HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

عنوان البحث

# وسائل وإجراءات التحقيق الابتدائي في الجرائم الإلكترونية

هشام محمد مهيدي صالح[1]، د. محمد هاني فرحات[1]

[1] باحث دكتوراه، الجامعة الإسلامية في لبنان، كلية الحقوق، لبنان، خلدة. بريد الكتروني: Real77644@gmail.Com.

[2] تدريسي في الجامعة الاسلامية في لبنان، كلية الحقوق، لبنان، خلدة. بريد الكتروني: Mohammad.farhat@iul.edu.lb.

HNSJ, 2026, 7(6); https://doi.org/10.53796/hnsj76/28

المعرف العلمي العربي للأبحاث: https://arsri.org/10000/76/28

تاريخ الاستقبال: 2026/05/15م تاريخ القبول: 2026/05/20م تاريخ النشر: 2026/06/01م

## المستخلص

تتناول هذه الدراسة وسائل وإجراءات التحقيق الابتدائي في الجرائم الإلكترونية، في ضوء ما فرضه التطور المتسارع في تقنيات المعلومات والاتصالات من أنماط إجرامية مستحدثة تتسم بالتعقيد الفني وصعوبة الإثبات. وتهدف الدراسة إلى بيان أهم الوسائل التقنية والمهارات الفنية اللازمة لتمكين سلطات التحقيق من جمع الأدلة الرقمية وتحليلها وحفظها بصورة تضمن سلامتها ومشروعيتها، فضلًا عن توضيح إجراءات التحقيق الابتدائي الملائمة لطبيعة الجرائم الإلكترونية، ولا سيما الاستجواب، والشهادة، والاستعانة بالخبرة الفنية، والتفتيش، والضبط. اعتمدت الدراسة المنهج التحليلي من خلال عرض الأدوات والبرامج التقنية المستخدمة في التحقيق، وتحليل دورها في كشف الجريمة، مع بيان الإطار الإجرائي في التشريعين العراقي واللبناني. وتوصلت الدراسة إلى أن التحقيق في الجرائم الإلكترونية لا يمكن أن يحقق غاياته بالاعتماد على الوسائل التقليدية وحدها، بل يتطلب تأهيلًا فنيًا متخصصًا للمحققين، وتعاونًا فعالًا مع الخبراء، وتحديثًا مستمرًا للتشريعات والإمكانات التقنية. كما خلصت إلى أن سلامة الدليل الرقمي ترتبط ارتباطًا وثيقًا بمدى الالتزام بالإجراءات الفنية والقانونية منذ لحظة ضبطه وحتى عرضه أمام القضاء. وتوصي الدراسة بضرورة تدريب الكوادر التحقيقية، وتطوير البنية التقنية للأجهزة المختصة، واعتماد آليات حديثة لحفظ الأدلة الرقمية بما يعزز فاعلية العدالة الجنائية في مواجهة الجرائم الإلكترونية.

**الكلمات المفتاحية:** الجرائم الإلكترونية، التحقيق الابتدائي، الدليل الرقمي، التفتيش الإلكتروني، الضبط الإلكتروني، الخبرة الفنية، الإجراءات الجزائية.

RESEARCH TITLE

# Means and Procedures of Preliminary Investigation in Cybercrimes


## Abstract

This study examines the means and procedures of preliminary investigation in cybercrimes in light of the rapid development of information and communication technologies, which has produced new forms of criminal activity characterized by technical complexity and evidentiary difficulty. The study aims to identify the most important technological tools and technical skills required to enable investigative authorities to collect, analyze, and preserve digital evidence in a manner that ensures its integrity and legality. It also seeks to clarify the preliminary investigation procedures appropriate to the nature of cybercrimes, particularly interrogation, testimony, the use of technical expertise, search, and seizure. The study adopts the analytical method by presenting the technical tools and programs used in investigation and analyzing their role in detecting cybercrimes, while also examining the procedural framework under Iraqi and Lebanese legislation. The study concludes that investigations into cybercrimes cannot achieve their objectives by relying solely on traditional methods; rather, they require specialized technical training for investigators, effective cooperation with experts, and continuous updating of legislation and technological capabilities. It further concludes that the integrity of digital evidence is closely linked to adherence to technical and legal procedures from the moment of seizure until it is presented before the judiciary. The study recommends training investigative personnel, developing the technical infrastructure of competent authorities, and adopting modern mechanisms for preserving digital evidence in a manner that enhances the effectiveness of criminal justice in confronting cybercrimes.


**Key Words:** Cybercrimes, Preliminary Investigation, Digital Evidence, Electronic Search, Electronic Seizure, Technical Expertise, Criminal Procedures.

**المقدمة**

تُعد مرحلة التحقيق الابتدائي من الركائز الأساسية في سير الدعوى الجزائية لما تضطلع به من دور جوهري في كشف الحقيقة وجمع الأدلة تمهيدًا للتصرف في الدعوى وإحالتها إلى الجهات القضائية المختصة، ومع التطور المتسارع في مجال تكنولوجيا المعلومات والاتصالات وظهور الجرائم الإلكترونية بوصفها نمطًا إجراميًا مستحدثًا، برزت تحديات نوعية أمام سلطات التحقيق تستلزم اعتماد وسائل فنية متقدمة ومهارات متخصصة تتجاوز الإطار التقليدي للتحقيق الجنائي، ومن ثم فإن فاعلية التحقيق في هذا المجال ترتبط بمدى كفاءة الأدوات المستخدمة وخبرة القائمين عليه في التعامل مع الأدلة الرقمية، الأمر الذي يقتضي بيان الوسائل والمهارات الفنية اللازمة للتحقيق الابتدائي، فضلًا عن توضيح إجراءاته وذلك من خلال تناول الجوانب الفنية من جهة والإجراءات القانونية من جهة أخرى.

**أولًا: أهمية البحث:**

تتمثل أهمية هذا الموضوع في كونه يتناول جانبًا حيويًا من جوانب التحقيق الابتدائي في الجرائم الإلكترونية، يتمثل في الوسائل التقنية والمهارات الفنية التي يعتمد عليها المحقق في جميع الادلة الرقمية وتحليلها، إذ إن خصوصية هذا النوع من الجرائم وطبيعته غير المادية تفرض على السلطات التحقيقية الاعتماد على أدوات وبرامج متقدمة إلى جانب امتلاك مهارات تقنية متخصصة، بما يسهم في كشف الحقيقة وضمان مشروعية الإجراءات وسلامة الدليل الرقمي، الأمر الذي يعزز من فعالية العدالة الجنائية في مواجهة هذا النمط المستحدث من الإجرام.

**ثانيًا: إشكالية البحث:**

تتمحور إشكالية هذا الموضوع حول مدى كفاية الوسائل الفنية والمهارات التقنية المتوافرة لدى الجهات التحقيقية لمواجهة تعقيدات الجرائم الالكترونية، ومدى قدرتها على التعامل مع الأدلة الرقمية بكفاءة تضمن كشف الجريمة ونسبتها إلى مرتكبها، في ظل التطور التكنلوجي المتسارع وتنامي أساليب ارتكاب هذا النوع من الجرائم.

**ثالثًا: منهجية البحث:**

يعتمد هذا الموضوع على المنهج التحليلي من خلال عرض الوسائل والبرامج التقنية المستخدمة في التحقيق في الجرائم الالكترونية وتحليل دورها في جمع الأدلة، إلى جانب بيان المهارات الفنية الواجب توافرها لدى المحقق، مع الاستناد إلى النصوص القانونية ولآراء الفقهية ذات الصلة.

**رابعًا: هيكلية البحث:**

ينقسم هذا الفرع إلى فقرتين متكاملتين تُعنى الأولى بيان الوسائل والمهارات الفنية اللازمة للتحقيق الابتدائي، التي تستعين بها السلطة المختصة في جمع الأدلة الرقمية وتحليلها، في حين تُخصص الثانية لعرض اجراءات التحقيق الابتدائي، بما يمكنه من التعامل مع طبيعة الجرائم الالكترونية بكفاءة وفعالية.

**ولغرض بيان وسائل وإجراءات التحقيق الابتدائي في الجرائم الإلكترونية، سيتم تقسيم هذه الدراسة على فرعين، يُعنى الفرع الأول ببيان الوسائل والمهارات الفنية اللازمة للتحقيق الابتدائي، في حين يُخصص الفرع الثاني لعرض إجراءات التحقيق الابتدائي، وذلك على النحو الآتي:**

**الفرع الاول**

**الوسائل والمهارات الفنية اللازمة للتحقيق الابتدائي**

عند شروع السلطة المختصة في إجراء التحقيق في جريمة معينة فإنها تكون مقيدة بوجوب الالتزام بأحكام القوانين والتشريعات النافذة وبالقواعد الفنية التي تكفل سلامة ومشروعية الإجراءات، وحيث إن الجرائم الإلكترونية تتسم بخصوصية تميزها عن الجرائم التقليدية، فإن التحقيق فيها يقتضي إلمامًا وافياً بوسائل ارتكابها بما يساعد على كشف حقيقتها والوصول إلى مرتكبيها، كما أن طبيعتها التقنية تفرض ضرورة توافر مهارات فنية متخصصة لدى الجهة القائمة بالتحقيق، وبناءً على ذلك سنعمد في هذا الفرع إلى بيان الوسائل والمهارات الفنية اللازمة للتحقيق في الجرائم الإلكترونية، وذلك من خلال فقرتين على النحو الآتي:

**فقرة أولى: وسائل التحقيق في الجرائم الالكترونية:**

تتوفر العديد من البرامج التي تؤدي دورًا مهمًا في مساعدة السلطة المختصة بالتحقيق على جمع الأدلة في الجرائم الإلكترونية بصورة أسرع وأكثر دقة، وتنقسم هذه البرامج إلى نوعين رئيسين، هما:

**أولاً: برامج خاصة بأمن الحاسوب والشبكات:** تتواجد هذه البرامج ضمن أجهزة الحواسيب والشبكات التي تُشكّل المسرح الافتراضي للجريمة قبل وقوعها وتهدف أساسًا إلى حماية الشبكات من أي اعتداء محتمل، من خلال مراقبة الأنشطة والعمليات الحاسوبية التي تجري بداخلها والاحتفاظ بسجلات خاصة بها، وتُمكّن هذه السجلات سلطات التحقيق من الحصول على معلومات مهمة قد تسهم في كشف غموض الجريمة والتوصل إلى مرتكبيها، ومن أبرز هذه البرامج ما يأتي:

1. **جدار الحماية (Firewall):** يعمل هذا البرنامج على حماية أجهزة الحاسوب والشبكات من خلال تنظيم وضبط الاتصالات الحاسوبية الصادرة منها والواردة إليها، وبعبارة أخرى يهدف إلى حماية جهاز الحاسوب أثناء اتصاله بشبكة الإنترنت من المخاطر المحتملة إذ يتولى "جدار الحماية" فحص كافة المعلومات والبيانات الواردة من الإنترنت أو من أي شبكة أخرى[1]، قد يُركَّب برنامج جدار الحماية على الحاسوب المراد حمايته أو على أجهزة إلكترونية مستقلة تُربط بالشبكة بحيث تمر جميع الاتصالات الحاسوبية عبرها وتُطبَّق شروط محددة على حزم البيانات لتحديد ما يُسمح بانتقاله بين طرفي الجدار، وتتولى هذه البرامج توثيق الاتصالات الصادرة والواردة بإنشاء سجلات تبيّن مصدر ووجهة كل اتصال وتُحفظ هذه السجلات في ملفات إلكترونية قابلة للمراجعة في أي وقت، وعند إعداد برنامج جدار الحماية بصورة صحيحة يكون قادرًا على تزويد سلطة التحقيق ببيانات مهمة تمكّنها من تحديد مصدر الاتصال الإلكتروني المرتبط بالجريمة محل التحقيق مما يسهم في تضييق دائرة الاتهام[2].

2. **البروكسي (Proxy Server):** وهو برنامج خاص يوفّر الاتصال عبر بروتوكول الإنترنت بين الشبكة الداخلية المحمية والعالم الخارجي أي شبكة الإنترنت، ويتولى مراقبة جميع الاتصالات الواردة إلى الشبكة والصادرة منها والتحكم في حجب بعضها وفقًا للإعدادات المسبقة من قبل مدير الشبكة، ويتلقى مزوّد البروكسي عبر الإنترنت طلبًا من المستخدم

---

[1] زياد محمد عبود و غسان حميد عبد المجيد واخرون، اساسيات الحاسوب وتطبيقاته المكتبية، ج1، الدار الجامعية للطباعة والنشر والتأليف والترجمة، وزارة التعليم العالي والبحث العلمي العراقية، بغداد، 2014، ص95.

[2] محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، (دراسة مسحية على ضباط الشرطة في المنطقة الشرقية)، رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الامنية، الرياض، 2004، ص83.

للوصول إلى صفحة معينة ضمن ذاكرة محلية تُعرف بالذاكرة المخبأة أو ذاكرة التخزين المؤقت (Cache)[3]، يتحقق مزوّد البروكسي مما إذا كانت الصفحة المطلوبة قد تم تنزيلها سابقًا، فإن وُجدت يُعيدها إلى المستخدم دون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم تكن موجودة في ذاكرة التخزين المؤقت (Cache) فإنه يعمل بوصفه مزودًا زبونًا ويرسل الطلب إلى الشبكة العالمية باستخدام أحد عناوين (IP)، وتكمن أهم مزايا مزوّد البروكسي في أن ذاكرة التخزين المؤقت لديه تحتفظ بالعمليات التي تمت عبره الأمر الذي يجعل لها دورًا مهمًا في الإثبات من خلال فحص تلك العمليات المحفوظة والمتعلقة بالمتهم والمودعة لدى مزود الخدمة، إذ قد يعثر المحقق على أدلة جرى حذفها عمدًا مما يفيد التحقيق ويساعد في كشف الجريمة[4].

3. **نظام كشف الاختراق (Intrusion Detection System)**: ويُرمز لهذا النظام اختصارًا بـ (IDS)، وهو يمثل فئة من البرامج التي تتولى مراقبة بعض العمليات ورصدها[5]، تعمل هذه البرامج على مراقبة العمليات التي تجري في الحاسوب أو الشبكة وتحليلها بحثًا عن مؤشرات تدل على وجود تهديد قد يمس أمنهما وذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومتابعة بعض ملفات نظام التشغيل المخصّصة لتسجيل الأحداث فور وقوعها، وتُقارن نتائج هذا التحليل بمجموعة من السمات المشتركة للاعتداءات على الأنظمة الحاسوبية فإذا اكتشف النظام وجود إحدى هذه السمات، يُرسل إنذارًا فوريًا إلى مدير النظام بطرق متعددة ويسجل البيانات المتعلقة بالاعتداء في سجلات إلكترونية خاصة، وتُعد هذه السجلات ذات قيمة مهمة لسلطة التحقيق إذ يمكن أن تسهم في التعرف على أسلوب ارتكاب الجريمة ووسائلها ومصادرها[6].

4. **نظام جرة العسل Honeypot**: هو نظام حاسوبي يُصمَّم خصيصًا لصدّ واعتراض الهجمات عبر الشبكة، ويعتمد على خداع المهاجم وإيهامه بسهولة اختراقه بغية إغرائه بمهاجمته ومن ثم منعه من الاعتداء على أي حاسوب آخر ضمن الشبكة، وفي الوقت ذاته يعمل النظام على جمع أكبر قدر ممكن من المعلومات المتعلقة بالأساليب التي يعتمدها المهاجم في محاولاته وتحليلها واتخاذ الإجراءات الوقائية الملائمة، وتُعد هذه المعلومات ذات أهمية في تحليل أبعاد الجريمة عند وقوعها، إذ تزوّد سلطة التحقيق ببيانات تسهم في توضيح معالمها[7].

**ثانياً: برامج خاصة مساعدة للتحقيق في الجرائم الالكترونية:** نظرًا لكون مرتكبي هذا النوع من الجرائم المستحدثة يتمتعون بقدرات ومهارات فنية متقدمة فإنهم غالبًا ما يحرصون على عدم ترك أي دليل يدينهم، إذ قد يلجأ مرتكب الجريمة

---

[3] تستعمل هذه الذاكرة لحفظ البيانات بشكل يسمح باسترجاعها بشكل أسرع في الطلبات اللاحقة، وقد تكون هذه البيانات نسخًا من بيانات أصلية مخزنة في مكان آخر، أو قيم تم حسابها مسبقا، فإذا كانت البيانات المطلوبة موجودة في الذاكرة المخبأة فإنه يمكّن الاستجابة للطلب بقراءة البيانات من الذاكرة المخبأة، والتي تكون القراءة منها أسرع بالمقارنة مع محاولة قراءتها من مخزنها الأصلي أو إعادة حسابها. ينظر: مقال بعنوان ذاكرة مخبئية منشور على شبكة المعلومات الدولية (الانترنت)، الموقع الالكتروني: ويكيبيديا الموسوعة الحرة، الرابط الالكتروني: https://ar.wikipedia.org، تاريخ الزيارة 2025/7/29.

[4] ممدوح عبد الحميد عبد المطلب، جرائم الكمبيوتر وشبكة المعلومات العالمية، مكتبة الحقوق، الشارقة، 2001، ص219.

[5] ومن الأمثلة على تلك البرامج، برنامج Hack Tracer v12 وهو مصمم للعمل في الأجهزة المكتبية Web وساكناً في خلفية سطح المكتب، وعندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسب الآلي يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ في عملية مطاردة تستهدف اقتفاء اثر مرتكب عملية الاختراق حتى يصل إلى الجهاز الذي حدثت العملية من خلاله، وقد تمت إجراء تجربة عملية على البرنامج محليا، وتم التأكد من أنه برنامج فعال، وذكر صاحب التجربة، أنه خلال اختبار البرنامج تعرض جهازه، لأكثر من (١٧) محاولة اختراق في فترة قصيرة، وبعد اقتفاء الأثر قاد البرنامج صاحب التجربة إلى أفراد من مدن. للمزيد ينظر: سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، اكاديمية نايف العربية للعلوم الامنية، الرياض، 2003، ص100.

[6] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد الرابع، كلية الحقوق والعلوم السياسية، جامعة البليدة، الجزائر، 2018، ص55.

[7] حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، (دراسة مقارنة)، اطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 2009، ص401.

الإلكترونية إلى تشفير البرامج أو تغيير كلمات المرور أو إخفاء المعلومات أو التلاعب بها أو إتلاف أدوات الحفظ الخارجية أو تدمير البيانات باستخدام أدوات الجريمة كالفيروسات وغيرها، وبناءً على ذلك فإن المحقق يحتاج إلى الاستعانة بأدوات وبرامج مساعدة، كبرامج استرجاع المعلومات من الأقراص التالفة مثل (View Disk) وبرامج كسر كلمات المرور وبرامج الضغط وفك الضغط (Pkzip)، وبرامج البحث عن الملفات العادية والمخفية مثل ( Xtreepro Gold)، فضلًا عن برامج تشغيل الحاسوب مثل (Bootable Diskette) وبرامج نسخ البيانات مثل (Lap Link)[8]، وقد يعمد الجاني إلى حذف الملفات من الحاسب الآلي بصورة نهائية غير أنّه يمكن استرجاعها باستخدام برامج مخصصة لذلك ومن أبرزها برنامج (Windows For Rescue File) وبرنامج (Research Regnerud)، كما أن المحقق يحتاج أيضًا إلى استخدام برامج منع الكتابة على القرص الصلب عقب ارتكاب الجريمة وذلك حفاظًا على مسرح الجريمة وحماية الأدلة الإلكترونية من العبث أو الضياع[9].

كما توجد برامج تحرير الملفات الست عشري (Hexadecimal Editors) وهي برامج تتيح للمحقق الاطلاع على محتوى أي ملف حاسوبي بصيغته الثنائية، بما يمنحه قدرة أكبر على تحليل الملف والتعرف على طبيعة البيانات التي يتضمنها لاسيما وأن بعض الأنظمة قد تعجز عن تحديد الفئة التي ينتمي إليها الملف، وهناك أيضًا برامج البحث عن المفردات النصية التي تُستخدم للبحث داخل البيانات عن ملفات تتضمن كلمات محددة غالبًا ما تكون مرتبطة بالقضية فضلًا عن برامج استعراض الصور التي تُستخدم لعرض الصور الرقمية على شاشة الحاسوب، مما يساعد المحقق في مشاهدة واستعراض الصور المخزنة داخل أجهزة الحاسوب أو وسائط التخزين الخارجية وتبرز أهمية هذه البرامج على نحو خاص في جرائم الإباحة[10].

**فقرة ثانية: المهارات الفنية للتحقيق في الجرائم الالكترونية:**

إنَّ ظهور الجرائم الإلكترونية الناجمة عن التطور التكنولوجي قد ألقى بأعباء جديدة على الأجهزة المختصة بالتحقيق، ذلك أن التصدي لهذه الجرائم يتطلب قدرات فنية لم تألفها تلك الأجهزة من قبل، وهو ما يستلزم توفير الإمكانات والمهارات اللازمة في هذا المجال بما يختلف عن المهارات التقليدية التي يفترض توافرها لدى القائم بالتحقيق، مثل التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها والتي تُعد من أساسيات العمل التحقيقي، غير أنّه في إطار الجرائم الإلكترونية يتعين على المحقق امتلاك جملة من المهارات الفنية المستحدثة التي تمكّنه من أداء عمله على نحو أمثل، وعليه فإن التركيز سينصرف إلى تلك المهارات الفنية التي تُعد إفرازًا للتطور الإنساني في مجال الاتصالات والحوسبة وتشكل عنصرًا مستجدًا في تعامل المحقق مع هذا النمط من الجرائم، ومن أبرز هذه المهارات ما يلي:

**أولاً: التعرف على المكونات المادية للحاسب الآلي والتعامل المبدئي معها:** إذ يتعين على المحقق الإلمام بالشكل المميز لأجهزة الحاسوب وملحقاتها ومعرفة مسمى كل منها والغرض من استخدامها فضلًا عن احتمالات توظيفها في ارتكاب الجرائم الإلكترونية، ذلك أن جهله بها قد يؤدي إلى إهمالها أو حتى إتلافها دون قصد أو التسبب في تعديل البيانات المخزنة عليها نتيجة سوء التعامل معها[11].

**ثانياً: معرفة أساسيات عمل شبكات الحاسب الآلي وأهم مصطلحاتها:** وبما أن الجرائم الإلكترونية تُرتكب عبر شبكة

---

[8] حسن طاهر داود، جرائم نظم المعلومات، ط1، مركز الدراسات والبحوث، اكاديمية نايف العربية للعلوم الامنية، الرياض، 2000، ص228-229.

[9] سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، اكاديمية نايف العربية للعلوم الامنية، الرياض، 2003، ص102.

[10] محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، (دراسة مسحية على ضباط الشرطة في المنطقة الشرقية)، رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الامنية، الرياض، 2004، ص85 وما بعدها.

[11] جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002، ص115.

الاتصالات الدولية (الإنترنت)، فإن المحقق يكون بحاجة إلى الإلمام بمبادئ الاتصال الشبكي وأنواعه المختلفة وكيفية انتقال البيانات من جهاز إلى آخر على شكل حزم فضلًا عن معرفة المبادئ الأساسية للبروتوكولات الرئيسة الخاصة بالاتصال بالشبكة، وتكمن أهمية إلمام المحقق بهذه المبادئ في كونها ضرورية لتصوّر كيفية ارتكاب الفعل الإجرامي في الفضاء السيبراني، سواء تعلق الأمر باختراق الشبكات والحواسيب أو اعتراض حزم البيانات أثناء انتقالها عبر الشبكة أو التجسس عليها وتحويل مسارها، كما أنها تمكّنه من تكوين تصور واضح حول مدى إمكانية تتبع مصدر الاعتداء على الشبكة والمعوقات الفنية التي قد تحول دون ذلك[12].

**ثالثاً: التعرف على الصيغ المختلفة للملفات وتطبيقات الحاسوب الرئيسية التي يتعامل معها:** تُعدّ الملفات الوعاء الحقيقي لأدلة الإدانة في العديد من القضايا المرتبطة بالجرائم الإلكترونية نظرًا لما تتضمنه من بيانات، ومن ثم فإن تمكّن المحقق من الإلمام بصيغ هذه الملفات وما قد تحتويه ومعرفته بأهم التطبيقات التي تتيح له قراءة محتواها أو سماعه أو مشاهدته يُعد أمرًا على قدرٍ كبيرٍ من الأهمية[13].

**رابعاً: تمييز أنظمة تشغيل الحاسوب المختلفة:** يتعيّن على المحقق أن يمتلك على الأقل فهمًا مبدئيًا لأنواع أنظمة تشغيل الحاسب الآلي وما تتميز به من خصائص، فضلًا عن الإلمام بأساسيات أنظمة الملفات التي تستند إليها إذ إن إلمامه بهذه الأنظمة يُعد أمرًا ضروريًا لتمكينه من المشاركة في متابعة وفحص وتفتيش مسرح الجريمة، كما قد يجد المحقق نفسه في بعض الأحيان أمام قرارات فنية معقدة تستلزم التشاور مع الخبير غير أن افتقاده للحد الأدنى من المعرفة التقنية قد يجعل القرار النهائي بيد الخبير وحده[14].

**خامساً: إجادة التعامل مع خدمات الإنترنت الرئيسية:** تُعد شبكة الإنترنت أداة فعّالة لجمع المعلومات وإجراء التحريات بالنسبة للمحقق إذ أوجدت مجتمعًا افتراضيًا يشبه إلى حد كبير المجتمعات الواقعية ويدور في إطاره كثير من النقاشات التي قد تسهم في كشف غموض بعض الجرائم، كما يمكن أن تُستخدم الإنترنت كوسيلة تعليمية للاطلاع على أحدث مستجدات الجرائم الإلكترونية وسبل التصدي لها فضلاً عن كونها وسيلة اتصال وتبادل للمعلومات بين رجال إنفاذ القانون[15].

**سادساً: معرفة الادوات والأساليب المستخدمة في ارتكاب الجرائم الالكترونية:** إن إلمام السلطات التحقيقية بهذه الأساليب وكيفية استخدام الأدوات المرتبطة بها يُعد أمرًا ضروريًا، ولا سيما بالنسبة للقائمين على مناقشة الشهود واستجواب المتهمين إذ إن غياب هذه المعرفة يحول دون طرح الأسئلة المتصلة مباشرة بالفعل الإجرامي وبالأسلوب الذي ارتُكب به، كما أن إدراك المحقق لتلك الأدوات يُمكّنه من استيعاب تقارير الخبراء الفنيين المتعلقة بأجهزة الحاسوب الأمر الذي يساعده على تحديد الأساليب المستخدمة في ارتكاب الجريمة[16].

ومن وجهة نظرنا فإن مكافحة الجرائم الإلكترونية والكشف عنها وملاحقة مرتكبيها يتطلب تأهيلاً فنياً وعلمياً خاصاً يجب أن يتوافر لدى كل من يتصل عمله بهذه الجرائم بدءاً من مرحلة الاستقصاء وجمع الاستدلالات مروراً بمرحلة

---

[12] حسين بن سعيد بن الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص395.

[13] محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، مرجع سابق، ص97.

[14] عبدالله بن حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، رسالة ماجستير، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الامنية، الرياض، 2014، ص61.

[15] حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص396.

[16] محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، مرجع سابق، ص99.

التحقيق الابتدائي وانتهاءً بمرحلة المحاكمة، وبناءً عليه يقتضي الأمر تدريب السلطات التحقيقية ذات الصلة بالجرائم الإلكترونية على تشغيل الحاسبات الآلية والتعرّف على أنواعها وأنظمتها المختلفة وملحقاتها بما يتيح لهم اكتساب المهارات والمعارف المرتبطة ببرمجة الحاسبات والمعالجة الإلكترونية للبيانات والجرائم الواقعة على أجهزة الحاسوب والأنظمة الإلكترونية وأساليب ارتكاب هذا النوع من الإجرام المستحدث فضلاً عن أمن الحاسبات ووسائل اختراقها، كما يستلزم ذلك دراسة حالات تطبيقية لجرائم إلكترونية ارتُكبت وكيف جرى التصدي لها للاستفادة من الخبرات السابقة بما يضمن مواجهة هذه الجرائم ذات الطبيعة المغايرة للجرائم التقليدية، ويُضاف إلى ذلك ضرورة إعادة النظر في وسائل وأساليب المكافحة التقليدية وطرق الوقاية منها ووضع خطط وبرامج استراتيجية لتحديث أجهزة العدالة الجنائية وتطويرها من حيث بنيتها المؤسسية وكوادرها البشرية بما يجعلها قادرة تقنياً على التصدي لهذا النوع من الجرائم وضبط مرتكبيها وتقديمهم للعدالة.

**الفرع الثاني**

**إجراءات التحقيق الابتدائي**

يتميّز التحقيق الابتدائي في الجرائم الإلكترونية بخصائص خاصة تفرّقه عن التحقيق الابتدائي في الجرائم التقليدية وذلك بالنظر إلى طبيعة هذه الجرائم من جهة، وصفات المجرم الإلكتروني من جهة أخرى، الأمر الذي يقتضي توافر مؤهلات خاصة لدى الجهة القائمة بالتحقيق فيها، كما أن التحقيق في هذا النوع من الجرائم يستلزم إجراءات مغايرة لتلك المتبعة في الجرائم التقليدية تستهدف جمع الأدلة الرقمية وفحصها بما يثبت وقوع الجريمة ونسبتها إلى مرتكبها، وتنقسم هذه الإجراءات بحسب غايتها إلى نوعين، أولهما الإجراءات الاحتياطية ضد المتهم، كأوامر القبض والإحضار وأوامر الحبس الاحتياطي وهي تهدف إلى صون الأدلة المتحصلة من أي مؤثر قد يضعف قيمتها الإثباتية أو يؤدي إلى زوالها[17]، وعليه يمكن تطبيقه في التحقيق بالجرائم الإلكترونية وفقًا للقواعد العامة من دون أن يثير أية صعوبات، لكونه لا يتطلب مهارة خاصة أو دراية تقنية بنظم المعلومات.

ما النوع الثاني فيتجسّد في إجراءات جمع الأدلة وفحصها مثل الاستجواب والشهادة والتي تُعرف أيضًا بـ(إجراءات جمع الأدلة القولية)، فضلاً عن الاستعانة بالخبراء والتفتيش والضبط والتي تُعرف بـ(إجراءات جمع الأدلة المادية والفنية)، ويُعد هذا النوع من أهم إجراءات التحقيق في جميع الجرائم إذ يمثل مصدرًا للمعلومات وأداة للوصول إلى الأدلة وضمان شروط صحتها بالإضافة إلى تعزيز قوتها الإثباتية أمام محاكم الموضوع المختصة، وتجدر الإشارة إلى أن تطبيق هذه الإجراءات في التحقيق بالجرائم الإلكترونية المستحدثة يواجه صعوبات عديدة نظرًا لما يستلزم من مهارات تقنية عالية للتعامل مع الأدلة الرقمية في البيئة الافتراضية[18]، وعليه ستكون دراستنا في هذا الفرع مقتصرة على النوع الثاني دون الأول، وهو ما سنعمل على توضيحه في الفقرات الآتية:

**فقرة أولى: استجواب المتهم في الجرائم الالكترونية:**

يقصد بالاستجواب "المناقشة التفصيلية للمتهم في الدلائل والادلة القائمة على نسبة التهمة اليه"[19]، ويُعد بذلك إجراءً من إجراءات التحقيق القولية يتم من خلاله مناقشة المتهم بالتهمة المنسوبة إليه ومواجهته بالأدلة القائمة ضده

[17] محمد عيد الغريب، مبادئ الاجراءات الجنائية، بلا دار نشر، 2004، ص373.

[18] سعيد عبداللطيف حسن، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنت (الجرائم الواقعة في مجال تكنولوجيا المعلومات)، ط1، دار النهضة العربية، القاهرة، 1999، ص134.

[19] محمود محمود مصطفى، شرح قانون الاجراءات الجنائية، ط12، دار النهضة العربية، القاهرة، 1983، ص300.

لتفنيدها أو الإقرار بها، مما يضفي عليه طبيعة مزدوجة إذ يُعد وسيلة للاتهام والدفاع في الوقت ذاته[20]، وقد خصَّ المشرّع إجراء الاستجواب بالنيابة العامة أو بقاضي التحقيق ويجوز أن يقوم به مأمور الضبط القضائي في حالات استثنائية، وبذلك يختلف الاستجواب عن سؤال المتهم، فإذا كان الاستجواب يعد من إجراءات التحقيق الابتدائي التي لا يجوز مباشرتها إلا من قبل القضاة أو المحققين وبصورة تحريرية، فإن سؤال المتهم يقصد به مطالبته بالرد على الاتهام الموجه إليه وهو من إجراءات جمع الأدلة التي يجوز لجميع موظفي الضبط مباشرتها شفاهة[21].

ونظرًا لأهمية وخطورة الاستجواب بوصفه إجراءً يتسم بطبيعة مزدوجة كونه وسيلة اتهام ودفاع في آن واحد فقد نظم المشرّع اللبناني أحكامه في المواد (74–84) من قانون أصول المحاكمات الجزائية في حين نظمها المشرّع العراقي في المواد (123–129) من القانون ذاته، وقد أحاط كلا المشرّعين هذا الإجراء بجملة من الضمانات التي تستهدف تأمين أفضل النتائج منه، من أبرزها التحقق من شخصية المتهم وإحاطته علمًا بالتهمة المسندة إليه وتدوين أقواله أثناء الاستجواب مع إثبات ما يقدمه من أدلة لنفي التهمة فضلاً عن تمكينه من الامتناع عن الإجابة على أسئلة المحقق باعتبار أنه غير ملزم بتقديم إفادته، كما حظر المشرّع استعمال أي وسيلة من وسائل الإكراه ضده ومنع تحليفه اليمين إلا إذا كان يشهد على غيره من المتهمين إضافةً إلى حظر فصله عن محاميه الحاضر معه أثناء التحقيق، وعدم جواز استجوابه خارج مقر جهة التحقيق أو بغير حضور محاميه إلا في حالة الضرورة التي يقدّرها المحقق، كما في حالة التلبس حيث تقتضي المصلحة ذلك خشية ضياع الأدلة[22].

ومن الجدير بالذكر أن المشرّع اللبناني قد أسند صلاحية إجراء الاستجواب إلى قاضي التحقيق[23]، غير أنّه يجوز للنائب العام والضابط العدلي في لبنان مباشرة الاستجواب في حالة الجرائم المشهودة حصراً، وذلك وفقًا لظروف استثنائية محددة وبشروط يتعيّن التقيد بها[24]، أما المشرّع العراقي فقد أناط مهمة استجواب المتهم بقاضي التحقيق أو بالمحقق حصراً[25]، أما بالنسبة لضابط التحقيق في مراكز ومديريات الشرطة، فعلى الرغم من تمتعه بصلاحية الاستجواب في الحالات التي خُوِّل فيها سلطة المحقق بموجب المادة (50/ب) من قانون أصول المحاكمات الجزائية إلا أن هذه الصلاحية تبقى استثناءً[26]، إذ لا يجوز له مباشرة إجراءات التحقيق ولا سيما الاستجواب، إلا بناءً على تكليف مباشر من القاضي أو في الحالات التي يترتب على إحالة الشخص المبلغ عنه إلى القاضي تأخير في الإجراءات التحقيقية بما قد يؤدي إلى طمس معالم الجريمة أو تمكين المشتبه فيه من الهروب أو الإضرار بسير التحقيق، وفي كلتا الحالتين يلتزم ضابط الشرطة بإعلام القاضي أو المحقق بالإجراءات المتخذة وتسليمه الأوراق التحقيقية فور الانتهاء منها[27].

---

[20] عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، ط1، منشورات الحلبي الحقوقية، بيروت، 2015، ص293.

[21] جلال حماد عرميط الدليمي، ضَمَانات المتهم في إجراءات التحقيق الابتدائي المقيدة لحريته والماسة بشخصه (دراسة مقارنة)، ط1، منشورات الحلبي الحقوقية، بيروت، 2015، ص126.

[22] للمزيد ينظر: المواد (74–84) من قانون اصول المحاكمات الجزائية اللبناني رقم (328) لسنة 2001 المعدل. وكذلك المواد (123–129) من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل.

[23] المواد (56 و60) من قانون اصول المحاكمات الجزائية اللبناني.

[24] المادتين (32 و 41) من قانون اصول المحاكمات الجزائية اللبناني.

[25] المادة (123) من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل.

[26] نصت المادة (50/ ب) من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل، على أن ((يكون للمسؤول في مركز الشرطة في الاحوال المبينة في هذه المادة والمادة 49 سلطة محقق)).

[27] المادة (50/أ) من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل.

**فقرة ثانية: الشهادة في الجرائم الالكترونية:**

تُعد الشهادة من إجراءات التحقيق القولية وهي تتمثل في المعلومات المتعلقة بالجريمة وظروف ارتكابها التي يدلي بها الشاهد أمام سلطات التحقيق، ويُقصد بها على وجه العموم "إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه بطريقة مباشرة أو غير مباشرة"[28]، وتنقسم الشهادة في جرائم الإلكترونية شأنها شأن الشهادة في الجرائم التقليدية إلى شهادة مباشرة وأخرى غير مباشرة[29]، وبذلك فإن الشهادة في الجرائم الإلكترونية لا تختلف في ماهيتها عن الشهادة في الجرائم التقليدية، إذ تقضي القاعدة العامة بأن يلتزم الشاهد بالإفصاح عمّا وصل إلى علمه من معلومات ووقائع تتعلق بالجريمة المرتكبة في أي مرحلة من مراحلها والإدلاء بكل ما من شأنه أن يسهم في كشف الحقيقة[30].

أما الشاهد في الجرائم الإلكترونية فيُقصد به الخبير الفني المتخصص في تقنيات الحاسوب الآلي والشبكات، والذي يمتلك معلومات جوهرية أو ضرورية تُمكِّن من النفاذ إلى نظام المعالجة الآلية للبيانات متى اقتضت مصلحة التحقيق ذلك ويُطلق على هذا النوع من الشهود مصطلح (الشاهد الإلكتروني) تمييزًا له عن الشاهد التقليدي، ويشمل هذا المصطلح عدة فئات من أبرزها، القائم على تشغيل الحاسوب الآلي وهو المسؤول عن تشغيل الجهاز والمعدات المتصلة به ويتطلب أن تكون لديه خبرة واسعة في تشغيل الجهاز ومعرفة بقواعد كتابة البرامج، والمبرمجون وهم المتخصصون في كتابة أوامر البرامج وينقسمون إلى فئتين: كُتّاب برامج التطبيقات وكُتّاب برامج النظم، وكذلك المحللون وهم الذين يتولون دراسة نظام معين من خلال تقسيمه إلى وحدات، وتجميع بياناته وتحليلها وتتبع تدفق البيانات داخله باستخدام مخططات تدفق البيانات وصولاً إلى استنتاج المواقع بواسطة الحاسوب الآلي، فضلاً عن مهندسي الصيانة والاتصالات المسؤولين عن أعمال الصيانة المرتبطة بتقنيات الحاسوب ومكوناته وشبكاته[31].

أما بشأن قيمة الشهادة ودورها في إثبات الجريمة الإلكترونية فإنها تخضع لمبدأ "الاقتناع الذاتي للقاضي الجزائي"، إذ يتمتع القاضي سواء أكان محققاً أم حاكماً بسلطة تقديرية في تقييم الشهادة ووزنها، فله أن يأخذ بها أو يستبعدها وله أن يبني قناعته على شهادة شاهد واحد أو أكثر وأن يرجّح شهادة على أخرى، وهو غير ملزم ببيان أسباب تكوين قناعته ولا يخضع في تقديره للشهادة لرقابة مرجع أعلى ما دام استخلاصه للأدلة سائغاً ومقبولاً عقلاً ومنطقاً[32].

وبالرجوع إلى موقف التشريعين اللبناني والعراقي بشأن الشهادة في جرائم الإلكترونية نجد أن المشرّع اللبناني لم يرد في قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم (81) لسنة 2018 نصّ صريح يجيز لسلطة التحقيق الاستماع للشهود، باستثناء المادة (124) التي اشتملت على إشارة غير مباشرة إلى هذا الإجراء التحقيقي، إذ

---

[28] حسن جوخدار، شرح قانون اصول المحاكمات الجزائية الاردني، ج1، دار الثقافة للنشر والتوزيع، عمان، 1993، ص316.

[29] يقصد بالشهادة المباشرة هي المعلومات التي يدلي بها الشخص، والتي وصلت إلى حواسه من خلال مباشر ودون وساطة شخص كأن يكون هذا الشاهد قد رأى أو سمع أو شم.... الخ، أي أن يقوم الشاهد بالإدلاء بما شاهده من قيام مرتكب الجريمة بأية ترتيبات برمجية تتعلق بمرتكب الجريمة، أو من خلال ما شاهده من قيام مرتكب الجريمة بعملية الاختراق لأي ملفات الكترونية، أو القيام بأي من أنواع التزوير الالكتروني، أما الشهادة غير المباشرة فالشاهد هنا لم يرى الجريمة ترتكب أو لم يسمع الجاني يتهدد ويتوعد المجني عليه، ولكنه سمع من خلال شخص آخر وهي تفترض رواية الشاهد عن غيره، فهو لم يعاين الواقعة بنفسه، وإنما سمع غيره يذكر معلومات بشأن ارتكاب الجريمة الالكترونية. ينظر: احمد سعد محمد الحسيني، الجوانب الاجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية، مرجع سابق، ص210-211.

[30] سعود علي عبدالله اللوغاني، الدليل الالكتروني وحجيته في الإثبات الجنائي (دراسة مقارنة)، رسالة ماجستير، كلية القانون، جامعة الشارقة، الامارات، 2011، ص147.

[31] هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية (دراسة مقارنة)، ط2، دار النهضة العربية، القاهرة، 2008، ص 35.

[32] سمير عالية، الجرائم الالكترونية، في القانون الجديد (رقم2018/81) ط1، منشورات الحلبي الحقوقية، 2020، ص436.

نصّت على أن: "يمكن للمرجع القضائي أَن يطلب من اي شخص له معرفة بطرق عمل نظام معلوماتي او وسائل الحماية المطبقة عليه، أَن يزود المرجع المكلف بالتحقيق بالمعلومات المطلوبة من اجل الوصول إلى البيانات والبرامج المطلوبة، وله ايضاً، الطلب من اي شخص لديه بيانات او برامج قد تكون موضوع دليل معلوماتي اجراء نسخة عنها وحفظها لديه لحين ضبطها منه"، وقد أكّد المشرّع في المادة (3) من ذات القانون سالف الذكر على الرجوع إلى المبادئ العامة في كل ما لم ينص عليه هذا القانون، حيث نصّ على أن: "تطبق الاحكام المنصوص عليها في القوانين المرعية الاجراء في كل ما لم يرد وما لم ينص عليه هذا القانون، وفي كل ما لا يتعارض مع احكامه".

وبالعودة إلى موقف قانون أصول المحاكمات الجزائية اللبناني بشأن الشهادة، نجد أن المشرّع خصص المواد (85-97) للحديث عن الشهود وما يتعلق بالاستماع إليهم، ويستمع قاضي التحقيق بحضور كاتبه، إلى كل شاهد على حدة وذلك بهدف استبعاد تأثير شهادة أي شاهد آخر، ويتوجب على قاضي التحقيق سؤال الشاهد عن اسمه وشهرته واسم والديه وعمره ومهنته ومحل إقامته أو سكنه، وما إذا كان متزوجاً من أحد الفريقين أو خادماً لأحدهما أو من ذوي قرابته وعن درجة القرابة ومن ثم يحلفه باليمين الآتية: "اقسم بالله العظيم بأن اشهد بالحق كل الحق ولا شيء غير الحق"، ويُدوَّن ذلك في المحضر ويجوز للشاهد الإدلاء بإفادته شفاهة كما يمكنه الاستعانة بالمستندات لتأييدها[33].

أما بالنسبة لموقف المشرّع العراقي بشأن الشهادة في جرائم الإلكترونية، نجد أن مشروع قانون جرائم الإلكترونية لسنة 2011 نصّ على أن: "يتولى قاضي التحقيق او المحقق المباشرة في اجراءات الضبط وجمع الادلة او اي اجراء تحقيقي نص عليه قانون اصول المحاكمات الجزائية"[34]، ومن بين هذه الإجراءات سماع الشهود، إذ أكّد المشرّع العراقي في قانون أصول المحاكمات الجزائية على أن: "يشرع في التحقيق بتدوين افادة المشتكي او المخبر ثم شهادة المجني عليه وشهود الاثبات الاخرين ومن يطلب الخصوم سماع شهاداتهم، وكذلك شهادة من يتقدم من تلقاء نفسه للإدلاء بمعلوماته اذا كَانَت تفيد التحقيق وشهادة الاشخاص الذين يصل إلى علم القاضي او المحقق أَن لهم معلومات تتعلق بالحادث"[35].

**فقرة ثالثة: الاستعانة بالخبرة الفنية في الجرائم الالكترونية:**

تُعرف الخبرة، كإجراء من إجراءات التحقيق الابتدائي بأنها "تقدير مادي أو ذهني يبديه اصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها بمعلوماته الخاصة سواء كانت متعلقة بشخص المتهم ام بجسم الجريمة ام المواد المستعملة في ارتكابها ام آثارها"[36]، كما تُعرف بانها "الاستشارة الفنية التي يستعين بها القاضي او المحقق لمساعدته في تكوين عقيدته في المسائل التي يحتاج تقديرها إلى معرفة او دراية علمية خاصة لا تتوافر لدى السلطة التحقيقية"[37].

ويقوم بإجراء الخبرة شخص يُسمّى الخبير وفي سياق الجرائم الإلكترونية يُعرف بالخبير الإلكتروني وله دور مهم وكبير في كشف الأدلة المتعلقة بهذه الجرائم وتفنيدها، إذ تكاد الاستعانة بالخبراء تصبح ضرورة لا غنى عنها نظرًا للطابع الفني والتقني الذي تتميز به هذه الجرائم كما أنها تلعب دورًا بارزًا في إثبات الجريمة، فالاستعانة بالخبرة الفنية سواء في مرحلة التحقيق الأولي أو الابتدائي أو أمام المحكمة، تُعد من أقوى مظاهر الأدلة في هذه النوعية من الجرائم المستحدثة

---

[33] المادة (87) من قانون اصول المحاكمات الجزائية اللبناني رقم (328) لسنة 2001 المعدل.

[34] المادة (24/ثالثا) من مشروع قانون جرائم المعلوماتية العراقي لسنة 2011.

[35] المادة (58) من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل.

[36] سعيد حسب الله عبدالله، شرح قانون اصول المحاكمات الجزائية، دار الحكمة للطباعة والنشر، الموصل، 1990، ص 184.

[37] عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، مرجع سابق، ص184.

حتى أُطلق عليها عبارة (الإلكترونية الشرعية)، والتي تعني عملية البحث التي يقوم بها الخبير الإلكتروني للحصول على الدليل الرقمي بغية إعادة بناء مجريات القضية وتوضيحها للمحكمة، علمًا أن الخبراء لا يحلفون يمين الخبرة إلا إذا كانوا من خارج جدول الخبراء أما المدرجون في الجدول فيحلفون اليمين بعد قبولهم، وبالنسبة للتقرير المعد من قبل الخبير فهو يُعد من الأدلة العادية كالشهادة ولا يُلزم القاضي، إذ أن نظام الإثبات قائم على مبدأ القناعة الشخصية للقاضي الذي له تقدير القيمة العلمية للخبرة[38].

ومن أجل ذلك يلجأ الخبير إلى مجموعة من الوسائل التي تمكنه من تحديد الجاني وطريقة ارتكابه للجريمة وأهمها الوسائل المادية والإجرائية، فالمادية تتمثل في الأدوات الفنية التي يستخدمها الخبير لتنفيذ أساليب التحقيق وإجراءاته بما يُسهم في الكشف عن حقيقة الجرم المرتكب، أما الإجرائية فهي الآليات التي تُوظف لإعمال ثوابت التحقيق والتي تؤكد وقوع الجرم وتحدد مرتكبه[39]، ويتوجب أن تتوافر لدى الخبير الإمكانات والمعارف العلمية والعملية المتعلقة بالواقعة موضوع الخبرة، فالأمر لا يقتصر على مجرد امتلاك الخبير شهادة علمية وإنما يشترط تحقق الممارسة العملية كون الأخيرة تنمي الكفاءة والقدرة الفنية، علمًا أنه لا يوجد خبير إلكتروني يمتلك خبرة متكاملة في جميع برامج الحاسوب وشبكاته المتنوعة[40].

وفيما يتعلق بموقف المشرّعين اللبناني والعراقي من هذا الإجراء، يلاحظ أنّ المشرّع اللبناني قد أشار بصورة ضمنية إلى تمكين سلطة التحقيق في إحدى الجرائم الإلكترونية من الاستعانة بالخبراء للاستفادة من معارفهم في التقنيات الإلكترونية[41]، غير أنّه قد نصّ على الخبرة بصورة صريحة في قانون أصول المحاكمات الجزائية[42]، إذ ورد النص بصيغة مطلقة تتسع لتشمل هذا الصنف من الجرائم، لاسيما وأنّ المشرّع أجاز الاستعانة بالخبير لبيان بعض المسائل التقنية والفنية، وهي مسائل ترتبط ارتباطًا مباشرًا وتظهر بوضوح في الجرائم ذات الطابع التقني والفني العالي.

أما في العراق، فقد نصّ مشروع قانون جرائم الإلكترونية لسنة 2011 بصورة صريحة ومباشرة على تمكين القاضي، سواء في مرحلة التحقيق أم في مرحلة المحاكمة من الاستعانة بالخبراء العراقيين والأجانب بقصد الإفادة من خبراتهم في إنجاز مهام التحقيق والوصول إلى الأدلة، كما أكدت الفقرة (24/ثالثًا) من المشروع ذاته على أنّ لقاضي التحقيق والمحقق سلطة القيام بجميع الإجراءات المنصوص عليها في قانون أصول المحاكمات الجزائية، الذي تضمن بدوره النص على الاستعانة بالخبراء كأحد إجراءات التحقيق الابتدائي، وذلك بموجب نص عام يمتد نطاقه ليشمل مختلف صور الجرائم[43].

---

[38] سمير عالية، الجرائم الالكترونية، مرجع سابق، ص434.

[39] للمزيد بشأن الوسائل المادية والوسائل الإجرائية التي يستعين بها الخبير الالكتروني في اكتشاف الدليل الإلكتروني، ينظر: أحمد عاصم عجيلة، الحماية الجنائية للمحررات الالكترونية (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2014، ص444-446.

[40] طه السيد احمد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات واثرها على اجراءات التحقيق في النظام الجزائي المصري والسعودي، ط1، دار الكتب والدراسات العربية، الاسكندرية، 2016، ص121-122.

[41] المادة (124) من قانون المعاملات الالكترونية والبيانات ذات الطابع الشخصي اللبناني رقم (81) لسنة 2018، والتي جاء فيها ((يمكن للمرجع القضائي الطلب من اي شخص له معرفة بطرق عمل نظام معلوماتي او وسائل الحماية المطبقة عليه بأن يزود المرجع المكلف بالتحقيق بالمعلومات المطلوبة من اجل الوصول إلى البيانات والبرامج المطلوبة)).

[42] المادة (34) من قانون اصول المحاكمات الجزائية اللبناني رقم (328) لسنة 2001 المعدل، والتي نصت على أنه ((اذا استلزمت طبيعة الجريمة او آثارها الاستعانة بخبير او اكثر لجلاء بعض المسائل التقنية او الفنية فيعين النائب العام الخبير المختص ويحدد مهمته بدقة)).

[43] المادة (69/أ) من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل، والتي نصت على أنه ((يجوز للقاضي او المحقق من تلقاء نفسه او بناء على طلب احد الخصوم أن يندب خبيرًا او اكثر لإبداء الرأي في ما له صلة بالجريمة التي يجري التحقيق فيها)).

**فقرة رابعة: التفتيش في الجرائم الالكترونية:**

يُقصد بالتفتيش بوجه عام أنّه "عبارة عن إجراء من إجراءات التحقيق يهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة"[44]، أمّا تفتيش النظام الإلكتروني أو ما يُعرف بالولوج إلى داخل النظام الإلكتروني[45]، فيقصد به "الاطلاع على محل منحة القانون حماية خاصة باعتباره مستودع سر صاحبه ويستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الإنترنت"[46].

مما تقدّم يتبيّن أنّ التفتيش بوصفه إجراءً تحقيقيًا إنما يستهدف ضبط الأشياء المتصلة بالجريمة والتي تسهم في كشف الحقيقة وقد تُستمد منها أهم أدلة الجريمة، غير أنّ تحقيق هذا الهدف في نطاق الجرائم الإلكترونية من خلال الولوج إلى الأنظمة الإلكترونية والبحث في البرامج المستعملة والبيانات المخزنة في الأجهزة الحاسوبية وشبكات الإنترنت، يثير جملة من التساؤلات من أبرزها، هل يُعدّ الولوج إلى النظام الإلكتروني نوعًا من التفتيش؟ وهل يندرج ضمن نطاق التفتيش بمعناه القانوني التقليدي؟ وما مدى قابلية النظام الإلكتروني أو مكوّنات الحاسوب المادية والمعنوية وشبكات الإنترنت لأن تكون محلاً صالحًا للتفتيش؟ وهو ما سنحاول الإجابة عنه في فقرتين على النحو الآتي:

**اولاً: مدى اعتبار الولوج في النظام الالكتروني نوعًا من التفتيش:** اختلف الفقه الجنائي في الإجابة عن هذا التساؤل وانقسم إلى اتجاهين، أولهما يدعو إلى تعديل التشريعات الإجرائية النافذة وإضافة نصوص تكميلية تتلاءم مع متطلبات كشف الحقيقة في الجرائم الإلكترونية من خلال البحث والاستقصاء في البيئة الافتراضية، وبما يضمن أن يتم الحصول على البيانات الإلكترونية بطرق مشروعة، الأمر الذي يُمكّن من اعتبار الولوج إلى النظام الإلكتروني صورة من صور التفتيش[47]، في المقابل يتجه الرأي الثاني إلى التوسّع في تفسير القواعد العامة للتفتيش، بحيث يمتد نطاقها ليشمل الولوج إلى النظام الإلكتروني دون الحاجة إلى استحداث نصوص تشريعية جديدة[48].

وقد ذهب بعض الفقه إلى القول بأن هذا الرأي الأخير يخالف إحدى القواعد الراسخة في القانون الجزائي المتمثلة في عدم جواز القياس أو التوسّع في تفسير النصوص الجزائية[49]، غير أنّه يمكن الردّ على ذلك بأن القياس والتفسير الواسع محظور في النصوص الجزائية الموضوعية الإيجابية أي تلك التي تحدد الجرائم والعقوبات، أما في ما يخصّ النصوص الجزائية الموضوعية السلبية كالنصوص التي تحدد أسباب الإباحة وموانع المسؤولية والأعذار القانونية المخففة فإن القياس والتفسير الواسع جائز فيها، إذ أنّه في إطار هذه الحالات لا يؤدي قياس القاضي أو تفسيره الواسع للنص إلى الاعتداء على سلطة المشرّع في التجريم وفرض العقاب، بما أنّ ذلك يظل ضمن استصحاب الأصل العام في الأفعال أي

---

[44] محمود نجيب حسني، شرح قانون الاجراءات الجنائية، ط2، دار النهضة العربية، القاهرة، 1988، ص770.

[45] يعود استخدام هذا المصطلح إلى جهد العديد من المنظمات والمعاهدات الدولية المهتمة بمكافحة الجرائم الالكترونية، وذلك في إطار تطوير بعض المصطلحات القانونية المستخدمة في مجال التحقيق الجنائي في هذه الجرائم، وذلك باستحداث مصطلحات إلكترونية جديدة تتلاءم مع البيئة الالكترونية التي تستخدم فيها، مع الاحتفاظ بجذورها التقليدية، ومن المصطلحات التي لحقها التطوير (التفتيش)، واستخدام مصطلح (الولوج) بدلاً منه، وهو ما نصت عليه المادة 19 بفقرتيها الأولى والثانية من الاتفاقية الأوروبية بشأن الجريمة الإلكترونية. نقلًا عن: محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي، (دراسة مقارنة)، دار الجامعة الجديدة، الاسكندرية، 2018، ص271.

[46] علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت، ط1، مؤسسة فخراوي للدراسات والنشر، مملكة البحرين، 2010، ص20. و هلالي عبد اللاه احمد: اتفاقية بودابست لمكافحة جرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2007، ص242 وما بعدها.

[47] هشام محمد فريد رستم، الجوانب الاجرائية للجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 1998، ص66.

[48] نبيلة هبه هروال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، 2007، ص74.

[49] محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي، مرجع سابق، ص278.

الإباحة، ومن ثم لا يشكّل أي تجاوز أو اعتداء على مبدأ الشرعية الجزائية (لا جريمة ولا عقوبة إلا بنص).

وكذلك يجوز للقاضي القياس والتفسير الواسع للنصوص الجزائية الإجرائية، إذ أنّها قواعد شكلية لا تحدّد أحكامًا موضوعية تتعلق بالتجريم والعقاب، إلا أنّه ينبغي الإشارة إلى أنّ القياس والتفسير الواسع للنصوص الإجرائية لا يجوز إذا كان النص المراد تفسيره ينتقص من ضمانات المتهم، ذلك أنّ هذه النصوص استثنائية، والاستثناء لا يجوز القياس عليه أو تفسيره بشكل واسع، أما إذا كان النص الاستثنائي في صالح المتهم، فيجوز عندها القياس عليه والتوسّع في تفسيره.

ومن وجهة نظرنا فإن كلا الاتجاهين وعلى الرغم من اختلاف وجهات النظر بينهما يعبران عن الاعتراف بالولوج إلى النظام الإلكتروني واعتباره صورة من صور التفتيش، مع عدم التسليم بما انتهى إليه أيّ منهما، إذ نرى أنّ هناك ضرورة ملحة لجمع النصوص الجزائية الموضوعية والإجرائية الخاصة بمكافحة الجرائم الإلكترونية في وثيقة قانونية واحدة، يحدد فيها المشرّع الأفعال المجرمة وعقوبتها والإجراءات الواجب اتباعها بشأنها، نظرًا للطبيعة الخاصة التي تميّز هذه الجرائم عن غيرها من الجرائم التقليدية، وحرصًا على تفادي تشتت النصوص القانونية المتعلقة بمواجهة الجريمة الإلكترونية في قوانين متفرقة.

**ثانياً: مدى صلاحية النظام الالكتروني او مكونات أجهزة الحاسوب الآلية المادية والمعنوية وشبكات الحاسوب بأن تكون موضوعًا أو محلًا ممكنًا لتفتيشها:** إن التفتيش أو الولوج في البيئة الافتراضية قد يمتد إلى المكونات المادية للحاسب الآلي وملحقاته، والمتمثلة بوحدات الإدخال والإخراج ووحدة المعالجة والمنطق ووحدة التحكم والذاكرة الرئيسية، إضافة إلى البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية، وذلك وفق المكان أو الحيز الذي تتواجد فيه، وهذه المكونات تخضع بلا خلاف يُذكر للتفتيش والضبط طبقًا للقواعد العامة المنصوص عليها في القوانين الإجرائية[50]، فإذا وُجدت هذه المكونات في مسكن المتهم أو أحد ملحقاته فإنها تخضع للقواعد نفسها التي تحكم تفتيش المسكن، إذ يجوز تفتيشها وضبطها متى كان تفتيش المسكن جائزًا، أما إذا وُجدت في مكان عام فتنطبق عليها الأحكام المقررة لذلك المكان، وفي حال كانت المكونات في حوزة شخص خارج مسكنه فإن تفتيشها يخضع للقواعد نفسها التي تسري على تفتيش الشخص بوصفه أحد متعلقاته، سواء كان الحائز مالك الجهاز أم شخصًا آخر، مع ضرورة الالتزام بالشروط الموضوعية والشكلية للتفتيش[51].

كما أنّ التفتيش قد يمتد إلى المكونات المعنوية للحاسب الآلي، وقد ثار خلاف فقهي حول مدى جواز تفتيش هذه المكونات تمهيدًا لضبط الأدلة الرقمية المخزنة فيها، فقد ذهب بعض الفقه إلى أنّ محل تفتيش نظم الحاسب الآلي للبحث عن أدلة مرتبطة بجريمة إلكترونية يمكن أن يشمل المكونات المادية والمعنوية معًا، إضافة إلى شبكات الاتصال الخاصة به، سواء وُجدت في حوزة شخص أو وُضعت في مكان يحظى بحرمة المسكن[52].

بينما ذهب اتجاه آخر في الفقه إلى أنّ الغاية من التفتيش تنحصر في الحصول على أدلة إثبات مادية من شأنها أن تعين الجهات المختصة على كشف الحقيقة، وبالتالي فإن هذا المفهوم لا يمتد ليشمل الأدلة الرقمية ذات الطبيعة غير

---

[50] اسامة احمد المناعسة، جلال الزعبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والإنترنت (دراسة تحليلية مقارنة)، ط1، دار وائل للطباعة والنشر والتوزيع، عمان، 2000، ص105.

[51] وتتمثل الشروط الموضوعية للتفتيش بما يلي: 1- بسببه: وقوع جريمة من نوع جناية أو جنحة، وان يوجه اتهام إلى الشخص المراد تفتيشه أو تفتيش مسكنه. 2- الغاية منه: ضبط أشياء تفيد في كشف الحقيقة. أما الشروط الشكلية فتتحدد بما يلي: 1- أن يكون الأمر بالتفتيش مسبباً. 2- حضور المتهم أو من ينيبه أو الغير أو من ينيبه التفتيش -3- تحرير محضر بالتفتيش. للمزيد ينظر: محمد ابو العلا عقيدة، شرح قانون الاجراءات الجنائية، ج1، دار النهضة العربية، القاهرة، 2001، ص431 وما بعدها.

[52] هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)، ط2، دار النهضة العربية، القاهرة، 2008، ص126.

المادية، ومن بينها البيانات والمعلومات المخزّنة داخل الحاسوب الآلي، إذ إن الإشارات والنبضات الإلكترونية لا تُعدّ أشياء ملموسة، مما يجعلها غير قابلة للتفتيش[53].

ومن جانبنا نرى أن الرأي الأرجح يتمثل في الاتجاه الفقهي الأول الذي يذهب إلى أنّ تفتيش نظم الحاسوب الآلي بحثًا عن الأدلة الرقمية يمتد ليشمل المكونات المادية والمعنوية للحاسوب معًا، ذلك أنّ الغاية من إجراء التفتيش بوجه عام تكمن في الحصول على الأدلة التي تسهم في كشف الحقيقة بما في ذلك الأدلة الإلكترونية، كما أنّ هذا الاتجاه الفقهي يجد سنده فيما أقرت به اتفاقية بودابست بشأن الجرائم الإلكترونية[54].

أمّا فيما يتعلق بتفتيش شبكات الحاسوب[55]، فلا بد من التمييز بين حالتين، الأولى إذا كان حاسوب المتهم متصلاً بحاسوب آخر داخل إقليم الدولة، فإن ذلك يعني أنّ جميع عناصر الجريمة قد ارتكبت داخل دولة واحدة، وبناءً عليه إذا كان الحاسوب موجودًا في المكان المشمول بإذن التفتيش جاز تفتيشه، أمّا الحالة الثانية فتتمثل في اتصال الحاسوب المشمول بإذن التفتيش بحاسوب آخر موجود في موقع مختلف، حيث يرى الفقه أنّه يجوز امتداد التفتيش ليشمل سجلات البيانات الموجودة في ذلك الموقع متى كانت ضرورية لكشف الحقيقة، على أن يتم ذلك مع مراعاة الضوابط والشروط المقررة للتفتيش في الأماكن الأخرى، سواء كانت أماكن تتمتع بالحصانة أو مساكن خاصة أو تخص أشخاصًا غير المتهم[56]، أمّا الحالة الثانية فيتعلق باتصال حاسوب المتهم بحاسوب آخر خارج حدود الدولة، وقد اختلف الفقه حول مدى جواز امتداد التفتيش أو الولوج إلى الأنظمة الإلكترونية الكائنة خارج الإقليم الوطني، غير أنّ الرأي الراجح – والذي نؤيده – يذهب إلى عدم جواز هذا الامتداد إلا استنادًا إلى اتفاقية ثنائية أو دولية أو بناءً على إذن صريح من الدولة التي يقع النظام الإلكتروني في إقليمها، وذلك ضمانًا لاحترام مبدأ سيادة الدول على أراضيها وصونًا لحقوق الأفراد في الخصوصية الإلكترونية[57]، في المقابل ذهب اتجاه فقهي آخر إلى جواز امتداد التفتيش ليشمل نظامًا إلكترونيًا موجودًا في دولة أخرى معتبراً أنّ ذلك لا يُشكّل مساسًا بسيادة تلك الدولة، بالنظر إلى الطبيعة العالمية لشبكة الإنترنت التي تتيح مثل هذا الإجراء، كما يرى هذا الاتجاه أنّ مقتضيات السرعة في تنفيذ عملية التفتيش تستلزم عدم انتظار الحصول على إذن مسبق من الدولة التي يوجد فيها النظام الإلكتروني المتصل بالحاسوب الوطني على أن يتم إخطار تلك الدولة في وقت لاحق[58].

وبالرجوع إلى موقف المشرّع اللبناني يتضح أنّه قد ساير الاتجاه الفقهي القائل بجواز تفتيش أجهزة الحاسوب الآلي بمكوناتها المادية والمعنوية، كما أكد في الوقت ذاته على إمكانية ضبط الأدلة الرقمية المخزنة داخل الأنظمة الإلكترونية

---

[53] للمزيد حول آراء هؤلاء الفقهاء ينظر: احمد عاصم عجيلة، الحماية الجنائية للمحررات الالكترونية، مرجع سابق، ص413.

[54] المادة (1/19) من اتفاقية بودابست الصادرة عن مجلس أوربا بتاريخ 2001/11/23 بشأن الجرائم المعلوماتية، والتي نصت على أنه ((يجب على كل طرف أن يتبنى الإجراءات التشريعية واية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي أو لجزء منه، وكذلك للبيانات المعلوماتية المخزنة فيه، أو لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية)). مشار إليها عند: هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مرجع سابق، ص237 وما بعدّها.

[55] يقصد بشبكات الانترنت او الحاسب الآلي: بأنها مجموعة مكونة من جهازين أو أكثر من أجهزة الحاسب الآلي المتصلة ببعضها اتصالاً سلكياً أو لاسلكياً، فهناك شبكات واسعة في أماكن متفرقة ترتبط ببعضها البعض من خلال الأجهزة الحاسوبية. ينظر: خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2011، ص158.

[56] بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، ط1، دار الفكر الجامعي، الاسكندرية، 2011، ص81 وما بعدها.

[57] هلالي عبد اللاه احمد، تفتيش نظم الحاسب الالي وضمانات المتهم المعلوماتي (دراسة مقارنة)، مرجع سابق، ص79. و محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي، مرجع سابق، ص290.

[58] سمير عالية، الجرائم الالكترونية، مرجع سابق، ص488.

سواء أكانت موجودة في الإقليم اللبناني أم خارجه، متى كان الوصول إليها ممكنًا عبر النظام المطلوب تفتيشه[59]، وبذلك يتبيّن أنّ المشرّع اللبناني قد نصّ صراحة على جواز تفتيش المكونات المادية والمعنوية للنظام الإلكتروني، وضبط الأدلة التي يمكن الإفادة منها في التحقيق بشأن الجريمة الإلكترونية المرتكبة، وقد أحسن المشرّع صنعًا حين أحال إجراءات التفتيش وشروطه إلى الأحكام المقررة في قانون أصول المحاكمات الجزائية، بوصفه الشريعة العامة للإجراءات الجزائية في لبنان.

أمّا في العراق فقد نصّت المادة (24/أولًا) من مشروع قانون جرائم الإلكترونية لسنة 2011 على منح قضاة التحقيق والمحققين سلطة مباشرة لإجراء الضبط وجمع الأدلة، فضلاً عن منحهم الحق في القيام بأي من الإجراءات التحقيقية المنصوص عليها في قانون أصول المحاكمات الجزائية، ومن ضمنها التفتيش الذي نظم المشرّع أحكامه وشروطه في المواد (72–86) من ذات القانون، كما أجازت المادة (26) من المشروع للقاضي المختص الدخول إلى أجهزة الحاسوب والاطلاع على البيانات المخزنة فيها بغرض البحث عن الأدلة الرقمية، بما يعني أنّ المشرّع العراقي قد قرّر صراحة إمكانية تفتيش المكونات المعنوية للحاسوب الآلي في جميع جرائم الإلكترونية.

**فقرة خامسة: الضبط في الجرائم الالكترونية:**

تمثل الغاية من التفتيش في ضبط الأشياء التي قد تساعد المحقق في الكشف عن الحقيقة المتعلقة بالجريمة بشكل عام، ويُعد تحقيق هذه الغاية الشرط الأساسي لمشروعية إجراء التفتيش[60]، ويقصد بالضبط عمومًا أنّه إجراء من إجراءات التحقيق: "وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها"[61]، وفي مجال جرائم الإلكترونية يقصد به: "وضع اليد على المكونات المادية والمعنوية للأنظمة المعلوماتية، وكل شيء يفيد في كشف الحقيقة عن الجريمة المعلوماتية"[62].

ويتم ضبط المعطيات الإلكترونية سواء كانت مثبتة على دعامات مادية أم في شكل معنوي، وبناءً عليه فإن الأشياء التي ينبغي إخضاعها لإجراء الضبط في الجرائم الإلكترونية والتي تُعدّ كيانات ذات قيمة يمكن الاستفادة منها في إثبات الجريمة أو نسبتها إلى الجاني هي[63]:

**أولاً: الشرائط الممغنطة:** وهي كافة الشرائط ووسائط التخزين والنقل التي يُعتقد أنها تحتوي على بيانات تسهم في كشف الحقيقة أو تحديد مرتكبها.

**ثانياً: ضبط المستندات والكيانات الورقية:** التي ترتبط بالجريمة أو بمرتكبيها وقد تتمثل في محررات مزورة داخل نظام الحاسب الآلي أو خارجه، أو توجد ضمن سلة المهملات.

**ثالثاً: وحدة المدخلات:** المكوَّنة من لوحة المفاتيح والشاشة والفأرة والخادم بالإضافة إلى برامج معالجة النصوص وبرامج عرض الشرائح.

**رابعاً: ضبط المراسلات الإلكترونية:** التي تُستخدم لإرسال البريد الإلكتروني عبر شبكة الإنترنت ويتم من خلالها نقل

---

[59] المادتان (123 و124) من قانون المعاملات الالكترونية والبيانات ذات الطابع الشخصي اللبناني رقم (81) لسنة 2018 النافذ.

[60] فوزية عبد الستار، شرح قانون الاجراءات الجنائية، دار النهضة العربية، القاهرة، 1986، ص615.

[61] محمود نجيب حسني، شرح قانون الاجراءات الجنائية، مرجع سابق، ص561.

[62] محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي، مرجع سابق، ص319.

[63] سعيد سالم المزروعي، و عزمان عبدالرحمن، اجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقًا للتشريع الاماراتي، مجلة العلوم الاقتصادية والادارية والقانونية، العدد الثالث عشر، المجلد الثاني، المركز القومي للبحوث، فلسطين، 2018، ص122.

الرسائل ومحتوى المستندات الورقية، وتتميز هذه الوسيلة بنظام حماية قائم على رموز وشفرات لا يمكن الاطلاع عليها إلا من قبل الجهة المستقبلة، كما تحتفظ بنسخ من المواد المرسلة والمستقبلة يمكن استرجاعها والاطلاع عليها وضبطها.

**خامساً: ضبط الطابعات وأجهزة التصوير بأنواعها** كافة: خصوصاً أن الأجهزة الحديثة قادرة على تخزين المستندات والمواد المطبوعة أو المنسوخة، مما يتيح إعادة استخراجها والتعرف على محتوياتها.

**سادساً: ضبط وحدة الذاكرة الرئيسية ووحدة التحكم والمودم:** وهي الوسيلة التي تمكّن أجهزة الحاسوب من الاتصال ببعضها البعض عبر خطوط الهاتف.

تخضع عملية ضبط الأدلة الرقمية لإجراءات خاصة تهدف إلى حفظها وصيانتها من أي عبث أو تلاعب، ومن أبرز هذه الإجراءات تأمين مسرح الجريمة الإلكتروني من التدخل غير المشروع وذلك بعزل الحواسيب عن الشبكة لمنع إجراء أي تعديل على الأدلة الرقمية من قبل الغير، كما يتعين رفع البصمات عن الأجهزة لمقارنتها لاحقًا ببصمات المشتبه به وحجز الحاسوب أو القرص الصلب وكافة الحاويات المادية والأقراص المدمجة، ويُضاف إلى ذلك وضع ملصقات على المواد المضبوطة وتوثيقها وتغليفها وإعدادها للنقل بالحالة ذاتها التي كانت عليها إلى مكان الفحص والاختبار، مع تنظيم محضر رسمي يتضمن عرضًا تفصيليًا للإجراءات المتخذة وبوجه خاص تلك المتعلقة بضمان سلامة الدليل ومنع إدخال أي تغيير عليه منذ لحظة ضبطه[64].

وقد نظّم المشرّع اللبناني قواعد ضبط الأدلة الإلكترونية في قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي، حيث نصّ على أنه: "تقوم الضابطة العدلية بإجراءات ضبط الأدلة المعلوماتية وحفظها بناء لقرار المرجع القضائي المختص، ويؤازرها في ذلك مكتب متخصص"[65]، بينما نصّت المادة (123) من القانون ذاته على أنه: "مع مراعاة الأحكام الواردة في هذا الفصل –السابع– تطبق على ضبط الأدلة المعلوماتية أو البيانات على وسيطة إلكترونية قابلة للنقل، مثل الأقراص المدمجة أو جهاز حاسوب، أحكام قانون أصول المحاكمات الجزائية المتعلقة بالتفتيش وبضبط الأدلة بالجريمة المشهودة وغير المشهودة، لا سيما المادتين 33 و 41 منه"، وبناءً على ذلك لا يثور في التشريع اللبناني أي إشكال بشأن خضوع المكوّنات المعنوية للإنترنت لقواعد الضبط وفقًا لقانون المعاملات الإلكترونية، وكذلك بمقتضى قانون أصول المحاكمات الجزائية، مع الالتزام بالقواعد التي نصّت عليها المادة (124) منه، ومن أبرز هذه القواعد وجوب مراعاة حقوق الشخص المعني والأشخاص حسني النية وعدم ضبط البرامج أو البيانات المستخدمة لأغراض مشروعة، فضلاً عن ضرورة بيان مصدر كل تنزيل للبيانات أو نقل للأدلة الرقمية من موقع إلكتروني أو أي جهاز حاسوب، إضافةً إلى ختم المكان الذي تتواجد فيه الوسائط الإلكترونية والبيانات بالشمع الأحمر لحين حضور الخبير الفني[66].

كما أجاز المشرّع اللبناني في قانون المعاملات الإلكترونية للمحكمة الناظرة في الدعوى وبموجب قرارها النهائي، أن تقرّر وقف الخدمات الإلكترونية أو حجب المواقع الإلكترونية أو إلغاء الحسابات، إذا تعلّق الأمر بجرائم الإرهاب أو المواد الإباحية أو ألعاب المقامرة الممنوعة أو عمليات الاحتيال الإلكتروني المنظّمة أو تبييض الأموال أو الجرائم الماسّة بأمن الدولة الداخلي والخارجي، فضلًا عن الجرائم المتعلّقة بالاعتداء على سلامة الأنظمة الإلكترونية كإدخال الفيروسات ونشرها[67].

---

[64] سمير عالية، الجرائم الالكترونية، مرجع سابق، ص491.

[65] المادة (121) من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي اللبناني رقم (81) لسنة 2018 النافذ.

[66] للمزيد ينظر: المادة (124) من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي اللبناني رقم (81) لسنة 2018 النافذ.

[67] المادة (125) من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي اللبناني رقم (81) لسنة 2018 النافذ.

أما بالنسبة لموقف المشرّع العراقي من ضبط الأدلة الإلكترونية، فيُلاحظ أنّه قد نظّم أحكام الضبط في مشروع قانون جرائم الإلكترونية لسنة 2011، حيث نصّت المادة (24/ثالثاً) منه على أنّ: "يتولى قاضي التحقيق أو المحقق المباشرة في إجراءات الضبط وجمع الادلة أو أي إجراء تحقيقي نص عليه قانون أصول المحاكمات الجزائية".

في حين أكّدت المادة (26/أولاً) من المشروع ذاته على الإجراءات التي يتعيّن على القاضي المختص اتباعها عند ضبط الأدلة الإلكترونية، إذ نصّت على أنّ: "للقاضي المختص ما يأتي: أ–إصدار الأوامر لأية جهة لحفظ بيانات الحاسوب، بما في ذلك المعلومات أو البيانات المتناقلة التي تخزن في أجهزة الحاسوب أو ملحقاته أو توابعه ومخرجاته التي يظهر احتمال تعرضها للتغيير أو الفقدان، ب–إصدار الأوامر لجهات تزويد خدمات شبكة المعلومات أو الخدمات التقنية بأنواعها لتقديم بيانات الاشتراك والمرور لجهة التحقيق إذا كان من شأنها أن تساهم في الكشف عن الجريمة، ج–الدخول إلى أجهزة الحاسوب والشبكات أو أي جزء منها وإلى البيانات المخزنة فيها وإلى أية واسطة أو وسيلة يمكن أن تخزن فيها بيانات الحاسوب الموجودة داخل العراق وله اعتراض البيانات ورصدها ومراقبتها بقرار مسبب ولمدة وغرض محددين، د–تتبع المعلومات إلى نظم الحاسوب والشبكات الأخرى المرتبطة بنظام الحاسوب أو الشبكات محل الاشتباه على أن تبلغ الجهات التي تملك هذه النظم والشبكات بالإجراء ونطاقه وعلى أن ينحصر نطاق هذا الإجراء بما يتعلق بالتصرف محل التحقيق دون انتهاك أو مساس بحقوق الغير، هـ–ضبط أجهزة الحاسوب أو جزء منها أو الواسطة التي خزنت فيها البيانات ونقلها إلى جهة التحقيق لتحليلها ودراستها، وله نسخها دون نقل النظام وازالة البيانات المانعة من الدخول إلى الحاسوب دون الحاق الضرر بالنظام أو المساس بسلامة البيانات والبرامج المخزنة فيه".

ومن الملاحظ أنّه بعد انتهاء إجراءات التحقيق الابتدائي التي تُعدّ مرحلة فحص الأدلة المتوافرة من قبل قاضي التحقيق أو المحقق يتعيّن حسم مصير الدعوى الجزائية والتصرف فيها، وبالرجوع إلى موقف المشرّعين اللبناني والعراقي بشأن التصرف في الدعوى بعد انتهاء التحقيق، نجد أنّ المشرّع اللبناني أوجب على قاضي التحقيق عقب استكمال جميع الإجراءات التحقيقية إصدار قرار باختتام التحقيق وإحالة الدعوى إلى النيابة العامة لإبداء مطالعتها النهائية، لتُعاد بعدها إلى قاضي التحقيق كي يصدر قراره باختتام التحقيق والتصرف فيها[68]، فإذا تبيّن لقاضي التحقيق بعد استكمال تحقيقاته عدم توافر سند قانوني أو واقعي يُسوّغ الظن بالمدعى عليه بشأن الجرم المنسوب إليه، جاز له أن يصدر قراراً بمنع المحاكمة متى توافر أحد الأسباب القانونية الآتية، إذا كان الفعل المدعى به لا يشكّل جريمة جزائية كأن يكون نزاعاً ذا طبيعة مدنية أو تجارية أو إذا كانت عناصر الجريمة غير مكتملة وهو ما يُعد نتيجة من نتائج مبدأ شرعية الجرائم والعقوبات، أو إذا صدر بعد تحريك الدعوى قانون جديد يجرّد الفعل من أي وصف جرمي أو إذا زالت الصفة الجرمية عن الفعل المدعى به لقيام أحد أسباب التبرير القانونية المنصوص عليها في المادة (183) من قانون العقوبات، أو إذا انقضت الدعوى العامة بأحد أسباب الانقضاء المحددة قانوناً في المادة (10) من قانون أصول المحاكمات الجزائية، كمرور الزمن أو العفو العام أو الوفاة وغيرها[69].

أما إذا تبيّن لقاضي التحقيق أنّ الأدلة المتوافرة تكفي للظن بالمدعى عليه بارتكاب الجرم المنسوب إليه وكان الفعل المدعى به من نوع المخالفة أو الجنحة التي لا تستوجب الحبس، وجب عليه أن يطلق سراح المدعى عليه فوراً إذا كان موقوفاً، وأن يحيل ملف الدعوى إلى القاضي المنفرد عن طريق النيابة العامة[70]، في حين إذا تبيّن لقاضي التحقيق

[68] المادة (121) من قانون اصول المحاكمات الجزائية اللبناني رقم (328) لسنة 2001 المعدل.

[69] المادة (122/ثانيا) من قانون اصول المحاكمات الجزائية اللبناني رقم (328) لسنة 2001 المعدل.

[70] المادة (123) من قانون اصول المحاكمات الجزائية اللبناني رقم (328) لسنة 2001 المعدل.

أنّ الجريمة من نوع الجناية، تعيّن عليه إحالة ملف الدعوى إلى النيابة العامة لتقوم بدورها بإيداعه لدى الهيئة الاتهامية باعتبارها الجهة المختصة بتحريك الاتهام[71].

أما بشأن موقف المشرّع العراقي من التصرف في الدعوى بعد انتهاء الإجراءات التحقيقية، فيُلاحظ أنّه قد أكّد في قانون أصول المحاكمات الجزائية على أنّ: "أ–اذا وجد قاضي التحقيق ان الفعل لا يعاقب عليه القانون او ان المشتكي تنازل عن شكواه وكانت الجريمة مما يجوز الصلح عنها دون موافقة القاضي او ان المتهم غير مسؤول قانونا بسبب صغر سنه فيصدر القاضي قرارا برفض الشكوى وغلق الدعوى نهائيا، ب– اذا كان الفعل معاقبا عليه ووجد القاضي ان الادلة تكفي لمحاكمة المتهم فيصدر قرارا بإحالته على المحكمة المختصة، اما اذا كانت الادلة لا تكفي لإحالته فيصدر قرارا بالأفراج عنه وغلق الدعوى مؤقتا مع بيان اسباب ذلك، ج–اذا وجد القاضي ان الفاعل مجهول او ان الحادث وقع قضاء وقدرا فيصدر قرارا بغلق الدعوى مؤقتا، د–يخلى سبيل المتهم الموقوف عند صدور القرار برفض الشكوى او الافراج عنه، هـ–يخبر القاضي الادعاء العام بالقرارات التي يصدرها بمقتضى هذه المادة"[72].

مما تقدّم يتبيّن أنّ القرارات التي يصدرها قاضي التحقيق بعد استكمال جميع الإجراءات التحقيقية وفقاً للتشريع العراقي تنحصر في قرارين، الأول قرار غلق التحقيق ويكون على صورتين، فإمّا أن يكون غلقاً مؤقتاً إذا لم تكن الأدلة كافية للإدانة أو غلقاً نهائياً إذا تنازل المشتكي عن شكواه أو تبيّن أنّ المتهم غير مسؤول جزائياً أو أنّ الفعل لا يشكّل جريمة معاقباً عليها قانوناً، أما القرار الثاني فيتمثّل بإحالة المتهم إلى المحكمة المختصة متى تبيّن للقاضي أنّ الأدلة المتوافرة تكفي لمحاكمته[73]، فإذا كان الفعل الجرمي من نوع المخالفة فقد أوجب المشرّع على قاضي التحقيق أن يفصل فيه مباشرة متى لم يتضمن طلباً بالتعويض أو برد المال وذلك دون إحالته إلى محكمة الجنح، أمّا إذا كان الفعل الجرمي من نوع الجنحة وجب إحالته إلى محكمة الجنح بدعوى غير موجزة إذا كان معاقباً عليه بالحبس مدة تزيد على ثلاث سنوات وبدعوى موجزة أو غير موجزة في غير ذلك من الأحوال، وفي حالة ما إذا كان الفعل الجرمي يشكّل جناية فإنّ الدعوى تُحال إلى محكمة الجنايات بدعوى غير موجزة[74].

وكما يتضح فقد أذن المشرّع العراقي في الفقرة (هـ) من المادة (130) أعلاه لقاضي التحقيق بإحالة الدعوى مباشرة إلى المحكمة المختصة، سواء كان الفعل المرتكب جنحة أم جناية على أن يُخطر الادعاء العام بقراره، أمّا المشرّع اللبناني فقد أذن لقاضي التحقيق بإحالة المدعى عليه إلى القاضي المنفرد الجزائي (محكمة الجنح) في حال كان الفعل الجرمي من نوع المخالفة أو الجنحة ولا يستوجب الحبس، في حين أنّه إذا كان الفعل من نوع الجناية فلا يجوز لقاضي التحقيق إحالة المدعى عليه مباشرة إلى المحكمة، بل يتعيّن المرور بالهيئة الاتهامية التي تصدر قرار الاتهام وتُحيل بموجبه الدعوى إلى محكمة الجنايات.

---

[71] المادة (125) من قانون اصول المحاكمات الجزائية اللبناني رقم (328) لسنة 2001 المعدل.

[72] المادة (130) من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل.

[73] المادة (134) من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل.

[74] يقصد بالدعوى غير الموجزة الدعوى التي يجري فيها التحقيق كامل وتوجه فيها التهمة إلى المتهم، ام الدعوى الموجزة فيقصد بها الدعوى التي لا يجري فيها التحقيق كامل. ينظر: رعد فجر فتيح الراوي، شرح قانون اصول المحاكمات الجزائية، ج1، ط1، مكتب الهاشمي للكتاب الجامعي، بغداد، 2016، ص215.

**الخاتمة:**

**أولًا: الاستنتاجات:**

1. تتميز الجرائم الالكترونية بطبيعة تقنية معقدة تفرض اعتماد وسائل فنية متخصصة في التحقيق.
2. تلعب البرامج التقنية دورًا جوهريًا في جمع الأدلة الرقمية وكشف ملابسات الجريمة.
3. إن سلامة الدليل الرقمي ترتبط بمدى الالتزام بالاجراءات الفنية والقانونية أثناء جمعه وتحليله.
4. يتطلب التحقيق في الجرائم الإلكترونية توافر مهارات تقنية حديثة لدى المحقق تختلف عن المهارات التقليدية.
5. لا يمكن الاستغناء عن الخبرة الفنية في هذا النوع من الجرائم نظرًا لطبيعتها التقنية المعقدة.

**ثانيًا: التوصيات:**

1. ضرورة تدريب الكوادر التحقيقية على المهارات التقنية المرتبطة بالجرائم الإلكترونية.
2. تطوير البنية التحتية التقنية للأجهزة التحقيقية بما يواكب التطور التكنلوجي.
3. تعزيز التعاون بين الجهات التحقيقية والخبراء الفنيين في مجال الأدلة الرقمية.
4. تحديث التشريعات الإجرائية بما يتلاءم مع خصوصية الجرائم الالكترونية.
5. اعتماد برامج وتقنيات حديثة لضمان جمع الأدلة الرقمية وحفظها بصورة سليمة.

**قائمة المراجع**


1. أبو العلا عقيدة، محمد .(2001) **.شرح قانون الإجراءات الجنائية**، ج1. القاهرة: دار النهضة العربية.

Mohamed Abu Al-Ela Aqida. (2001). *Explanation of the Criminal Procedure Law*, Vol. 1. Cairo: Dar Al-Nahda Al-Arabiya.

2. أحمد، هلالي عبد اللاه .(2007) **.اتفاقية بودابست لمكافحة جرائم المعلوماتية**، ط1. القاهرة: دار النهضة العربية.

Hilali Abdel-Lah Ahmed. (2007). *The Budapest Convention on Combating Cybercrimes*, 1st ed. Cairo: Dar Al-Nahda Al-Arabiya.

3. أحمد، هلالي عبد اللاه .(2008) **.التزام الشاهد بالإعلام في الجرائم المعلوماتية: دراسة مقارنة**، ط2. القاهرة: دار النهضة العربية.

Hilali Abdel-Lah Ahmed. (2008). *The Witness's Obligation to Provide Information in Cybercrimes: A Comparative Study*, 2nd ed. Cairo: Dar Al-Nahda Al-Arabiya.

4. أحمد، هلالي عبد اللاه .(2008) **.تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي: دراسة مقارنة**، ط2. القاهرة: دار النهضة العربية.

Hilali Abdel-Lah Ahmed. (2008). *Searching Computer Systems and the Guarantees of the Cyber-Accused: A Comparative Study*, 2nd ed. Cairo: Dar Al-Nahda Al-Arabiya.

5. الحسيني، أحمد سعد محمد .**الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية**.

Ahmed Saad Mohamed Al-Husseini. *Procedural Aspects of Crimes Arising from the Use of Electronic Networks*.

6. الحسيني، عمار عباس .(2015) .**التحقيق الجنائي والوسائل الحديثة في كشف الجريمة**، ط1. بيروت: منشورات الحلبي الحقوقية.

Ammar Abbas Al-Husseini. (2015). *Criminal Investigation and Modern Methods of Crime Detection*, 1st ed. Beirut: Al-Halabi Legal Publications.

7. الحلبي، خالد عياد .(2011) .**إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، ط1. عمان: دار الثقافة للنشر والتوزيع.

Khaled Ayyad Al-Halabi. (2011). *Inquiry and Investigation Procedures in Computer and Internet Crimes*, 1st ed. Amman: Dar Al-Thaqafa for Publishing and Distribution.

8. الخوالبة، علي حسن .(2010) .**التفتيش الجنائي على نظم الحاسوب والإنترنت**، ط1. مملكة البحرين: مؤسسة فخراوي للدراسات والنشر.

Ali Hassan Al-Tawalbeh. (2010). *Criminal Search of Computer and Internet Systems*, 1st ed. Kingdom of Bahrain: Fakhrawi Foundation for Studies and Publishing.

9. الدليمي، جلال حماد عرميط .(2015) .**ضمانات المتهم في إجراءات التحقيق الابتدائي المقيدة لحريته والماسة بشخصه: دراسة مقارنة**، ط1. بيروت: منشورات الحلبي الحقوقية.

Jalal Hammad Armit Al-Dulaimi. (2015). *Guarantees of the Accused in Preliminary Investigation Procedures Restricting Freedom and Affecting the Person: A Comparative Study*, 1st ed. Beirut: Al-Halabi Legal Publications.

10. الراوي، رعد فجر فتيح .(2016) .**شرح قانون أصول المحاكمات الجزائية**، ج1، ط1. بغداد: مكتب الهاشمي للكتاب الجامعي.

Raad Fajr Futeih Al-Rawi. (2016). *Explanation of the Code of Criminal Procedure*, Vol. 1, 1st ed. Baghdad: Al-Hashimi Office for University Books.

11. الرشيدي، طه السيد أحمد .(2016) .**الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق في النظام الجزائي المصري والسعودي**، ط1. الإسكندرية: دار الكتب والدراسات العربية.

Taha Al-Sayed Ahmed Al-Rashidi. (2016). *The Special Nature of Information Technology Crimes and Their Impact on Investigation Procedures in the Egyptian and Saudi Criminal Systems*, 1st ed. Alexandria: Dar Al-Kutub wa Al-Dirasat Al-Arabiya.

12. السرحاني، محمد بن نصير محمد. (2004). **مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت: دراسة مسحية على ضباط الشرطة في المنطقة الشرقية**. رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض.

Mohamed bin Nusayr Mohamed Al-Sarhani. (2004). *Technical Criminal Investigation Skills in Computer and Internet Crimes: A Survey Study of Police Officers in the Eastern Region*. Master's thesis, College of Graduate Studies, Department of Police Sciences, Naif Arab University for Security Sciences, Riyadh.

13. الصغير، جميل عبد الباقي. (2002). **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت**. القاهرة: دار النهضة العربية.

Jamil Abdel-Baqi Al-Saghir. (2002). *Procedural Aspects of Internet-Related Crimes*. Cairo: Dar Al-Nahda Al-Arabiya.

14. العنزي، سليمان مهجع. (2003). **وسائل التحقيق في جرائم نظم المعلومات**. رسالة ماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

Suleiman Muhajja Al-Enezi. (2003). *Methods of Investigation in Information Systems Crimes*. Master's thesis, College of Graduate Studies, Department of Police Sciences, Naif Arab Academy for Security Sciences, Riyadh.

15. الغافري، حسين بن سعيد بن سيف. (2009). **السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة**. أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة.

Hussein bin Saeed bin Saif Al-Ghafri. (2009). *Criminal Policy in Confronting Internet Crimes: A Comparative Study*. PhD dissertation, Faculty of Law, Ain Shams University, Cairo.

16. الغريب، محمد عيد. (2004). **مبادئ الإجراءات الجنائية**. بلا دار نشر.

Mohamed Eid Al-Gharib. (2004). *Principles of Criminal Procedures*. No publisher stated.

17. اللوغاني، سعود علي عبد الله. (2011). **الدليل الإلكتروني وحجيته في الإثبات الجنائي: دراسة مقارنة**. رسالة ماجستير، كلية القانون، جامعة الشارقة، الإمارات العربية المتحدة.

Saud Ali Abdullah Al-Loughani. (2011). *Electronic Evidence and Its Evidentiary Value in Criminal Proof: A Comparative Study*. Master's thesis, College of Law, University of Sharjah, United Arab Emirates.

18. المزروعي، سعيد سالم، وعبد الرحمن، عزمان. (2018). إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقًا للتشريع الإماراتي. **مجلة العلوم الاقتصادية والإدارية والقانونية**، 2(13)، 122. المركز القومي للبحوث، فلسطين.

Saeed Salem Al-Mazrouei, & Azman Abdul Rahman. (2018). Criminal investigation procedures in information technology crimes under Emirati legislation. *Journal of Economic, Administrative and Legal Sciences*, 2(13), 122. National Research Center, Palestine.

19.المناعسة، أسامة أحمد، والزعبي، جلال، والهواوشة، صايل فاضل .(2000) .**جرائم الحاسب الآلي والإنترنت: دراسة تحليلية مقارنة**، ط1. عمان: دار وائل للطباعة والنشر والتوزيع.

Osama Ahmed Al-Manaaseh, Jalal Al-Zoubi, & Sayel Fadel Al-Hawawsheh. (2000). *Computer and Internet Crimes: A Comparative Analytical Study*, 1st ed. Amman: Dar Wael for Printing, Publishing and Distribution.

20.بكري، بكري يوسف .(2011) .**التفتيش عن المعلومات في وسائل التقنية الحديثة**، ط1. الإسكندرية: دار الفكر الجامعي.

Bakri Youssef Bakri. (2011). *Searching for Information in Modern Technological Means*, 1st ed. Alexandria: Dar Al-Fikr Al-Jami'i.

21.جوخدار، حسن .(1993) .**شرح قانون أصول المحاكمات الجزائية الأردني**، ج1. عمان: دار الثقافة للنشر والتوزيع.

Hassan Jokhdar. (1993). *Explanation of the Jordanian Code of Criminal Procedure*, Vol. 1. Amman: Dar Al-Thaqafa for Publishing and Distribution.

22.حسن، سعيد عبد اللطيف .(1999) .**إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت: الجرائم الواقعة في مجال تكنولوجيا المعلومات**، ط1. القاهرة: دار النهضة العربية.

Saeed Abdel-Latif Hassan. (1999). *Proof of Computer Crimes and Crimes Committed via the Internet: Crimes in the Field of Information Technology*, 1st ed. Cairo: Dar Al-Nahda Al-Arabiya.

23.حسني، محمود نجيب .(1988) .**شرح قانون الإجراءات الجنائية**، ط2. القاهرة: دار النهضة العربية.

Mahmoud Naguib Hosni. (1988). *Explanation of the Criminal Procedure Law*, 2nd ed. Cairo: Dar Al-Nahda Al-Arabiya.

24.داود، حسن طاهر .(2000) .**جرائم نظم المعلومات**، ط1. الرياض: مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية.

Hassan Taher Dawood. (2000). *Information Systems Crimes*, 1st ed. Riyadh: Center for Studies and Research, Naif Arab Academy for Security Sciences.

25.رستم، هشام محمد فريد .(1998) .**الجوانب الإجرائية للجرائم المعلوماتية**، ط1. القاهرة: دار النهضة العربية.

Hisham Mohamed Farid Rustom. (1998). *Procedural Aspects of Cybercrimes*, 1st ed. Cairo: Dar Al-Nahda Al-Arabiya.

26.شاهين، محمد كمال .(2018) .**الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي: دراسة مقارنة** . الإسكندرية: دار الجامعة الجديدة.

Mohamed Kamal Shaheen. (2018). *Procedural Aspects of Cybercrime at the Preliminary Investigation Stage: A Comparative Study*. Alexandria: Dar Al-Jami'a Al-Jadida.

27.عبد الله، سعيد حسب الله .(1990) .**شرح قانون أصول المحاكمات الجزائية** .الموصل: دار الحكمة للطباعة والنشر.

Saeed Hasab Allah Abdullah. (1990). *Explanation of the Code of Criminal Procedure*. Mosul: Dar Al-Hikma for Printing and Publishing.

28.عبد المطلب، ممدوح عبد الحميد .(2001) .**جرائم الكمبيوتر وشبكة المعلومات العالمية** .الشارقة: مكتبة الحقوق.

Mamdouh Abdel-Hamid Abdel-Muttalib. (2001). *Computer Crimes and the World Wide Information Network*. Sharjah: Law Library.

29.عبود، زياد محمد، وعبد المجيد، غسان حميد، وآخرون .(2014) .**أساسيات الحاسوب وتطبيقاته المكتبية**، ج1. بغداد: الدار الجامعية للطباعة والنشر والتأليف والترجمة، وزارة التعليم العالي والبحث العلمي العراقية.

Ziad Mohamed Abboud, Ghassan Hamid Abdel-Majid, et al. (2014). *Computer Basics and Office Applications*, Vol. 1. Baghdad: University House for Printing, Publishing, Authorship and Translation, Iraqi Ministry of Higher Education and Scientific Research.

30.عجيلة، أحمد عاصم .(2014) .**الحماية الجنائية للمحررات الإلكترونية: دراسة مقارنة** .القاهرة: دار النهضة العربية.

Ahmed Asim Ajila. (2014). *Criminal Protection of Electronic Documents: A Comparative Study*. Cairo: Dar Al-Nahda Al-Arabiya.

31.عثماني، عز الدين. (2018). إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية .**مجلة دائرة البحوث والدراسات القانونية والسياسية**، العدد الرابع. الجزائر: كلية الحقوق والعلوم السياسية، جامعة البليدة.

Ezzedine Othmani. (2018). Investigation and search procedures in crimes affecting communication and information systems. *Journal of the Department of Legal and Political Research and Studies*, Issue 4. Algeria: Faculty of Law and Political Sciences, University of Blida.

32.عالية، سمير .(2020) .**الجرائم الإلكترونية في القانون الجديد رقم 2018/81**، ط1. بيروت: منشورات الحلبي الحقوقية.

Samir Aliya. (2020). *Cybercrimes under the New Law No. 81/2018*, 1st ed. Beirut: Al-Halabi Legal Publications.

33.فوزية عبد الستار .(1986) .**شرح قانون الإجراءات الجنائية** .القاهرة: دار النهضة العربية.

Fawzia Abdel-Sattar. (1986). *Explanation of the Criminal Procedure Law*. Cairo: Dar Al-Nahda Al-Arabiya.

34.محمود مصطفى، محمود .(1983) .**شرح قانون الإجراءات الجنائية**، ط12. القاهرة: دار النهضة العربية.

Mahmoud Mahmoud Mustafa. (1983). *Explanation of the Criminal Procedure Law*, 12th ed. Cairo: Dar Al-Nahda Al-Arabiya.

35.هروال، نبيلة هبة .(2007) .**الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات** .الإسكندرية: دار الفكر الجامعي.

Nabila Hiba Harwal. (2007). *Procedural Aspects of Internet Crimes at the Evidence-Gathering Stage*. Alexandria: Dar Al-Fikr Al-Jami'i.

36.القحطاني، عبد الله بن حسين آل حجراف .(2014) .**تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية** . رسالة ماجستير، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض.

Abdullah bin Hussein Al-Hajraf Al-Qahtani. (2014). *Developing Criminal Investigation Skills in Confronting Cybercrimes*. Master's thesis, Department of Police Sciences, College of Graduate Studies, Naif Arab University for Security Sciences, Riyadh.

37.ويكيبيديا، الموسوعة الحرة .(2025) .**ذاكرة مخبئية** .متاح على https://ar.wikipedia.org :، تاريخ الزيارة: 2025/7/29.

Wikipedia, the Free Encyclopedia. (2025). *Cache Memory*. Available at: https://ar.wikipedia.org, accessed on 29/7/2025.

**القوانين والاتفاقيات**

38.**اتفاقية بودابست بشأن الجرائم المعلوماتية**، الصادرة عن مجلس أوروبا بتاريخ 2001/11/23.

*Budapest Convention on Cybercrime*, issued by the Council of Europe on 23 November 2001.

39.**قانون أصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971 المعدل.**

*Iraqi Code of Criminal Procedure No. 23 of 1971, as amended*.

40.**قانون أصول المحاكمات الجزائية اللبناني رقم 328 لسنة 2001 المعدل.**

*Lebanese Code of Criminal Procedure No. 328 of 2001, as amended*.

41.**قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي اللبناني رقم 81 لسنة 2018.**

*Lebanese Electronic Transactions and Personal Data Law No. 81 of 2018*.

42.**مشروع قانون جرائم المعلوماتية العراقي لسنة 2011.**

*Draft Iraqi Cybercrimes Law of 2011*.