تتمثل المعوقات المادية لإثبات الجريمة المعلوماتية في الصعوبات المرتبطة بطبيعة الدليل الرقمي والبيئة التقنية التي تُرتكب فيها الجريمة، إذ يتسم هذا الدليل بطابع غير مادي وقابلية عالية للمحو أو التعديل أو التلاعب، بما يُعقّد عملية استخلاصه والمحافظة على سلامته وحجيته في الإثبات. كما أن الآثار الفنية للجريمة المعلوماتية تتسم بالهشاشة وسرعة الزوال، الأمر الذي ينعكس مباشرة على فعالية إجراءات البحث والتحقيق.

وعليه، سيتم تناول هذه المعوقات المرتبطة بالدليل الرقمي في **(الفرع الأول)**، بينما يتناول **(الفرع الثاني)** المعوقات المتعلقة بالآثار الفنية للجريمة المعلوماتية وإمكانية محوها أو التلاعب بها.

- **الفرع الأول: المعوقات المرتبطة بالدليل الجنائي الرقمي.**

يثير الدليل الجنائي الرقمي العديد من الصعوبات العملية والفنية التي تحد من فعالية إثبات الجريمة المعلوماتية، بالنظر إلى طبيعته التقنية وما يحيط به من وسائل حماية وأنظمة تأمين إلكترونية تعيق الوصول إليه أو استخلاصه بالطرق التقليدية.

كما أن خصوصية هذا الدليل من حيث قابليته للتعديل أو الإخفاء أو التشكيك في سلامته تطرح إشكالات تتعلق بحجيته وقيمته في الإثبات الجنائي، وعلى هذا الأساس، سيتم تناول بيان المعوقات المتعلقة بطبيعة الدليل الرقمي ذاته **(أولا)**، ومن ثم نتناول المعوقات المرتبطة بالحماية الفنية وصعوبة الحصول على الأدلة الرقمية **(ثانيا)**.

- **أولا: معوقات متعلقة بالدليل ذاته:**

يختلف الدليل الجنائي في الجريمة المعلوماتية اختلافًا جوهريًا عن نظيره في الجرائم التقليدية، سواء من حيث طبيعته أو كيفية استخلاصه وإثباته. ففي الجرائم التقليدية يكون الدليل – في الغالب– ذا طبيعة مادية محسوسة، كالسلاح المستخدم في القتل أو أدوات التزوير أو المحررات محل الجريمة، بما يتيح لمأمور الضبط القضائي إدراكه مباشرة بإحدى الحواس ومعاينته وضبطه وفق الإجراءات المعتادة. أما في الجريمة المعلوماتية، فإن الدليل يتخذ صورة رقمية غير مادية، تتمثل في بيانات أو إشارات إلكترونية تنتقل عبر أنظمة الحاسب الآلي والشبكات المعلوماتية، الأمر الذي يجعله غير قابل للإدراك الحسي المباشر بالمعنى التقليدي.

ولا تقتصر خصوصية الدليل الرقمي على كونه غير مرئي، بل تمتد إلى كونه ذا طبيعة تقنية معقدة، إذ تظهر البيانات الإلكترونية في صورة رموز أو نبضات رقمية لا يمكن فهمها أو قراءتها إلا بواسطة الأنظمة والبرمجيات المخصصة لذلك، وهو ما يجعل التعامل معها متوقفًا على الخبرة الفنية والتقنية المتخصصة. كما أن هذا الدليل يتميز بقابليته السريعة للمحو أو التعديل أو الإخفاء دون أن يترك أثرًا ماديًا ظاهرًا، بما يتيح للجاني إمكانية طمس معالم الجريمة وإزالة آثارها الرقمية في وقت وجيز، الأمر الذي ينعكس سلبًا على إمكانية اكتشاف الجريمة أو تحديد هوية مرتكبها.

ويبرز هذا الإشكال بصورة واضحة في جرائم الدخول غير المشروع أو التسلل الإلكتروني[47]، التي تُعد من أبرز صور السلوك الإجرامي المعلوماتي المنصوص عليها في قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م)، حيث يعتمد الجاني على وسائل تقنية متطورة لاختراق الأنظمة المحمية أو الوصول غير المشروع إلى قواعد البيانات والمعلومات الإلكترونية، ويتم ذلك غالبًا عن بُعد من خلال استغلال وسائل الاتصال والشبكات الرقمية، دون حضور مادي للجاني إلى مكان ارتكاب

[47] كما نصت المادة (11، 12) من القانون رقم (05 لسنة 2022م) بشأن مكافحة الجرائم الالكترونية.

الجريمة، الأمر الذي يجعل آثار الفعل الإجرامي خفية ودقيقة، ويُصعّب من مهمة تتبعها أو كشفها بالوسائل التقليدية للإثبات الجنائي.

- **ثانيا: معوقات ترتبط بفقدان الآثار المتعلقة بالجريمة:**

تتميز الجريمة المعلوماتية بصعوبة اكتشافها وافتقارها في الغالب إلى الآثار المادية التقليدية التي تُميز الجرائم العادية، الأمر الذي يجعل الكشف عنها مرتبطًا – في كثير من الأحيان– بالإبلاغ عنها من قبل الجهات أو الأشخاص المتضررين. فهذه الجرائم تُرتكب داخل بيئة رقمية افتراضية لا تخلّف بالضرورة آثارًا محسوسة يمكن إدراكها أو معاينتها بالوسائل التقليدية، خلافًا لما هو عليه الحال في الجرائم التقليدية التي تترك عادةً آثارًا مادية ظاهرة، كجثة المجني عليه في جرائم القتل أو اختفاء المال في جرائم السرقة.

ويرجع غياب الآثار التقليدية للجريمة المعلوماتية إلى طبيعة النظم الإلكترونية ذاتها، حيث تتم العديد من العمليات والمعاملات الرقمية مباشرة عبر أنظمة الحاسب الآلي دون الاعتماد على محررات أو مستندات ورقية يمكن الرجوع إليها أو الاستدلال بها. فالمعاملات الإلكترونية الحديثة، خاصة في المجالات المصرفية والتجارية، تعتمد على برامج وأنظمة رقمية مخزنة مسبقًا، تتيح للمستخدم تنفيذ العمليات المطلوبة بمجرد إدخال الأوامر أو اختيار البيانات إلكترونيًا، دون أن يواكب ذلك وجود مادي ملموس للمعاملة أو آثار تقليدية تدل عليها.

ومن ثم، قد تتحقق بعض صور الجرائم المعلوماتية – كالاختلاس أو التزوير الإلكتروني– عن طريق إدخال بيانات غير صحيحة إلى النظام المعلوماتي أو تعديل البرامج والبيانات المخزنة داخل أجهزة الحاسب الآلي، بما يؤدي إلى تغيير النتائج أو تحويل القيم المالية بصورة آلية، دون استعمال مستندات ورقية أو وسائل مادية ظاهرة، ويترتب على ذلك فقدان الجريمة لآثارها التقليدية، وصعوبة اكتشافها أو تتبعها، خاصة إذا تمكن الجاني من محو أو إخفاء الآثار الرقمية المرتبطة بالفعل الإجرامي.

وتبرز هذه الصعوبات بصورة واضحة في الجرائم المنصوص عليها في قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م)، لاسيما تلك المتعلقة بالدخول غير المشروع، والتلاعب بالبيانات والأنظمة المعلوماتية، والاعتداء على سلامة المعالجة الإلكترونية للبيانات، حيث تتسم الأفعال الإجرامية فيها بطابع تقني خفي يجعل من فقدان الآثار الرقمية أو سرعة زوالها أحد أبرز معوقات الإثبات الجنائي المعلوماتي.

- **الفرع الثاني:**

الإشكالات الفنية المرتبطة بالآثار الرقمية للجريمة المعلوماتية.

في إطار الجريمة المعلوماتية، وفي ضوء قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م)، تبرز جملة من الإشكالات الفنية التي تمس سلامة الآثار الرقمية وتحد من إمكانية ضبطها أو الاستدلال بها، وهو ما ينعكس سلبًا على فعالية إجراءات الإثبات الجنائي في البيئة الرقمية، وتزداد هذه الإشكالات تعقيدًا بالنظر إلى الطبيعة التقنية للأنظمة المعلوماتية واعتمادها المتزايد على وسائل الحماية والتشفير وإدارة البيانات عن بُعد **(أولا)**، الأمر الذي يجعل من الوصول إلى الدليل الرقمي أو تتبعه مسألة شديدة الدقة والصعوبة **(ثانيا)**.

- **أولاً: تعدد وسائل الحماية الفنية وتعقيد الحصول على الدليل الرقمي:**

تلجأ المؤسسات والجهات التي تعتمد في نشاطها على النظم المعلوماتية – سواء كانت خدمية أو أمنية أو اقتصادية– إلى تبني منظومات متقدمة لحماية بياناتها ومعلوماتها، من خلال تقنيات التخزين الآمن، والتشفير، وأنظمة التحقق من الهوية، ويبرز ذلك بوضوح في مجال التجارة الإلكترونية والمعاملات الرقمية، لاسيما في عمليات الدفع الإلكتروني وتبادل البيانات والتعاقد عبر الإنترنت.

وفي هذا السياق، تعتمد هذه الجهات على آليتين رئيسيتين لضمان أمن المعاملات: تتمثل الأولى في استخدام تقنيات التشفير المتفق عليها بين الأطراف، بحيث لا يمكن فك رموز البيانات إلا من قبل الأطراف المصرح لهم بذلك، بما يضمن سرية الاتصال وسلامة المضمون. أما الآلية الثانية فتتمثل في التحقق من هوية المتعاقدين عبر تقنيات التوقيع الرقمي وشفرات المفاتيح العامة، بما يسمح بالتأكد من صحة الهوية الرقمية وسلامة المستندات الإلكترونية المتبادلة.

غير أن هذا التطور في وسائل الحماية، رغم أهميته في تأمين المعاملات، يطرح في المقابل صعوبات حقيقية أمام سلطات البحث والتحقيق، إذ قد يشكل حاجزًا تقنيًا يحول دون الوصول إلى الأدلة الرقمية أو تحليلها، بما يحد من فعالية الكشف عن الجريمة المعلوماتية وتتبع آثارها بشكل فعّال قبل أن تُخفى معالمها.

- **ثانيًا: تطور أساليب الإخفاء الرقمي وتعطيل الوصول إلى الآثار الإلكترونية:**

إلى جانب وسائل الحماية المشروعة، قد يلجأ مرتكبو الجرائم المعلوماتية إلى توظيف تقنيات متقدمة في إخفاء الأدلة الرقمية أو تعطيل الوصول إليها، من خلال اختراق الأنظمة المعلوماتية

والاستيلاء على البيانات السرية أو الأسرار التجارية، أو التلاعب بالأرقام والبيانات بما يغير من محتواها ونتائجها. كما قد يتعمد الجناة اتخاذ تدابير أمنية مضادة، مثل استخدام كلمات مرور معقدة أو أنظمة إخفاء متطورة، تهدف إلى منع أي محاولة تفتيش أو تتبع للنشاط الإجرامي.

ولا يقتصر هذا الإشكال على حدود المؤسسة الواحدة أو الدولة الواحدة، بل يتجاوز ذلك إلى نطاق عابر للحدود، حيث يمكن أن يكون المتدخل في الجريمة موجودًا خارج الإقليم الوطني، مستفيدًا من طبيعة الفضاء الرقمي الذي ألغى القيود الجغرافية التقليدية، وهو ما يزيد من صعوبة ضبط الأدلة وتتبع مصادرها، وذلك لاتساع جغرافيتها لأكثر من إقليم دولة أو دول متعددة.

ومن ثم، فإن الطبيعة العابرة للحدود للجريمة المعلوماتية، مقرونة بتطور وسائل الحماية والإخفاء الفني، تفرض ضرورة تعزيز آليات التعاون الدولي وتكثيف الجهود التشريعية والتقنية لمواجهة هذا النوع من الجرائم، بما يضمن فعالية الملاحقة الجنائية وحماية الأمن المعلوماتي.

- **المطلب الثاني:**

المعوقات الإجرائية المتعلقة بالتحقيق والتعاون الدولي.

تُعد المعوقات الإجرائية من أبرز التحديات التي تواجه إثبات الجريمة المعلوماتية، بالنظر إلى ما تفرضه طبيعتها التقنية والعابرة للحدود من صعوبات على مستوى إجراءات التحري والتحقيق. فهذه الجرائم لا تُرتكب في بيئة مادية تقليدية يسهل ضبطها، بل في فضاء رقمي متغير وسريع التلاشي، الأمر الذي ينعكس على فعالية الإبلاغ عنها، وعلى قدرة الجهات المختصة في التعامل مع أدلتها وفق ما تقتضيه القواعد الإجرائية التقليدية.

كما أن مواجهة هذا النمط من الجرائم تستلزم مستوى متقدمًا من الكفاءة الفنية والخبرة التقنية لدى سلطات البحث والتحقيق، وهو ما قد لا يتوافر بالقدر الكافي في بعض الحالات، فضلًا عن الإشكالات التي تثيرها طبيعة الجريمة المعلوماتية ذات الامتداد الدولي، والتي تجعل من التعاون القضائي بين الدول عنصرًا حاسمًا في نجاح إجراءات الملاحقة الجنائية، رغم ما يعتريه من بطء وتعقيد واختلاف في النظم القانونية، وعلى هذا الأساس، سيتم في **(الفرع الأول)**: تناول صعوبات الإبلاغ ونقص خبرة سلطات البحث والتحقيق في الجرائم الإلكترونية، بينما نتناول في **(الفرع الثاني)**: معوقات التعاون الدولي وضخامة البيانات في الجرائم المعلوماتية.

- **الفرع الأول:**

معوقات الإبلاغ وضعف الخبرة الفنية لدى سلطات البحث والتحقيق.

تُعد صعوبات الإبلاغ عن الجريمة المعلوماتية، إلى جانب محدودية الخبرة الفنية لدى جهات الاستدلال والتحقيق، من أبرز الإشكالات الإجرائية التي تعترض فعالية مكافحة هذا النمط المستحدث من الإجرام في إطار قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م)، ويُعزى ذلك إلى الطبيعة غير المادية لهذا النوع الجرائم، وما تتسم به من خفاء وتعقيد تقني يجعل اكتشافها أو التبليغ عنها من قبل الأفراد أو المؤسسات المتضررة أمرًا غير يسير، خلافًا لما هو عليه الحال في الجرائم التقليدية التي غالبًا ما تُبلغ عنها بصورة مباشرة إلى سلطات الضبط القضائي طبقا لما نصت عليه المواد (3، 14، 15، 16) إجراءات.

- **أولا: صعوبة الإبلاغ عن الجريمة المعلوماتية:**

تقوم الجريمة في صورتها التقليدية على واقعة مادية محسوسة يسهل إدراكها والإبلاغ عنها عبر الشكوى أو التبليغ، بما يترتب عليه مباشرة إجراءات الضبط والتحقيق. أما في الجريمة المعلوماتية، فإنها كثيرًا ما تظل في نطاق غير ظاهر، ولا يُكشف عنها إلا بصعوبة بالغة، الأمر الذي يجعل وصولها إلى علم السلطات المختصة مرهونًا بوعي المتضرر وقدرته على اكتشافها تقنيًا.

وقد ثار جدل فقهي حول سبل تعزيز الإبلاغ في هذا المجال، حيث طُرحت بعض الاتجاهات التي تدعو إلى إلزام العاملين في الجهات المتضررة بالإبلاغ عن أي واقعة معلوماتية تصل إلى علمهم، ضمانًا لسرعة اكتشاف الجريمة وتدارك آثارها. غير أن هذا الطرح قوبل بتحفظ في بعض التطبيقات المقارنة، على أساس ما قد يثيره من إشكالات قانونية تتعلق بتغيير صفة الجهة المتضررة من مجني عليه إلى موضع مساءلة، مما قد يخل بالتوازن الإجرائي.

وعليه، اتجهت بعض الحلول البديلة في القانون المقارن إلى اعتماد آليات أكثر مرونة، تتمثل في الإبلاغ إلى جهات إشرافية مختصة أو إنشاء قنوات مؤسسية لتبادل المعلومات بين الهيئات المعنية، بما يحقق فعالية الإبلاغ دون المساس بالضمانات القانونية للأطراف. كما برز دور الأجهزة الدولية المتخصصة، وفي مقدمتها المنظمة الدولية للشرطة الجنائية "الإنتربول"، من خلال تطوير وحدات متخصصة في مكافحة الجرائم المعلوماتية وتعزيز التعاون وتبادل البيانات بين الدول.

- **ثانيا: نقص الخبرة لدى سلطات البحث والتحقيق:**

إلى جانب صعوبة الإبلاغ، يبرز عامل آخر لا يقل أهمية يتمثل في محدودية الخبرة الفنية لدى سلطات الضبط القضائي والنيابة العامة وأجهزة الإدارة الأخرى في مجال الجريمة المعلوماتية، خاصة فيما يتعلق بفهم البنية التقنية للنظم المعلوماتية وآليات ارتكاب هذا النوع من الجرائم بحكم طابعها الالكتروني والتعامل مع أدلتها الرقمية.

ويُلاحظ أن هذا التحدي يتفاقم في بعض البيئات القانونية، لاسيما في الدول التي شهدت دخولًا متأخرًا لتقنيات الحاسب الآلي والتحول الرقمي مقارنة ببعض الأنظمة المتقدمة، وهو ما انعكس على مستوى التأهيل الفني والتكوين المتخصص للقائمين على إنفاذ القانون. كما أن وتيرة التطور التشريعي والإجرائي في مجال الجرائم المعلوماتية لا تزال في كثير من الحالات أقل من سرعة التطور التقني ذاته، الأمر الذي يخلق فجوة عملية تؤثر سلبًا على فعالية البحث والتحقيق.

ومن ثم، فإن مواجهة هذه الإشكالية تقتضي إرساء برامج تأهيل وتدريب متخصصة ومستمرة لسلطات الاستدلال والتحقيق والاتهام، بما يضمن إكسابها القدرات الفنية اللازمة للتعامل مع الأدلة الرقمية وفهم طبيعة الجريمة المعلوماتية، بما يُعزز من كفاءة المنظومة الجنائية في هذا المجال.

- **الفرع الثاني:**

معوقات التعاون الدولي وضخامة البيانات في الجرائم المعلوماتية.

من خصوصيات الجريمة المعلوماتية أنها تُعد من الجرائم ذات الطبيعة العابرة للحدود، الأمر الذي يجعل مكافحتها مرتبطة ارتباطًا وثيقًا بمدى فعالية التعاون الدولي بين الدول في مجالات التحري والتحقيق وتبادل المعلومات. غير أن هذا التعاون، رغم ضرورته العملية، يواجه جملة من الإشكالات القانونية والفنية التي تحد من فعاليته، إلى جانب التحديات الناتجة عن ضخامة البيانات الرقمية وتعقيد معالجتها في إطار إجراءات البحث الجنائي، وذلك في ضوء متطلبات قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022م).

- **أولا: صعوبات التعاون الدولي في مكافحة الجريمة المعلوماتية:**

لقد أفرز الانتشار الواسع لشبكة المعلومات الدولية وتعدد استخداماتها في المجالات الاقتصادية والأمنية والثقافية والعسكرية واقعًا جديدًا فرض التفكير في آليات دولية متخصصة لمكافحة الجريمة

المعلوماتية، تقوم على إنشاء وحدات أو شبكات تعاون بين أجهزة إنفاذ القانون على المستوى الدولي، بما يضمن تبادل الخبرات والمعلومات وتنسيق الجهود في تتبع مرتكبي هذا النوع من الجرائم.

غير أن هذا الطموح يصطدم بعدة عوائق جوهرية، من أبرزها غياب نموذج قانوني دولي موحد يحدد بدقة صور السلوك الإجرامي المعلوماتي، نظرًا لاختلاف التشريعات الوطنية وعدم اتفاقها على تعريف جامع مانع لإساءة استخدام نظم المعلومات أو الجرائم المرتبطة بها، وهو ما يعكس قصورًا تشريعيًا عامًا في مواكبة التطور التقني المتسارع.

كما يبرز إشكال آخر يتمثل في عدم توحيد الإجراءات الجنائية بين الدول، خاصة فيما يتعلق بإجراءات الاستدلال والتحقيق وجمع الأدلة الرقمية، مما ينعكس سلبًا على سرعة وفعالية التعاون القضائي الدولي، ويُضاف إلى ذلك محدودية أو غياب الاتفاقيات الثنائية والجماعية المتخصصة في هذا المجال، أو عدم كفايتها لمواكبة التطور السريع في تقنيات الحاسب والاتصال، الأمر الذي يضعف من جدوى التعاون الدولي في صورته التقليدية.

إلى جانب ذلك، تطرح مسألة الاختصاص القضائي في الجرائم المعلوماتية إشكالًا بالغ التعقيد، نظرًا للطبيعة الشبكية للفضاء الرقمي، حيث قد يمتد الفعل الإجرامي وآثاره عبر أكثر من دولة في آن واحد، مما يثير تنازع الاختصاص القضائي ويؤثر على تحديد القانون الواجب التطبيق والإجراءات الواجب اتباعها.

- **ثانيا: الصعوبات المتعلقة بضخامة البيانات الرقمية:**

تواجه سلطات البحث والتحقيق في الجرائم المعلوماتية تحديًا بالغًا يتمثل في ضخامة حجم البيانات الرقمية الواجب فحصها وتحليلها لاستخلاص الدليل الجنائي، إذ تتسم هذه البيانات بكثافة هائلة وتنوع كبير في مصادرها، سواء كانت مخزنة على أجهزة الحاسب الآلي أو على وسائط تخزين متعددة أو موزعة عبر الشبكات الرقمية.

وتكمن الإشكالية في أن تحليل هذا الكم الكبير من البيانات يتطلب قدرات تقنية متقدمة وخبرات فنية دقيقة في مجال المعلوماتية، بما يسمح بفرز البيانات ذات الصلة بالجريمة من غيرها، وغالبًا ما يؤدي الحجم الضخم للمعلومات إلى إبطاء إجراءات التحقيق وإرهاق الجهات المختصة، خاصة وأن العديد من هذه البيانات قد لا يكون ذا قيمة إثباتية مباشرة رغم ضخامة حجمها.

ومن ثم، فإن التعامل مع هذا التحدي يستوجب تطوير أدوات تحليل رقمية متقدمة وتعزيز الكفاءات الفنية لأجهزة العدالة الجنائية، بما يضمن القدرة على استخلاص الدليل من وسط هذا التراكم الهائل من البيانات، على نحو يحقق التوازن بين فعالية التحقيق ومتطلبات السرعة والدقة في الإثبات الجنائي.

- **الخاتمة:**

أظهرت دراسة إثبات الجريمة المعلوماتية أن الدليل الرقمي أصبح محوراً أساسياً في تحقيق العدالة الجنائية داخل البيئة الإلكترونية، إلا أن خصوصيته التقنية فرضت تحديات تختلف عن الإثبات في الجرائم التقليدية.

فقد تبين أن وسائل الإثبات التقليدية، كالإقرار والشهادة والمعاينة والتفتيش والضبط والخبرة، ما زالت تحتفظ بأهميتها متى تم تكييفها مع طبيعة الدليل الرقمي، في حين ظهرت وسائل إثبات حديثة تعتمد على التقنيات المعلوماتية، مثل تتبع الاتصالات، وتحليل البيانات الرقمية، وبرامج كشف الاختراق، بما يعزز قدرة سلطات التحقيق على كشف الجريمة وتحديد مرتكبها.

وفي المقابل، كشفت الدراسة عن وجود معوقات متعددة تحد من فعالية الإثبات الجنائي المعلوماتي، أبرزها الطبيعة غير المادية للدليل الرقمي، وقابليته للمحو والتعديل، وصعوبة الحفاظ على سلامته، فضلاً عن الإشكالات الفنية المرتبطة بالحماية والتشفير والإخفاء الرقمي.

كما اتضح أن الجانب الإجرائي يمثل تحدياً مهماً، سواء من حيث صعوبة الإبلاغ عن الجرائم المعلوماتية، أو الحاجة إلى خبرات فنية متخصصة، أو ما تثيره الجرائم العابرة للحدود من إشكالات تتعلق بالتعاون الدولي والاختصاص القضائي وضخامة البيانات الرقمية.

وعليه، فإن فعالية مكافحة الجرائم المعلوماتية لا تتحقق بمجرد وجود نصوص تجريمية، وإنما تتطلب بناء منظومة متكاملة تقوم على:

1. تطوير قواعد الإثبات الجنائي الرقمي.
2. تأهيل جهات البحث والتحقيق فنياً وتقنياً.
3. تعزيز التعاون القضائي الدولي.
4. تحقيق التوازن بين مقتضيات كشف الحقيقة وحماية الحقوق والحريات الرقمية.

فالتحول الرقمي لم يغيّر فقط شكل الجريمة، بل أعاد تشكيل مفهوم الدليل الجنائي وطرق الوصول إلى الحقيقة في العصر المعلوماتي.

كلمة .. في الختام ..

- **أبنائي الطلبة.**

نختتم اليوم رحلتنا في مقرر قانون مكافحة الجرائم الإلكترونية، وقد أدركنا أن الجريمة في العصر الرقمي لم تعد تقاس بآثارها المادية فقط، بل أصبحت تعتمد على دليل رقمي يحتاج إلى علمٍ وفهمٍ تقنيٍ إلى جانب المعرفة القانونية.

لقد تعلمنا أن مواجهة الجرائم المعلوماتية لا تتحقق بالنصوص وحدها، وإنما بكفاءة رجل القانون وقدرته على الجمع بين دقة التحليل القانوني ووعي التطور التقني، وتحقيق التوازن بين حماية المجتمع وصون الحقوق والحريات.

تذكروا دائماً أن القانون رسالة ومسؤولية، وأن مستقبل العدالة الجنائية سيكون لمن يمتلك العلم والقدرة على مواكبة التحولات الرقمية.

وفقكم الله، وجعل العلم طريقكم لخدمة الحق والعدل

والله من وراء القصد ...

المستشار الدكتور مسعود محمد خليفة شلندي

صرمان: 21. يونيو. 2026م

- **المراجع:**

- **أولًا: الكتب:**

1. إبراهيم أحمد إبراهيم، *الجوانب والحماية الدولية لبرامج الكمبيوتر وحق المؤلف في الدول العربية*، مجموعة أبحاث، 1994م.
2. إبراهيم أحمد الصعيدي، *نظام التشغيل الإلكتروني للبيانات*، مطبعة المعرفة، 1981م.
3. أحمد أنور زهران، *نظم المعلومات والحاسبات الآلية*، مكتبة غريب، 1989م.
4. أحمد محمد صلاح، *هوس الإنترنت*، كتاب الهلال، العدد (615)، مارس 2002م.
5. أسامة شوقي المليجي، *استخدام مخرجات التقنيات العلمية الحديثة وأثره على قواعد الإثبات المدني: دراسة مقارنة*، دار النهضة العربية، 2000م.
6. جميل عبد الباقي الصغير، *القانون الجنائي والتكنولوجيا الحديثة: الكتاب الأول – الجرائم الناشئة عن استخدام الحاسب الآلي*، دار النهضة العربية، القاهرة، 1992م.
7. حسام محمد عيسى، *نقل التكنولوجيا: دراسة في الآلية القانونية للتبعية الدولية*، دار المستقبل العربي، القاهرة، 1987م.
8. حسن طاهر داود، *الحاسب وأمن المعلومات*، معهد الإدارة العامة، الرياض، 1421هـ.
9. حكيم سياب، الاعلام الآلي والقانون– حقوق LMD، ط.1، دار وائل، عمان الأردن، 2014م.
10. خالد المخناز والمهندس إسماعيل أبو بكر، *التحقيق الجنائي في جرائم الحاسوب*، دار عزة للطباعة والنشر، 2010م.
11. رشيدة بورك، *جرائم الاعتداء على نظم المعالجة الآلية*، منشورات الحلبي الحقوقية، 2009م.
12. سعيد عبد اللطيف حسن، *إثبات جرائم الكمبيوتر*، دار النهضة العربية، 2007م.
13. عبد الرحمن عبد العزيز الشنيفي، *أمن المعلومات وجرائم الحاسب الآلي*، الرياض، 1414هـ.
14. عبد الفتاح بيومي حجازي، *الإثبات في جرائم الكمبيوتر والإنترنت*، دار الكتب القانونية، القاهرة، 2007م.
15. عبد المجيد سيد أحمد منصور، *السلوك الإجرامي والتفسير الإسلامي*، مركز أبحاث الجريمة، الرياض، 1410هـ.

16. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات ودور الشرطة والقانون: دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003م.
17. فهد محمد كيت، *الخصوصية في عصر المعلومات*، ترجمة محمد محمود شهاب، مركز الأهرام للترجمة والنشر، 1999م.
18. صلاح جواد كاظم، *التكنولوجيا الحديثة والسرية الشخصية: مباحث في القانون الدولي*، دار الشؤون الثقافية العامة، بغداد، 1991م.
19. محمد السيد خشبة، *مقدمة في التجهيز الإلكتروني للبيانات*، جامعة الأزهر، القاهرة، 1984م.
20. محمد إبراهيم السيف، *الظاهرة الإجرامية في ثقافة وبناء المجتمع السعودي بين التصور الاجتماعي وحقائق الاتجاه الإسلامي*، مكتبة العبيكان، الرياض، 1417هـ.
21. محمد زكي عبد المجيد وآخرون، *فيروسات الحاسب وأمن البيانات*، موسوعة دلتا كمبيوتر (8)، المكتب المصري الحديث، 1992م.
22. محمد المرسي زهرة، *الحاسوب والقانون*، مؤسسة الكويت للتقدم العلمي، الكويت، الطبعة الأولى، 1995م.
23. مصطفى محمد مرسي، *التحقيق الجنائي في الجرائم الإلكترونية*، مطابع الشرطة، القاهرة، الطبعة الأولى، 2008م.
24. محمود نجيب حسني، *شرح قانون العقوبات – القسم العام*، الطبعة السادسة، دار النهضة العربية، القاهرة، 1989م.
25. نهلا عبد القادر المومني، *الجرائم المعلوماتية*، دار الثقافة للنشر والتوزيع، 2008م.
26. نبيل جتيلش وآخرون، *المعلوماتية بعد الإنترنت (طريق المستقبل)*، ترجمة أحمد عبد السلام رضوان، سلسلة عالم المعرفة، العدد (231)، مارس 1998م.
27. كمال ناشف، *فيروس الكمبيوتر ومخاطر العدوى*، مجلة الكمبيوتر، دار المعارف، العدد (30)، يناير 1989م.
28. زيني زكي حسونة، *جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات*، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، 1993م.
29. يونس عرب، موسوعة القانون وتقنية المعلومات، الكتاب الثاني، دليل أمن المعلومات والخصوصية، الجزء الأول، ط.1، منشورات اتحاد المصارف العربية، بيروت، 2007م.

- **ثانيًا: البحوث وأوراق المؤتمرات:**

30. إسماعيل عبد النبي شاهين، "الحماية القانونية والشرعية لأمن المعلومات في الإنترنت"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 1–3 مايو 2001م.

31. سمير حامد عبد العزيز الجمال، "الحماية الجنائية للتوقيع الإلكتروني"، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 10–12 مايو 2003م.

32. علي عبد القادر القهوجي، "الحماية الجنائية للبيانات المعالجة إلكترونيًا"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 1–3 مايو 2000م.

33. علاء الدين محمد شحاتة، "جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات"، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25–28 أكتوبر 1993م.

34. عماد علي الخليل، "التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 1–3 مايو 2000م.

35. غنام محمد غنام، "عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، 1–3 مايو 2000م.

36. غنام محمد غنام، "الحماية الجنائية لبطاقات الائتمان الممغنطة"، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 10–12 مايو 2003م.

37. كامل السيد، "جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا"، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25–28 أكتوبر 1993م.

38. محمد أبو زهرة، "مدى حجية التوقيع الإلكتروني في الإثبات في المسائل المدنية والتجارية"، بحث مقدم ضمن أعمال مؤتمر الحاسب الآلي بالكويت، نوفمبر 1989م.

39. محمد محي الدين عوض، "مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)"، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، 25–28 أكتوبر 1993م.
40. ممدوح عبد الحميد عبد المطلب، "استخدام شبكة المعلومات العالمية عبر الإنترنت"، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 1–3 مايو 2000م.
41. ممدوح خليل بحر، "بطاقات الائتمان والآثار القانونية المترتبة بموجبها: دراسة قانونية مقارنة"، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 10–12 مايو 2003م.
42. هدى حامد شقفون، "الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني"، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، 1–3 مايو 2000م.
43. هدى حامد شقفون، "جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات"، المؤتمر السادس للجمعية المصرية للقانون الجنائي، 25–28 أكتوبر 1993م.
44. هدى حامد شقفون، "استخدام شبكة المعلومات العالمية عبر الإنترنت"، مؤتمر الاتصالات والتلفون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، 30 مايو 2000م.

- **ثالثًا: المقالات والدوريات:**

45. حسام كامل الأهواني، "الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني"، مجلة العلوم القانونية والاقتصادية، يناير–يوليو 1990م، العدد الأول والثاني، السنة 32.
46. حكيم سياب، التعليم الالكتروني الجامعي في الوطن العربي– الواقع والتحديات، مجلة الواحات، العدد 06، جامعة غرداية، الجزائر، 2014م.
47. فاضل نصر الله عوض، "تعليق على حكم محكمة الاستئناف الكويتية رقم 87/1589 جزائي بشأن الطبيعة القانونية للاستيلاء على الأموال من البنك الآلي"، مجلة الحقوق، الكويت، 1998م، الجزء الأول، السنة 22.

- **الفهرس:**

والحمد لله رب العالمين