Arab Journal of Forensic Sciences and Forensic Medicine 2022; Volume 4 Issue (2), **-**

Naif Arab University for Security Sciences
Arab Journal of Forensic Sciences and Forensic Medicine
المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي
https://journals.nauss.edu.sa/index.php/AJFSFM

Procedural Problems Facing a Criminal Investigator in Cybercrimes

المشاكل الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية

كريم معروف
قانون جنائي وعلوم جنائية، جامعة غليزان، الجزائر

Karim Maarouf
Criminal Law and Forensic Science, Relizane University

Received 24 Jan. 2022; Accepted 15 Jun. 2022; Available Online 04 Dec. 2022

Abstract

We aim through our study of this topic to reveal the problems and difficulties facing the agencies charged with judicial investigation of crimes in cyberspace. The biggest obstacle is the availability and access of the advanced technical and scientific means and techniques that investigation bodies must follow during the course of investigation.

In addition to the impediments related to the privacy of the investigation of cyber crimes, the procedures and methods carried out by the security and judicial agencies are considered among the most complex operations facing the investigators. This includes the perpetrator encrypting and coding the computer during inspections, or the difficulty of controlling data if it is on information networks belonging to another country, or the obstacles related to subrogation judicial or extradition procedures.

Keywords: Forensic Science, investigation devices, cybercrimes, electronic evidence, search and investigation devices, criminal proof, procedural problems, information criminal.

المستخلص

نهدف من خلال دراستنا لهذا الموضوع إلى الكشف عن المشاكل والصعوبات التي تواجه الأجهزة المكلفة بالتحقيق القضائي في الجرائم التي ترتكب في الفضاء الإلكتروني؛ وذلك من خلال دراسة العراقيل التي تواجه المحققين أثناء إجراءات البحث والتحري؛ مثل: العراقيل المتعلقة بخصوصية الدليل الإلكتروني لكونها من بين أكبر العوائق التي يسعى الخبراء من خلالها للوصول إلى الطرق التي تمكن من إثباتها، ويتطلب ذلك ضرورة الاستعانة بوسائل وتقنيات فنية وعلمية متطورة يجب أن تتبعها الأجهزة الأمنية والقضائية في أثناء سير عمليات التحري.

إضافة إلى العراقيل المرتبطة بخصوصية التحقيق في الجرائم السيبرانية؛ فالإجراءات والأساليب التي تقوم بها الأجهزة المعنية بالتحقيق تعتبر من أعقد العمليات التي تواجه المحققين؛ مثل قيام الجاني بتشفير وترميز الحاسب الآلي، وهذه من بين الصعوبات المتعلقة بالتفتيش، وصعوبة ضبط البيانات إذا كانت في شبكات معلوماتية لدولة أخرى، والعراقيل المتعلقة بإجراءات الإنابة القضائية أو تسليم المجرمين.

الكلمات المفتاحية: علوم الأدلة الجنائية، أجهزة التحقيق، الجرائم السيبرانية، الدليل الإلكتروني، البحث والتحري، الإثبات الجنائي، المشاكل الإجرائية، المجرم المعلوماتي.

* Corresponding Author: Karim Maarouf
Email: karimmaarouf001@gmail.com
doi: 10.26735/NMXK4072

1. مقدمة

تعتبر عمليات البحث والتحقيق في الجرائم السيبرانية من أعقد وأصعب الإجراءات التي تتطلب استخدام تقنيات ووسائل متطورة وحديثة ومحققين ذوي خبرة وكفاءة عالية ومهارة في التعامل مع البرامج المعلوماتية والكشف عن الأدلة الإلكترونية وإثباتها، ولهذا على الجهات الأمنية والقضائية المعنية بالتحقيق استخدام تقنية المعلومات كوسيلة من وسائل ضبط الجريمة السيبرانية، ويتميز المجرم المعلوماتي بمجموعة من الصفات والمميزات تختلف اختلافًا جذريًا عن الصفات التي يتميز بها المجرم العادي والتي من بينها أنه اجتماعي وذكي يتمتع بالخبرة في مجال التقنيات الحديثة.

وتقوم الأجهزة الأمنية والقضائية عند مباشرتها لعمليات البحث والتحري من أجل الوصول إلى الدليل الجنائي في الجرائم السيبرانية بمجموعة من الإجراءات، ومن أبرز هذه الإجراءات المعاينة والتفتيش والخبرة القضائية والضبط وسماع الشهود وتسجيل ومراقبة المحادثات والاستجواب والاعتراف وغيرها من الإجراءات التي تباشرها سلطات التحقيق للوصول إلى الدليل الإلكتروني، فإجراءات الاستجواب والمواجهة وسماع الشهود تكون في مواجهة المتهم أو الضحية، وأما المعاينة والخبرة والتفتيش فهي إجراءات فنية تتعلق بالأشياء، وهي إجراءات متعلقة بالجرائم السيبرانية، وهذا ما يهمنا في دراستنا، غير أن هذه الإجراءات قد تعترضها مجموعة من العراقيل والمشاكل تحول دون تحقيق الهدف من الوصول إلى فك لغز الجريمة الإلكترونية والقبض على المجرم المعلوماتي وتقديمه للعدالة من أجل محاكمته.

وقد برز الدليل الإلكتروني في منتصف القرن التاسع عشر مع ظهور مرحلة جديدة من مرحلة الإثبات العلمي التي تعتمد على الاستخدام المشروع للوسائل العلمية الحديثة في ميدان الإثبات الجنائي، والدليل الإلكتروني من الأدلة التي أثار قبولها جدلًا واسعًا في الوسط الفقهي والقضائي، ويمتاز عن غيره بصعوبة فهمه؛ لكونه يحتاج إلى خبرة تقنية وفنية وقدرة في معالجة المعلومات والبيانات، وهو ضروري للإثبات الجنائي، وخاصة في الجرائم المعلوماتية، ومن خلاله تتحدد قدرة القاضي الجنائي في كشف الحقيقة والوصول إليها، ويعتبر الدليل الإلكتروني أو الرقمي الوسيلة الوحيدة والرئيسة في إثبات الجرائم المعلوماتية.

وعليه فإن التصدي للجرائم السيبرانية ومكافحتها يستوجب تأهيل وتدريب المكلفين بمهام البحث والتحري والتحقيق على أعلى مستوى؛ لأن أي غلط أو خطأ في أي مرحلة من مراحل التحقيق وإجراءات الضبط أو التفتيش قد تؤدي إلى ضياع فرصة كشف غموض الجريمة والفشل في معرفة الجاني الإلكتروني والتحقق من الأدلة.

أسباب اختيار الموضوع

الأسباب الذاتية التي دفعتنا للتطرق لهذا الموضوع هو الرغبة في الاطلاع على الدراسات المستحدثة المتعلقة بالجرائم التي ترتكب في الفضاء الإلكتروني ورفع الرصيد المعرفي والثقافي في هذا المجال، إضافة إلى أنه سبق وأن تطرقنا في دراسة سابقة لموضوع العراقيل الموضوعية المتعلقة بالبحث في الجرائم الإلكترونية وسنحاول في هذه الدراسة بإذن الله إتمام الدراسة المتعلقة بالعقبات والصعوبات التي تواجه المحقق الجنائي في التحقيق في هذا النوع من الجرائم بالتطرق إلى المشاكل الإجرائية.

أما الأسباب الموضوعية التي دفعتنا لاختيار هذا الموضوع فهو تصاعد حدة الجرائم السيبرانية وكثرة وقوعها في السنوات الأخيرة وقصور الأحكام والقواعد الإجرائية التقليدية في التصدي للجرائم الإلكترونية، ووجود العديد من الجرائم التي عرفت صعوبات وعراقيل في إجراءات استخلاص الدليل الإلكتروني لإدانة المجرمين بسبب الطبيعة الخاصة بإجراءات جمع الأدلة والاستدلالات الفنية والتقنية وما صاحبها من مشاكل عملية، إضافة إلى أن جرائم الحاسوب وما يقع عليها من جرائم معلوماتية تعتبر تحديًا كبيرًا للأجهزة الأمنية والقضائية المكلفة بالتحقيق فيها واستخلاص الأدلة الرقمية التي تثبت وقوعها وتدين مرتكبيها.

أهمية الموضوع

تكمن أهمية دراسة هذا الموضوع في كونه من الموضوعات التي أثارت العديد من المشاكل في نطاق قانون الإجراءات الجزائية، إضافة إلى أنه من الموضوعات المستجدة والحديثة؛ لأن الجهات المعنية بالتحقيق في الجرائم متعودة على التعامل مع الجرائم بصورها العادية التي يمكن إدراكها بالحواس من خلال ما يخلفه مرتكبوها من آثار مادية مثل: البصمات أو بقع الدماء، إضافة إلى أنه من الموضوعات التي تبدأ فيه المشاكل الإجرائية التي تواجه الأجهزة الأمنية والقضائية عند تعاملها مع الجرائم السيبرانية من طبيعة البيئة الافتراضية التي ترتكب فيها فهي لا تترك ولا تخلف أي آثار مادية ومحسوسة؛ لكونها تتم في الخفاء.

أهداف الموضوع

نهدف من خلال التطرق لهذا الموضوع محل المعالجة إلى ما يلي:

- معرفة العراقيل التي يثيرها الإثبات الجنائي في الدليل الجنائي الإلكتروني.
- معرفة الصعوبات والعراقيل المتعلقة بخصوصية التحقيق في الجرائم السيبرانية.

- المساهمة في معالجة المشاكل الإجرائية التي تثيرها الجرائم المعلوماتية أو التقليل منها.
- الوصول إلى الحلول التي يمكن من خلالها للأجهزة الأمنية والقضائية استخلاص الدليل الجنائي الإلكتروني.
- كما نأمل أن تكون لدراستنا قيمة مضافة للبحث العلمي وبداية لدراسات جديدة وحلًا من الحلول التي تمت في دراسات سابقة في مجال الجرائم السيبيرانة وإجراءات البحث والتحري والتحقيق فيها.

المنهج المستخدم

اعتمدنا في دراستنا على المنهج الوصفي التحليلي؛ وذلك من خلال وصف المشاكل المتعلقة بخصوصية الدليل الإلكتروني والأسباب التي أدت إلى وجود عقبات في استخلاص الدليل الإلكتروني مثل وصف سهولة محو الدليل الإلكتروني وصعوبة الوصول والحصول عليه، إضافة إلى تحليل المشاكل المتعلقة بخصوصية التحقيق مثل: تحليل المشاكل المتعلقة بالتفتيش والعقبات التي تواجه عملية الضبط وتحليل مشاكل التعاون الدولي التي تعترض الأجهزة الأمنية والقضائية أثناء مباشرتها للتحقيق.

الإشكالية:

الإشكالية الرئيسة التي طرحناها للدراسة:

- ما أبرز الصعوبات والعراقيل الإجرائية التي تعوق عملية التحقيق في الجرائم السيبرانية؟

أما الأسئلة الفرعية التي نسعى للإجابة عنها فهي:

- هل التصدي للجرائم السيبرانية يتطلب أحكامًا وقواعد إجرائية فقط؟ أم لا بد من سن قواعد وأحكام موضوعية حتى تتمكن الأجهزة الأمنية والقضائية من كشف الجرائم المعلوماتية وإدانة الجناة؟
- كيف يمكن معالجة المشاكل الإجرائية التي تثيرها الجرائم السيبرانية؟
- ما الضوابط التي على الأجهزة الأمنية والقضائية الالتزام بها أثناء البحث والتحري في الجرائم السيبرانية؟

للإجابة عن هذه الإشكالية الرئيسة والأسئلة الفرعية نقترح خطة دراسة ممنهجة في مطلبين على النحو التالي:

المطلب الأول: المشاكل المتعلقة بخصوصية الدليل الجنائي الإلكتروني.

المطلب الثاني: المشاكل المتعلقة بخصوصية التحقيق في الجرائم الإلكترونية.

2. المطلب الأول: المشاكل المتعلقة بخصوصية الدليل الجنائي الإلكتروني

إثبات الدليل الإلكتروني والوصول إليه من المشاكل التي تواجه الأجهزة الأمنية والقضائية المكلفة بالتحقيق، وهي من أبرز العقبات التي يسعى الخبراء إلى إيجاد وسائل لإثباتها؛ لكونها تتطلب خبرات فنية عالية، إضافة إلى أسلوب فعال ومتطور في البحث والتحري والتحقيق، وذلك لأن نوعية الأدلة في الجرائم السيبرانية تمتاز بالصعوبة في كشفها والغموض في فك ألغازها، فالمجرم الإلكتروني في غالب الأحيان لا يترك أي آثار يمكن أن تقود إلى اكتشاف أمره أو إلى إدانته؛ وذلك لأن الجريمة السيبرانية ترتكب في مسرح افتراضي.

فالمجرم المعلوماتي يحاول قدر المستطاع إعاقة المحققين للوصول إلى الدليل بشتى السبل والطرق والوسائل، ويلجأ إلى تشفير المعلومات وترميز البيانات حتى يصعِّب من عملية التحقيق، ولهذا يجب أن تكون لدى المحقق الجنائي والأجهزة الأمنية والقضائية المكلفة بالتحقيق في هذا النوع من الجرائم الدراية العلمية الشاملة والكاملة لأنظمة الحاسب الآلي.

الدليل الإلكتروني الذي تسعى الأجهزة الأمنية والقضائية إلى الوصول إليه واستخلاصه من المسرح الافتراضي الذي ترتكب فيه لا يمكن كشفه بالطرق الكلاسيكية، فهو يستمد طبيعته من نفس العمليات الرقمية، ويحتاج إلى الاستعانة بأدوات ووسائل وتقنيات علمية متطورة تتبعها الأجهزة الأمنية والقضائية في إجراءات البحث والتحري والتحقيق في الجرائم السيبرانية.

وتتمثل هذه الخصوصية في كون الأدلة الرقمية أدلةً غير مرئية وتخلف آثارًا إلكترونية، إضافة إلى سهولة محوها وصعوبة الوصول إليها وصعوبة فهمها وسنتناول في هذا المطلب، الأدلة الرقمية، وهي أدلة غير مرئية، وجرائم تخلف آثارًا إلكترونية، مع سهولة محو الدليل الجنائي الإلكتروني، وصعوبة الوصول إلى الدليل الجنائي الإلكتروني، وصعوبة فهم الدليل الإلكتروني، وهذا في الفروع التالية:

الفرع الأول: الأدلة الرقمية أدلة غير مرئية

يقصد بهذه الخاصية هو أن الجرائم التي ترتكب بواسطة الحاسب الآلي أو ترتكب عليه وما ينتج عن الأنظمة المعلوماتية من أدلة تعتبر بيانات غير مرئية لا تشير إلى شخصية معينة أو إلى وسائل معينة ومحددة؛ لأن هذه البيانات مسجلة رقميًا بكثافة وبشكل مشفر ومخزنة بوسائل ضوئية وممغنطة لا يستطيع المحقق الجنائي قراءتها وحتى وإن تمكن من قراءتها فإن تعديلها لا يترك أي آثار، وبالتالي يقطع أي علاقة بين المجرم المعلوماتي وجريمته والوصول إلى الدليل الإلكتروني الذي يمكن أن يدينه (الطيبي، 2019، ص، 269).

الفرع الثاني: جرائم تخلف آثارًا إلكترونية

وتتمثل هذه الخاصية في أن الجرائم السيبرانية تترك آثارًا إلكترونية هي عبارة عن نبضات إلكترونية ورقمية لا يمكن رؤيتها بالعين المجردة، فاكتشافها يحتاج إلى الاستعانة بأجهزة ووسائل تقنية متطورة حتى تظهرها للعيان؛ لأن حجم هذه الآثار الإلكترونية يكاد يكون منعدمًا، إضافة إلى ضخامة البيانات والملفات

الرقمية المجرمة من بين الكم الهائل لفصلها عن تلك البريئة منها (جاسم، 2016، ص، 09).

في حين جميع الوقائع المتعلقة بالجرائم العادية تخضع لسيطرة الأجهزة الأمنية والقضائية والآثار التي تخلفها آثار مادية مثل: البصمات أو السكاكين أو الأسلحة أو بقع الدماء، أما الجرائم السيبرانية فالمعلومات والبيانات فيها تتمثل في نبضات إلكترونية وتكون دون رؤية ومشاهدة أدلة الإدانة.

الفرع الثالث: سهولة محو الدليل الجنائي الإلكتروني

من بين المشاكل التي تواجه الأجهزة الأمنية والقضائية في التحقيق في الجرائم السيبرانية سهولة محو، وتدمير الدليل في فترة قصيرة، فالمجرم المعلوماتي يمكنه محو الدليل القائم ضده، ولا تستطيع السلطات كشف الجريمة وإقامة الدليل ضد الجاني، فهو يحرص كل الحرص على محو الآثار التي تدل على ارتكابه لجريمته من خلال اعتماد بعض التقنيات التي تساعده في محو وتعديل البيانات الإلكترونية، كما أن الدليل الإلكتروني غالبًا ما يترك آثارًا في حالة محوه وتعديله والخبراء المختصون فقط من يستطيعون كشف هذه التلاعبات التي يقوم بها الجناة الرقميون في الأنظمة الرقمية، فالمجرم المعلوماتي الذي يستخدم هذه الوسائل الإلكترونية في ارتكاب جرائمه يتميز بالذكاء والإتقان الفني للعمل الذي يتمثل في الطبيعة الفنية، ولذلك فإنه يتمكن من إخفاء الأفعال غير الشرعية التي يقوم بها أثناء تشغيله لهذه الوسائل الإلكترونية، ويستخدم في ذلك التلاعب غير المرئي في النبضات والذبذبات الإلكترونية التي يتم عن طريقها تسجيل البيانات (عماد وجغلولي، 2021، ص، 79).

الفرع الرابع: صعوبة الوصول إلى الدليل الجنائي الإلكتروني

أصبحت طرق تجميع وحفظ وتقديم الأدلة العلمية إلى المحكمة محل تشكيك من طرف المتهم (خيراني، 2012، ص، 142) والأصل أن الوصول إلى هذه الأدلة يتم عن طريق الشكاوى التي يقدمها المجني عليهم غير أن الأمر معقد في الجرائم السيبرانية، فجهات التحقيق ينبغي لها إحاطة كاملة بالتكنولوجيا الحديثة ومعرفة واسعة بالعراقيل التي تصعب من الوصول إلى الدليل الإلكتروني والمتمثلة فيما يلي:

الفقرة الأولى: إحاطته بوسائل الحماية الفنية

الدليل الإلكتروني يتم إحاطته بوسائل الحماية الفنية؛ وذلك بترميزه وتشفيره لتعطيل أي محاولة للوصول إليه أو استنساخه (الفيل، 2011، ص، 80) فالمعلومات والبيانات المخزنة إلكترونيًا محاطة بجدار من الحماية الفنية يمنع من الاطلاع عليها واستنساخها، وهذا الأمر يصعب من عملية التفتيش التي قد تباشر للحصول على الأدلة التي تدين الجاني، وعليه فإن استخدام تقنيات الترميز والتشفير يعد إحدى أكبر العقبات والمشاكل التي تعوق رقابة البيانات المخزنة أو المنقولة والتي تضعف وتقلل من قدرة

جهات البحث والتحري والتحقيق والملاحقة من الاطلاع عليها (الديربي وإسماعيل، 2012، ص 330).

الفقرة الثانية: سلوكيات الجاني

المجرم المعلوماتي يقوم بتشفير البيانات التي تتضمن محتويات غير مشروعة لمنع الغير من الاطلاع عليها وكشفها مثلما هو الحال في جرائم غسل الأموال عبر الإنترنت بعد تشفيرها، ويحرص الجاني بعد ارتكاب جريمته على محو آثارها من خلال القيام بتقنيات مجهزة ومعدة لهذا الغرض والأخذ بعين الاعتبار سهولة وسرعة التخلص من المعلومات والبيانات الإلكترونية في زمن قياسي وفي أقل فترة ممكنة (جاسم، 2016، ص، 08).

الفقرة الثالثة: الامتناع عن التبليغ

كذلك من بين المشاكل التي تواجه الأجهزة الأمنية والقضائية المعنية بالتحقيق في الجرائم السيبرانية في الوصول إلى الدليل الجنائي الإلكتروني الذي يدين المجرم المعلوماتي هو أنه في أغلب الأحيان يمتنع المجني عليه (الضحية) عن التبليغ في هذا النوع من الجرائم، وقد يسعى إلى تضليل المحققين؛ لذلك فمعظم الجرائم السيبرانية يتم كشفها بمحض الصدفة، وقد يكون المجني عليه شخصًا معنويًا مثل: المؤسسات المالية الكبرى كالبنوك التي تفضل في معظم الأحيان عدم التبليغ عن الإصابة بفيروس حتى لا تهتز ثقة المتعاملين معها، وينتج عنها سحب الودائع والاستثمارات (الحمد، 2014، ص، 149). كما قد ترفض بعض الجهات التعاون مع الأجهزة المكلفة بالتحقيق خشية معرفة العامة بوقوع الجريمة ويسعون بدلًا من محاولة تجاوز آثارها حتى لو كانت الوسيلة مكافأة المجرم (خليفة، 2007، ص، 35).

الفرع الخامس: صعوبة فهم الدليل الإلكتروني

إن فهم مضمون الدليل الجنائي الإلكتروني يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه، ولذلك فكل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلًا إلكترونيًا، وذلك لعدم إمكانية الاستدلال به على معلومة معينة؛ ما يقلل قيمته الإثباتية في إثبات الجريمة ونسبها إلى الجاني؛ نظرًا لحداثة الجرائم الإلكترونية وتعقد عملية الحصول على الدليل الإلكتروني لما تتسم به تلك العملية من طبيعة فنية وتقنية بحتة، فإن الجانب الفني لدى المحققين قد يكون في ذلك الشأن ضعيفًا، فتنتفي لديهم القدرة الفنية على التعامل مع مثل تلك الأدلة، سواء من حيث استخلاصها أو تقدير قيمتها، إلى جانب ضرورة إتقان اللغة الإنجليزية بشكل جيد حتى يمكن التعامل مع الأدلة الإلكترونية وهو أيضًا ما يغيب لدى البعض، ويجعل من الصعوبة التعامل مع الدليل وفهمه. (هلالي، 2006، ص، 73).

3. المطلب الثاني: المشاكل المتعلقة بخصوصية التحقيق في الجرائم الإلكترونية

تعتبر عملية التحقيق في الجرائم الإلكترونية من أصعب الأساليب والإجراءات التي تقوم بها الأجهزة الأمنية والقضائية في البحث والتحري والتحقيق من أجل الوصول إلى الأدلة التي تدين المجرم المعلوماتي وتقديمه للعدالة ومحاكمته، وذلك من خلال معرفة البيانات واكتشاف الجهات القضائية المختصة، وقد تعترض عمليات البحث والتحري والتحقيق مشاكل يمكن أن تعرقل عملية التحقيق، وتؤدي إلى نتائج سلبية ومخالفة للهدف المنشود الذي كانت تسعى إليه الأجهزة الأمنية والقضائية المكلفة بالتحقيق في الوصول إليه، وهذه النتائج تؤدي إلى زعزعة ثقة المحقق بنفسه وبأدائه وبإمكاناته، وتؤدي بالمجتمع إلى عدم ثقته أيضًا في الأجهزة الأمنية والقضائية التي يعول عليها في حمايته من الجرائم التي ترتكب في الفضاء الإلكتروني، وعلى النقيض من ذلك تزداد ثقة المجرم المعلوماتي بنفسه في الإفلات أو اكتشاف أمره، وعليه سنتطرق إلى المشاكل المتعلقة بخصوصية التحقيق التي تواجه الأجهزة الأمنية والقضائية أثناء التحقيق في الجرائم السيبرانية من خلال العقبات المتعلقة بكشف غموض الجرائم السيبرانية، والعقبات المتعلقة بالتفتيش عن الدليل الجنائي الإلكتروني، والعقبات المتعلقة بعمليات الضبط، والعقبات المرتبطة بالتعاون الدولي، وهذا في الفروع التالية:

الفرع الأول: العقبات المتعلقة بكشف غموض الجرائم السيبرانية

التحقيق في كشف غموض الجريمة السيبرانية تعترضه مجموعة من المشاكل متمثلة في الكم الهائل للمعلومات والبيانات وإلى حداثة أساليب ارتكاب الجريمة السيبرانية وإلى عدم قدرة وصلاحية أساليب البحث والتحري التقليدية في التصدي ومواجهة هذه الجرائم.

الفقرة الأولى: الكم الهائل للبيانات والمعلومات

من أكبر المشاكل التي تواجه الأجهزة الأمنية والقضائية في التحقيق في الجرائم الإلكترونية وجود الكم الهائل للمعلومات والبيانات التي يتم تداولها خلال الأنظمة المعلوماتية ومن أمثلتها أن عملية طباعة ما يوجد على الدعامات المشفرة والمغنطة لمركز حاسب متوسط الأهمية يحتاج إلى توفر ووجود مئات الآلاف من الصفحات، غير أن هذه الصفحات قد لا يمكن أن تثبت شيئًا ولن توصل لأي نتيجة (الديربي وإسماعيل، 2012، ص، 340).

الفقرة الثانية: حداثة الجرائم السيبرانية

كذلك من بين المشاكل التي يمكن أن تثيرها عمليات التحقيق هو حداثة أساليب ارتكاب هذا النوع من الجرائم التي تتميز بسرعة تنفيذها وسهولة إخفائها وسرعة محو آثارها؛ لكونها تعتمد على التدليس والمراوغة في ارتكابها وتضليل المحققين، وبالتالي فهي تحتاج لخبراء فنيين مهاريين؛ لأن الخبير التقليدي يصعب عليه التعامل معها أو التعرف على مرتكب الجريمة (الحمد، 2014، ص، 101).

وعليه يجب أن تكون الأجهزة الأمنية والقضائية المكلفة بالتحري في جميع مراحل التحقيق، سواء في مرحلة الاستدلال أو التحقيق أو المحاكمة على دراية واسعة من المعرفة بأنظمة الحاسب الآلي وكيفية تشغيله وأساليب الجرائم التي ترتكب بواسطته أو عليه، وبدراية أيضًا بالأساليب التي يستخدمها المجرم المعلوماتي في ارتكاب جريمته، وأن تكون هذه الأجهزة مدربة ومؤهلة من الناحية الفنية تدريبًا عالي الجودة يمكنها من اكتشاف الجرائم والوصول إلى أهدافها وتحقيق مهامها الموكلة إليها في فك لغز الجرائم السيبرانية (الطيبي، 2019، ص، 276).

الفقرة الثالثة: عدم صلاحية أساليب التحري والتحقيق التقليدية

استخدام الأساليب التقليدية في البحث والتحري لا يصلح لكشف الجرائم التي ترتكب في الفضاء الإلكتروني، ولهذا استحدثت العديد من التشريعات أساليب تحرٍ وتحقيق تتلاءم وتتناسب مع حجم وخطورة الجرائم السيبرانية، ومن بينها المشرع الجزائري الذي جاء بأساليب مستجدة تتوافق مع الطبيعة التقنية للتحري في هذا

النوع من الجرائم؛ وذلك بموجب القانون رقم 09/04 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (القانون رقم 09/04 المؤرخ في 14 شعبان عام 1430ه الموافق ل 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها الجزائري، الجريدة الرسمية للجمهورية الجزائرية، العدد 47. 25 شعبان 1430ه الموافق 16 غشت 2009).

وقد عمد المشرع الجزائري من أجل تسهيل مهام الأجهزة الأمنية والقضائية إلى وضع ترتيبات تقنية وفنية حديثة، مثل المراقبة الإلكترونية التي جاء بها القانون رقم 09/04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، وإجراء التسرب(الاختراق) وهو أسلوب جديد للبحث والتحقيق أضافه المشرع الجزائري في القانون رقم 06/22 المؤرخ في 20/12/2006 المعدل والمتمم لقانون الإجراءات الجزائية بسبب عدم فاعلية الأساليب التقليدية للبحث والتحري والتحقيق، وإجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور، وإجراءات التفتيش في الأنظمة المعلوماتية وحجز الأدلة الإلكترونية وحفظ المعطيات وغيرها من الإجراءات المستحدثة دون مراعاة لحرمة الحياة الخاصة والدافع إلى ذلك هو خطورة الجرائم السيبرانية، ومع سرية المراسلات والمضمونة دستوريا وفي المواثيق الدولية (زيدان، 2011، ص، 161).

وعليه فإن إثبات الجرائم السيبرانية عن طريق استخدام الوسائل الرقمية يتأثر بطبيعة هذه الجرائم وبالوسائل العلمية التي ترتكب بها، وهذا يؤدي إلى عدم اكتشاف أغلب الجرائم في الوقت الذي ترتكب فيه، وبالتالي عدم الوصول إلى المجرمين الذين يرتكبون الجرائم السيبرانية (جورج، 2016، ص، 16).

الفرع الثاني: العقبات المتعلقة بالتفتيش عن الدليل الجنائي الإلكتروني

كذلك من بين المشاكل التي تواجه الأجهزة الأمنية والقضائية أثناء عمليات التحقيق في الجرائم السيبرانية مشاكل في أثناء إجراء عملية التفتيش، وهذه المشاكل والعراقيل والصعوبات قد تتعلق بالجريمة ذاتها، أو تتعلق بالمجني عليه أو صعوبات تتعلق بنقص أو قلة خبرة جهات التحقيق أو صعوبات تتعلق بإجراءات التفتيش من أجل الحصول على الدليل المعلوماتي والتي سنتناولها على النحو التالي:

الفقرة الأولى: صعوبات التفتيش المتعلقة بالجريمة ذاتها

الصعوبات التي تجدها الأجهزة الأمنية والقضائية في أثناء إجراء التفتيش هي إخفاء الجريمة وغياب الدليل المرئي وصعوبة الوصول إليه، فعند قيام المحقق بتفتيش الحاسب الآلي قد يصطدم بأن الجهاز محاط بوسائل الحماية الفنية مثل: استخدام المجرم المعلوماتي كلمات سر بشكل يمنع المحقق من الوصول إلى الأدلة الإلكترونية، أو أنها مرمزة ومشفرة، إضافة إلى سهولة محو الدليل وتدميره في وقت قصير؛ مما يجعل سلطات التفتيش عاجزة عن الوصول إليه، كذلك ضخامة البيانات والمعلومات الواجب تفتيشها أو وجودها خارج إقليم الدولة (العبيدي، 2013، ص، 122).

الفقرة الثانية: صعوبات التفتيش المتعلقة بالمجني عليه (الضحية)

أيضًا من بين مشاكل التفتيش عدم إدراك الضحايا والمجني عليه لخطورة الجرائم السيبرانية، وبالتالي يبقى هذا النوع من الجرائم خفيًا ما لم يتم الإبلاغ عن حدوثه، وتكمن صعوبتها في أنها لا تصل إلى علم الجهات المعنية بالتفتيش بالطرق العادية، إضافة إلى صعوبة اكتشافها من قبل المجني عليهم والضحايا، أو رفضهم الإبلاغ عن الجرائم التي تعرضوا لها خوفًا من النتائج السلبية المترتبة على التفتيش، أو محاولة تلافي الفضائح في الجرائم غير الأخلاقية التي تتم عن طريق الإنترنت وغيرها من مواقع التواصل الاجتماعي، إضافة إلى أن رفض الإبلاغ عن هذا النوع من الجرائم قد يكون بسبب أن الإبلاغ قد يؤدي إلى معرفة المجرمين بنقاط ضعف أنظمة الأمن والحماية لدى الضحايا خاصة البنوك والشركات الكبرى، أو خوف تلك المؤسسات من أن تؤدي عمليات التفتيش إلى احتجاز أجهزة الحاسب الآلي وتعطيل شبكاتها؛ مما يسبب لها خسائر مالية كبيرة (البشير، 2004، ص، 17).

الفقرة الثالثة: صعوبات التفتيش المتعلقة بنقص خبرة الأجهزة الأمنية والقضائية المعنية بالتحقيق

وتتمثل هذه المشاكل في عدم تمكن الأجهزة الأمنية والقضائية المكلفة بالتحقيق في الجرائم السيبرانية من تقنيات الحاسب الآلي والقدرة على استخدام شبكة الإنترنت، وعدم متابعة الأجهزة الأمنية والقضائية للمستجدات المتعلقة بالحاسب الآلي والجرائم السيبرانية، إضافة إلى أنه قد لا تتوافر لهذه الأجهزة المهارة الفنية في التفتيش في الجرائم الإلكترونية وعدم معرفتها لأساليب ارتكاب هذا النوع من الجرائم، وقلة خبرتها في مجال التفتيش في الجرائم التي ترتكب في الفضاء الإلكتروني (حجازي، 2007، ص، 67).

إضافة إلى أنه للمختصين في مجال الحاسب الآلي مصطلحات

علمية خاصة بهم تشكل الطابع المميز لمحادثاتهم وطرق التفاهم بينهم، وبالتالي تكوين لغة خاصة بمستخدمي الحاسب الآلي تعرف باسم (المختصرات).

الفقرة الرابعة: صعوبات التفتيش المتعلقة بإجراءات الحصول على الدليل الجنائي الإلكتروني

إذا كانت الأجهزة الأمنية والقضائية تجري عمليات التفتيش بكل سهولة وبساطة في الجرائم التقليدية للوصول إلى الدليل؛ فإن الأمر يختلف تمامًا عند إجراء التفتيش للحصول على الدليل الإلكتروني في الجرائم السيبرانية؛ لأن المجرم المعلوماتي يستخدم كلمات سر تزيد من صعوبة إجراءات التفتيش التي يتوقع حدوثها للبحث عن الأدلة التي تدينه، ومن خلال استخدام كلمات السر قد لا تتمكن الأجهزة الأمنية والقضائية من الوصول إلى الأدلة والبيانات المخزنة إلكترونيًا، وقد يلجأ المجرمون إلى دس تعليمات خفية بين هذه البيانات أو التشفير حتى يستحيل على غيرهم الاطلاع عليها والوصول إلى الأدلة (الغافري، 2009، ص، 528).

الفرع الثالث: العقبات المتعلقة بعمليات الضبط

يمكن إجمال أبرز وأهم المشاكل التي تواجه عمليات الضبط فيما يلي:

أولًا: وجود المعلومات والبيانات الإلكترونية في شبكات أو أنظمة معلوماتية تابعة لدول أخرى؛ مما يستدعي تعاون تلك الدولة مع الأجهزة الأمنية والقضائية في عملية الضبط (هلالي، 2006، ص، 197)

ثانيًا: الحجم الكبير للشبكة التي تحتوي على البيانات الإلكترونية، وبالتالي ضرورة البحث المضني في تلك الشبكة للوصول إلى الأدلة، كما قد يؤدي الضبط إلى عزل النظام المعلوماتي عن مشغليه ومستخدميه لفترة زمنية قد تطول؛ مما ينتج عنه أضرار بهؤلاء المستخدمين.

ثالثًا: الجاني يستطيع محو وإتلاف البيانات المطلوب ضبطها لتعلقها بارتكاب جريمة معينة خلال مدة زمنية قصيرة لا تتعدى الثواني، كما يستطيع المجرم تفسير وجود هذه البيانات في حالة ضبطها بوجود خطأ في النظام المعلوماتي، وبالتالي يحاول نفي المسؤولية عنه (حجازي، 2007، ص، 210).

رابعًا: إحجام الضحايا عن إبلاغ السلطات في الجرائم السيبرانية؛ خوفًا من النتائج السلبية والأضرار الناجمة عن الإبلاغ مثل: الخوف على سمعتهم من الاهتزاز.

خامسًا: عدم كفاءة وأهلية الأجهزة الأمنية والقضائية في التعامل مع هذه البيانات وضبطها؛ الأمر الذي يؤدي إلى إهمال الدليل وإتلافه (الفيل، 2011، ص، 174).

سادسًا: الضبط قد يشمل اعتداء على حقوق الغير أو على حرمة حياتهم الخاصة؛ فيجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق والواجبات (الحمد، 2014، ص، 176).

الفرع الرابع: العقبات المتعلقة بالتعاون الدولي

هناك العديد من المشاكل التي تقف عائقًا أمام التعاون الدولي في التصدي للجرائم السيبرانية رغم وجود العدد من الاتفاقيات الدولية الثنائية والإقليمية والجماعية المبرمة بين الدول في هذا المجال، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، واتفاقية الأمم المتحدة لمكافحة الفساد التي جاءت بإجراءات جديدة في المسائل المتعلقة بالتعاون القضائي الدولي، ومن بين هذه العقبات القصور التشريعي للدول لاختلاف الأنظمة القانونية والإجرائية، وتنازع الاختصاص القضائي الدولي، إضافة إلى الإشكاليات الخاصة بالإنابات القضائية وتسليم المجرمين.

الفقرة الأولى: القصور التشريعي للدول لاختلاف أنظمتها القانونية والإجرائية

أي بمعنى عدم وجود نظام قانوني موحد خاص بمكافحة الجرائم السيبرانية؛ ما قد يكون مباحًا في نظام أو دولة معينة قد يكون نفس الفعل مجرمًا في نظام ودولة أخرى (جميل، 2002، ص، 157). وهذا مرتبط بعدة عوامل نذكر منها:

أ- اختلاف العادات والتقاليد والديانات والثقافات من مجتمع إلى آخر.

ب- تنوع الأنظمة القانونية والإجرائية، فمثلًا طرق التحري والتحقيق قد تكون فعالة في دولة معينة غير أنها قد لا تكون لها أي فائدة في دولة أخرى أو لا يسمح بإجرائها.

وهذا يعني عدم وجود تنسيق بين مختلف الدول فيما يتعلق بالإجراءات الجنائية المتخذة في الجرائم السيبرانية، سواء تعلق الأمر بأعمال الاستدلال أو التحقيق أو المحاكمة.

الفقرة الثانية: تنازع الاختصاص القضائي

بسبب ما تتسم به الجرائم السيبرانية من سمات وخصائص، وكونها جرائم عابرة للحدود الوطنية للدول وذات طبيعة عالمية التأثير؛ فإنها تعتبر من أكثر الجرائم التي يثار بشأنها تنازع الاختصاص القضائي بين الدول؛ ما يعني تقديم الدعوى من ذات الجريمة أو عدة جرائم مرتبطة إلى جهتين من جهات التحقيق أو الحكم وادعاء كل

جهة اختصاصها، وهو ما يسمى بتنازع الاختصاص الإيجابي، أو رفض كلتا الجهتين النظر على أساس عدم الاختصاص، وهو ما يسمى بتنازع الاختصاص السلبي.

الفقرة الثالثة: الصعوبات المتعلقة بالإنابة القضائية وتسليم المجرمين

تتمثل أبرز مشاكل الإنابة القضائية وتسليم المجرمين في النقاط التالية:

أولًا: مشاكل الإنابة القضائية

فكرة السيادة الوطنية قد تعوق التعاون القضائي بين الدول في مكافحة الجرائم السيبرانية، إضافة إلى إشكالية البطء في الإجراءات، والأصل بالنسبة لطلبات الإنابة القضائية الدولية أن تسلم بالطرق الدبلوماسية، وهذا ما يجعلها تتسم بالبطء والتعقيد، وهو يختلف جذريًا عن طبيعة أعمال الإنترنت التي تتميز بالسرعة، وهو ما ينعكس سلبًا على التعاون الدولي في مكافحة الجرائم السيبرانية.

ثانيًا: مشاكل تسليم المجرمين

أما فيما يتعلق بالمشاكل والصعوبات والعراقيل التي تواجه التعاون الدولي في مجال تسليم المجرمين، فهي ترجع أساسًا لمبدأ ازدواجية التجريم كشرط أساسي لتسليم المجرمين، وما يعرف بالتزاحم في طلبات التسليم، أي بعنى أن عدة دول قد تطلب نفس الشخص الذي ارتكب الجريمة السيبرانية، ولا يشترط في تزاحم الطلبات أن تتعاصر في وصولها إلى الدولة المطلوب إليها، يكفي أن تتوالى إلى الدولة المطلوب إليها ما دام الشخص المطلوب لا يزال متواجدًا على إقليمها ولم يتم تسليمه إلى أي دولة من الدول المطالبة بالتسليم (خراشي، 2015، ص، 251).

4. الخاتمة

الغاية الأساسية والرئيسة التي نسعى إليها مستقبلًا من وراء إجراء هذا البحث والدراسة هي الوصول إلى حلول تمكن المحقق الجنائي من القيام بعمله في ظروف أفضل ووفق أساليب أنجع وأكثر تطورًا، ومحاولة إزالة العراقيل الإجرائية التي تواجهه أثناء تسييره لعمليات البحث والتحري والوصول إلى مجتمع عربي تكون فيه نسبة الإجرام أقل، إضافة إلى تنوير المشرع العربي حتى يتسنى له النص على تشريعات وقوانين تكون أكثر حداثة تمنح الأجهزة المكلفة بالتحقيق الأمني والقضائي صلاحيات أوسع وتكون ضمن لجان أو مراكز ذات مستوى أعلى.

النتائج

وتوصلنا من خلال بحثنا إلى ما يلي:

أن الأجهزة الأمنية والقضائية تواجه صعوبات عديدة ومتنوعة فيما يتعلق بإجراءات ضبط الجرائم الإلكترونية وإضفاء الوصف القانوني الملائم والمناسب على الوقائع المتعلقة بهذه الجرائم، ويرجع ذلك إلى الطبيعة الخاصة لهذا النوع من الجرائم، فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود الوطنية.

وتبدأ المشاكل الإجرائية في الوصول إلى الدليل الجنائي الإلكتروني في الجرائم السيبرانية بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونيًا وكيانات غير مادية، وبالتالي يصعب من ناحية كشف هذه الجرائم ويستحيل من ناحية أخرى أحيانًا جمع أدلتها.

ومما يزيد من المشاكل الإجرائية في هذا المجال سرعة ودقة تنفيذ الجرائم الإلكترونية وإمكانية محو آثارها وإخفاء الأدلة المتحصلة عنها عقب التنفيذ مباشرة، وتواجه عمليات التفتيش وجمع الأدلة صعوبات متنوعة وعديدة قد تتعلق ببيانات مخزنة في أنظمة أو شبكات إلكترونية موجودة في الخارج، ويثير مسألة الدخول إليها ومحاولة جمعها وتحويلها إلى الدولة التي يجرى فيها التحقيق مشكلات تتعلق بسيادة الدولة.

ومما يزيد أيضًا من صعوبة إثبات الجرائم الإلكترونية والوصول إلى الأدلة هو إحجام المجني عليه عن الإبلاغ عن الجرائم الإلكترونية التي ترتكب ضدهم، وفي حالة استطاعت السلطات المختصة اكتشاف الجريمة فإنهم يرفضون تقديم المساعدة.

إضافة إلى مشاكل التعاون الدولي، مثل القصور التشريعي للدول واختلاف الأنظمة القانونية والإجرائية، فمثلًا نفس الفعل الذي قد يكون مباحًا في دولة معينة، وقد يكون مجرمًا في دولة أخرى.

التوصيات

ومن بين التوصيات نوصي بما يلي:

أولًا: ندعو إلى سن نصوص قانونية وتشريعية إجرائية خاصة تتلاءم وتتناسب مع الطبيعة الخاصة للجرائم السيبرانية واشتمالها على قواعد وأحكام تضمن فاعلية التحقيق.

ثانيًا: ندعو إلى ضرورة التأهيل الفني للأجهزة الأمنية والقضائية المكلفة بالتحقيق في الجرائم الإلكترونية والتدريب في كل ما يتعلق بمجال التقنيات الأساسية لتكنولوجيا الإعلام والاتصال.

ثالثًا: ندعو إلى منح الأجهزة الأمنية والقضائية المزيد من السلطات والصلاحيات والاختصاصات في التحقيق في الجرائم التي ترتكب في

الفضاء الإلكتروني وتوفير الظروف الملائمة والأساليب التقنية الحديثة المساعدة في إثبات الجرائم السيبرانية والقبض على مرتكبيها.

رابعًا: ندعو الأجهزة الأمنية والقضائية التي تقوم بعملية البحث والتحقيق إلى حماية خصوصية الأشخاص أثناء إجراء التفتيش؛ وذلك بحضور مالك الحاسب الآلي أثناء التفتيش وتفادي وتجنب التفتيش غير القانوني.

خامسًا: ندعو الضحايا والمجني عليهم إلى ضرورة تبليغ السلطات الأمنية والقضائية عن الجرائم السيبرانية وتقديم الشكاوى والبلاغات ومساعدة أجهزة التحقيق في التصدي للجرائم السيبرانية.

سادسًا: ندعو إلى إجراء الأبحاث والدراسات حول الأساليب المتطورة والحديثة التي يستخدمها المجرم المعلوماتي في ارتكاب جرائمه وعقد الملتقيات والندوات حول هذا النوع من الجرائم وسبل مكافحتها والتصدي لها.

وأخيرًا: ندعو إلى تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية من خلال المساعدة القضائية والقانونية المتبادلة وتسهيل إجراءات الإنابة القضائية وتسليم المجرمين وغيرها من إجراءات التعاون الدولي التي تسهم في محاربة الجرائم السيبرانية وعقد المزيد من الاتفاقيات الثنائية والإقليمية والدولية.

وتبادل المعلومات والبيانات والخبرات.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس لديه أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل المقالة

يعلن المؤلف بأن البحث المنشور لم يتلق منحة مالية من أية جهة تمويل في القطاعات العامة أو التجارية أو المؤسسات غير الربحية.

المصادر والمراجع

1. البشير، محمد الأمين. (2004). التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض.
2. جاسم، خريبط خلف. (2016). الدليل الجنائي في الجريمة المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، جامعة ذو قار، الناصرية، العراق.
3. جميل، عبد الباقي. (2002). الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة.
4. حنين، جورج إسحق. (2016). دراسة عن الجرائم المعلوماتية والإلكترونية عبر شبكة الإنترنت وسبل مواجهتها، الإدارة العامة المركزية لمركز المعلومات والتوثيق بوزارة المالية، مصر.
5. خالد، عياد الحلبي. (2011). إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن.
6. خراشي، عبد العال إبراهيم. (2015). إشكالية التعاون الدولي في مكافحة الجرائم الإلكترونية وسبل التغلب عليها، دار الجامعة الجديدة للنشر، الإسكندرية.
7. خيراني، فوزي. (2012). الأدلة العلمية ودورها في الإثبات الجنائي، مذكرة مقدمة لنيل درجة الماجستير في العلوم القانونية والإدارية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر.
8. الديربي عبد العال ومحمد صادق إسماعيل. (2012). الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة.
9. زبيحة، زيدان. (2011). الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر.
10. الطيبي، البركة. (2019). إشكالية الإثبات في الجرائم الإلكترونية، مجلة آفاق علمية، المجلد 11، العدد 01، الجزائر.
11. عبد الفتاح، حجازي. (2007). مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة.
12. العبيدي، أسامة بن غانم. (2013). التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، الرياض.
13. علي عدنان، الفيل. (2011). إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، عمان.
14. عماد بلغيث وجغلولي يوسف. (2021). صعوبات التحقيق في الجرائم الإلكترونية، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 06، العدد 03، الجزائر.
15. الغافري، حسين سعيد. (2009). السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة.
16. محمد، خليفة. (2007). الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية.
17. مسرة، خالد الحمد. (2014). الدليل الرقمي ومعايير جودته، الطبعة الأولى، مركز الكتاب الأكاديمي، عمان.
18. الفيل، علي عدنان. (2012). إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة،

ماجستير قانون، كلية الحقوق، جامعة الموصل، المكتب الجامعي الحديث، الإسكندرية.

19. هلالي، عبد الله أحمد. (2006). تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة.
20. القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430ه الموافق 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها الجزائري، الجريدة الرسمية للجمهورية الجزائرية، العدد 47. 25 شعبان 1430ه الموافق 16 غشت 2009.
21. القانون رقم 22/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.
22. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 1 تشرين الثاني/نوفمبر 2000.
23. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000.صادقت عليها الجزائر بتاريخ 22 فبراير 2002، بموجب المرسوم الرئاسي رقم 02 /55 المؤرخ في 09 نوفمبر 2003 .
24. اتفاقية الأمم المتحدة لمكافحة الفساد صادقت عليها الجزائر في 19 إبريل 2004 بموجب المرسوم الرئاسي رقم 128/04.