

الطبيعة الخاصة لإجراءات ضبط وإثبات الجرائم المرتبطة بتكنولوجيا

الإعلام والاتصال

The Specific Nature of Procedures for Detecting and Proving Crimes Related to Information and Communication Technology

بن قويدر الطاهر*، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي - الأغواط -

t.benkouider@lagh-univ.dz

تاريخ إرسال المقال: 2025/05/18 تاريخ قبول المقال: 2026/04/13 تاريخ نشر المقال: 2026/05/31

الملخص:

تعدّ جرائم تكنولوجيايات الإعلام والاتصال من الظواهر الحديثة والمتطورة، مما استدعى اهتمام الجهات المعنية لمواجهتها على المستويين الدولي والوطني، وتبرز أهمية دراسة هذا الموضوع من جهة حدّاته، ومن جهة أخرى لما يمثله من تهديد للحريات الشخصية للأفراد. فمن الناحية النظرية، تتجلى أهمية الدراسة في تقييم مدى استجابة المشرّع الجزائري للتطورات السريعة في مجال مكافحة جرائم تكنولوجيايات الإعلام والاتصال، أما من الناحية العملية، فإن نظم المعلوماتية تثير العديد من التحديات القانونية، الأمر الذي دفع المشرّع إلى وضع نصوص قانونية تتناسب مع الخصوصية التي تميز هذه الجرائم والأدلة الرقمية المرتبطة بها، وذلك لوعي المشرّع بعدم كفاية الإجراءات الجزائية التقليدية لمواجهة هذه الظواهر المستحدثة. نهدف من خلال ورقتنا البحثية هاته إلى تسليط الضوء على خصوصية الإجراءات المتعلقة بالجرائم المرتبطة بتكنولوجيايات الإعلام والاتصال، مع التركيز بشكل خاص على الجوانب الإجرائية المتعلقة بمتابعة هذا النوع من الجرائم في الجزائر. وقد اعتمدت في دراستي هاته على المنهج التحليلي الوصفي، حيث قمت بوصف الظاهرة وتوضيح المفاهيم القانونية المرتبطة بها، مع تحليل هذه المفاهيم وشرحها بشكل مفصل. وقد تم تقسيم هذا الموضوع وفق خطة منهجية إلى مبحثين رئيسيين، بما يتيح تناول الموضوع بشكل شامل ودقيق.

الكلمات المفتاحية: الجرائم المتصلة بتكنولوجيايات الإعلام والاتصال، إجراءات ضبط الجرائم

المتصلة بتكنولوجيايات الإعلام والاتصال، إثبات الجرائم المتصلة بتكنولوجيايات الإعلام والاتصال.

Abstract:

Crimes related to information and communication technologies (ICT) are modern and evolving phenomena, necessitating attention from relevant authorities to address them at both international and national levels. The significance of studying this subject lies, on the one hand, in its novelty and, on the other hand, in its potential threat to individuals' personal freedoms. From a theoretical perspective, the importance of this study is evident in assessing the extent to which the Algerian legislator has responded to the rapid developments in combating ICT-related crimes. Practically, information systems pose numerous legal challenges, prompting the

* المؤلف المرسل

legislator to enact laws tailored to the unique characteristics of these crimes and the digital evidence associated with them. This stems from the legislator's awareness of the inadequacy of traditional criminal procedures in addressing these emerging phenomena.

Through this research paper, we aim to shed light on the specific procedural aspects related to ICT-related crimes, with a particular focus on the procedural measures involved in addressing such crimes in Algeria. This study employs a descriptive-analytical methodology, describing the phenomenon and clarifying the associated legal concepts, while analyzing and elaborating on these concepts in detail.

The subject is structured methodologically into two main chapters, allowing for a comprehensive and precise exploration of the topic.

Key words: Crimes related to information and communication technologies, procedures for controlling crimes related to information and communication technologies, proving crimes related to information and communication technologies..

المقدمة:

تخضع متابعة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال للأحكام العامة المنصوص عليها في قانون الإجراءات الجزائية، بالإضافة إلى مجموعة من القواعد الإجرائية الجديدة التي أقرها المشرع الجزائري بموجب القانون رقم 04-09، بناءً على ذلك سنحاول من خلال هذه الورقة البحثية دراسة موضوع بالغ الأهمية يتمثل في خصوصية الإجراءات المتعلقة بمتابعة هذه الجرائم، مع التركيز على الأحكام الواردة في القانون سالف الذكر، كما سنتناول من خلالها جانباً مهماً يتمثل في إثبات هذه الجرائم، وللتمكن من تناول هذا الموضوع بشكل منهجي، نطرح الإشكالية التالية:

"كيف ضبط المشرع الجزائري الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وما هي الوسائل المتاحة لإثباتها في ظل التحدّيات التي تواجهها".

وللإجابة على هذه الإشكالية اخترنا المنهج الوصفي التحليلي نظراً لما تتطلبه دراستنا من وصف وتحليل، معتمدين في ذلك التقسيم الثنائي لموضوع البحث من خلال المبحثين التاليين:

المبحث الأول: ضبط الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المبحث الثاني: إثبات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المبحث الأول: إجراءات ضبط الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

نظراً للطبيعة الخاصة للجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، تدخل المشرع لتعزيز الإجراءات الجزائية من خلال توفير وسائل قانونية للتحقيق تهدف إلى جمع الأدلة الرقمية. وقد تم ذلك عبر تعديل قانون الإجراءات الجزائية، إلى جانب الأحكام والإجراءات الواردة في القانون رقم 04-09، بما يتيح تفعيل المتابعة الجزائية لهذا النوع من الجرائم. وفي هذا السياق، سيتم تناول الإجراءات ذات الخصوصية في هذا المبحث من خلال تقسيمه إلى مطلبين رئيسيين:

المطلب الأول: يخصص لدراسة الإجراءات الواردة في قانون الإجراءات الجزائية.

المطلب الثاني: يعالج الإجراءات المنصوص عليها في القانون رقم 04-09.

المطلب الأول: الإجراءات الواردة في قانون الإجراءات الجزائية.

سنتعرض في هذا المطلب للإجراءات المستحدثة من قبل المشرع الجزائري ضمن قانون الإجراءات الجزائية، مع التركيز على إبراز الخصوصية التي تميز بعض هذه الإجراءات في إطار مكافحة جرائم تكنولوجيايات الإعلام والاتصال.

الفرع الأول: معاينة مسرح الجريمة.**أولاً: تعريف المعاينة.**

المعاينة هي إجراء ينتقل بموجبه المحقق إلى موقع وقوع الجريمة ليعاين آثارها بشكل مباشر، حيث يتطلب هذا الإجراء توثيق حالة الأشخاص والأشياء⁽¹⁾، وكل ما يمكن أن يسهم في كشف الحقيقة. وبناءً على ذلك، تستلزم المعاينة في الجرائم التقليدية الحضور إلى موقع الحادثة أو أي مكان يحتوي على أدلة أو آثار يُعتقد أنها مرتبطة بالجريمة.

في الجرائم التقليدية تلعب المعاينة دوراً حيوياً في تصور كيفية وقوع الجريمة، وظروفها وملابساتها، وتوفير أدلة مادية. أما في الجرائم الإلكترونية، فإن المعاينة لا تؤدي الدور ذاته في الكشف عن الأدلة وإثبات الجريمة ونسبتها إلى مرتكبيها، نظراً لعدم وجود آثار مادية واضحة في الغالب. وغالباً ما يتم العبث بالأدلة القليلة المتاحة، أو تغييرها أو إتلافها خلال الفترة الطويلة التي قد تفصل بين وقوع الجريمة واكتشافها أو التحقيق فيها، مما يُضعف من دلالة الأدلة التي يتم جمعها من المعاين، لذلك، ينبغي عند إجراء المعاينة اتباع خطوات دقيقة، منها توثيق الأجهزة ذات الصلة بالحادثة، وحماية المواد الرقمية لتجنب فقدانها أو العبث بها، والتأكد من عدم تأثير أي عوامل خارجية على الأدلة الموجودة، ومن الإجراءات الواجب اتباعها عند إجراء المعاينة ما يلي: ⁽²⁾

- توثيق جهاز الحاسوب مع جميع الأجهزة الطرفية المتصلة به وتسجيل محتوياته بشكل دقيق.
- التحقق بدقة قبل نقل أي بيانات رقمية، لضمان عدم تأثرها بأي حقول مغناطيسية خارجية.
- التخلص من المستندات الورقية الناتجة عن إدخال البيانات أو مخرجات الحاسوب بشكل آمن.
- توصيل الأقراص التي تحتوي على أدلة بجهاز خاص يمنع الكتابة عليها، مما يضمن قراءة البيانات دون تغييرها أو التلاعب بها.

ثانياً: خصوصية إجراء المعاينة.

يتمتع ضباط الشرطة القضائية باختصاص إقليمي ووطني عند متابعة جرائم المساس بأنظمة المعالجة الآلية للبيانات، وقد أشارت المادة 16 من قانون الإجراءات الجزائية في فقرتها 07 على أنه فيما يتعلق بالتحقيق في جرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنية، والجرائم التي تمس بأنظمة المعالجة الآلية للبيانات يمتد اختصاص ضباط الشرطة القضائية ليشمل كامل الإقليم الوطني.⁽³⁾، ويعدّ هذا

الاختصاص عامًا يشمل جميع ضباط الشرطة القضائية وأعوانهم، بغض النظر عن الجهة التي ينتمون إليها، سواء كانت الدرك أو الشرطة أو الأمن العسكري⁽⁴⁾.

إنّ الهدف من إجراء المعاينة هو ضبط وسائل الجريمة أو ما نتج عنها، حيث تتم المعاينة في الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ضمن بيئة الحاسوب. ويجب أن يتعامل مع هذه البيئة أعوان ذوو كفاءة علمية وخبرة فنية في مجال الحاسوب واسترجاع المعلومات، لتتمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة قابلة للقراءة أو الحفاظ عليها لحين القيام بأعمال الخبرة دون إتلافها. أما الخبرة، فهي "مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته حول المسائل التي تحتاج إلى معرفة فنية أو دراية علمية لا تتوفر لديه".⁽⁵⁾

الفرع الثاني: إجراءات التحري الخاصة.

يُعرف التحري أنّه "مجموعة من الإجراءات الأولية التي يبدأ أعوان الضبطية القضائية في تنفيذها فور علمهم بارتكاب الجريمة، والتي تتضمن البحث عن الأدلة والقرائن التي تهدف إلى إثبات وقوع الجريمة".⁽⁶⁾

في إطار مكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، وبموجب القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية، تم توسيع اختصاص النيابة العامة في مجال البحث والتحري عن الجرائم من خلال منحها الإذن بالتفتيش للقيام باعتراض المراسلات، تسجيل الأصوات، والنقاط الصور، حيث نصّت المادة 65 مكرر 05 من قانون الإجراءات الجزائية على إجراءات التحري الخاصة التي تشمل:

أولاً: اعتراض المراسلات وتسجيل الأصوات والنقاط الصور.

القانون لقاضي التحقيق إصدار أمر إلى ضابط الشرطة القضائية، بموافقة كتابية وتحت إشرافه المباشر، للقيام باعتراض المراسلات التي تتم عبر وسائل الاتصال السلكية واللاسلكية، كما يحقّ له اتّخاذ التدابير التقنية اللازمة دون الحاجة لموافقة الشخص المعني، بهدف النقاط وتثبيت وبثّ وتسجيل الصوت والصّور لأي شخص في الأماكن العامة أو الخاصة، حتّى وإن كان ذلك يتعارض مع الحقّ في الخصوصية.

1- تعريف اعتراض المراسلات: يُعرف بأنه: "إجراء تحقيقي يُنفذ خلصة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية وفقًا للإجراءات القانونية المحددة"⁽⁷⁾، وقد حصر المشرع الجزائري اعتراض المراسلات في المعاملات التي تتم عبر وسائل الاتصال السلكية واللاسلكية، دون المراسلات التقليدية، نظرًا لأن غالبية الجرائم تُرتكب باستخدام هذه الوسائل المتطورة.

يشير هذا الإجراء إلى مراقبة الاتصالات الإلكترونية أثناء بثّها، وليس إلى الحصول على الاتصالات الإلكترونية المخزنة. وقد قام المشرع الجزائري باستحداث هذا الإجراء بموجب القانون رقم: 09-04 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، حيث حدّد الحالات التي يستوجب فيها اللجوء إلى المراقبة الإلكترونية، مثل الأفعال التي تُصنّف كجرائم إرهاب أو تخريب، أو الجرائم التي تمس بأمن

الدولة، أو في حال وجود معلومات تشير إلى تهديد محتمل للمنظومة المعلوماتية بما يعرض النظام العام أو مؤسسات الدولة للخطر، أو في سياق تنفيذ طلبات التعاون القضائي الدولي، أو لأغراض التحريات والتحقيقات القضائية، وذلك وفقاً للمادة 04 من القانون رقم 09-04.

تترتب على المراقبة السرية للاتصالات بشكل عام، بما في ذلك الاتصالات الإلكترونية، غالباً عملية تسجيل محتوى تلك الاتصالات وتخزينها على وسائط مادية قابلة للنقل لاستخدامها لاحقاً لإثبات الجريمة المرتكبة، ويختلف نوع التسجيل بناءً على نوع الاتصال المراقب؛ ففي حالة الاتصال الصوتي فقط يكون التسجيل صوتياً فقط، بينما إذا كان الاتصال يتضمن صوتاً وصورة يتم التسجيل بشكل صوتي مرئي، ومن المهم أيضاً الإشارة إلى أن المراقبة السرية للاتصالات الإلكترونية، بما في ذلك المحادثات الهاتفية، لا تُعتبر نوعاً من التفتيش، فالمراقبة الإلكترونية تتعلق بالبيانات الإلكترونية المتحركة (الاتصالات أثناء إجرائها)، بينما التفتيش يتعلق بالبيانات الإلكترونية الساكنة أو المخزنة (الاتصالات التي تمت وتم تخزينها)، وتتم عملية المراقبة في جميع الحالات بناءً على إذن مكتوب من السلطة القضائية المختصة وفقاً للمادة 04 من القانون رقم 09-04 التي أشارت أنه لا يمكن إجراء عمليات المراقبة في الحالات المذكورة أعلاه، إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة.⁽⁸⁾

2-تعريف تسجيل الأصوات: يعرّف تسجيل الأصوات بأنه: "النقل المباشر والآلي للموجات الصوتية من مصادرها بسمياتها الفردية إلى شريط التسجيل لحفظ الإشارات الكهربائية".⁽⁹⁾

3-تعريف التقاط الصور: يتمثل في التقاط صورة لشخص أو عدة أشخاص في الوضعية التي يتواجدون فيها في مكان معين، سواء كان عاماً أو خاصاً، دون موافقتهم، بهدف استخدامها كأدلة إثبات.

ثانياً: التسرب.

عالج المشرع الجزائري مسألة التسرب كوسيلة خاصة للتحري في نص المادة 65 مكرر 11 من قانون الإجراءات الجزائية، حيث استخدم مصطلح "الاختراق" في القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته، وتحديداً في المادة 56 منه.

1-تعريف التسرب: يعرف التسرب وفقاً للمادة 65 مكرر 12 من قانون الإجراءات الجزائية بأنه: "قيام ضابط أو عون الشرطة القضائية، تحت إشراف ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة من خلال إيهامهم بأنه فاعل معهم أو شريك لهم أو خاف".

2-شروط صحة التسرب: إذا اقتضت ضرورة التحري أو التحقيق في إحدى الجرائم المنصوص عليها في المادة 65 مكرر 05، يصدر إذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، على أن يكون الإذن مكتوباً ومسبباً، ويتضمن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة المعني به، كما يتم تحديد مدة عملية التسرب التي لا يجوز أن تتجاوز أربعة أشهر، مع إمكانية تجديدها، وهذا الإجراء أشارت إليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية.

المطلب الثاني: الإجراءات الواردة في القانون رقم 09-04.

إلى جانب الإجراءات العامة المنصوص عليها في قانون الإجراءات الجزائية، تضمن القانون رقم 09-04 مجموعة من الإجراءات الخاصة التي تتميز بخصوصية فريدة في التعامل مع الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.

الفرع الأول: تفتيش المنظومة المعلوماتية.

التفتيش هو أحد إجراءات التحقيق التي ينفذها موظف مختص وفقاً لما تنص عليه القوانين المعمول بها⁽¹⁰⁾، ويتم في مكان يتمتع بحصانة قانونية بغرض العثور على أدلة مادية تتعلق بجناية أو جنحة، بهدف التأكد من وقوع الجريمة وإثباتها أو ربطها بالمتهم.⁽¹¹⁾ هذا الإجراء يخضع لمجموعة من القيود التي يجب الالتزام بها لضمان سلامة العملية وتحقيق العدالة، وتشمل ما يلي:⁽¹²⁾

- أن يتم التحقيق بواسطة ضابط شرطة قضائية، أو بحضوره وتحت إشرافه، وفقاً لما تنص عليه المادة 15 من قانون الإجراءات الجزائية.
- أن يكون لدى الضابط إذن مسبق من الجهة القضائية المختصة.
- أن يمارس الإجراء خلال الفترة الزمنية التي يحددها القانون.⁽¹³⁾
- فيما يخص الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال، نجد أن المادة 05 من القانون 09-04 أشارت إلى إمكانية القيام بعمليات التفتيش، وفقاً لأحكام قانون الإجراءات الجزائية سواء بالحضور الميداني أو عن بُعد من طرف السلطات القضائية المختصة، وكذلك ضباط الشرطة القضائية، وفي الحالات المنصوص عليها في المادة 04 من نفس القانون، وذلك على النحو التالي:
- الوصول إلى منظومة معلوماتية أو أي جزء منها، بالإضافة إلى المعطيات المعلوماتية المخزنة فيها.
- تفتيش منظومة تخزين معلوماتية.

محل التفتيش في هذه الحالات يشمل نظام المعالجة الآلية للمعطيات بجميع مكوناته، سواء المادية أو المعنوية⁽¹⁴⁾، كما تحدد المادة السالفة الذكر الظروف التي تستدعي إجراء مثل هذا النوع من التفتيش. حسب الفقرة الثالثة من المادة 05 في من نفس القانون، فإنه في حال تبين أن البيانات المطلوبة، والتي يمكن الوصول إليها من المنظومة الأولى، مخزنة في منظومة معلوماتية خارج حدود الإقليم الوطني، فإن الحصول عليها يتم بالتعاون مع السلطات الأجنبية المختصة، وذلك وفقاً للاتفاقيات الدولية ذات الصلة وبما يتماشى مع مبدأ المعاملة بالمثل. كما أكدت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أهمية تفتيش البيانات المخزنة ضمن هذا السياق.⁽¹⁵⁾

الفرع الثاني: حجز المعطيات المعلوماتية.

نصت الفقرة الثانية من المادة 84 من قانون الإجراءات الجزائية على قواعد تنظيم حجز الأشياء ذات الأهمية للتحقيق، ووفقاً لهذه المادة يتعين فوراً جرد جميع الوثائق والأدلة المضبوطة ووضعها في أحرار

مختومة لضمان سلامتها، وفي سياق الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال، تشمل المحجوزات نوعين:⁽¹⁶⁾

- **دعائم مادية:** مثل الأقراص المضغوطة، مفاتيح تخزين (FlashDisk USB)، والهواتف النقالة، ويتم وضعها في أحرار مختومة للحفاظ عليها.

- **دعائم معنوية:** تتعلق بالمعلومات والبيانات الرقمية ذات الصلة بالجريمة.

يهدف هذا الإجراء إلى ضمان نزاهة الأدلة وسلامتها للاستخدام في التحقيقات.

حدد القانون السالف الذكر في مادته 06 الآليات الخاصة بحجز المعطيات المعلوماتية، وقد تبني المشرع طريقتين أساسيتين لهذا الغرض:

- **نسخ المعطيات الرقمية:** يتم نسخ البيانات الموجودة على كافة وسائل التخزين الرقمية لضمان الحفاظ على الأدلة.

- **منع الوصول إلى المعطيات:** يشمل هذا الإجراء منع الوصول إلى البيانات المخزنة داخل المنظومة المعلوماتية، وكذلك حظر نسخ تلك البيانات، بهدف حماية سلامتها وضمان عدم التلاعب بها. تسهم هذه الأساليب في تعزيز فاعلية الإجراءات التحقيقية وضمان سلامة الأدلة الرقمية.

الفرع الثالث: مراقبة الاتصالات الإلكترونية.

يشير هذا الإجراء إلى مراقبة الاتصالات الإلكترونية أثناء بثها، وليس إلى الحصول على الرسائل الإلكترونية المخزنة⁽¹⁷⁾، وقد أدخل المشرع الجزائري هذا الإجراء بموجب المادة 04 من القانون 09-04. يتم اللجوء إلى هذا الإجراء في الحالات التالية:

- الأفعال التي تُصنف كجرائم إرهابية أو الجرائم التي تهدد أمن الدولة.

- وجود معلومات تشير إلى احتمال حدوث هجوم على نظام معلوماتي قد يُهدد النظام العام أو مؤسسات الدولة أو الاقتصاد الوطني.

- لأغراض التحقيقات والتحريات القضائية عندما يصعب الوصول إلى نتائج مهمة للأبحاث الجارية دون استخدام المراقبة الإلكترونية.

- في إطار تنفيذ طلبات التعاون القضائي الدولي المتبادل.

تخضع هذه الإجراءات للأحكام العامة الواردة في قانون الإجراءات الجزائية، خاصة تلك المتعلقة باعتراض المراسلات وتسجيل الأصوات والنقاط الصور، ولصحة تنفيذ هذا الإجراء، يجب الحصول على إذن مكتوب من القاضي المختص الذي تُنفذ العملية تحت إشرافه المباشر، كما يجب أن تتم مراقبة الاتصالات الإلكترونية دون علم الأشخاص المعنيين بها، ودون المساس بسرية المراسلات المقررة في قانون الإجراءات الجزائية، وحسب المادة 05 الفقرة 04 من هذا القانون، يجوز للسلطة المعنية بالتفتيش تكليف أي موظف مؤهل من جهة عامة أو خاصة تعمل في مجال الاتصالات السلكية واللاسلكية لتنفيذ المراقبة.

المبحث الثاني: إثبات الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.

يمكن القول أنه مع ظهور شبكة الإنترنت وانتشار النظم المعلوماتية الحديثة، نشأت تحديات جديدة لم تكن موجودة من قبل أمام القانون الجنائي، سواء من الناحية الموضوعية أو الإجرائية فعلى المستوى الموضوعي، ظهرت ما يعرف بالجرائم المعلوماتية، بينما على المستوى الإجرائي، أصبح جوهر إثبات هذه الجرائم يعتمد على الأدلة الجنائية الرقمية، ويتميز الدليل الجنائي الرقمي بعدة خصائص تجعله مختلفاً عن الأدلة التقليدية؛ فهو دليل علمي ذو طابع تقني يصعب محوه أو إتلافه، كما يمكن نسخه بسهولة.

أما فيما يتعلق بحجية هذا الدليل، فإن القاضي الجنائي يتمتع بسلطة تقديرية واسعة في قبوله، ولقبول هذا الدليل يجب توافر عدة شروط من أبرزها: مشروعيته وبلوغ اقتناع القاضي لدرجة اليقين، بالإضافة إلى ضرورة مناقشة هذا الدليل بشكل دقيق، وتحدد سلطة القاضي الجنائي في قبول الأدلة الجنائية الرقمية وفقاً لطبيعة النظام القانوني المعمول به، فمثلاً في النظام اللاتيني الذي يُعرف بنظام الإثبات الحر يتمتع القاضي بمرونة أكبر في تقييم الأدلة، أما في النظام الأنجلو ساكسوني الذي يُسمى بنظام الإثبات المقيد، فإنّ القبول يخضع لقيود وشروط أكثر تحديداً.

يُعتبر الدليل الجنائي أساساً للإثبات ووسيلة لإثبات الواقعة الإجرامية أو نفيها عن المتهم، مما يجعله بالغ الأهمية في جميع مراحل الدعوى، ويمثل الدليل الجنائي الرقمي كلّ وسيلة قانونية معترف بها لإثبات وجود أو عدم وجود الواقعة المرتكبة أو صحة أو كذب وقوعها.⁽¹⁸⁾

يهدف الدليل الجنائي إلى تحقيق الإثبات، ومفاده إقامة الدليل لدى السلطات المختصة بالتحري في المسائل الجنائية لأجل القيام بإثبات واقعة تتعلق بأشخاص ترتبط بهم، باستخدام الطرق المحددة وفقاً للقانون.⁽¹⁹⁾

ومع التقدم العلمي والتكنولوجي، ظهرت الأنظمة المعلوماتية التي تتضمن قواعد بيانات وبرامج ومعلومات متطورة، وانتشرت لتشمل شريحة كبيرة من الأفراد بفضل الشبكات المعلوماتية، وما حققته من مزايا كبيرة على مختلف الأصعدة الثقافية والعلمية والسياسية، إلا أن هذا التوسع قد فتح أيضاً المجال لمخاطر كبيرة، حيث أصبح النظام المعلوماتي وسيلة لارتكاب ما يُعرف بالجرائم المعلوماتية.⁽²⁰⁾

تعتبر الجرائم المعلوماتية نوعاً جديداً من الجرائم نظراً لارتباطها بتقنيات حديثة، مثل تكنولوجيا المعلومات والاتصالات، مما أدى إلى ظهور نوع جديد من المجرمين، وتحولت الجريمة من صور تقليدية إلى أخرى إلكترونية حديثة ولهذا كان من الضروري أن يتطور الدليل الجنائي من صورته التقليدية إلى الرقمية، في حين أن الدليل الجنائي التقليدي يشترط لقبوله أمام القضاء أن يكون صريحاً ومباشراً ويُدلّل بذاته على الواقعة المراد إثباتها، كما أنّ الدليل الجنائي الرقمي أيضاً يجب أن يتسم بخصائص معينة ليتم قبوله أمام القضاء.

في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال يمكن حصر وسائل الإثبات في الدليل الرقمي، نظراً للطابع التقني لهذه الجرائم والتي لا يمكن إثباتها إلا بالدليل العلمي القاطع الذي يمكن للخبير أن يستنتج في المجال المعلوماتي، بناءً على ما سبق سنتناول في هذا المبحث ماهية الدليل التقني في (المطلب الأول)، بينما نُخصص (المطلب الثاني) للحديث عن مشروعية الدليل التقني وحجّيته.

المطلب الأول: ماهية الدليل التقني.

تعتمد عملية الإثبات في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال على الدليل الإلكتروني كوسيلة أساسية لإثبات هذه الجرائم، لهذا سنحاول أن سنعرض من خلال هذا المطلب، أولاً تعريف الدليل الجنائي الرقمي، ثم نتناول خصائصه ثانياً.

الفرع الأول: مفهوم الدليل الرقمي.

لقد تعدّدت التعاريف المتعلقة بالدليل الرقمي أو الإلكتروني، حيث تفاوتت بين توسيع مفهومه وتحديدّه بشكل ضيق، فنجد أنّ المنظمة العالمية لدليل الكمبيوتر (IOCE) عرّفته في أكتوبر 2001 على أنّه: "المعلومات ذات القيمة المحتملة، المخزنة أو المنقولة في شكل رقمي".⁽²¹⁾

يعرف الدليل على أنّه: "ذلك الدليل المستند للمنطق والعقل في إطار الشرعية الإجرائية بهدف إثبات صحّة افتراض معيّن أو رفع درجة اليقين الإقناعي بشأن واقعة ما محل خلاف".⁽²²⁾

كما يرى البعض بأنّه: "الدليل المأخوذ من أجهزة الحاسب الآلي والذي يتخذ شكل مجلّات أو نبضات مغناطيسية أو كهربائية، يمكن جمعها وتحليلها باستخدام برامج وتطبيقات وتقنيات خاصّة، ثم تقديمها في صورة دليل يمكن قبوله أمام القضاء".⁽²³⁾ كما عرّفه آخرون بأنّه: "الدليل الذي يستند إلى أساس في العالم الافتراضي ويقود إلى الجريمة".⁽²⁴⁾ وفي تعريف آخر، ذكر الدكتور مصطفى محمد بأنّه: "المعلومات المخزنة أو المنقولة بشكل رقمي، والتي يعتمد عليها في التحقيقات وأمام المحكمة سواء للإدانة أو البراءة".⁽²⁵⁾

الفرع الثاني: خصائص الدليل الرقمي.

يتّسم الدليل الجنائي الرّقمي بعدة خصائص تميّزه عن غيره من الأدلة الجنائية، فهو دليل علمي غير مرئي، ذو طبيعة تقنية، يصعب التخلّص منه، ويُعدّ قابلاً للنسخ، كما هو موضّح فيما يلي:

أولاً: دليل غير مرئي.

يتكون الدليل الرقمي من بيانات ومعلومات ذات طبيعة إلكترونية غير ملموسة، ويعتمد إدراكه على استخدام أجهزة ومعدات الحاسب الآلي (Hardware) ونظم البرمجيات الخاصّة (Software).

ثانيًا: الدليل الرقمي كدليل علمي.

ينطبق على الدليل الرقمي ما ينطبق على الأدلة العلمية، فهو يخضع لقواعد تضمن توافقه مع الحقيقة الكاملة، وفقًا للعدالة في القانونية، حيث يسعى القانون لتحقيق العدالة بينما يسعى العلم للوصول إلى الحقيقة.⁽²⁶⁾

ثالثًا: الدليل الرقمي من طبيعة تقنية.

تتميز الطبيعة التقنية للدليل الرقمي بخصائص تجعله يختلف عن الأدلة التقليدية، من أبرزها قابليته للنسخ، مما يشكل ضماناً فعّالاً للحفاظ عليه ضد الفقد أو التلف أو التغيير.⁽²⁷⁾

رابعًا: الدليل الرقمي هو دليل متنوع متطور.

يشمل الدليل الرقمي جميع أشكال وأنواع البيانات الرقمية القابلة للتداول، بحيث تكون هناك علاقة خاصة تربط بين هذه البيانات والجريمة المرتكبة. وتعني هذه الخاصية أنه على الرغم من أن الدليل الرقمي يتميز بتوحيد تكوينه بلغة الحوسبة والرقمية، إلا أنه يمكن أن يظهر في أشكال متعددة.⁽²⁸⁾

خامسًا: صعوبة التخلص من الدليل الرقمي.

حتى في حالة إصدار الجاني أمرًا بإزالته، فإن إمكانية استرجاعه تظل قائمة من خلال استخدام برامج استرجاع البيانات.

الفرع الثالث: أشكال الدليل الرقمي.

يتم تقسيم الدليل الرقمي إلى نوعين رئيسيين:

- **الدليل الرقمي الأصلي**، والذي يتكون من العناصر المادية أو الحسية، بالإضافة إلى المستندات البيانية المرتبطة بهذه العناصر عند حجزها.
- **الدليل الرقمي المكرر**، وهو نسخة رقمية دقيقة لكافة المستندات البيانية التي يحتوي عليها الدليل الرقمي الأصلي.⁽²⁹⁾

أولًا: الصورة الرقمية.

هي تمثيل للحقائق المرتبطة بالجريمة، وعادة ما تُعرض الصورة إما في شكل ورقي أو بصيغة مرئية.⁽³⁰⁾

ثانيًا: التسجيلات الصوتية:

تتمثل في التسجيلات التي تُحفظ وتُخزن بواسطة الأجهزة الرقمية، وتشمل المحادثات الصوتية التي تتم عبر الإنترنت.⁽³¹⁾

ثالثًا: النصوص المكتوبة.

تشمل النصوص التي تم إنشاؤها باستخدام الأجهزة الرقمية، مثل الرسائل الإلكترونية والبيانات المسجلة على أجهزة الحاسب الآلي.

المطلب الثاني: مشروعية الدليل التقني وحجّيته.

تعد حرية الإثبات من المبادئ الأساسية والمستقرة في نظرية الإثبات الجنائي، لذلك نجد أن المشرع أقر هذا المبدأ بموجب المادة 12 من قانون الإجراءات الجزائية.

الفرع الأول: مشروعية طريقة الحصول على الدليل التقني.

وفقاً لمبدأ المشروعية الذي ينظم قواعد الإثبات في النظام الجزائي، فإن الدليل الجنائي، بما في ذلك الأدلة المستخلصة من الوسائل الإلكترونية، لا يعد مشروعاً إلا إذا تمّ جمعه أو الحصول عليه وتقديمه أمام القضاء وفقاً للإجراءات القانونية التي تضمن تحقيق توازن عادل ودقيق بين حق الدولة في فرض العقوبات وحق المتهم في الحصول على الضمانات الكافية لحماية كرامته الإنسانية.⁽³²⁾

أولاً: مشكلة المصلحة الأولى بالرعاية.

تتمثل هذه المشكلة في حالة يكون فيها الدليل الإلكتروني غير مشروع نتيجة التعدي على حرمة الحياة الخاصة من جهة، وفي الوقت ذاته يعد وسيلة لإثبات جرائم تهدد الأمن الاجتماعي والأخلاقي. ومن الضروري هنا النظر في مدى خطورة هذا العدوان أو المساس بالنظام الاجتماعي، إذ لا يمكن استبعاد أي وسيلة لمجرد مخالفتها للقواعد العامة دون دراسة معمقة لأثرها على المجتمع.⁽³³⁾

ثانياً: قيمة الدليل غير المشروع.

نميز هنا بين نوعين من الأدلة، أدلة الإدانة، وأدلة البراءة.

1- بالنسبة لدليل الإدانة: استناداً إلى قرينة البراءة المرتبطة بالمتهم، يجب أن تستند أحكام الإدانة إلى أدلة مشروعة. وبالتالي، يُبطل أي دليل يتم الحصول عليه بطريقة غير مشروعة، بما في ذلك الدليل الإلكتروني.⁽³⁴⁾ وفي هذا السياق، أشارت المادة 191 على أن غرفة الاتهام تتولّى فحص صحة الإجراءات المرفوعة إليها، وإذا تبين لها وجود سبب من أسباب البطلان، تصدر حكماً ببطلان الإجراء المشوب بهذا السبب، وعند الحاجة، تبطل الإجراءات اللاحقة له جزئياً أو كلياً، وبعد الإبطال يحق لها إما التصدي مباشرة لموضوع الإجراء أو إحالة الملف إلى قاضي التحقيق نفسه أو إلى قاضٍ آخر لمواصلة إجراءات التحقيق.

2- بالنسبة لدليل البراءة: لقد اختلف حول اشتراط المشروعية في دليل البراءة بشكل عام، ويمكن تصنيف هذا الاختلاف إلى ثلاثة اتجاهات:⁽³⁵⁾

- **الاتجاه الأول:** يعتبر المشروعية شرطاً أساسياً لكل دليل.
- **الاتجاه الثاني:** يقتصر اشتراط المشروعية على دليل الإدانة فقط.
- **الاتجاه الثالث:** يميز بين ما إذا كانت طريقة الحصول على الدليل غير المشروعة تشكل جريمة من عدمه.

ويُرجح الاتجاه الثاني لعدة اعتبارات نوجزها كما يلي:⁽³⁶⁾

- القاعدة العامة هي افتراض البراءة في حق المتهم، وبالتالي يجب قبول أي دليل يسهم في تأكيد هذه القاعدة دون النظر إلى اعتبارات أخرى.
- إن قيد المشروعية يعد بمثابة ضمان لحقوق الدفاع، مما يستدعي تقييد هذا الشرط فقط على دليل الإدانة الذي يؤثر في حق الدفاع، في حين أن قيد البراءة لا يخضع لهذا القيد.
- كما أن العدالة لا تتأثر سلباً إذا تم الإفراج عن مجرم استناداً إلى دليل غير مشروع، بقدر ما تتضرر إذا تم إدانة بريء.

الفرع الثاني: حجية الدليل الإلكتروني.

تعد مسألة تقييم الدليل الجنائي مسألة ذات طابع موضوعي بحت، حيث يخول القانون القاضي سلطة تقديرية واسعة في قبول الدليل وتحديد قيمته القانونية.

أولاً: شروط قبول الدليل الرقمي.

- يُعد الدليل الرقمي دليلاً علمياً يتسم بالموضوعية والحياد والكفاءة. ولضمان قربه من الحقيقة وقبوله كدليل في الإثبات الجزائي، يجب أن تتوافر فيه مجموعة من الشروط الأساسية، تشمل:⁽³⁷⁾
- ضرورة أن تكون الأدلة قاطعة وخالية من أي شك.
 - تقييم الدليل الرقمي من حيث سلامة الإجراءات الفنية المتبعة في جمعه.
 - ضرورة مناقشة الأدلة الرقمية المستخلصة من أجهزة الحاسوب بشكل دقيق.

ثانياً: تقدير القاضي الجزائي للدليل الرقمي.

نظراً لأن الدليل الرقمي يُعد أحد تطبيقات الدليل العلمي، فلا يمكن للطرف الآخر التشكيك في قوته الاستدلالية، حيث إنه يستند إلى أسس علمية مؤكدة. وبالتالي، إذا توافرت في الدليل التقني الشروط المتعلقة بسلامته من التلاعب أو الخطأ، فإنه لا يجوز رفضه بناءً على السلطة التقديرية للقاضي، وفقاً للمادة 307 من قانون الإجراءات الجزائية الجزائري.⁽³⁸⁾

ويبقى دور القاضي يقتصر على تقدير الظروف والملابسات المحيطة بالدليل، حيث يقع ضمن نطاق تقديره الشخصي. ورغم أن الدليل الرقمي يعد قاطعاً من الناحية العلمية، إلا أنه يمكن للقاضي رفضه إذا تولد لديه شك في عدم توافقه مع ظروف الواقعة وملابساتها. فمجرد توافر الدليل العلمي لا يعني بالضرورة أن القاضي ملزم بالحكم بناءً عليه مباشرة، سواء بالإدانة أو البراءة، دون أن يتم التحقق من الظروف والملابسات المحيطة بالواقعة.⁽³⁹⁾

خاتمة:

وفي الختام نشير إلى أن المشرع الجزائري يُعتبر من بين الأوائل الذين قاموا بتحديد مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، الذي يعكس الجرائم المتعلقة بأنظمة معالجة المعطيات الإلكترونية والجرائم التي ترتكب عبر المنظومات المعلوماتية أو أنظمة الاتصال الإلكتروني. وقد انفرد المشرع الجزائري

بهذا المصطلح، في حين اعتمدت التشريعات المقارنة مصطلح "الجريمة المعلوماتية"، تتميز هذه الجرائم بطابع خاص نظراً لارتكابها في فضاء افتراضي داخل نظام معلوماتي يشمل مكونات مادية ومعنوية، قد تصبح إما هدفاً للجريمة أو أداة لارتكابها. هذا الواقع الافتراضي منح هذه الجرائم خصوصية كبيرة أثرت على طبيعة الأفعال الإجرامية محل التحقيق، وكذلك على الإجراءات اللازمة لمتابعتها.

وفي إطار هذا البحث، سعينا جاهدين إلى دراسة الخصوصية التي تتسم بها إجراءات متابعة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال من خلال مبحثين رئيسيين. وبالرجوع إلى الانتشار الواسع للجرائم الإلكترونية عبر الأنظمة المعلوماتية وما تشكله من تهديدات للأفراد والمجتمع على حد سواء، أصبح من الضروري تدخل المشرع الجزائري لضبط هذه الظاهرة، لا سيما في ظل الاستخدام المكثف للتقنيات الحديثة في جميع القطاعات. وبلاستجابة لهذه الحاجة، قام المشرع بتعديل قانون 15/04 وصياغة القانون رقم 04/09 بما يتماشى مع الظاهرة المستجدة، وهو ما تناولناه بالتفصيل في هذا البحث.

قد خصصنا المبحث الأول لدراسة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال من خلال تناول الإجراءات الخاصة بمتابعتها في نفس هذا القانون السالف الذكر وقانون الإجراءات الجزائية، كما خصصنا المبحث الثاني لدراسة كيفية إثبات هذه الجرائم عبر الدليل التقني، وناقشنا مشروعية هذا الدليل وحجيته، وفي الختام، توصلنا إلى مجموعة من النتائج التي يمكن تلخيصها على النحو التالي:

1- يشترط في الدليل الرقمي أن يكون مشروعاً، أي أن يتم الحصول عليه بطرق قانونية. ورغم أن الدليل العلمي يتمتع بقيمة علمية قاطعة في دلالة الحقائق، إلا أنه لا يخرج عن مبدأ حرية القاضي الجزائي في تقدير الإثبات.

2- يتطلب التصدي لجرائم تكنولوجيات الإعلام والاتصال تنسيقاً دولياً، وذلك باعتبار هذه الجرائم سريعة التطور وعابرة للحدود.

3- قام المشرع الجزائري بمكافحة الجريمة الإلكترونية مماثلاً بذلك باقي الدول، من خلال تعديل قانون 15-04، حيث اعتبر دخول النظام المعلوماتي بطريقة غير مشروعة، والمساس بمنظوماته، وعدد من الأفعال الأخرى أفعالاً إجرامية وعقابها، كما استدرك النقص في المجال الإجرائي بإصدار قانون رقم 04-09، الذي تضمن قواعد إجرائية وقائية، وهو خطوة إيجابية، لكنها تظل غير كافية لمكافحة الجريمة الإلكترونية بكفاءة.

4- لم يحدد المشرع الجزائري بشكل دقيق الجريمة المرتكبة باستخدام النظام المعلوماتي، ما يتيح مجالاً واسعاً لاستيعاب كافة الأفعال الناتجة عن تطورات التقنية الحديثة. وفي ضوء هذه النتائج، نوصي بالتالي:

1- ضرورة تشديد الوصف الجزائي والعقوبات المقررة لأنماط الإجرامية المرتبطة بالجريمة المعلوماتية، بهدف تحقيق الردع الفعال والقضاء على الجرائم المعلوماتية.

- 2- الاستفادة من التجارب الدولية في هذا المجال، لتطوير المهارات اللازمة لمكافحة الجريمة الإلكترونية.
- 3- الاستعانة بالمختصين والخبراء لضبط الجرائم الإلكترونية، وتكوين فرق من الضبطية القضائية والقضاة المتخصصين، مع توفير كافة الوسائل المادية والتقنية اللازمة لضمان نجاح هذه المهام.

الهوامش

- ¹- عبد الله دغش العجمي، "المشكلات العملية والقانونية للجرائم الإلكترونية"، دراسة مقارنة، رسالة مكملة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص 77.
- ²- عبد الفتاح بيومي حجازي، "الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت"، دار الكتب القانونية، د.ط، مصر، 2002، ص ص 20-21.
- ³- المادة 16 الفقرة 07 من القانون رقم 06-22، مؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 ديسمبر 2006، يعدل ويتم الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 08 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ص ص 04-05.
- ⁴- عبد الله أوهابيه، شرح قانون الإجراءات الجزائية، دار هومة، د.ط، الجزائر، 2008، ص 222.
- ⁵- عبد الله بن مسعود بن محمد السرائي، فاعلية الأساليب المستحدثة في إثبات جريمة التزوير المعلوماتي، دار الثقافة للنشر والتوزيع الطبعة الأولى، اليمن، ص 96.
- ⁶- محمد محدة، ضمانات المشتبه فيه أثناء التحريات الأولى، دار الهدى، الطبعة الثانية، الجزائر، 1991-1992، ص 22.
- ⁷- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، دار المطبوعات الجامعية، الطبعة الأولى، مصر، 2009، ص 150.
- ⁸- القانون رقم 09-04 مؤرخ في 14 شعبان 1430 هـ، الموافق لـ 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر عدد 47، مؤرخة في 16 غشت 2009، ص 06.
- ⁹- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، دار المطبوعات الجامعية، الطبعة الأولى، مصر، 2009، ص 153.
- ¹⁰- الأمر رقم 66-156، المؤرخ في 08 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المادة 45، ص 19.
- ¹¹- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار النهضة العربية الطبعة الأولى، مصر، د.ذ.س، ص 192.
- ¹²- عبد الله أوهابيه، شرح قانون الإجراءات الجزائية، دار هومة، د.ط، الجزائر، 2008، ص 269.
- ¹³- أنظر المادة 47 فقرة 01، قانون الإجراءات الجزائية.
- ¹⁴- رشيدة بوكري، جرائم الاعتداء على نظام المعالجة الآلية، منشورات الحلبي الحقوقية، الطبعة الأولى، لبنان، 2012، ص 396.
- ¹⁵- المادة 26 من المرسوم الرئاسي رقم 14-252، المؤرخ في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة، بتاريخ 11 ديسمبر 2010، ج.ر عدد 57، صادرة في 28 سبتمبر 2014.

- 16- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة لنيل شهادة الماجستير، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2012-2013، ص 94.
- 17- أحمد مسعود مريم، نفس المرجع، ص 94.
- 18- طه أحمد طه متولي، الدليل العلمي وأثره في الإثبات الجنائي، رسالة للحصول على درجة الدكتوراه في الحقوق، جامعة طنطا، 2007، ص 10.
- 19- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، ط 1، الإسكندرية، 2009، ص 177.
- 20- قارة أمال، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون، كلية الحقوق بن عكنون، 2002، ص 17.
- 21- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، ط 1، القاهرة، 2008، ص 213.
- 22- منصور عبد المعايطة، الأدلة الجنائية والتحقيق الجنائي، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2009، ص 27.
- 23- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، د.ط، مصر، 2006، ص 88.
- 24- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس، 2004، ص 969.
- 25- مصطفى محمد موسى، نفس المرجع السابق، ص 217.
- 26- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013، ص 122.
- 27- سعيداني نعيم، نفس المرجع السابق، ص 123.
- 28- سعيداني نعيم، نفس المرجع، ص 124.
- 29- ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول TCP/IP، في بحث وتحقيق الجرائم على الكمبيوتر، بحث منشور على الصفحة 08، الموقع: <http://www.info.com>، تاريخ الزيارة 07 أفريل 2023، 10:30.
- 30- سعيداني نعيم، المرجع السابق، ص 127.
- 31- سعيداني نعيم، نفس المرجع السابق، ص 128.
- 32- رشيدة بوكري، جرائم الاعتداء على نظام المعالجة الآلية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012، ص 489.
- 33- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، د.ط، مصر، 2010، ص 216.
- 34- عائشة بن قارة مصطفى، نفس المرجع، ص 218.
- 35- أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، د.ط، مصر، 2015، ص 209.
- 36- عائشة بن قارة مصطفى، مرجع سابق، ص 221.
- 37- سعيداني نعيم، مرجع السابق، ص 214.
- 38- الأمر رقم 66-156، المتضمن قانون الإجراءات الجزائية، مرجع السابق، ص 72، 88.
- 39- جميل عبد القادر الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، د.ط، دار النهضة العربية، القاهرة، 2002، ص 22.