Journal Of the Iraqia University (76-2) 31 – May (2026)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at
https://iasj.rdd.edu.iq/journals/journal/view/247

# الاثبات الجنائي في جرائم الانظمة المعلوماتية

م.م محمد ثامر نوري

جامعة ديالى رئاسة الجامعة /شعبة العقود الحكومية

# Criminal evidence in information systems crimes

## الملخص

تبرز الحاجة إلى استحداث قوانين خاصة لمواجهة الإجرام المعلوماتي بسبب القصور التشريعي في التعامل مع هذا النوع من الجرائم، ولا سيما قدرة المجرم المعلوماتي على إخفاء الأدلة، وصعوبة ضبط البيانات المتداولة عبر الإنترنت وفق القواعد الإجرائية التقليدية التي لم تُصمَّم لعالم افتراضي تُرتكب فيه الاعتداءات على الأنظمة والبيانات الرقمية. وقد ظهرت منذ انتشار المعلوماتية مشكلات إجرائية متعددة تمس التحري والاستدلال والتحقيق والاختصاص، ويُعد إخفاء الأدلة الإلكترونية وتغييرها من أخطر هذه الإشكالات، إلى جانب صعوبة تحديد الفاعل الحقيقي، وتزداد هذه التعقيدات عندما تكون البيانات داخل شبكات وأنظمة ذات طابع دولي، مما يثير مشكلات تتعلق بالدخول إليها أو جمعها ونقلها عبر الحدود، وما يرتبط بذلك من مخاطر على سيادة الدولة وعدم شرعية الإجراءات خارج الإقليم الوطني. وبسبب الطبيعة التقنية لهذه الجرائم، أصبح من الضروري إعادة النظر في القوانين الإجرائية الجنائية، ووضع قواعد تتيح استخدام أدوات وتقنيات معلوماتية في التحري والتحقيق، لمواجهة الإجرام المعلوماتي بطريقة تتلاءم مع طبيعته الرقمية.الكلمات المفتاحية:الإجرام المعلوماتي؛ الجرائم الإلكترونية؛ الأدلة الرقمية؛ القصور التشريعي؛ التحري الإلكتروني؛ التحقيق الجنائي الرقمي؛ الاختصاص القضائي؛ السيادة الرقمية؛ الإجراءات الجنائية؛ التعاون الدولي.

## Abstract

There is a pressing need to introduce specialized legislation to confront cybercrime due to the inadequacy of traditional criminal procedures, particularly given offenders' ability to conceal or alter digital evidence and the difficulty of controlling the vast flow of online data. Traditional procedural rules were not designed for a virtual environment in which transactions and attacks occur on digital systems or data transmitted between information networks.The rise of information technology has generated several procedural challenges related to investigation, evidence collection, jurisdiction, and the identification of offenders. Among the most serious issues are the concealment and manipulation of electronic evidence and the difficulty of identifying the actual perpetrator. These challenges become even more complex when the data involved is stored on international networks, raising issues concerning cross-border access, evidence collection, and potential violations of state sovereignty due to extraterritorial investigative actions.Accordingly, it has become essential to reconsider criminal procedural laws so they can effectively address cybercrimes. Given the inherently technological nature of these offenses, they must be confronted through equally advanced technological tools and digital investigative methods

**Keywords:**Cybercrime; Electronic Crimes; Digital Evidence; Legislative Gaps; Electronic Investigation; Digital Forensics; Jurisdiction Challenges; Digital Sovereignty; Criminal Procedure; International Cooperation.

## المقدمة

### اولا : بيان المسألة

ارتبطت الجريمة بالإنسان منذ بدايات التاريخ نتيجة اختلاف الطباع والدوافع بين الأفراد، وكانت الجرائم التقليدية تعتمد غالبًا على الجهد البدني والذهني. إلا أنّ التطور السريع في تكنولوجيا المعلومات أدى إلى ظهور نمط جديد من الجرائم يعتمد على المهارات التقنية بدل القوة الجسدية، وهو ما عُرف بـ"الجريمة المعلوماتية". وقد ساهم الانتشار الواسع للإنترنت في بروز هذا النوع من الانتهاكات التي تستهدف الحقوق والمصالح في البيئة الرقمية.استجابةً لذلك، اتجهت العديد من الدول إلى سن تشريعات خاصة لمكافحة الجرائم الإلكترونية، وظهرت اتفاقيات دولية مهمة مثل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات واتفاقية بودابست للجرائم السيبرانية. ومع تزايد اعتماد الأفراد والمؤسسات على التقنيات الرقمية،

ارتفعت معدلات الجريمة الإلكترونية وتطورت أساليب ارتكابها، مما وضع الأجهزة الأمنية أمام تحديات كبيرة في تتبع الجناة والحد من مخاطر هذه الجرائم على المؤسسات الحكومية وغير الحكومية.ورغم خطورة الظاهرة، ما تزال معظم الدول العربية . ومنها العراق . تفتقر إلى نصوص قانونية متكاملة تواكب الأساليب التقنية الحديثة في مراحل التحري والاستدلال والتحقيق والمحاكمة، الأمر الذي يبرز الحاجة إلى تطوير تشريعات فعّالة للتعامل مع هذا النوع المتنامي من الجرائم..

## ثانياً: أهمية الدراسة

تزداد أهمية هذا الموضوع في ظل التحول الرقمي وانتشار الجرائم المعلوماتية التي تمس الأمن العام، والاقتصاد، والخصوصية الفردية, يواجه نظام العدالة الجنائية تحديات متعلقة بإثبات الجرائم المرتكبة عبر الوسائط الرقمية، نظراً لسرعة طمس الأدلة، والحاجة إلى أدوات تقنية متطورة, يهدف البحث إلى بيان كيفية تعامل التشريعات الجنائية مع وسائل الإثبات الحديثة، ومدى كفاية القواعد الإجرائية الحالية في مواجهة هذه الجرائم، مع تسليط الضوء على التحديات العملية.

## ثالثاً: إشكالية الدراسة

تُعد من أبرز الإشكاليات التي قد تُثار في إطار هذه الدراسة مسألة مدى إمكانية تطبيق القواعد والنصوص الإجرائية التقليدية، المعتمدة في جمع الأدلة وإجراءات التحقيق، على الجرائم المعلوماتية، وذلك في ظل الطبيعة الخاصة والمعقدة لهذا النوع من الإجرام.

## رابعاً: أهداف الدراسة

يهدف هذا البحث إلى إبراز التحديات التي تواجه القوانين الجنائية التقليدية عند التعامل مع الجرائم المعلوماتية، إذ صيغت تلك النصوص في زمن لم يشهد التطور التقني الحالي، وعلى يد مشرعين غير متخصصين في المجال المعلوماتي، مما جعلها تعتمد على مفاهيم تقليدية ترتبط بالجوانب المادية للجريمة. وتنطلق الدراسة من توضيح أوجه القصور في الإجراءات الجنائية، ولا سيما ما يتعلق بجمع الأدلة والتحقيق في الجرائم الإلكترونية، مع اقتراح حلول لمعالجة هذا القصور ، والافادة من التشريعات المقارنة التي اعتمدت قواعد أكثر تطورًا ومرونة لمواكبة التحولات التقنية المتسارعة.

## خامساً: نطاق الدراسة

ينحصر نطاق هذه الدراسة في تناول الجوانب الإجرائية المرتبطة بعمليات التحري والتحقيق الأولي في الجرائم المعلوماتية، وذلك من خلال تحليل النصوص القانونية الإجرائية ذات الصلة، سواء في التشريعات الوطنية أو في القوانين المقارنة. كما تسعى الدراسة إلى الوقوف على أبرز الآراء الفقهية والقانونية التي تناولت هذه المسائل، بهدف إبراز أوجه القوة والقصور في الإطار الإجرائي المعتمد حاليًا، وبيان مدى كفايته في مواجهة طبيعة هذا النوع المستحدث من الإجرام.

## سادسا : هيكلية الدراسة

من أجل تحقيق الاهداف التي نسعى إلى بلوغها سنقسم موضوع دراستنا المبحث الاول خصصناه لبيان اجراءات ما قبل المحاكمة وقسمنا هذا المبحث إلى فرعين وتناولنا في الأول منه موضوع التحري وأما الفرع الثاني فقد افردناه لبيان المعاينه وجمع الاستدلال وأما المبحث الثاني فقد خصصناه لدراسة اجراءات التحقيق ضبط الادلة ، وقسمنا هذا المبحث إلى فرعين ، أفردنا الأول منه لبيان اجراءات التحقيق في حين اشتمل الفرع الثاني منه على الجوانب المتعلقة بإجراءات ضبط الادلة ، وقد انتهت هذه الدراسة بخاتمة تناولت أهم ما توصنا اليه من نتائج

## المبحث الاول : اجراءات ما قبل المحاكمة

تُعد مرحلة ما قبل المحاكمة من أهم المراحل الإجرائية لكونها الأساس في كشف الجريمة وتحديد مرتكبها من خلال إجراءات التحري وجمع الاستدلالات، وهي المرحلة التي تسبق التحقيق القضائي الرسمي. وقد عرّفت المذكرة الإيضاحية لقانون أصول المحاكمات الجزائية الاستدلال بأنه منح سلطات معينة لأعضاء الضبط القضائي لجمع المعلومات وحماية الأدلة وتوثيق الإجراءات الأولية (الحديثي، ٢٠١٦، ص ١٩٨). ويقوم أفراد الضبط القضائي، ومعظمهم من الشرطة، بهذه المهام ضمن الصلاحيات القانونية، كما تضطلع الشرطة بالضبط الإداري ذي الطابع الوقائي، من خلال مراقبة الالتزام بالقوانين والتصدي لجرائم المعلوماتية قبل وقوعها، مثل متابعة تراخيص محال البرمجيات ومراقبة الأنشطة الرقمية. وقد طورت بعض الدول—كالصين—أنظمة رقابة مسبقة تُعرف بـ"شرطة الإنترنت" لمنع الجرائم الإلكترونية (الصغير، ٢٠٠٢، ص ١١). وعلى الصعيد القانوني، يمنح المشرّع العراقي القائمين بهذه المهام صفة "أعضاء الضبط القضائي"، بينما يطلق عليهم القانون الجزائري "ضباط الشرطة القضائية"، مع اتحاد الدور في جمع الاستدلالات وضمان فاعلية مرحلة ما قبل التحقيق.

**المطلب الاول : التحري**

تختلف آليات التحري الرقمي عن التحري التقليدي باختلاف طبيعة الوسائل المستخدمة، إذ يعتمد التحري الرقمي على أجهزة وتقنيات إلكترونية تتعامل مع أدلة غير مادية، مثل البيانات والملفات الرقمية. وتتمثل أبرز مهام هذا النوع من التحري في تحديد هوية المخترق، وبيان الأسلوب المستخدم في تنفيذ الاختراق، وذلك وفق إجراءات تقنية تضمن الحفاظ على سلامة الأدلة الرقمية وعدم تغييرها أثناء جمعها أو فحصها (الديحاني، ٢٠٠٧).وتبرز أهمية مرحلة التحري بصورة أكبر عند ارتكاب الجرائم عبر الوسائل الإلكترونية الحديثة، حيث لا تكون الأساليب التقليدية كافية لمواجهتها. ولذلك تزداد الحاجة إلى قواعد إجرائية متطورة تتلاءم مع طبيعة الجرائم المعلوماتية وآليات ارتكابها. وتُعد من أبرز الإشكالات الإجرائية في هذه المرحلة استقبال الشكاوى والبلاغات عبر الإنترنت، فضلًا عن صعوبة الكشف الأولي على الأدلة الإلكترونية ومعاينتها، لما تتطلبه من أدوات تقنية وإجراءات دقيقة تضمن موثوقيتها وقابليتها للاستخدام القضائي (الديحاني، ٢٠٠٧)..

**الفرع الأول: الاخبار والشكاوى**

سنخصص هذا الفرع لتوضيح إجراءات تلقي الأخبار والشكوى بالطرق التقليدية في الفرع الأول، ثم نعرض بالتفصيل كيفية تلقيها عبر الإنترنت في الفرع الثاني من هذا الفرع.

**أولاً: الطرق التقليدية**

يمثل تقديم البلاغ إلى السلطات المختصة خطوة أساسية في تحريك الإجراءات الجزائية، إذ يعد هذا البلاغ إشعارًا رسميًا بوقوع جريمة يوجب على أجهزة الضبط اتخاذ التدابير اللازمة للتحري عنها والكشف عن مرتكبيها. وقد ألزمت التشريعات أعضاء الضبط القضائي بتلقي الشكاوى والبلاغات، وفحصها، والانتقال إلى مكان الحادث لمعاينته، والحفاظ على الأدلة، وسماع الشهود أو الأشخاص الذين كانوا حاضرين عند وقوع الجريمة (المادة ٤١ من قانون أصول المحاكمات الجزائية العراقي رقم ٢ لسنة ١٩٧١؛ المادة ١٧ من قانون الإجراءات الجزائية الجزائري رقم ٠٨-٠١ لسنة ٢٠٠٦)ويُقصد بالأخبار إبلاغ السلطات المختصة قانونًا بوقوع جريمة، سواء وقعت على المبلِّغ أو على غيره، بما يمس النفس أو الشرف أو المال (العكيلي، ٢٠١٥). أما الشكوى، فهي طلب يقدمه المجني عليه أو من ينوب عنه قانونيًا بهدف تحريك الدعوى بشأن الجريمة الواقعة عليه (الحديثي، ٢٠١٦، ص ٧٨).وقد بيّن قانون أصول المحاكمات الجزائية الجهات المختصة بتلقي الشكاوى والأخبار في المادة (١/أ)، كما اعتبر تقديم البلاغ واجبًا أخلاقيًا يحركه الشعور بالمصلحة العامة (العكيلي، ٢٠١٥). ولم يحدد القانون شكلًا معينًا للشكوى، إذ يمكن أن تكون شفوية أو تحريرية، وبأي صيغة أو لغة (الحديثي، ٢٠١٦، ص ٨٣).ويقوم أعضاء الضبط القضائي، ضمن حدود اختصاصهم، بقبول البلاغات والتحري عنها وتقديم الدعم لجهات التحقيق، وتدوين الإجراءات كافة في محاضر رسمية. كما يلتزمون بالانتقال الفوري إلى مكان الجريمة المشهودة بعد إخطار قاضي التحقيق أو النيابة العامة، وضبط الأدلة وأدوات الجريمة وتوثيق إفادات الأطراف. ورغم وضوح هذه الإجراءات في الجرائم التقليدية، إلا أن تلقي البلاغات عبر الإنترنت في الجرائم المعلوماتية يثير تساؤلات حول مدى إمكانية قبولها وفحصها إلكترونيًا، ومدى كفاية الإطار الإجرائي التقليدي للتعامل معها.تكمن المشكلة في مدى قانونية تلقي هذه الشكاوى والبلاغات إلكترونياً، وقيمتها القانونية، وما هو الموقف التشريعي في العراق مقارنة بالقوانين المقارنة في هذا الشأن.

**ثانيا : : الطرق الحديثة عبر الأنترنت**

ان دراسة إمكانية قبول الشكاوى والبلاغات المقدمة عبر الإنترنت تستلزم تحديد طبيعتها وأهميتها مقارنة بالبلاغات التقليدية، وبيان مدى كفاية النصوص الإجرائية الحالية لمعالجتها. وتزداد أهمية هذا النوع من البلاغات في الدول المتقدمة التي تعتمد منظومات إلكترونية متطورة لاستقبال الشكاوى والتحقق منها دون أن يشكّل التقديم الإلكتروني عائقًا أمام إجراءات التحري (يونس، ٢٠٠٤، ص ٨٢٤). وتظهر المشكلات غالبًا لدى الجهات المتضررة التي تتردد في الإبلاغ خشية المساس بسمعتها (عفيفي، ٢٠٠٠، ص ٣٥٦)، أو في الدول ذات البنية التكنولوجية الضعيفة التي تعاني نقص الأجهزة والكوادر الفنية.وتشير التشريعات العراقية إلى اختصاص أعضاء الضبط القضائي بتلقي الشكاوى دون نصوص تنظم آلية التقديم الإلكتروني (المادة ٤١ من قانون أصول المحاكمات الجزائية العراقي). الأمر ذاته يظهر في قانون الإجراءات الجزائية الجزائري، رغم أن الشكاوى الإلكترونية لا تختلف قانونيًا عن التقليدية ما دامت تهدف إلى الإبلاغ عن جريمة، ويُعد إهمالها خطأ بالغًا لسرعة انتشار آثار الجرائم المعلوماتية. ويستحسن أن يمتلك المبلّغ معرفة تقنية أولية، وأن يتمتع أعضاء الضبط القضائي بخبرة فنية لمناقشة البلاغات الرقمية (علي، ٢٠١٢، ص ٦٧).ولا يوجد مانع قانوني من قبول الشكاوى عبر الإنترنت إذا توافرت القدرات التقنية لدى الجهات المختصة، مع استمرار فاعلية الوسائل التقليدية (عالية، ٢٠٢٠، ص ٤٥٩-٤٦٠). ويبرز أسلوبان للتبليغ الرقمي: إرسال رسالة إلكترونية إلى جهة أمنية رسمية كما تعمل وكالات مثل

الـFBI وCIA، أو ملء نموذج إلكتروني مخصص للإبلاغ كما في المكتب المركزي الفرنسي، مع منح المبلّغ رقمًا مرجعيًا (الخن، ٢٠١٢، ص ٩٧). ورغم سرعة التقديم الإلكتروني، يعاني من مشكلات أهمها غياب هوية المبلّغ واستخدام الأسماء المستعارة مما يضعف مصداقيته (يونس، ٢٠٠٤، ص ٨٣٠)وتتعلق الإشكالية الأساسية بمدى اختصاص الجهة التي تتلقى البلاغ وقدرتها الفنية على التعامل مع الأدلة الرقمية (سعيدان، ٢٠١٣، ص ١٠٦). وقد أنشأت بعض الدول—كالمصرية—أجهزة متخصصة مثل إدارة مكافحة الحسابات وشبكة الإنترنت (قرار ٢٠٠٢/١٣٥٠٧)، إضافةً إلى أقسام لمكافحة جرائم الحاسوب. أما الدول الأجنبية، فقد بادرت مبكرًا؛ فأنشأت بريطانيا وحدة متخصصة عام ٢٠٠١، فيما طورت الولايات المتحدة شرطة الإنترنت ونيابة جرائم الحاسوب والاتصالات (الصغير، ٢٠٠١، ص ٧٧؛ هروال، ٢٠٠٧، ص ١٠٨).وتبقى مشكلة عدم الإبلاغ من أبرز التحديات، إلى جانب صعوبة كشف الأدلة الرقمية غير المرئية التي تتطلب إجراءات تقنية دقيقة، ولا سيما عند تشتتها عبر أنظمة داخلية ودولية، مما يزيد من تكاليف الفحص (رستم، ٢٠٠٣، ص ٤٢٥). لذا تبرز الحاجة إلى إنشاء معامل جنائية رقمية متخصصة قادرة على جمع الأدلة وتحليلها بكفاءة عالية..

**الفرع الثاني : الانتقال إلى مسرح الجريمة المعلوماتية :**

يُعد الانتقال إلى مسرح الجريمة من أهم إجراءات جمع المعلومات في التحقيق بالجرائم التقليدية، وقد منحه المشرّع اهتمامًا خاصًا نظرًا لدوره في تثبيت حالة المكان وضبط الآثار المادية التي تساعد في كشف الحقيقة وإسناد الجريمة لمرتكبها. إلا أن هذا الإجراء لا يصلح لجميع الجرائم، فهناك جرائم لا تترك آثارًا مادية، مثل الرشوة والذم والقدح، مما يجعل المعاينة الميدانية دون جدوى (عالية، ٢٠٢٠، ص ٤٦٥).

أما في الجرائم المعلوماتية، فيأخذ الانتقال إلى مسرح الجريمة شكلًا مختلفًا، إذ يتمثل بالدخول إلى الفضاء الإلكتروني ومواقع الجريمة الرقمية، باعتبارها مسرحًا افتراضيًا للجريمة. ويُعد مفهوم الانتقال في الجرائم الإلكترونية مفهومًا حديثًا، إذ لا يقتصر على الدخول إلى المواقع الإلكترونية، بل يشمل أيضًا إجراءات تقنية خارج الفضاء الافتراضي تتعلق بجمع وتحليل الأدلة الرقمية (علي، ٢٠١٢، ص ٨٣).

**أولاً: طرق الانتقال إلى العالم الافتراضي**

توجد عدة وسائل يمكن لمأمور الضبط القضائي من خلالها معاينة مسرح الجريمة الإلكتروني، منها (إبراهيم، ٢٠١٠، ص ١٥٦–١٥٧):

١. استخدام أجهزة الحاسوب المتصلة بالإنترنت داخل مقار المحاكم.

٢. الدخول إلى الشبكة من خلال مقاهي الإنترنت مع مراعاة الضوابط الأمنية.

٣. الانتقال إلى مقر مزود خدمة الإنترنت، وهو من أكثر الأماكن ملاءمة للفحص الفني (يونس، ص ٨٩٥).

٤. إجراء المعاينة داخل مكتب الخبير الفني المختص، كما نظمته التشريعات المصرية ضمن إدارة مكافحة جرائم تكنولوجيا المعلومات.

ويُستخلص من ذلك أن الانتقال إلى الفضاء الإلكتروني لا يشكّل عقبة بحد ذاته، إلا أن التحدي يكمن في ضرورة سرعة الانتقال للمحافظة على الأدلة الرقمية قبل طمسها أو حذفها، وهو ما أكدته المادة (٤٣) من قانون أصول المحاكمات الجزائية العراقي (قانون أصول المحاكمات الجزائية العراقي، ١٩٧١).

**ثانياً: الإجراءات الواجب اتخاذها قبل الانتقال إلى مسرح الجريمة**

قبل البدء في المعاينة الإلكترونية، يتوجب اتخاذ مجموعة من الإجراءات الأساسية (إبراهيم، ٢٠١٠، ص ١٥٨):

١. توفير الأجهزة والبرامج الفنية اللازمة للفحص والتشغيل.

٢. الحصول على إذن قضائي بالتفتيش وفقًا للنصوص القانونية.

٣. قطع التيار الكهربائي لفصل قدرة الجاني على تعديل البيانات أو محوها.

٤. تشكيل فريق تحقيق متخصص في الجرائم المعلوماتية.

٥. إعداد خطة عمل واضحة يتفق عليها جميع أعضاء الفريق.

ويتكون فريق التحقيق عادة من محقق رئيسي مختص، وخبراء شبكات وحاسوب، وخبراء نظم وبرمجيات، وخبراء في ضبط الأدلة الرقمية، إضافة إلى متخصصين في البصمات والتصوير وخبير استشاري (علي، ٢٠١٢، ص ٧٠).

**ثالثاً: الإجراءات الواجب اتخاذها فور الوصول إلى مسرح الجريمة**

بعد الوصول إلى الموقع الإلكتروني أو المادي المرتبط بالجريمة الرقمية، يجب اتخاذ مجموعة من التدابير الإجرائية لضمان سلامة الأدلة (حجازي، ٢٠٠٩، ص ٢١٧–٢١٨):

١. تأمين مداخل ومحيط المكان وإغلاقه عند الضرورة.

٢. توفير حراسة كافية ورصد الاتصالات الصادرة والواردة، وتعطيل الهواتف عند الحاجة.

٣. التحفظ على الموجودين داخل الموقع لحين استكمال التحقيق.

٤. تخصيص موقع منفصل لاستجواب المتهمين والشهود.

٥. تنفيذ خطة العمل من قِبل فريق التحقيق وفق اختصاص كل عضو.

٦. وضع حراسة مباشرة على الأجهزة الإلكترونية لمنع العبث بها.

٧. تحديد أماكن الأجهزة الإلكترونية وتعطيل وسائل الاتصال المرتبطة بها عند الضرورة.

وتُعد هذه الإجراءات ضرورية لضمان الحفاظ على الأدلة الرقمية وحمايتها من التغيير أو التحريف، نظرًا لطبيعتها السريعة الزوال.

## المطلب الثاني : المعاينة وجمع الاستدلال

### الفرع الاول : المعاينة

للمعاينة أهمية كبيرة في اثبات الواقعة الجرمية نظراً لما توفره من أدلة اثبات، فهي الوسيلة التي تسمح بالكشف عن مسرح الجريمة وتبيت حالة الأشخاص والأماكن والاشياء التي ترتبط بالجريمة، وتزداد هذه الأهمية عند تعلقها بالجرائم المعلوماتية جرائم غير مألوفة عند النظر إلى السلوك الإجرامي فيها، والذي يستدعي ابتكار تقنيات مناسبة لمعاينة مسرح الجريمة، وهذا ما سنتناوله في الفرعين الآتيتين.

### الفرع الثاني : مسرح الجريمة المعلوماتية

يختلف مسرح الجريمة المعلوماتية عن المسرح التقليدي، إذ يتطلب التعامل معه خبرة فنية خاصة. وينقسم إلى نوعين:

١. المسرح التقليدي: وهو الموقع الفيزيائي المرتبط بالجريمة، مثل أجهزة الحاسوب ووسائط التخزين والمتعلقات الشخصية، ويتم التعامل معه وفق إجراءات الجرائم العادية (يوسف، ٢٠١٣، ص ٨٤).

٢. المسرح المعلوماتي: وهو البيئة الرقمية التي تضم البيانات والسجلات الإلكترونية والشبكات، وتمثل معاينته أحد أكثر جوانب التحقيق صعوبة بسبب تعقيدها الفني (السوفي، ٢٠١٧، ص ٣٢).ويستلزم التعامل مع هذا المسرح اتباع قواعد تقنية دقيقة، من أبرزها: جمع معلومات مسبقة عن موقع الجريمة الإلكترونية، تحديد الأجهزة ذات العلاقة، توفير المعدات الفنية اللازمة، الالتزام بالمشروعية أثناء الإجراءات، وعدم نقل المواد قبل التأكد من عدم تعرضها لمجالات قد تمحو البيانات (حجازي، ٢٠٠٤، ص ٦٠). كما توصي الأدبيات بعدة خطوات أساسية مثل: توثيق الأجهزة تصويرًا كاملًا، إخطار الفريق الفني، وضع خطة عمل، دراسة إعدادات النظام، توثيق التوصيلات، والتحفظ على وسائط التخزين والأوراق (علي، ٢٠١٢، ص ٨٤–٨٥). ويجب أيضًا التحفظ على الموقع لإمكانية العودة إليه لاستكمال الفحص.

ثالثًا: أهمية المعاينة

تُعد المعاينة من الأدلة الجوهرية في الجرائم التقليدية، إذ تساعد في كشف ملابسات الجريمة وجمع الآثار المادية وتوجيه التحقيق (رستم، ١٩٩٤، ص ٥٩). إلا أن دورها في الجرائم المعلوماتية محدود لعدة أسباب، أهمها:

١. عدم وجود آثار مادية واضحة لأن الجريمة تتم في بيئة رقمية غير محسوسة (إبراهيم، ٢٠١٠، ص ١٥٤).

٢. احتمال تغيير الآثار في المكان الطبيعي للجريمة قبل اكتشافها، مما يضعف موثوقية المعاينة.

٣. قدرة الجاني على محو أو إخفاء البيانات باستخدام برامج متخصصة، مما يجعل المعاينة التقليدية غير كافية لإثبات الجريمة (الصغير، ٢٠٠٢، ص ٢٩).وعليه، فإن المعاينة تبقى أداة مهمة، لكنها غير فعّالة وحدها في الجرائم المعلوماتية، ما يتطلب الاعتماد على وسائل تقنية متقدمة تتوافق مع طبيعة الأدلة الرقمية..

### الفرع الثاني :جمع الاستدلال

#### أولاً: استدراج الجاني عبر شبكة الإنترنت

يُعد الاستدراج الإلكتروني وسيلة فعّالة لعضو الضبط القضائي لجمع المعلومات عن الجرائم المعلوماتية، ويتم من خلال دخول العنصر المختص إلى غرف الدردشة والمنتديات باستخدام هوية مستعارة بهدف كشف ظروف الجريمة دون تحريض الجاني. ويختلف عن الاستدراج التقليدي بكونه لا يُمارس إلا من قبل عنصر رسمي وبعد الحصول على إذن من الجهة المختصة (عالية، ٢٠٢٠، ص ٤٦١–٤٦٢). ويجمع عنصر الضبط المعلومات المتعلقة بطرق الاحتيال واختراق الأنظمة ثم يرفعها إلى رؤسائه لاتخاذ الإجراءات المناسبة لضبط المشتبه بهم.

**ثانياً: التحفظ على أدوات الجريمة المعلوماتية**

تنص المادة (٤٢) من قانون أصول المحاكمات الجزائية العراقي على ضبط كل ما يفيد في كشف الحقيقة، ويظهر ذلك في جرائم المعلوماتية بصورتين:

١. ضبط الكيانات المادية مثل الحواسيب ووسائط التخزين، ويمكن ضبطها مباشرة.

٢. ضبط الكيانات المنطقية (البيانات الرقمية) وهي الأكثر تعقيدًا وتستلزم خبراء مختصين لضبط وتحليل الأدلة الرقمية (العفيفي، ٢٠١٣، ص ١٠٧–١٠٨). ويعمل الخبير تحت إشراف عضو الضبط القضائي، ويقوم بتشغيل الأجهزة وتأمين النظام واستخراج البيانات وتحويلها إلى شكل كتابي لعرضها على المحكمة.

**ثالثاً: سماع أقوال الشهود وتحرير المحضر**

يجيز القانون لعضو الضبط القضائي سماع الشهود الذين يمتلكون معلومات حول الجريمة، وسؤال المتهم دون استجوابه، وله منع الحاضرين من مغادرة مكان الجريمة حتى إتمام الإجراءات (المواد ٤٣–٤٤). غير أن وجود شاهد مباشر في الجرائم المعلوماتية نادر بسبب طابعها السري وعدم وجود آثار مادية ظاهرة (العفيفي، ٢٠١٣، ص ١٠٢)ويلتزم عضو الضبط القضائي بتنظيم محضر يتضمن جميع الإجراءات والمعلومات وتاريخ تنفيذها، ليُشكّل هذا المحضر الأساس الذي تُبنى عليه مراحل التحقيق اللاحقة..

## المبحث الثاني : اجراءات التحقيق وضبط الادلة

يُعرَّف التحقيق الجنائي بأنه مجموعة إجراءات تهدف إلى جمع الأدلة المتعلقة بجريمة واقعة وتقييمها لتحديد كفايتها لإحالة المتهم إلى المحاكمة. وينقسم التحقيق إلى قسمين: أولهما إجراءات البحث عن الحقيقة، عبر جمع الأدلة وتمحيصها لإثبات وقوع الجريمة ونسبتها إلى المتهم، وثانيهما ضبط الأدلة وتحريزها لحمايتها من العبث، وهي إجراءات احتياطية كأوامر الحضور والقبض، ولا تدخل ضمن نطاق هذا البحث (إبراهيم، ٢٠١٠، ص ١٤٣).ومنح المشرّع المصري المحقق سلطة تقديرية واسعة لاتخاذ ما يراه مناسبًا من إجراءات القسم الأول للوصول إلى الحقيقة، ما دامت لا تمس حرية الأفراد أو حرمة مساكنهم، كما ألزمه باستجواب المتهم دون ترتيب محدد لبدء التحقيق (إبراهيم، ٢٠١٠، ص ١٤٤).أما الجرائم المرتكبة عبر شبكات المعلومات، ولا سيما الإنترنت، فتطرح تحديات كبيرة في جمع الأدلة والتفتيش والضبط، وتتطلب خبرة فنية خاصة. وقد أدت هذه الصعوبات إلى إفلات العديد من الجناة من العقاب، إذ تُقيَّد الجرائم المعلوماتية غالبًا ضد مجهول، أو يتعذر إقامة الدليل فيها بسبب طبيعتها التقنية وسرعة زوال آثارها..

### المطلب الاول : إجراءات التحقيق الخاصة بجرائم الانظمة المعلوماتية

سنقسم هذا الفرع إلى أربعة فروع، سنتناول في الفرع الأول سماع الشهود، ونتناول في الفرع الثاني إجراءات التفتيش، في حين يُخصص الفرع الثالث للخبرة، أما الفرع الرابع سيكون لبيان إجراءات ضبط مكونات الجريمة.

**الفرع الأول: سماع الشهود**

تُعد الشهادة إحدى أهم وسائل الإثبات المباشرة في الدعوى الجنائية، إذ تقوم على إخبار الشاهد بما رآه أو سمعه أو أدركه مباشرة بحواسه، مما يجعلها أداة محورية في كشف حقيقة الوقائع. وفي إطار الجرائم المعلوماتية، يقتضي تحليل مفهوم الشهادة تقسيم الدراسة إلى فرعين: يتناول الفرع الأول الشهادة المعلوماتية، بينما يخصص الفرع الثاني لبحث الشهادة الإلكترونية عن بُعد.

**أولاً: الشاهد المعلوماتي**

يُعرَّف الشاهد المعلوماتي بأنه الشخص المتخصص في تقنيات الحاسوب والشبكات، الذي يمتلك خبرة فنية تؤهله لتقديم معلومات أساسية في الدعوى، وخصوصًا تلك المرتبطة بالنفاذ إلى أنظمة المعالجة الآلية للبيانات، متى اقتضت مصلحة التحقيق ذلك (إبراهيم، ٢٠١٠، ص ٢٦٣).

وتندرج تحت مسمى "الشاهد المعلوماتي" عدة فئات رئيسية، أبرزها (هلالي، ١٩٩٧، ص ٢٣–٢٤):

١. القائم على تشغيل الحاسوب وهو الشخص المكلف بتشغيل أجهزة الحاسوب والمعدات المرتبطة بها، ويشترط أن يمتلك خبرة واسعة في تشغيل الأجهزة والبرامج، إضافة إلى معرفة تقنية دقيقة بالبرمجة (فتحي، ١٩٩١، ص ٢٣).

٢. المبرمجون وهم المتخصصون في كتابة الشفرات البرمجية، وينقسمون إلى فئتين: مبرمجو تطبيقات، ومبرمجو نظم تشغيل.

٣. المحللون

وهم القادرون على تحليل الأنظمة وتدفق البيانات، وتقسيم النظام إلى وحدات وظيفية، واستنتاج العلاقات التقنية داخل النظام، وتحديد نقاط الأتمتة المناسبة.

٤. مديرو النظم وهم المسؤولون عن إدارة وإشراف الأنظمة المعلوماتية.

٥. مهندسو الصيانة والاتصالات المختصون بصيانة الأجهزة والشبكات وأنظمة التشغيل، ومعالجة الأعطال التقنية ذات الصلة.

يمثل هؤلاء الشهود الركيزة الأساسية لفهم الجوانب الفنية ذات العلاقة بالجريمة المعلوماتية، ما يجعل شهادتهم مكملة للخبرة الفنية ومؤثرة في تكوين القناعة القضائية.

**ثانياً: الشهادة الإلكترونية عن بُعد**

يُقصد بالشهادة الإلكترونية عن بُعد تلك الأقوال التي لا يُدلى بها بحضور الشاهد ماديًا في جلسة التحقيق، بل يتم الإدلاء بها عبر وسائط تقنية، مثل الإنترنت أو أنظمة الاتصال المرئي (إبراهيم، ٢٠١٠، ص ٢٦٠–٢٦٣)ويقتضي بحث مشروعية هذا النوع من الشهادة التمييز بين صورتين:

١. الشهادة المُسجَّلة مسبقًا

وهي الشهادة التي تُدلي بها الشهود مسبقًا ليُعاد عرضها لاحقًا أمام المحكمة أثناء التحقيق النهائي. ويُمثل هذا الأسلوب ضمانة لحماية الشاهد من الضغوط أو الإكراه، ويُسهم في تثبيت الوقائع تجنبًا للإنكار لاحقًا، خاصة في الجرائم التقنية التي تتسم بالسرية وسرعة التلاعب بالأدلة.

٢. الشهادة الإلكترونية الفورية (المباشرة) وتُؤخذ أقوال الشاهد في هذه الصورة عبر تقنية الاتصال السمعي–المرئي، بحيث يظهر الشاهد أمام المحكمة بالصوت والصورة كما لو كان حاضرًا ماديًا. وقد كان القضاء—لا سيما القضاء الأمريكي—يرفض سابقًا الأخذ بالشهادة التي تُدلى خارج الجلسة معتبرًا إياها شهادة سماع لا حجية لها. إلا أن التطور التقني أدى إلى إعادة النظر في هذا الاتجاه، وأصبحت الشهادة الإلكترونية المباشرة مقبولة فقهيًا وقضائيًا، بعد ضمان الضوابط التي تكفل علانية الجلسة، وحضور المتهم، وتمكينه من مناقشة الشاهد (إبراهيم، ٢٠١٠، ص ٢٦٢). أضحى هذا النوع من الشهادات اليوم من الأدلة المعترف بها في العديد من الأنظمة القضائية، خصوصًا في القضايا التي تتطلب حماية الشهود أو التي يتعذر فيها الحضور المادي بسبب الطبيعة التقنية للجريمة أو موقع الشاهد.

**الفرع الثاني: التفتيش**

يُعدّ التفتيش من أخطر الإجراءات الجنائية، لما ينطوي عليه من مساس مباشر بحقوق الأفراد وحرياتهم التي كفلتها الدساتير، إذ يؤدي إلى الكشف عن مستودع أسرار الشخص وحياته الخاصة. ولهذه الخطورة، أحاط المشرّع هذا الإجراء بجملة من الضمانات الصارمة التي حدّدت الجهة المختصة بإجرائه، والسلطة التي تملك الإذن به، والحالات والشروط التي تبرّر مباشرته (إبراهيم، ٢٠١٠، ص ١٨٠). وبالنظر إلى أهمية التفتيش في مجال الجرائم المعلوماتية، يُقسّم هذا المطلب إلى ثلاثة فروع: يتناول الفرع الأول المقصود بالتفتيش، ويُعنى الفرع الثاني بتحديد محل التفتيش، بينما يُخصّص الفرع الثالث لبيان شروط تفتيش النظام المعلوماتي.

**أولاً: المقصود بالتفتيش**

يُعدّ التفتيش أحد أهم إجراءات التحقيق الهادفة إلى البحث عن الأدلة المادية المرتبطة بالجريمة وضبطها، ولا يُمارس إلا في أماكن منحها القانون حرمة خاصة وبمقتضى نص يجيز ذلك. وقد عرّفه الفقه بأنه إجراء يرمي إلى البحث عن أدلة تثبت وقوع الجناية أو الجنحة ونسبتها إلى المتهم وفقًا للقانون (سرور، ١٩٩٣، ص ٥٤٤)، كما وُصف بأنه البحث في "مستودع السر" (عوض، ٢٠٠٢، ص ٢٨٤)، أو وسيلة لكشف الأشياء الخفية أو ضبط الأشخاص الفارّين من العدالة (عثمان، ١٩٨٩، ص ٣٠٥)وفي مجال الجرائم المعلوماتية، يبقى المفهوم القانوني للتفتيش ثابتًا، غير أن طبيعته الرقمية أفرزت تعريفات أكثر تخصيصًا؛ منها اعتباره دخولًا إلى نظم المعالجة الآلية للبيانات للبحث عن أنشطة غير مشروعة تمثل جناية أو جنحة بهدف الوصول إلى الأدلة (هلالي، ١٩٩٧، ص ٧٣)، أو بأنه فحص للأشخاص أو الأماكن بحثًا عن الأدلة الرقمية المتعلقة بجريمة معلوماتية (مهدي، ٢٠٠٨، ص ٤٤٧). ويرى آخرون أنه يشمل تفتيش الحواسيب والهواتف والشبكات للعثور على البيانات المخزنة أو الاتصالات الإلكترونية المرتبطة بالفعل الجرمي (جاد المولى، ٢٠١٩، ص ١١٧–١١٨)وقد أكدت محكمة النقض المصرية أن التفتيش لا يُجرى إلا عند وجود جريمة واقعة بالفعل تُسند إلى شخص معيّن، وبناءً على دلائل كافية تبرّر الإجراء (إبراهيم، ٢٠١٠، ص ١٨٣–١٨٤). ويظل التفتيش في النهاية أداة أساسية لدعم الأدلة ومنع الجاني من الإفلات من العقاب..

**ثانياً: محل التفتيش**

ينصرف التفتيش المعلوماتي في جرائم الإنترنت إلى الأجهزة الحاسوبية والشبكات المرتبطة بها، بما في ذلك الخادم (Server)، والمضيف (Host)، والمزود الآلي، وسائر الملحقات التقنية ذات الصلة. ويُلاحظ أن محل التفتيش في هذا السياق ليس كيانًا مستقلاً، بل يرتبط بمكان معيّن أو يكون بحيازة شخص ما، سواء كان مالكًا للجهاز أو مجرد حائز له. ولذلك، تمثل الدقة في تحديد محل التفتيش ضمن الإذن القضائي ضمانة إجرائية أساسية، تهدف إلى منع تجاوز نطاق الإجراء أو اتساعه بصورة غير مشروعة، لما قد يترتب على ذلك من بطلان التفتيش والإجراءات اللاحقة له، اتساقًا مع مبدأ الشرعية الإجرائية وضمانات حماية الحياة الخاصة (عزت، ٢٠١٠، ص ٦٣٩).

وبناءً عليه، ينصب التفتيش المعلوماتي في جوهره على ثلاثة عناصر رئيسة، هي:

١. المكونات المادية (Hardware)

وتشمل الأجهزة الحاسوبية، والطابعات، وأجهزة النسخ، والوسائط القابلة للنقل كالأقراص الصلبة المحمولة ووسائط USB.

٢. المكونات المنطقية (Software)

وتتضمن نظم التشغيل، والبرمجيات المثبتة، وقواعد البيانات، والملفات الإلكترونية الظاهرة أو المخفية داخل النظام.

٣. شبكات الاتصال عن بُعد

وتشمل شبكات الاتصال السلكية واللاسلكية، المحلية والدولية، بما في ذلك الإنترنت، وبروتوكولات IP، والبريد الإلكتروني، وتطبيقات التواصل الرقمي.

**أولاً: تفتيش المكونات المادية لجهاز الحاسوب**

يخضع تفتيش المكونات المادية للحاسوب لأحكام التفتيش المنصوص عليها في التشريعات الإجرائية، ويتحدد نطاقه وفق طبيعة المكان الذي توجد فيه تلك الأجهزة، نظرًا لاختلاف المركز القانوني للأماكن العامة عن الأماكن الخاصة.فإذا وُجد الجهاز في مكان خاص كالمسكن، فلا يجوز تفتيشه إلا في الحالات التي يحددها القانون، وبموجب إذن صادر من جهة مختصة، مع مراعاة الضمانات المتصلة بحضور صاحب المكان أو المتهم أثناء التفتيش، وفقًا لأحكام قوانين أصول المحاكمات (المواد ٧٣ و٨٢ من قانون أصول المحاكمات الجزائية العراقي؛ قانون الإجراءات الجزائية الجزائري، المادة ٦٤)أما إذا وُجد الحاسوب في مكان عام أو كان الشخص يحمل المكونات المادية للحاسوب في إحدى الأماكن العامة – سواء كانت عامة بطبيعتها كالطرق والحدائق، أو عامة بالتخصيص كالمقاهي والفنادق ووسائط النقل – فيطبق التفتيش وفق الضوابط القانونية المقررة دون إخلال بالضمانات الأساسية.

**ثانيًا: تفتيش المكونات المنطقية لجهاز الحاسوب**

ثار خلاف فقهي بشأن مدى خضوع البيانات والمعطيات الإلكترونية لإجراءات التفتيش التقليدية، وانقسم الفقه إلى اتجاهين:

الاتجاه الأول

يرى إمكانية إخضاع المكونات المنطقية للتفتيش، استنادًا إلى أن الذاكرة الإلكترونية تشغل حيزًا قابلًا للقياس، مما يجعلها مماثلة للأشياء المادية. ويستند هذا الاتجاه إلى تعديلات تشريعية كالتعديل الذي أدخله المشرّع الفرنسي على المادة (٩٤) من قانون الإجراءات الجزائية، بإضافة عبارة "المعطيات المعلوماتية" ليصبح من الجائز تفتيشها قانونًا (نايري، ٢٠١٧؛ القانون الفرنسي رقم ٤٩-٦٥٣ لسنة ١٩٩٤).كما ذهب بعض الفقه إلى أن النصوص التي تجيز ضبط "أي شيء" يمكن تفسيرها لتشمل البيانات الرقمية بمختلف أشكالها، المحسوسة أو غير المحسوسة (إبراهيم، ٢٠١٠).

الاتجاه الثاني

ينكر خضوع المكونات المنطقية لإجراءات التفتيش، بحجة أن البيانات غير ملموسة ولا ينطبق عليها وصف "الشيء"، مما يستدعي تدخلًا تشريعيًا صريحًا يجيز تفتيش الحواسيب والمعطيات الإلكترونية (إبراهيم، ٢٠١٠).ويقابل هذين الاتجاهين رأي ثالث، يؤكد أن البيانات لا تعد قابلة للضبط إلا إذا اكتسبت شكلًا ماديًا، كالطباعة أو النسخ، استنادًا إلى قانون الإجراءات الجنائية الألماني (المادة ٩٤).

ورغم الخلاف الفقهي، فقد استقرّ العمل التشريعي والقضائي في عدة دول – مثل اليونان وإنجلترا – على جواز تفتيش البيانات الإلكترونية متى كان ذلك ضروريًا لكشف الحقيقة وتقييم الأدلة (جاد المولى، ٢٠١٩؛ علي، ٢٠١٢).أما في القانون العراقي، فلا إشكال في تفتيش المكونات المادية للحاسوب وفق المادة (٧٤) من قانون أصول المحاكمات الجزائية، إلا أن شمول التفتيش للمعطيات الإلكترونية يحتاج إلى تعديل تشريعي

بإضافة عبارة "أو معطيات معالجة إلكترونيًا" إلى نص المادة.وقد استجاب مشروع قانون جرائم المعلوماتية العراقي لهذا الاتجاه، إذ أجاز تتبع الأدلة المعلوماتية داخل الأنظمة والشبكات، وذلك بموجب المادة (٢٦/أولًا/ج).

**ثالثًا: تفتيش الشبكات المعلوماتية المتصلة بالحاسوب**

ترتبط الشبكات المعلوماتية بربط أكثر من جهاز داخل الدولة أو خارجها، وتبرز الإشكالية عند امتداد التفتيش إلى أنظمة بعيدة أو خارج الحدود.

**الاول: تفتيش جهاز داخل الدولة متصل بأنظمة أخرى**

أجازت عدة تشريعات، كالقانون الجزائري (٠٤/٠٩) والأردني، امتداد التفتيش ليشمل الأنظمة المرتبطة بالجهاز متى اقتضت الضرورة، وهو ما أكدته أيضًا اتفاقية بودابست (٢٠٠١) التي سمحت بتوسيع نطاق التفتيش إلى الأنظمة المتاحة عبر الجهاز الأصلي. وأخذت التشريعات الألمانية والبلجيكية الاتجاه ذاته. وفي العراق، أجاز قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (٢٠١٣) توسيع التفتيش إلى الأنظمة المرتبطة داخل الإقليم الوطني وفق المادة (٢٦).

**الثاني: تفتيش أجهزة أو نظم موجودة خارج حدود الدولة**

قد يخزن الجناة بياناتهم في أنظمة خارج الدولة بهدف عرقلة التحقيق، مما يثير مسألة مدى امتداد إذن التفتيش إلى الخارج.

الرأي الأول (الرافض):

يرى أن التفتيش خارج الحدود غير جائز دون موافقة الدولة المعنية، استنادًا إلى مبدأ السيادة، ولا يتم إلا عبر اتفاقيات أو آليات التعاون القضائي الدولي (هلالي، ١٩٩٧؛ عزت، ٢٠١٠).

الرأي الثاني (المؤيد بشروط):

يجيز التفتيش العابر للحدود في حالات الضرورة القصوى وبشروط، منها:

١. أن يكون الإجراء محدودًا بالقدر اللازم،

٢. إخطار الدولة المعنية متى أمكن،

٣. وجود استعجال حقيقي،

٤. عدم المساس بسيادة الدولة الأخرى (هيان الرشيد، ٢٠٠٤).

وعزّزت اتفاقية بودابست هذا الاتجاه، إذ سمحت بالتفتيش في حال كانت البيانات متاحة للعامة أو بموافقة المالك.

الموقف العراقي:

لم يعالج مشروع قانون جرائم المعلوماتية التفتيش عبر الحدود، لكن قانون أصول المحاكمات الجزائية أقر الإنابة القضائية وسيلة رسمية لتنفيذ الإجراءات خارج الإقليم (المواد ٣٥٣–٣٥٦).

**الثالث: التنصت والمراقبة الإلكترونية لشبكات الحاسوب**

يثير التنصت الإلكتروني إشكالات تتعلق بسرية الاتصالات، إلا أن معظم التشريعات أجازته بضوابط. فقد كفل الدستور العراقي (٢٠٠٥) حرية الاتصالات، لكنه سمح بالمراقبة عند الضرورة وبقرار قضائي مسبّب. وأجاز مشروع قانون جرائم المعلوماتية اعتراض البيانات ورصدها وفق شروط محددة (مادة ٢٦)واتخذت دول أخرى مسارًا مشابهًا؛ فالقانون الفرنسي لعام ١٩٩١ أجاز اعتراض الاتصالات، وفي هولندا منح قاضي التحقيق صلاحية إصدار أمر بالتنصت في الجرائم الخطيرة، بينما اشترط القانون الأمريكي إذنًا قضائيًا يحدد نطاق الاعتراض ومدته.يميل الاتجاه التشريعي الغالب إلى السماح بالمراقبة والتفتيش في الجرائم المعلوماتية، مع وضع ضمانات مشددة لتحقيق التوازن بين الأمن الرقمي وحماية الخصوصية وحقوق الأفراد..

**الفرع الثالث: الخبرة**

تُعدّ الاستعانة بالخبراء ضرورة أساسية في التحقيق بالجرائم المعلوماتية، نظرًا للطبيعة الرقمية المعقدة لمحلّ الجريمة وصعوبة فهم آليات ارتكابها دون دعم فني (عبد الله، ٢٠٠٤، ص ٣٩٤–٣٩٥). ويُعرَّف الخبير بأنه الشخص المختص الذي يقدم رأيًا فنيًا يعجز المحقق عن تقديره بنفسه، سواء تعلق الأمر بالأدلة، أو المتهم، أو أدوات الجريمة (حسني، ١٩٨٨، ص ٤٧٤؛ سعيد، ١٩٩٠، ص ١٨٤).

**أولاً: الخبراء الإلكترونيون ومهامهم**

١. تعريف الخبير الإلكتروني

هو مختص يمتلك خبرة تقنية متقدمة تمكّنه من تحليل الأنظمة والبرمجيات والشبكات وتقديم رأي فني في القضايا الرقمية (موسى، ٢٠٠٨، ص ٢٢١).

٢. أنواع الخبراء الإلكترونيين (موسى، ٢٠٠٨، ص ٢٢٣)

المبرمج: يكتب الأوامر البرمجية ويطوّر أنظمة التشغيل.

محلل النظم: يدرس تدفق المعلومات داخل النظام ويحدد آليات المعالجة.

مهندسو الصيانة والاتصالات: يعالجون الأعطال الفنية في الأجهزة والشبكات.

مشغلو الحاسوب والشبكات: لديهم خبرة في تشغيل الأنظمة وإدخال البيانات.

مدير النظام: يشرف على عمل النظام وسلامته وأمنه.

٣. المسائل التي تستلزم خبرة

أ. مسائل الوصف: تشمل تحديد نوع الأجهزة، بيئة الشبكة، مواضع الأدلة الرقمية، وتقييم الآثار الفنية (حجازي، ٢٠٠٩؛ براهيمي، ٢٠١٨؛ الغافري، ٢٠٠٨).

ب. مسائل البيان: مثل عزل النظام دون إتلاف الأدلة، نقل البيانات بوسائل آمنة، وتحويلها لصورة ورقية تعرض أمام القضاء (مصطفى، ٢٠١٠، ص ١٥٣-١٥٤).

**ثانياً: مدى كفاية النصوص التقليدية**

نظم قانون الخبراء رقم ١٦٣ لسنة ١٩٦٤ إجراءات الاستعانة بالخبراء، وأجاز قانون أصول المحاكمات الجزائية العراقي (٦٩-٧١) طلب الخبرة من القاضي أو المحقق، على أن يعمل الخبير تحت إشراف قاضي التحقيق. ورغم إمكانية تطبيق هذه النصوص على الجرائم المعلوماتية، إلا أنها لا تواكب خصوصية الدليل الرقمي.

النموذج البلجيكي

نصت المادة (٨٨) من قانون الإجرام الإلكتروني على صلاحية قاضي التحقيق في تعيين خبير مختص للحصول على نسخة من البيانات وتشغيل الأنظمة، مع إلزام الخبير بالاستجابة.

النموذج الجزائري

وسع القانون ٠٤/٠٩ نطاق الخبرة، وأجاز الاستعانة بأي شخص لديه دراية بالنظام المعلوماتي. كما أنشأ المرسوم ١٥-٢٦١ الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام لتقديم الدعم الفني للسلطات القضائية.

الموقف العراقي

لم يضع مشروع قانون جرائم المعلوماتية نظامًا متخصصًا للخبرة الرقمية، واقتصر على الإحالة إلى الخبراء المحليين أو الأجانب وفق تقدير القاضي، دون تطوير إطار خاص كما فعلت التشريعات المقارنة..

## المطلب الثاني: ضبط مكونات الجريمة

سنعرض في هذا المطلب تعريف ضبط الأدلة الإلكترونية، وأنواع الأدلة التي يمكن ضبطها في الجرائم المعلوماتية التي يجري التحقيق بشأنها.

**الفرع الأول: تعريف ضبط الأدلة الإلكترونية**

يُعدّ الضبط من أهم الإجراءات الجنائية، إذ يقوم على وضع اليد على الأدلة المتصلة بالجريمة بهدف كشف الحقيقة، سواء تعلقت بمرتكب الجريمة أو بظروف ارتكابها (مبارك، ٢٠١٤، ص ٣٦٨). وقد منح قانون أصول المحاكمات الجزائية العراقي للمحقق أو عضو الضبط القضائي سلطة تفتيش منزل المتهم وضبط الأشخاص أو الأشياء التي تُفيد في كشف الحقيقة عند وقوع جناية أو جنحة عمدية مشهودة (مادة ٧٩).وبما أن الضبط يُعدّ نتيجة مباشرة للتفتيش، فقد استقر الفقه على أن قواعد التفتيش تسري عليه، وأن بطلان التفتيش يؤدي إلى بطلان الضبط تبعًا له (موسى، ٢٠٠٩، ص ٢٠٨-٢٠٩). ولا يجوز ضبط إلا ما له صلة بالجريمة، سواء كان في مصلحة المتهم أو ضده، تحقيقًا لمبادئ العدالة الجنائية.وفي الجرائم التقليدية، لا يثير ضبط الأدلة المادية إشكالات كبيرة بسبب ملموسيتها. أما في الجرائم المعلوماتية، فتظهر عقبات متعددة، أبرزها صعوبة ضبط الأنظمة الرقمية دون التأثير على بيئتها التقنية، وتردد مستخدمي الأنظمة في التعاون، وإمكانية محو الأدلة غير المرئية بسهولة، ما يستلزم خبرة فنية متخصصة (إبراهيم، ٢٠١٠، ص ٢٧٤)وتزداد الصعوبة مع قدرة الجاني على الادعاء بوجود خلل تقني، وضخامة البيانات التي تتطلب

فرزًا دقيقًا من خبير مختص، إضافة إلى أنظمة الحماية القائمة على كلمات المرور أو التشفير التي قد تمنع الدخول إلى الجهاز (حجازي، ٢٠٠٩، ص ٢٦٧–٢٦٨). كما قد يتقاعس بعض المجني عليهم عن الإبلاغ خشية المساس بسمعتهم، مما يعرقل إجراءات الضبط (حجازي، ٢٠٠٩، ص ٢٦٨).أما بشأن حجية نسخ البيانات الرقمية، فقد تبنّى بعض القضاء اتجاهًا متشددًا لسهولة التلاعب بها، وقضت محكمة النقض الفرنسية بأن ضبط نسخة دون الجهاز الحامل لا يُعد ضبطًا صحيحًا (براهيمي، ٢٠١٨، ص ٥٥)..

**الفرع الثاني: ضبط الأدلة الإلكترونية في الجرائم المعلوماتية**

يقتضي البحث في ضبط الأدلة في الجرائم المعلوماتية التمييز بين الأدلة المادية والأدلة المعنوية لطبيعة كل منهما. ويعرض هذا المطلب كيفية التعامل مع النوعين وفق الأطر الإجرائية الحديثة.

**أولاً: ضبط الأدلة المادية في الجريمة المعلوماتية**

تشمل الأدلة المادية العناصر ذات الوجود الملموس التي يسهل ضبطها وفق القواعد التقليدية، وأهمها:

١. الأوراق التي قد يحتفظ بها المستخدمون رغم التطور التقني، وتظل ذات قيمة إثباتية عند ارتباطها بالجريمة (إبراهيم، ٢٠١٠، ص ٢٧٥).

٢. أجهزة الحاسوب وملحقاتها باعتبارها الوسيلة الأساسية لارتكاب الجرائم الرقمية، ويتطلب ضبطها خبرة فنية.

٣. البرمجيات خاصة إذا كان إنتاج الدليل الرقمي قائمًا على برنامج غير شائع.

٤. وسائط التخزين المنقولة كالUSB والأقراص الصلبة المحمولة.

٥. أجهزة الاتصال والمودم لما تحويه من سجلات اتصال وبيانات مرور إلكترونية.

٦. الأدلة التشغيلية مثل الأدلة التقنية المرافقة للأجهزة.

٧. البطاقات الممغنطة المستخدمة في العمليات الإلكترونية.

ثانياً: ضبط الأدلة المعنوية (غير المادية)

تُعد البيانات الرقمية من أصعب الأدلة ضبطًا، وقد أدى اختلاف طبيعتها إلى ظهور ثلاثة اتجاهات فقهية وتشريعية:

الاتجاه الأول: عدم قابلية البيانات الرقمية للضبط

يرى أن البيانات الإلكترونية لا تتمتع بخصائص مادية، فلا تُضبط إلا إذا حُوّلت إلى مخرجات ملموسة. وقد تبنت هذا الاتجاه قوانين:

الألماني (المواد ٩٤ و١٦١)،

الروماني (ضبط الدعامات فقط)،

الياباني (اشتراط المخرجات الورقية)،

الجزائري الذي عالج الأمر بنصوص مستقلة (٠٤/٠٩، المواد ٦–٧).

الاتجاه الثاني: قابلية البيانات للضبط وفق القواعد التقليدية

يعتبر البيانات الرقمية قابلة للضبط متى ارتبطت بالجريمة، وقد أخذت بهذا:

الولايات المتحدة خصوصًا في الجرائم الخطيرة (رستم، ١٩٩٤)،

كندا التي وسّعت مفهوم الضبط ليشمل جميع البيانات بغضّ النظر عن وعائها.

الاتجاه الثالث: التوسيع التشريعي لصلاحيات الضبط

يدعو إلى إدراج البيانات الرقمية صراحة ضمن الأشياء القابلة للضبط، وتبنته تشريعات:

السعودية (٢٠٠٧)، الإمارات (٢٠٠٦)، قطر، البحرين، عمان (حجازي، ٢٠٠٩).

آليات الحد من مخاطر ضبط البيانات غير المادية

اعتمدت بعض الدول ضمانات خاصة لتحقيق التوازن بين سلطة التحقيق وحماية الحقوق:

١. اليونان: منحت سلطات التحقيق إمكانية ضبط البيانات سواء كانت على وسيط مادي أو داخل الأنظمة الإلكترونية.

٢. المملكة المتحدة: أجازت نسخ البيانات الرقمية باستثناء المحمية قانونيًا، مما سمح بضبط السجلات الإلكترونية ضمن ضوابط واضحة.

وبذلك يتضح أن تطور الجرائم الرقمية فرض إعادة النظر في مفهوم الضبط التقليدي، باتجاه توسيعه ليشمل الأدلة غير المادية، مع وضع ضمانات تحمي الخصوصية وتمنع التعسف في الإجراءات.

## الخاتمة

### أولاً: النتائج

١. إمكانية تلقي الشكاوى والبلاغات عبر الإنترنت لا تُشكل عائقاً في الدول المتقدمة تقنياً، لما تمتلكه من أنظمة وأجهزة متخصصة تستقبل هذه البلاغات وتتعامل معها بفعالية. بينما لا تزال هذه المسألة تُشكل تحدياً في بعض الدول النامية نتيجة افتقارها للبنية التحتية التقنية وضعف الخبرات لدى الجهات الأمنية والقضائية، ولا سيما في ما يتعلق بتدريب أعضاء الضبط القضائي على استخدام الأنظمة الرقمية وأدوات التحري الإلكترونية.

٢. الاختصاص المكاني لأعضاء الضبط القضائي يمكن تجاوزه في حالات محددة. الحالة الأولى: عندما تكون الجريمة واقعة ضمن اختصاص العضو وإن تم التفتيش خارج دائرته. أما الحالة الثانية: فتكون عند الضرورة، كأن يظهر من المتهم ما يدل على حمله دليلًا للجريمة، أو في حال تعقبه أثناء المطاردة، ويجوز عندها تجاوز الحدود المكانية المقررة للاختصاص.

٣. الخلاف الفقهي حول إمكانية تفتيش وضبط المكونات المنطقية للحاسوب انقسم إلى اتجاهين: الأول يرى جواز التفتيش استنادًا إلى النصوص التي تُجيز ضبط "أي شيء"، ويُفسر ذلك ليشمل البيانات الرقمية المحسوسة وغير المحسوسة. أما الاتجاه الثاني، فيرى أن البيانات غير المادية لا تدخل ضمن هذا المفهوم. ورغم هذا الجدل، فإن الاتجاه الراجح اليوم يميل إلى قبول تفتيش بيانات الحاسوب واعتبارها أدلة جنائية مشروعة، طالما أن الهدف من التفتيش هو الوصول إلى أدلة الجريمة.

٤. تفتيش النظم المعلوماتية المرتبطة بالحاسوب أصبح مقبولًا في بعض التشريعات، حتى إذا كانت مرتبطة بحواسيب أخرى داخل الدولة. أما بالنسبة لامتداد الإذن خارج حدود الدولة، فقد انقسم الرأي إلى اتجاهين: الأول يشترط اتفاقيات دولية أو إذن من الدولة المعنية، أما الثاني فيجيز التفتيش العابر للحدود شريطة أن يكون محدودًا في الزمن وبعلم الدولة المتأثرة.

٥. الخبرة الفنية في الجرائم المعلوماتية يمكن تنظيمها وفق القواعد التقليدية المتعلقة بالاستعانة بالخبراء، غير أن عدداً من الدول قامت بتعزيز هذه القواعد من خلال نصوص خاصة تراعي طبيعة الجرائم المعلوماتية وتعقيداتها التقنية.

٦. الجدل الفقهي حول إمكانية ضبط الأدلة غير المادية (المعنوية) في جرائم الحاسوب أدى إلى ظهور اتجاهين: الأول ينكر إمكانية الضبط مستندًا إلى غياب الدعامة المادية، بينما يرى الاتجاه الثاني وهو الأرجح أن الضبط ممكن للبيانات المخزنة إلكترونيًا، وقد أيد هذا الاتجاه كل من الفقه الأمريكي والكندي ونصت عليه الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية لعام ٢٠٠٩.

### ثانيًا: المقترحات

١. ضرورة ملاءمة التشريع العراقي مع خصوصية الجرائم المعلوماتية، وذلك من خلال النص صراحةً على جواز تفتيش الأماكن الافتراضية وضبط محتوياتها، مع تحديد السلطات المختصة بإجراء التفتيش، وضمان أن يكون ذلك تحت إشراف قضائي فعال، مع توسيع نطاق التفتيش ليشمل الأنظمة المرتبطة بالحاسوب سواء داخل البلاد أو خارجها. ونقترح تعديل المادة (٤٧) من قانون أصول المحاكمات الجزائية بإضافة عبارة "معطيات إلكترونية" لتصبح: "إذا تراءى لقاضي التحقيق وجود أشياء أو معطيات إلكترونية تفيد في التحقيق..."

٢. وضع تنظيم قانوني متكامل لعمليتي التفتيش والضبط في سياق الجرائم المعلوماتية، بما يوازن بين حماية خصوصية الأفراد وضمان حقوقهم، وبين الحاجة إلى التدخل السريع لضبط أدلة الجريمة والحفاظ عليها.

٣. إنشاء جهاز وطني متخصص في مكافحة جرائم الأنظمة المعلوماتية، يعمل تحت إشراف قاضي تحقيق متمكن في هذا المجال، ويضم كوادر فنية من خريجي هندسة الحاسوب ومؤهلين بخبرة عملية في التكنولوجيا الرقمية، إلى جانب ضباط ومحققين قانونيين حاصلين على شهادات كفاءة في الحاسوب.

٤. دعم وتعزيز الجهود القائمة في وزارة الداخلية بشأن مكافحة الجرائم الإلكترونية، من خلال تطوير الأجهزة الأمنية القائمة وزيادة كفاءتها في رصد وتتبع الجرائم التي تُرتكب عبر شبكة الإنترنت.

## المصادر

### أولاً: الكتب

١. ابن منظور، لسان العرب، دار المعارف، القاهرة، ج ٤.

٢. الأمام محمد بن أبي بكر عبد القادر الرازي، مختار الصحاح، ترتيب محمود خاطر، القاهرة، ١٩٥١، ط١.

٣. بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، رسالة ماجستير، جامعة محمد خيضر، بسكرة، ٢٠١٥.

٤. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار الفكر العربي، القاهرة، ٢٠٠١.
٥. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، ٢٠٠٢.
٦. حنان ريحان مبارك، الجرائم المعلوماتية، دراسة مقارنة، ط١، منشورات الحلبي الحقوقية، لبنان، ٢٠١٤.
٧. حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ٢٠٠٤.
٨. حجازي، عبد الفتاح بيومي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ط١، ٢٠٠٩.
٩. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠١٠.
١٠. سمير عالية، الجرائم الإلكترونية في القانون الجديد رقم ٨١ لسنة ٢٠١٨ والمقارن، ط١، منشورات الحلبي الحقوقية، ٢٠٢٠.
١١. سعيد حسب الله عبد الله، شرح قانون أصول المحاكمات العراقية، دار الحكمة للطباعة والنشر، الموصل، ١٩٩٠.
١٢. سلطان محيا الديحاني، التحري في الجريمة المعلوماتية، جريدة القبس الكويتية، عدد (١٢٣٩٢)، نوفمبر ٢٠٠٧.
١٣. عبد الأمير العكيلي، شرح قانون أصول المحاكمات الجزائية، دار السنهوري، ٢٠١٥، الجزء الأول.
١٤. عبد الله حسين علي محمود، سرقة المعلومات المخزونة في الحاسوب الآلي، ط٣، دار النهضة العربية، القاهرة، ٢٠٠٤.
١٥. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤.
١٦. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ط١، ٢٠٠٩ (طبعة محدثة).
١٧. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ٢٠٠٤، ص ٦٠ وما بعدها.
١٨. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشورات الحلبي الحقوقية، ٢٠٠٠.
١٩. عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، منشأة المعارف، الإسكندرية، ٢٠٠٢.
٢٠. فخري عبد الرزاق صلبي الحديثي، شرح قانون أصول المحاكمات الجزائية، مكتبة السنهوري، ط١، ٢٠١٦.
٢١. فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، ط٢، دار النهضة العربية، القاهرة، ٢٠١٠.
٢٢. فخري عبد الرزاق صلبي الحديثي، شرح قانون أصول المحاكمات الجزائية، مكتبة السنهوري، ط١، ٢٠١٦، ص ٧٨، ٨٣، ١٩٨ (نفس المصدر بصفحات مختلفة).
٢٣. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ط٢، ١٩٨٨.
٢٤. محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي، دار الفكر الجامعي، الإسكندرية، ٢٠١٩.
٢٥. مأمون سلامة، قانون الإجراءات الجنائية معلقاً عليه بالفقه وأحكام النقض، دار الفكر العربي، القاهرة، ط١، ١٩٨٠.
٢٦. محمد طارق الخن، الجريمة المعلوماتية، برنامج الحقوق، الجامعة الافتراضية السورية، ٢٠١٢.
٢٧. محمد علي أحمد الكواري، مسرح الجريمة ودوره في كشف الجريمة، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٧.
٢٨. محمد فتحي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع الكتب المصرية الحديثة، ١٩٩١.
٢٩. هدى طلب علي، الإثبات الجنائي في جرائم الإنترنت والاختصاص القضائي بها، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة النهرين، ٢٠١٢.
٣٠. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤.
٣١. هشام محمد فريد رستم، أصول التحقيق الجنائي الفني في الجرائم المعلوماتية، بحث مقدَّم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ج٢، ط٣.
٣٢. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤.
٣٣. هلالي عبد الإله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، ١٩٩٧.
٣٤. هلالي عبد الإله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، ط١، ١٩٩٧.
٣٥. يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، ٢٠١٣.

٣٦. نبيلة هبة محمد هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة الاستدلال، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧.
٣٧. سمير عالية، الجرائم الإلكترونية في القانون الجديد رقم ٨١ لسنة ٢٠١٨ والمقارن، ط١، منشورات الحلبي الحقوقية، ٢٠٢٠ (إعادة تأكيد لطبعة الكتاب).

## ثانياً: الرسائل والأطاريح الجامعية

١. بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، رسالة ماجستير، قانون جنائي، جامعة محمد خيضر، بسكرة، ٢٠١٥.
٢. براهيمي جمال، التحقيق في الجرائم الإلكترونية، أطروحة دكتوراه في العلوم، كلية الحقوق، جامعة مولود معمري، ٢٠١٨.
٣. السوفي النور الهدى، التحقيق في الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة قاصدي مرباح – ورقلة، ٢٠١٦-٢٠١٧.
٤. سعيدان نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة الحاج الأخضر، ٢٠١٢-٢٠١٣.
٥. صغير يوسف، الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، ٢٠١٣.
٦. غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسوب والإنترنت)، أطروحة دكتوراه، كلية الحقوق، الجامعة الإسلامية، ٢٠٠٤.
٧. عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة القاهرة، دار النهضة العربية، ٢٠٠٤.
٨. يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، ٢٠١٣.
٩. هدى طلب علي، الإثبات الجنائي في جرائم الإنترنت والاختصاص القضائي بها، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة النهرين، ٢٠١٢.
١٠. نايري عائشة، الجرائم الإلكترونية في التشريع الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية – أدرار، ٢٠١٦-٢٠١٧.

## ثالثاً: القوانين والقرارات والنصوص النظامية

١. قانون أصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١ المعدل، ولا سيما المواد: ٢، ٤١، ٤٢، ٤٣، ٤٤، ٤٧، ٤٨، ٧٣، ٧٩، ٨٢.
٢. قانون الإجراءات الجزائية الجزائري رقم (٠١-٠٨) لسنة ٢٠٠١، ولا سيما المادة (١٧)، والمادة (٦٤).
٣. قانون رقم (٠٦-٢٢) المؤرخ في ٢٠ ديسمبر ٢٠٠٦ المعدِّل والمتمِّم لقانون الإجراءات الجزائية الجزائري، ولا سيما المادتان: ٦٥ مكرر ١١، ٦٥ مكرر ١٨.
٤. القانون رقم (٠٩-٠٤) لسنة ٢٠٠٩ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ولا سيما المواد: ٥، ٦، ٧، ١٣.
٥. قانون الإجراءات الفرنسي رقم (٤٩-٦٥٣) لسنة ١٩٩٤، المادة (٩٤).
٦. قانون الإجراءات الجنائية الألماني، المواد (٩٤) و(١٦١).
٧. قانون الإجراءات الجنائية اليوناني الصادر عام ١٩٩٣، المواد (١٨٣)، (٢٠٨)، (٢٥١)، (١/٢٦١).
٨. قرار وزارة الداخلية المصري رقم (١٣٥٠٧) لسنة ٢٠٠٢، الصادر في ٢٠٠٢/٧/٧.
٩. مشروع قانون جرائم المعلوماتية العراقي، ولا سيما المادة (٢٦/أولاً/ج).