عمادة الدراسات العليا
جامعة القدس

خصوصية التحقيق في الجرائم الإلكترونية

عاصف جودت أحمد النجاجره

رسالة ماجستير

القدس – فلسطين

1440 هـ -2019 م

خصوصية التحقيق في الجرائم الإلكترونية

إعداد

عاصف جودت أحمد النجاجره

بكالوريوس قانون وعلوم شرطية- أكاديمية الشرطة المصرية

المشرف: د. جهاد الكسواني

قدمت هذه الرسالةِ إستكمالاً لمتطلبات الحصول على درجة الماجستير في القانون الجنائي، كلية الحقوق، عمادة الدراسات العليا، جامعة القدس.

1440 هـ - 2019 م

جامعة القدس

عمادة الدراسات العليا

برنامج الماجستير في القانون الجنائي

إجازة الرسالة

خصوصية التحقيق في الجرائم الإلكترونية

إسم الطالب: عاصف جودت أحمد النجاجره

الرقم الجامعي: (21420077)

المشرف: د. جهاد الكسواني.

نوقشت هذه الدراسة وأُجيزت بتاريخ (2019/6/23)، من أعضاء لجنة المناقشة المدرجة أسماؤهم وتواقيعهم:

1- رئيس لجنة المناقشة: د. جهاد الكسواني التوقيع: .....

2- ممتحناً داخلياً: د. جميلة زيد التوقيع: .....

3- ممتحناً خارجياً: د. فادي شديد التوقيع: .....

القدس – فلسطين

1440 هـ – 2019 م

بسم الله الرحمن الرحيم

" إِنَّ اللَّهَ يَأْمُرُكُمْ أَن تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا وَإِذَا حَكَمْتُم
بَيْنَ النَّاسِ أَن تَحْكُمُوا بِالْعَدْلِ ۚ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُم بِهِ ۗ
إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا "

سورة النساء الآية 58

الإهداء

لن يَحتار قلمي ولا عقلي فيمن أختار لأُهدي له تعبي وسهري وعنائي، فالذي ذللَ لي الصعوبات، وقدم لي الغالي والنفيس دون إنتظار لمقابل، سوى أن يراني في مقدمة الصفوف وأعلى الدرجات، **والدي الغالي** جزاك الله عني خير الجزاء وجعلني وعملي الصالح في ميزان حسناتك، ومتعك بموفور الصحة والعافية.

وإلى من غمرتني بعطفها، ورعايتها، والتي ألمس في كفيها كل معاني الحب الخالص والصادق دون رجاء لمقابل، سوى رؤيتي أحيا بسعادة وهناء **والدتي الحبيبة** حفظها الله.

إلى من وقفت بجانبي في جميع الأوقات والمواقف، زوجتي العزيزة.

إلى سر السعادة والفرح الدائم في هذه الدنيا، **إبني الغالي قيس**.

إلى الأرواح الطاهرة، عمي الغالي الشهيد/ خلف نجاجره، وصِهري الغالي المرحوم/ خليل الفرحين.

إلى جميع طلاب العلم في الوطن والشتات، إليكم أُقدم وأُهدي هذا الجهد العلمي المتواضع.

عاصف جودت أحمد النجاجره

إقرار

أُقر أنا مُعِد الرسالة بأنّها قُدمت لجامعة القدس لنيل درجة الماجستير، وأنها نتيجة أبحاثي الخاصة، بإستثناء ما تمّ الإشارة له حيثما ورد، وأنّ هذه الدراسة أو أي جزء منها لم يُقدم لنيل درجة عليا لأي جامعة أو معهد آخر.

الاسم: عاصف جودت أحمد النجاجره

التوقيع .....

التاريخ: 23 / 6 / 2019

الشكر والتقدير

أحمد اللهم فاطر العباد، والهادي إلى سبيل الرشاد، وأُصلي وأُسلم علي خير خلقك سيدنا محمد سيد المرسلين وإمام المتقين، وأطلب العون والهدى والتوفيق وبعد:-

إن الكلمات تقف عاجزة عن الثناء والتقدير لأُستاذي الكبير الدكتور جهاد الكسواني والذي أسعدني بتفضله قبول الإشراف على هذه الرسالة، وهو الذي بذل الجهد الواسع في تقديم العون والإرشاد، فكل الحب لمن أرشد ونصح وسرد.

كما وأتقدم بخالص الشكر وعظيم الإمتنان إلى جميع أساتذتي الأفاضل، الذين تعلمت منهم الكثير طوال مرحلة دراستي، في سبيل الحصول على درجة الماجستير في القانون الجنائي.

ويُشرفني أن أشكر بخالص المحبة أساتذتي الأفاضل، أعضاء لجنة المناقشة على تفضلهم بقبول مناقشة هذه الرسالة وإبداء ملاحظاتهم القيمة عليها، والتي أثق بمدى أهميتها في إثراء هذا البحث.

عاصف جودت أحمد النجاجره

الملخص

التحقيق هو المرحلة الثانية من مراحل الإجراءات الجزائية، وتنطلق معه غالباً مرحلة الدعوى العمومية، وهو بشكل أصيل من اختصاص النيابة العامة، وبشكل ثانوي من إختصاص مأموري الضابطة القضائية، بتفويض صريح، ويسعى إلى استجلاء الحقيقة، حيث تقوم عليه سلطة قضائية ويستمر هذا حتى مع التشريعات الحديثة، والتي من ضمنها القرار بقانون رقم(10) لسنة 2018 بشأن الجرائم الإلكترونية، وما ورد فيه من خصوصيات ومن ضمنها خصوصية التحقيق.

ونجد أن هناك قصور لدى النيابة العامة في إجراءات التحقيق في الجرائم الإلكترونية، وذلك لضعف الخبرة الفنية والإمكانيات التقنية لديهم، وهو ما تعتمد عليه تلك الجرائم المستحدثة، الشيء الذي جعل مأموري الضبط القضائي ذات صلاحيات أوسع في العمل بها، لما يملكون من معرفة وخبرة تتوافق مع أسلوبها.

وما يجعل التحقيق المرحلة الأساسية، هو إعتماد القضاء على النتائج المستخلصة منه، لأجل كشف الحقيقة والوصول إلى العدالة، ما يجعل الدعوى إلى وجود تخصص في النيابة العامة بزيادة الخبرة، وخلق مزيد من الإجراءات في الدعوى الإلكترونية.

وقد وصلت هذه الدراسة، إلى مجموعة من النتائج والتوصيات تضمنتها الخاتمة.

Privacy of investigation of cyber-crimes

Prepared by: Assef Jawdat Ahmad Al- Najajrah

Supervisor: Dr. Jihad Al-Kiswani

Abstract:

Investigation is the second stage of penal procedures. Simultaneously, a public lawsuit is often initiated with it. It is primarily the jurisdiction of the public prosecution and secondarily the jurisdiction of the legal enforcement officer by virtue of an express authorization in pursuit of truth which is the basis of the judicial authority. These procedures also apply to modern legislations including Law number 15 of the year 2018 regarding cyber-crimes as well as provisions concerning the privacy of investigation.

It was concluded that there is inadequacy on part of the public prosecution with regard to investigation procedures into cyber-crimes on the grounds that they lack technical experience and technological facilities which are the basis of new crimes. This has lead law enforcement officers to enjoy larger powers thanks to their compatible knowledge and experience.

What makes investigation the fundamental stage is the reliance of the judiciary on the extracted conclusions in order to uncover the truth and fulfill justice. Thus, there should be jurisdiction in the public prosecution through experience and creation of more procedures in cyber cases.

The study reached several outcomes and recommendations stated in the conclusion.

المقدمة

يمر المجتمع الدولي في الوقت الحالي بثورة كبيرة جداً من التطورات، وهي التي عُرفت إصطلاحاً بظاهرة العولمة، ما أدى إلى تعزيز العلاقات والتواصل بين الأشخاص في جميع أرجاء العالم، وذلك بفضل تقنية المعلومات، والتي بدورها أظهرت مردوداً سلبياً ساعد على ظهور أساليب إجرامية مستحدثة من التقنية الإلكترونية، وأصبحت وسيلة إعتداء على قيم ومصالح الناس الأساسية[1].

ويجدر القول، أن التزايد في إستخدام الوسائل الإلكترونية وشبكات الإنترنت، أدى إلى ظهور أشكال جديدة من الجرائم وهي الجرائم الإلكترونية، كالإستيلاء على البيانات، أو إتلافها، أو كالدخول غير المصرح به إلى أنظمة الحاسوب، وكذلك جرائم الإعتداء على حقوق الملكية الفكرية لمؤلفيها[2].

وبما أن هذه الجرائم تتصل بالتطور التنكولوجي الحديث، فهي تتميز بخصوصية منفردة عن الجرائم التقليدية بحيث أنها تُرتكب عبر وسائط إلكترونية، وبالتالي يكون إجراء مكافحتها وكشف مرتكبيها ذات طبيعة خاصه.

وفقاً لما تقدم يمكن تعريف الجرائم الإلكترونية؛ بأنها كل فعل مخالف للقانون يتم إرتكابه بحق جميع الأشخاص سواء الطبيعيين أو المعنويين وذلك عبر الوسائل الإلكترونية والإنترنت.

وكذلك يُمكن تعريف التحقيق الإبتدائي؛ بأنه التصرف القانوني الذي تقوم به الهيئات الإتهامية المختصة بغرض البحث عن مرتكب الجريمة وعن أدلة البراءة والإدانة لتشخيص وقائع الجريمة المرتكبة.

---

[1] أحمد وهدان: الإنعكاسات الأمنية للعولمة، القاهرة، المجلة الجنائية القومية، مجلد 44، 2001، ص. 91.

[2] سرحان حسن محمد حسن المعيني: التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات 2011، ص. 17.

الناظر للتاريخ يجد أن الجرائم الإلكترونية أثارت العديد من الإشكاليات بالنسبة للقائمين على مكافحتها، ويرجع ذلك إلى أن القوانين العقابية وقوانين الإجراءات الجزائية التقليدية تُبسط حمايتها على الأشياء المادية الملموسة، أما بالنسبة للمعلومات الإلكترونية والأشياء المعنوية المرتبطة بها فلم تمتد إليها الحماية إلا حديثاُ إعتباراً لحداثة الجرائم الإلكترونية.

فنجد أن قانون العقوبات رقم 16 لسنة 1960، وكذلك قانون الإجراءات الجزائية رقم 3 لسنة 2001 لم تنص على الجرائم الإلكترونية.

وفي سبيل مكافحة الجرائم الإلكترونية على المستوى الدولي، تم إبرام إتفاقية بودابست لمكافحة الجرائم المعلوماتية 2001، والتي كانت تهدف إلى توحيد التدابير التشريعية بين الدول للوقاية من الجرائم الإلكترونية، وكذلك تفعيل خُطة عمل على الجانب الموضوعي والإجرائي للحد من تلك الجرائم، والتأكيد على التعاون الإقليمي والدولي في سبيل مكافحتها.

وعلى المستوى العربي فقد تم إبرام الإتفاقية العربية لمكافحة الجرائم المعلوماتية 2010 والتي صادقة عليها دولة فلسطين عام 2012, بحيث كانت تهدف هذه الإتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

وفي دولة فلسطين فقد تم إقرار القرار بقانون رقم 17 لسنة 2017 بشأن الجرائم الإلكترونية، والذي واجه بعض الإعتراضات ما أدى لإقرار القرار بقانون رقم 10 لسنة 2018 بشان الجرائم الإلكترونية.

ونستنتج أن الجرائم الإلكترونية جرائم حديثة متطورة، ظهرت وتزايدة مع إنتشار التطور التكنولوجي في جميع أنحاء العالم.

أهمية الموضوع:

1. الأهمية النظرية: تُعتبر الجرائم الإلكترونية من الجرائم المستحدثة حسب الوسيلة المُرتكبة بها، فقد تكون هناك جرائم تقليدية مرتكبة بوسائل حديثة، أو أن تكون جرائم حديثة أُنشأت مع الوسائل الإلكترونية كالجرائم المُرتكبة بالبطاقات الإلكترونية أو الواقعة عليها وتتجلى الأهمية النظرية للموضوع من خلال مدى تطور وسائل ملاحقة هذه الجرائم وبالأخص التحقيق فيها، بالإضافة إلى الجدل الفقهي الذي دار حول مدى كفاية القواعد التقليدية والحاجة إلى مواكبة هذه الجرائم بتطوير تشريعي.
2. الأهمية العملية: تبرز الأهمية العملية بالمواكبة التشريعية للجرائم الإلكترونية، فبالإضافة إلى القواعد التقليدية الواردة في قانون العقوبات الأردني رقم 16 لسنة 1960 وقانون الإجراءات الجزائية رقم 3 لسنة 2001 فقد أصدر المشرع القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية والذي لم يتسنى له التطبيق الواجب حتى هذه اللحظة ما أثر في غياب القرارات القضائية المتعلقة بخصوصية التحقيق في الجرائم الإلكترونية.

أهداف الموضوع:

1. توضيح المقصود بخصوصية التحقيق في الجرائم الإلكترونية.
2. إبراز الخصوصية في الجرائم الإلكترونية سواء بالتحقيق بشكل أصلي من قبل النيابة العامة أو بالتفويض لمأموري الضبط القضائي.
3. توضيح مدى سيطرة أجهزة العدالة وبالأخص النيابة العامة أو الضابطة القضائية على إجراءات التحقيق في الجرائم الإلكترونية.
4. بيان العقبات والصعوبات التي تواجه التحقيق في الجرائم الإلكترونية وسُبل تجاوزها.

المنهج المتبع:

لغايات تحقيق الأهداف المرجوه من هذا البحث، فقط تم الإعتماد على المنهجين الوصفي والتحليلي.

إشكالية الموضوع:

ما هي خصوصية التحقيق في الجرائم الإلكترونية ....؟

خطة الموضوع:

إجابةً عن الإشكالية المطروحة، فقط تم بيان الخصوصية فيما يلي:

الفصل الأول: خصوصية إجراءات التحقيق في الجرائم الإلكترونية.

الفصل الثاني: معوقات إجراءات التحقيق في الجرائم الإلكترونية.

الفصل الأول: خصوصية إجراءات التحقيق في الجرائم الإلكترونية.

أدى التطور العلمي والتكنولوجي الكبير الذي شهده العالم في الآونة الأخيرة، إلى تغيّر ملحوظ في أُسلوب التفكير، وذلك في ظل المعلومات والأحداث المتناقلة عبر وسائل التواصل الإجتماعي والإعلام، وبالتالي أصبح هناك إزدياد ملحوظ في إرتكاب الجرائم المستحدثة بأنماط مختلفة، الشيء الذي ساعد على ظهور صعوبات وتحديات أمام السلطة صاحبة الإختصاص الأصيل بإجراء التحقيق الإبتدائي[1].

"وتعتبر النيابة العامة هي صاحبة الإختصاص الأصيل في إجراء التحقيق"، وهو ما تم النص عليه صراحة في قانون الإجراءات الجزائية رقم (3) لسنة 2001 المادة رقم (1/55) والتي جاء فيها "تختص النيابة العامة دون غيرها بالتحقيق في الجرائم والتصرف فيها"[2].

وكذلك ذهبت المادة رقم (2/3) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية إلى أن المحاكم النظامية والنيابة العامة هي صاحبة الإخصاص بالنظر في دعاوي الجرائم الإلكترونية[3].

وتبرز الخصوصية فيما يمكن أن تتميز به إجراءات التحقيق في الجرائم الإلكترونية مقارنةً بالقواعد التقليدية الواردة في قانون الإجراءات الجزائية (3) لسنة 2001، وعليه تظهر الخصوصية في إجراءات التحقيق الأصلية (المبحث الأول)، وفي إجراءات التحقيق الإستثنائية (المبحث الثاني).

---

[1] ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، المجلة الكبري، 2006، ص. 28.

[2] قانون الإجراءات الجزائية رقم (3) لسنة 2001م، المادة رقم (1/55).

[3] قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، المادة رقم (2/3).

المبحث الأول: خصوصية في إجراءات التحقيق الأصلية

يُعتبر التحقيق مجموعة الإجراءات التي تقوم بها السلطة المختصة بالتحقيق بعد وقوع جريمة معينة، بقصد البحث عن الأدلة التي قد تساعد في الكشف عن الحقيقة[1]، وبالتالي يتم فيه تدوين أقوال الشهود والمشتبه بهم، ومواجهة المتهمين بالأدلة المتوافرة ضدهم، أما التحقيق في الجرائم الإلكترونية فلابد أن يتميز بنوع من الخصوصية، وذلك نظراً للطبيعة الخاصة لهذه الجرائم، وبسبب الصعوبات التي قد تواجه عملية التفتيش والبحث عن الأدلة[2].

فالتحقيق مع الأشخاص ذوي العلاقة في تلك الجرائم له خصوصية، وذلك من حيث، إجراء التفتيش عن الأدلة الإلكترونية، وإجراء المواجهة بين المتهمين، وبين المتهمين والشهود والذهاب بهم الى مسرح الجريمة عند الضرورة، لمناقشتهم حول الأجهزة الإلكترونية وملحقاتها.

كما أن إستجواب المتهم في الجرائم الإلكترونية يتميز بخصوصية، من حيث قيام القائم بالتحقيق والخبير المختص بتبادل المعلومات فيما بينهم، بحيث يوضح المحقق المختص للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم[3].

وتهدف إجراءات التحقيق الأصلية إلى الكشف عن الحقيقة، سواء من حيث ثبوت التهمة ونسبتها إلى المتهم، أو عدم ثبوتها[4]، ولهذا فإن من الإجراءات الأصلية صعوبة الإستجواب (المطلب الأول)، وخصوصية التفتيش (المطلب الثاني)، وخصوصية الشهادة (المطلب الثالث).

---

[1] خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، 2009، ص. 18.

[2] حنان ريحان مبارك المضحكي: الجرائم المعلوماتية، منشورات الحلبي الحقوقية، ص. 369.

[3] محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب (السعودية)، العدد 30، 2000، ص. 368/365.

[4] محمد بن حسن السراء: الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية، مجلة الفكر الشرطي– مركز بحوث الشرطة– القيادة العامة لشرطة الشارقة– الإمارات، مج. 21، ع. 81، 2012، ص. 38.

المطلب الأول: صعوبة الإستجواب.

من المعروف أن الإستجواب إجراء من إجراءات التحقيق، وهو من الإجراءات الخطيرة والمهمة جداً[1]، حيث يُستخدم في الكشف عن الحقيقة، ويمنح السلطة القائمة بالتحقيق طرح التساؤلات الدقيقة التفصيلية، والدخول في موضوع الدعوى للتعرف على أهم الأمور المتعلقة بالجريمة[2].

"إذا فالإستجواب يُعتبر أهم إجراءات التحقيق على الإطلاق"، وبناءً عليه يقوم القائم بالتحقيق بمناقشة المتهم تفصيلياً في التهمة المسندة إليه، كما يواجهه في الأدلة القائمة ضده لغاية الحصول على إعتراف منه بإرتكابه للجريمة أو نفيه لذلك[3].

وتبرز خصوصية الإستجواب في الجرائم الإلكترونية، من حيث أن قدرة مأموري الضبط القضائي على الإستجواب أكبر من قدرات النيابة العامة، وذلك كونهم يملكون من الوسائل التقنية والخبرات الفنية ما يتجاوز خبرات النيابة العامة، التي لا يوجد فيها أعضاء مختصين في الميدان، وهنا تتجلى صعوبة الإستجواب في تلك الجرائم.

إذاً فإجراء الإستجواب في الجرائم الإلكترونية قد يقوم به مأموري الضبط القضائي بشكل أكبر من الجرائم التقليدية رغم أنه إختصاص أصيل للنيابة العامة، ولا يجوز التفويض به لمأموري الضبط القضائي إلا في حدود القانون وفي جرائم معينة، ومن هنا يمكن توضيح تعريف الإستجواب (الفرع الأول)، وضعف ضمانات الإستجواب (الفرع الثاني).

---

[1] محمد سامي البتراوي: إستجواب المتهم، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1968، ص. 7.

[2] خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 241.

[3] إبراهيم راسخ: التحقيق الجنائي العملي، الطبعة الأولى، 1991، مطبعة البيان التجارية، دبي، ص. 436.

الفرع الأول: تعريف الإستجواب.

عَرفت المادة (94) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 الإستجواب بأنه "مناقشة المتهم بصورة تفصيلية بشأن الأفعال المنسوبة إليه ومواجهته بالإستفسارات والأسئلة والشبهات عن التهمة ومطالبته بالإجابة عليها"[1].

والإستجواب هو إجراء من إجراءات التحقيق، يقوم بناءً عليه القائم بالتحقيق بالتأكد من شخصية المتهم، ويناقشه في التهمة المسندة إليه بشكل تفصيلي، مع مطالبته بالرد على الأدلة القائمة ضد إما بتنفيذها أو التسليم بها[2].

وقد عرف الفقه الإستجواب بأنه "مجابهة المتهم بالأدلة القائمة ضده، ومناقشته مناقشة تفصيلية إن كان منكراً للتهمة أو يعترف بها إذا شاء الإعتراف"[3].

وقد عرفت محكمة النقض المصرية الإستجواب بأنه "مناقشة المتهم مناقشة تفصيلية في أُمور التهمة وظروفها ومجابهته بما قام عليه من الأدلة ومناقشته في أجوبته مناقشة يُراد بها إستخلاص الحقيقة التي يكون كاتماً لها[4].

ويتميز الإستجواب في الجرائم الإلكترونية بطبيعة خاصة، فلا بد أن يتم في مكان خاص مهيأ ومناسب لتلك الجرائم، من حيث وجود الأجهزة التقنية والفنية، كما أن هناك طبيعة خاصة للأسئلة التي يجب توجيهها للجُناة الذين يتميزون بالذكاء والحِنكة، ما يجعلهم قادرين على مناورة المحقق في سبيل عدم الوصول إلى كشف الحقيقة.

---

[1] قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة (94).

[2] محمد زكي أبو عامر: الإجراءات الجنائية، مُنشأة المعارف، الإسكندرية 1994، ص. 638.

[3] إدوارد غالي الذهبي: الإجراءات الجنائية، مكتبة غريب، ص. 438.

[4] نقض جنائي– جلسة 14 مارس 1985، مجموعة الأحكام، س. 36، رقم 69، ص. 403, نقض جنائي جلسة 3 مارس، 1990، س. 41، رقم 119، ص. 689.

وما يجعل الإستجواب في الجرائم الإلكترونية ذات صعوبة بالغة، إمكانية إرتكابها أو المساهمة فيها من مكان آخر خارج حدود الدولة، وهو ما يُثير التساؤل حول إمكانية إجراء الإستجواب عبر جهاز الكمبيوتر، أو بواسطة الوسائل الإلكترونية الحديثة، وهنا نجد أن الإستجواب في الجرائم الإلكترونية يتميز بطبيعة خاصة عن الإستجواب التقليدي، من حيث صعوبة القيام به، والمكان المخصص له، وطبيعة الأسئلة الموجهة للمتهم.

ويجدر القول، أن الجرائم الإلكترونية يقوم بإقترافها جُناة يتميزون بشخصية خاصة في التعامل مع التقنيات المعلوماتية، وعليه فلا بد لإجراء الإستجواب بالشكل الأمثل والصحيح، أن يتم تأهيل القائمين بالتحقيق في الجرائم الإلكترونية من الناحية الفنية والتقنية[1]، حتى تتم إجراءات إستجواب المتهم بطريقة تمنع فناء الأدلة، ويقوم المجرم بالإعتراف بارتكابه للجريمة.

الفرع الثاني: ضعف ضمانات الإستجواب.

هناك العديد من الضمانات التي تُحيط بالمتهم في مرحلة التحقيق الإبتدائي، وهذا ما تم التأكيد عليه في جميع التشريعات والقوانين والمبادئ العالمية لحقوق الإنسان، فقد نصت المادة رقم (11) من القانون الأساسي لسنة (2003) على أنه 1 " الحرية الشخصية حق طبيعي وهي مكفولة لا تمس" 2 لا يجوز القبض على أحد أو تفتيشه أو حبسه أو تقييد حريته بأي قيد أو منعه من التنقل إلا بأمر قضائي وفقاً لأحكام القانون، ويحدد القانون مدة الحبس الاحتياطي، ولا يجوز الحجز أو الحبس في غير الأماكن الخاضعة للقوانين الصادرة بتنظيم السجون"[2].

---

[1] لابد أن يكون القائم بالتحقيق في الجرائم الإلكترونية مؤهل فنياً وعملياً حتى يتمكن من الحصول على إعتراف المتهم، ومثال ذلك أن يقوم القائم بالتحقيق بإدخال رابط حساب الفيس بوك التابع للمشتكى عليه إلى جهاز المتهم فيتضح له أنه موجود على الجهاز وبالتالي يواجه المتهم ببينة واضحه تجعله يعترف بإرتكابه الجريمة.

[2] القانون الأساسي الفلسطيني لسنة 2003، المادة (11).

وتُعتبر ضمانات إستجواب المتهم في الجرائم الإلكترونية ضعيفة نسبياً، فنقص الخبرة والمعرفة لدى سلطات التحقيق يجعل إجراء الإستجواب منقوصاً، كما أن التفويض بالإستجواب، قد لا يمنح المتهم كامل حقوقه من قِبل المفوض له بإجراء الإستجواب، ما يؤدي لإنتهاك خصوصية المتهم، وهنا يمكن توضيح إجراء الإستجواب بواسطة السلطة المختصة بالتحقيق (الفقرة الأولى)، والإستعانه بمحام خاص (الفقرة الثانية).

الفقرة الأولى: إجراء الإستجواب بواسطة السلطة المختصة بالتحقيق.

بإعتبار أن الإستجواب من الإجراءات الخطيرة والهامة، فقد جعل المشرع مباشرته من قبل جهة قضائية محايدة وهي النيابة العامة، وقد نصت المادة رقم (95) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 على أنه" يتولى وكيل النيابة إستجواب المتهم في الجنايات جميعها، والجنح التي يرى إستجوابه فيها[1]، كما أن المادة رقم (199) من قانون الإجراءات الجنائية المصري نصت على ذلك بإعتبار أن النيابة العامة هي التي تباشر التحقيق في مواد الجنايات والجنح.

وقد نصت المادة رقم (2/55) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 على أنه " للنائب العام أو وكيل النيابة العامة المختص تفويض أحد أعضاء الضبط القضائي المختص، بالقيام بأي من أعمال التحقيق في دعوى محددة، وذلك عدا إستجواب المتهم في مواد الجنايات[2].

[1] قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة رقم (95).

[2] قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة رقم (55).

ولعدم وجود خبرات كافية لدى النيابة العامة، غالباً ما يتم تفويض مأموري الضبط القضائي للإستجواب في تلك الجرائم عدا الجنايات، وهو ما يعكس خصوصية الإستجواب والتحقيق في الجرائم الإلكتروني.

وهناك بعض الحالات التي قد تضيع فيها أدلة الجريمة بفوات الوقت، وهو ما قد يحدث غالباً في الجرائم الإلكترونية، التي تتم بواسطة نبضات كهرومغناطيسية غير ملموسة، ولذلك فقد أجازت المادة رقم (71) من قانون الإجراءات الجنائية المصري لمأمور الضبط القضائي إستجواب المتهم خوفاً من ضياع الوقت، حيث نصت على أنه " يجب على قاضي التحقيق في جميع الأحوال التي يندب فيها غيره لإجراء بعض التحقيقات، أن يُبين المسائل المطلوب تحقيقها والإجراءات المطلوب إتخاذها، وللمندوب أن يُجري أي عمل آخر من أعمال التحقيق أو أن يستجوب المتهم في الأحوال التي يخشى فيها فوات الوقت، متى كان متصلاً بالعمل المندوب له ولازماً في كشف الحقيقة[1].

ونؤيد رأي المشرع المصري الذي أعطى الصلاحية لمأموري الضبط القضائي في إستجواب المتهم إذا كان عامل الوقت قد يؤثر في إثبات أو نفي التهمة[2]، وهو ما ينطبق غالباً على الجرائم الإلكترونية التي لها طابع خاص، ونعتبر أن المشرع الفلسطيني قد جانب الصواب لعدم نصه الصريح على ذلك.

---

[1] قانون الإجراءات الجنائية المصري لسنة 2003، المادة رقم (71).

[2] إن عامل الوقت يعتبر مؤثراً في الجرائم الإلكترونية من حيث إثبات أو نفي التهمة، ومثال ذلك إمكانية قطع التيار الكهربائي أو التعرض لهجمة إلكترونية وقرصنة تؤدي لضياع الأدلة، وهو ما يمكن أن يتم في وقت قصير جداً.

الفقرة الثانية: الإستعانة بمحام خاص.

إن حق المتهم في الإستعانة بمحام أثناء التحقيق يُعتبر من الضمانات الأساسية، فقد نصت المادة رقم (1/96) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 على أنه " يجب على وكيل النيابة عند حضور المتهم لأول مرة إلى التحقيق أن يتثبت من هويته وإسمه وعنوانه ومهنته ويستجوبه بالتهمة المنسوبه إليه ويطالبه بالإجابة عليها، ويخطره أن من حقه الإستعانه بمحام، وأن كل ما يقوله يجوز تقديمه كدليل ضده في معرض البينه عند محاكمته[1].

ولِما تتميز به الجرائم الإلكترونية من خصوصية في الإستجواب والتحقيق، لا بد من وجود محام ذات خبرة ومعرفة في تلك الجرائم، وعليه يجب أن يتم تنظيم دورات وندوات حول طبيعة الجرائم الإلكترونية تساعد السادة المحاميين من حيث كيفية الدفاع في جريمة إلكترونية تعتبر ذات طابع خاص في الأسئلة الموجهة للمتهم.

المطلب الثاني: خصوصية التفتيش

يُعتبر التفتيش من الإجراءات المهمة في الدعوى الجزائية، كونه إجراء من إجراءات التحقيق الإبتدائي، التي تساعد كدليل مادي في الكشف عن الحقائق، وهو بذلك يختلف عن الأدلة الأُخرى مثل شهادة الشهود والإستجواب، كما ينطوي على التفتيش باعتباره إجراءً تحقيقياً الإجبار والمساس بحق السرية[2].

---

[1] قانون الإجراءات الجزائية رقم (3) لسنة 2001, المادة (1/96).

[2] عبد المهيمن بكر: إجراءات الأدلة الجنائية، الجزء الأول في التفتيش، الطبعة الأولى، دار النهضة العربية، القاهرة 1996، ص. 61.

وقد تطرقت معظم دول العالم للقوانين والتشريعات الإجرائية التي ينبع منها التفتيش وقواعده بإعتبار أنه يمس حرية الإنسان، سواء البدنية أو السكنية أو المعلومات الخاصة بالجرائم الإلكترونية في الإنترنت والحاسب الآلي.

وكون الجرائم الإلكترونية تتم بواسطة أجهزة وسيرفرات إلكترونية، لابد من إجراء التفتيش على تلك الأجهزة لأجل الوصول إلى الحقيقة وإثبات تلك الجرائم، الأمر الذي يتطلب مذكرة نفاذ بالإضافة لمذكرة التفتيش، وهو ما يجعل التفتيش الإلكتروني ذات طبيعة خاصة وصعبة، مقارنةً بالتفتيش التقليدي، ومن هنا يتم توضيح محددات التفتيش في الجرائم الإلكترونية (الفرع الأول)، وشروط صحة التفتيش في الجرائم الإلكترونية (الفرع الثاني).

الفرع الأول: محددات التفتيش في الجرائم الإلكترونية.

تُعد الجرائم الإلكترونية من أخطر الجرائم في الوقت الحالي، ومثالها جرائم الحاسب الآلي الخاصة بحرية الإنسان الشخصية، كبطاقات الائتمان التي تحتوي على معظم المعلومات الخاصة بالعميل في البنوك وحساباته، وكذلك جرائم سرقة المعلومات وبالذات الإستخباراتية على مستوى دول العالم، وبالتأكيد فإن هذه الجرائم تختلف عن الجرائم التقليدية شكلاً وموضوعاً، حيث من الممكن إتلاف الدليل الجنائي في أي لحظة.

ويتم التفتيش في الجرائم الإلكترونية بالدخول إلى نظم المعالجة الآلية للبيانات، بما تحتويه من مدخلات ومخرجات وتخزين، وذلك من أجل البحث فيها عن جرائم تم إرتكابها وتشكل جناية أو جنحة، والتوصل إلى أدلة تفيد في إثبات هذه الجرائم ونسبتها إلى المتهم.

ويجدر القول، أن التفتيش في الجرائم الإلكترونية يُعتبر من أخطر الإجراءات الجزائية التي يتم مباشرتها بحق شخص إرتكب جريمة بإستخدام الحاسوب أو شبكة الإنترنت، وذلك نظراً لطبيعة الدليل وصعوبة الوصول إليه[1].

ويُعتبر التفتيش وسيلة إثبات مادي، كونه يستهدف ضبط أشياء مادية تتعلق بالجريمة، أو تفيد في كشف الحقيقة، وهو ما يتعارض مع الطبيعة غير المادية لبيانات وبرامج الحاسب الآلي، وكذلك شبكة الإنترنت، فهي مجرد برامج وبيانات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي[2].

الفقرة الأول: السلطة المختصة بالتفتيش في الجرائم الإلكترونية.

يهدف التفتيش كإجراء من إجراءات التحقيق إلى البحث عن الحقيقة في مستودع السر، وهو من أهم الإجراءات في كشف الحقيقة، وتختص به السلطة المنوط لها مباشرة إجراءات التحقيق وهي النيابة العامة[3].

ويتضح، أن السلطة المختصة بإجراء التفتيش في الجرائم الإلكترونية، هي النيابة العامة ومن يساعدها من مأموري الضبط القضائي، وخبراء أجهزة الحاسوب، حيث أن التفتيش في الجرائم الإلكترونية يختلف عن التفتيش في الجرائم التقليدية، فالبحث عن الدليل في الجرائم

---

[1] هشام فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، القاهرة، النسر الذهبي، 2007، ص. 62 وما بعدها.

[2] أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص. 544، أنظر أيضاً نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية 2007، ص. 221 وما بعدها.

[3] طارق إبراهيم الدسوقي عطية: إجراءات البحث الجنائي في ضبط الجريمة الإلكترونية في ضوء إتفاقية بودابست الموقعة في 23 نوفمبر سنة 2001م والمتعلقة بالإجرام الكوني، مجلة الأمن والقانون، أكاديمية شرطة دبي، الإمارات 2015، ص. 385.

الإلكترونية يتطلب توافر خبرة فنيه معينة لدى المحقق والقائم بالتفتيش، وذلك من أجل المحافظة على الأدلة من الإتلاف والشطب، وإجراء العمل بالسرعة الممكنة.

ونجد، أن القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية نص في المادة رقم (1/32) على أن "للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة"[1].

وتظهر خصوصية التفتيش في الجرائم الإلكترونية في عدم قدرة جميع أعضاء النيابة العامة، أو مأموري الضبط القضائي بإجراءه، فلا بد من القائم بالتفيش أن تتوافر لديه الخبرة الفنية والتقنية في المجال الإلكتروني، فهو أكثر صعوبة من التفتيش التقليدي الذي يمكن لأي شخص القيام به وفقاً للقانون.

الفقرة الثانية: مدى قابلية خضوع أنظمة الحاسب الآلي للتفتيش.

يوجد للحاسب الآلي مكونات مادية، وأخرى معنوية، كما له شبكات إتصال سلكية ولا سلكية محلية ودولية[2].

ويُقصد بالتفتيش في إطار الجرائم الإلكترونية؛ العثور على الأدلة المادية للكشف عن الجرائم ومرتكبيها، وهذا يقود للبحث عن مدى قابلية خضوع الكيان المادي والمعنوي للحاسب الآلي والشبكات الإلكترونية للتفتيش[3].

---

[1] قرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية، مادة رقم (1/32).

[2] هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص. 71.

[3] رُهام سائد أحمد جبر: جريمة الإحتيال الإلكترونية وإجراءات الضبط والتحقيق المتعلق بها، رسالة ماجستير، جامعة القدس، فلسطين 2015، ص. 910.

أ. مدى قابلية خضوع مكونات الحاسوب المادية للتفتيش:

إن حكم تفتيش المكونات المادية للحاسوب[1] يتوقف على طبيعة المكان الذي توجد فيه تلك المكونات، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش هذا المسكن[2].

ولا بد من التمييز بين ما إذا كانت تلك المكونات المراد تفتيشها منفردة عن غيرها من أجهزة الحاسوب الأخرى، أم أنها متصلة بحاسوب آخر في مكان آخر كمسكن غير مسكن المتهم، ففي حال ذلك يجب مراعاة الضمانات التي يستلزمها المشرع لتفتيش هذا المكان[3].

والتفتيش في الجرائم التقليدية، يتم بعد تحديد المكان أو المنزل، أما في الجرائم الإلكترونية لا بد من تحديد مكان الجهاز الإلكتروني حتى يتم ضبطه، وهو ما يجعل ذلك التفتيش خاص بطبيعته وصعباً نوعاً ما.

ب. مدى قابلية خضوع مكونات الحاسوب المعنوية للتفتيش:

آثار تفتيش المكونات المعنوية للحاسب[4] الآلي جدلاً كبيراً في الفقه، بشأن جواز تفتيشها من عدمه، فقد ذهب رأي إلى جواز تفتيش مكونات الحاسوب المعنوية بمختلف أشكالها[5]، بينما ذهب رأي آخر إلى عدم جواز خضوع مكونات الحاسوب المعنوية للتفتيش، ما لم تنص القوانين على خلاف ذلك، بحيث تشمل جميع الأدلة المادية والمعنوية.

---

[1] المكونات المادية: هي مكونات الحاسوب الفعلية التي يمكن لمسها ومشاهدتها، ويشمل ذلك وحدة النظام وكل شيء متصل به مثل لوحة المفاتيح، الفأرة، الشاشة وغيرها، أنظر محرك البحث google.

[2] هلالي عبد اللاه أحمد: تفتيش تظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص. 73.

[3] خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 196.

[4] المكونات المعنوية: وهي الأجزاء التي لا يمكن لمسها في جهاز الحاسوب مثل نظام التشغيل والبرامج والتطبيقات، أنظر محرك البحث google.

[5] أُسامة بن غانم العبيدي: التفتيش عن الدليل في الجرائم المعلوماتية، مرجع سابق، ص. 89.

ويجدر القول، أن معيار تفتيش المكونات المعنوية للحاسب الآلي من عدمه، يرجع إلى النصوص القانونية لكل دولة، فيلاحظ أن القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإكترونية قد نص في المادة رقم (4/32) على أن "لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات"[1].

ونص قانون الإجراءات الجنائية اليوناني في المادة (251) منه على أن "لسلطات التحقيق صلاحية القيام بأي شيء يكون ضرورياً بجمع الدليل وحمايته" وهذا يشمل جميع المكونات المادية وغير المادية المتعلقة بالجريمة ما دام ضبطها يؤدي إلى الكشف عن الأدلة وتعزيزها[2]، وهو ما نص عليه أيضاً القانون الجنائي الهندي[3].

ويُمكن القول، أن إجراء تفتيش مكونات الحاسوب المعنوية في الجرائم الإلكترونية يتميز بخصوصية منفردة، وذلك من حيث ضرورة وجود مذكرة نفاذ مباشر لاحقة لمذكرة التفتيش، والتي يتم إصدارها أيضاً من قبل النيابة العامة.

ويتبين، أن المشرع الفلسطيني كان موفقاً عندما نص بشكل صريح على جواز تفتيش مكونات الحاسوب المعنوية، ما يؤدي إلى تسهيل إجراء التحقيق في الجرائم الإلكترونية، والتي تتم من خلال البرامج والتطبيقات الخاصه بأجهزة الحاسوب.

---

[1] قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية, المادة (4/32).

[2] حسين سعيد الغافري: التحقيق والأدلة في الجرائم المتعلقة بشبكة الإنترنت، ص. 20، منشور بموقع المنشاوي للدراسات والبحوث، على الموقع: www.minshawi.com .

[3] نصت المادة رقم (487) من القانون الجنائي الهندي بأن "صلاحية إصدار إذن التفتيش تمتد إلى أي شيء ما دامت توفرت أُسس معقولة للإعتقاد بأن الجريمة أُرتكبت علي محمود علي حمودة: الجوانب القانونية الأمنية للعمليات الإلكترونية، مجلد رقم (1)، محور القانون الجنائي، ص. 216.

ج. مدى قابلية خضوع شبكات الحاسوب للتفتيش:

تُعرف شبكات الحاسوب بأنها عبارة عن مجموعة مكونة من إثنين أو أكثر من أجهزة الحاسوب، والمتصلة ببعضها إتصالاً سلكياً أو لا سلكياً، كما أنه يوجد شبكات متسعة ومنتشرة في أماكن متفرقه ومرتبطه ببعضها بواسطة الهاتف أو من خلال خوادم ضخمة[1].

ويجدر القول، أن طبيعة التقنية الرقمية قد عقدت من التحدي أمام أعمال التفتيش والضبط، فالبيانات التي تحتوي على أدلة، قد تتوزع عبر شبكة حاسوبية في أماكن بعيدة عن الموقع المادي للتفتيش، وقد يكون موقع تلك البيانات داخل إختصاص قضائي آخر، أو حتى في بلد آخر، وهذا يقود للتميز بين حالتين:

1. إتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة:

وهنا يُثار التساؤل حول إمكانية إمتداد الحق في التفتيش إلى حاسوب أو نهاية طرفية موجودة في منزل آخر غير منزل المتهم؟

يجدر القول، أن الفقه الألماني أعطى الحق في إمتداد التفتيش إذا تبين أن الحاسوب أو النهاية الطرفية في منزل المتهم، متصلة بحاسوب أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم، وذلك إستناداً لمقتضيات القسم (103) من قانون الإجراءات الجنائية الألماني[2].

---

[1] عزة محمود خليل: مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب، جامعة القاهرة، 1994، ص. 520.

[2] عبد العال الديربي: محمد صادق اسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة، القاهرة، الطبعة الأولى، 2012، ص. 302.

كما نص مشروع قانون جرائم الحاسب الآلي في هولندا[1]، على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة في موقع آخر، بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس من المادة 125).

ويُستنتج، أنه يَحق لجهة التفتيش البحث عن الأدلة الجرمية في الأجهزة داخل نطاق إختصاص الدولة، مع مراعاة أن أساس إمتداد السلطة بالتفتيش هنا، هو إحتمال وجود أدلة جرمية تساهم في ظهور الحقيقة.

2. إتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة:

أدى ظهور الإنترنت في جميع أنحاء العالم إلى إرتباط الملايين من الأجهزة ببعضها لمجرد الإتصال بالشبكة، ويُعتبر ذلك من المشاكل التي تواجه السلطات المختصة في جمع الأدلة، فقد يقوم مرتكبي الجرائم الإلكترونية بتخزين المعلومات والبيانات في أنظمة تقنية خارج الدولة[2]، وعليه يثور التساؤل حول كيفية إجراء التفتيش هنا...؟

إن إمتداد الإذن بالتفتيش إلى خارج حدود الدولة التي وقعت فيها الجريمة ودخوله في الحدود الجغرافية لدولة أُخرى، قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها.

ويرى جانب من الفقه، أن إجراء التفتيش الإلكتروني في حدود دولة أخرى، يجب أن يتم بناءً على إتفاقيات خاصة أو دولية تُجيز هذا الإجراء تُعقد بين الدول المعنية[3].

---

[1] هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص. 77.

[2] هلالي عبد اللاه احمد: المرجع السابق، ص. 78.

[3] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، مرجع سابق، ص. 46.

ويجدر القول، أن مشروع قانون جريمة الحاسب الآلي في هولندا، نص على أنه يجوز لجهات التحقيق مباشرة التفتيش داخل الأماكن وبما ينطوي عليه تفتيش نظم الحاسب المرتبطة، حتى إذا كانت موجودة في دولة أخرى، بشرط أن يكون ذلك الإجراء مؤقتاً، وأن تكون المعلومات التي يتم التفتيش عنها لازمة لإظهار الحقيقة (المادة 125).

ويرى الفقه الألماني، أن إختراق حدود دولة أخرى، والسماح بإسترجاع المعلومات، يُعتبر إنتهاكاً لحقوق السيادة لتلك الدولة، وخرقاً للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون في مجال العدالة القضائية[1].

ويتبين، أنه لا بد من تطوير نظرية التفتيش عن بعد في معظم التشريعات، وتحديداً التشريع الفلسطيني، بحيث يتم معالجة هذه الحالات، وبالتالي تكثيف الجهود الدولية بتوقيع الإتفاقيات والمعاهدات للحد من هذه الجرائم.

الفرع الثاني: شروط صحة التفتيش في الجرائم الإلكتروني:

كما ذكرنا سابقاً، فالتفتيش يُعتبر أخطر إجراءات التحقيق، كونه يمس الحريات وينتهك حقوق الأشخاص، وعليه لابد من ضمانات يرتكز عليها إجراء التفتيش لحماية حقوق الأفراد، وهذا يقود للبحث في الشروط الشكلية والموضوعية للتفتيش الإلكتروني.

الفقرة الأولى: الشروط الشكلية للتفتيش الإلكتروني:

لا بد من توافر ضوابط شكلية يجب مراعاتها عند إجراء التفتيش الإلكتروني، وذلك حفاظاً على الحريات الفردية من التعسف في إستخدام السلطة، وهذه الضوابط هي:

[1] عبد العال الديربي: محمد صادق اسماعيل، الجرائم الإلكترونية، مرجع سابق، ص. 303.

أ. تسبيب مذكرة التفتيش الإلكتروني:

يُعتبر تسبيب مذكرة التفتيش من الضمانات المقررة في التشريعات الجزائية، ويقصد بالتسبيب؛ أن الأمر الصادر بالتفتيش يجب أن يكون بناءاً على عدة قرائن ودلائل، بأن المكان أو الشخص

المراد تفتيشه، يحتوي علي ما يفيد في كشف الحقيقة[1].

ويتبين، أنه لا بد أن يكون للتفتيش هدف محدد، فقد يكون مقرر بقصد كشف الحقيقة في جريمة قرصنة أو غيرها، وعليه لا يلزم أن يكون التفتيش شاملاً، وإنما ينبغي أن يكون متخصصاً حتى يصبح مبرراً القيام به[2].

ويجدر القول، أن القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، نص على تسبيب مذكرة التفتيش في المادة رقم (2/32) والذي جاء فيه "يجب أن يكون أمر التفتيش مسبباً ومحدداً ويجوز تجديده أكثر من مره، ما دامت مبررات هذا الإجراء قائمة"[3].

ويُستنتج، أن مذكرة التفتيش لا بد أن تتضمن الأسباب التي جعلت سلطة التحقيق تقوم بهذا الإجراء.

ب. موعد إجراء التفتيش الإلكتروني:

تَمنع بعض التشريعات الإجرائية القيام بتفتيش المنازل وما في حُكمها في وقت معين، وذلك حفاظاً على تضييق نطاق الإعتداء على الحرية الفردية وحرمة المساكن، إلا أن هناك تشريعات أُخرى تركت تحديد الوقت للقائم بالتفتيش[4].

---

[1] أُسامة بن غانم العبيدي: التفتيش عن الدليل في الجرائم المعلوماتية، مرجع سابق، ص. 100.

[2] خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 220-221.

[3] قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية, المادة (2/32).

[4] نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، مرجع سابق، ص. 258.

ونجد، أن قانون الإجراءات الجزائية رقم (3) لسنة 2001، قد حدد وقت إجراء التفتيش في النهار، إلا في حالات إستثنائية، وهو ما تم النص عليه سابقاً، وفي ذات السياق، منع القانون الجزائري والقانون الفرنسي[1] القيام بتفتيش المنازل وما في حكمها في وقت معين.

ويجدر القول، أن قانون الإجراءات الجنائية المصري لم يُحدد وقتاً معيناً يتم فيه إجراء التفتيش، وإنما ترك ذلك لسلطة القائم به، أي أن التفتيش يجوز في كل الأوقات سواء ليلاً أو نهاراً، بغض النظر عن الإعتبارات المتعلقة بالمحل المراد تفتيشه[2].

ونؤيد ما ذهب إليه القانون المصري، بأن ترك للقائم بالتفتيش تحديد الوقت المناسب للقيام به، وذلك نظراً لما تتميز به الجريمة الإلكترونية من حيث أنها ذات صفة عالمية، ويمكن إرتكابها في أي وقت، وأن أدلة الإدانه فيها سهلة المسح والتدمير، وأنها غير مرئية.

ج. حضور بعض الأشخاص أثناء إجراء التفتيش الإلكتروني:

إن حضور أشخاص أثناء التفتيش، يُعتبر من أهم الضمانات الشكلية الواجب إتباعها، وذلك لضمان الإطمئنان على سلامة الإجراء وصحة الضبط.

---

[1] حدد القانون الجزائري وقت إجراء التفتيش من الساعة الخامسة صباحاً إلى الساعة الثامنة مساءً وذلك من خلال نص المادة (47) إجراءات جزائية في فقرتها الأولى "لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحاً ولا بعد الساعة الثامنة مساءً .." ، كما وحدد القانون الفرنسي وقت إجراء التفتيش من الساعة السادسة صباحاً إلى الساعة التاسعة مساءً وذلك من خلال نص المادة 59 إجراءات جنائية "لا يجوز البدء في تفتيش ودخول المساكن قبل الساعة السادسة وبعد الساعة التاسعة".

[2] قضت محكمة النقض المصرية بأنه " من المقرر قانوناً أن لمأموري الضبط القضائي إذا ما صدر إليهم إذن من النيابة بإجراء التفتيش أن يتخذوا ما يرونه كفيلاً بتحقيق الغرض منه دون أن يلتزموا في ذلك طريقة بعينها ما داموا لا يخرجون في إجراءاتهم على القانون، ويكون لهم تخير الظرف المناسب لإجراءه بطريقة مثمرة وفي الوقت الذي يرونه ملائماً، ما دام ذلك يتم خلال الفترة المحددة بالإذن". نقض 8 نوفمبر سنة 1979، مجموعة أحكام النقض، س 30، رقم 170، ص. 799.

ويجدر القول، أن قانون الإجراءات الجزائية رقم (3) لسنة 2001، وكذلك قانون الإجراءات الجنائية الفرنسي، قد تم النص فيها على أن يتم التفتيش بحضور صاحب المسكن أو أشخاص من اقرباءه وجيرانه[1].

ويتبين، أنه يُشترط في جمع الحالات حضور شاهدين أثناء إجراء التفتيش، فذلك يُعتبر ضماناً للمتهم ورقابة على سلامة الإجراء وصحة الضبط[2].

وتبرز خصوصية التفتيش الإلكتروني هنا، في كونه يقع على الأجهزة الخاصه، التي تحتوي على معلومات وبيانات خاصه بصاحبها، فلا بد من إجراء التفتيش بحضور صاحب الجهاز، حفاظاً على عدم إنتهاك خصوصيته.

الفقرة الثانية: الشروط الموضوعية للتفتيش الإلكتروني:

تتضمن الشروط الموضوعية للتفتيش في الجرائم الإلكترونية ما يلي:

أ. وقوع جريمة إلكترونية وأن تكون جناية أو جنحة:

لقد تم تعريف الجرائم الإلكترونية سابقاً بأنها: كل فعل مخالف للقانون يتم إرتكابه بحق جميع الأشخاص سواء الطبيعيين أو المعنويين وذلك عبر الوسائل الإلكترونية والإنترنت.

ويمكن تعريفها أيضاً: كل فعل غير مشروع مرتبط بإستخدام الحاسب الآلي، لتحقيق أغراض غير مشروعه[3].

---

[1] أُنظر الفقرة الأولى مادة رقم (57) من قانون الإجراءات الجنائية الفرنسي وكذلك مادة رقم (43) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة (2001).

[2] هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص. 166.

[3] محمد سامي الشوا: ثورة المعلومات وإنعكاساتها على قانون العقوبات، دار النهضة العربية، الطبعة الثانية، 1998. ص. 8.

ويجدر القول، أن الأصل في القانون عدم جواز إصدار مذكرة تفتيش إلا بعد وقوع جناية أو جنحة وترجحت نسبتها إلى المتهم، وأن يكون هناك قرائن قوية على وجود أشياء تفيد في كشف الحقيقة، وهو ما أقرته محكمة النقض المصرية[1].

ب. إتهام موجه لشخص بإرتكاب الجريمة الإلكترونية أو الإشتراك بها:

يجب أن تتوافر في حق الشخص المطلوب تفتيشه أو تفتيش مسكنه أو حاسبة الآلي، دلائل كافية للإعتقاد بأنه قد ساهم في إرتكاب جريمة الكترونية، بصفته فاعلاً أو شريكاً في هذه الجريمة[2].

ويصح القول، أن تعبير الدلائل الكافية في الجرائم الإلكترونية يُقصد به؛ مجموعة المظاهر والإمارات التي تكفي وفقاً للسياق العقلي والمنطقي، أن ترجع إرتكابها ونسبتها إلى شخص معين، سواء كان وصفه فاعلاً لها أم شريكاً[3].

ويُستنتج، أنه لا يكفي لإجراء التفتيش وقوع جريمة الكترونية فقط، بل يجب أن يكون ذلك الوقوع مقترناً بنسبتها إلى شخص أو أشخاص معينين، إما بصفتهم فاعلين أصليين أو شركاء.

ج. وجود قرائن قوية على أن الشخص يحوز أشياء تتعلق بالجريمة الإلكترونية:

لا يكفي أن تقوم سلطة التحقيق لمجرد وقوع جناية أو جنحة، أو إتهام شخص بإرتكابها أو الإشتراك بها بإصدار مذكرة تفتيش، وإنما يجب أن تتوافر دلائل أو قرائن قوية على أن المتهم الإلكتروني يحوز أشياء أو معدات أو أجهزة تفيد في كشف الحقيقة.

---

[1] أنظر حكم محكمة النقض المصرية لعام 1968م، مجموعة أحكام النقض س. 18، رقم 195، ص. 965.

[2] ممدوح إبراهيم السبكي: حدود سلطات مأمور الضبط القضائي في التحقيق، دار النهضة العربية، القاهرة 1998م، ص. 350.

[3] خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 214.

ويجدر القول، أنه يُشترط لصحة إجراء التفتيش، أن يكون هناك تحريات وإستدلالات بأن جناية أو جنحة قد وقعت من شخص معين، أو أن يكون هناك دلائل وشبهات مقبولة ضد هذا الشخص، بقدر يُبرر تعرض التفتيش لحريته أو لحرمة مسكنه في سبيل كشف إتصاله بالجريمة الإلكترونية[1].

ويتبين، أن إجراء التفتيش لا يتم، إلا إذا توافرت لدى سلطة التحقيق أسباب كافية على أنه يوجد في المنزل أو لدى الشخص المراد تفتيشه أو لدى غيره أدوات أُستخدمت في إرتكاب الجريمة الإلكترونية، أو ناتجة عنها[2].

المطلب الثالث: خصوصية الشهادة.

الشهادة كإجراء من إجراءات التحقيق هي " المعلومات التي تتعلق بالجريمة التي يدلي بها الشاهد أمام سلطة التحقيق بشأن جريمة وقعت "[3]، سواء كانت هذه المعلومات لها صلة بثبوت الجريمة وظروف إرتكابها وإسنادها الى المتهم، أو براءته منها.[4]

والشاهد هو الشخص الذي تصل إليه المعلومات بشأن واقعة معينة عن طريق حاسة من حواسه، وعليه فإن من الطبيعي ألا تتطابق شهادة كل شاهد مع الآخر، نظراً لصعوبة توجيه الشهود جميعاً لحواسهم نحو دقائق واقعة معينة[5].

ويجدر القول، أن للشهادة في مجال الإجراءات الجنائية أهمية كبيرة، وذلك كون الجريمة ليست تصرفاً قانونياً، ولكنها عمل غير مشروع، حيث يجتهد الجاني في التكتم عند إرتكابها[6].

---

[1] نقض 26 يناير سنة 1981، مجموعة أحكام النقض س. 50، رقم 12، ص. 79.

[2] نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، مرجع سابق، ص. 233.

[3] رؤوف عبيد، مبادئ الإجراءات الجنائية: دار الفكر العربي، القاهرة، دون سنة نشر، ص. 455.

[4] تُعرف محكمة النقض المصرية الشهادة بأنها تقرير لشخص لِما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه، نقض 1976/1/25، أحكام النقض، س. 27، ص. 94.

[5] نقض جنائي جلسة 38 أُكتوبر 1962، مجموعة الأحكام، س. 14، رقم 127، ص. 700.

[6] علي عدنان الفيل: إجراء التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنه، مجلة البحوث والدراسات العربية، مصر 2010، ص. 46.

وتُعتبر الشهادة في الجرائم الإلكترونية ذات خاصية مختلفة، حيث أن الشاهد ليس شخص عادي، وإنما يكون غالباً شخص خبير وصاحب معرفة كبيرة في الجانب الإلكتروني، حتى يتم الإستفادة من شهادته في كشف غموض الجريمة والوصول إلى الحقيقة، وهو ما يدفعنا للبحث في أهمية الشهادة (الفرع الأول)، وصعوبة الشهادة في الجرائم الإلكترونية (الفرع الثاني).

الفرع الأول: أهمية الشهادة:

إتفق فُقهاء الشريعة الإسلامية على مشروعة الإثبات بالشهادة وإستدلوا في ذلك على قوله تعالى: "وَلَا تَكْتُمُوا الشَّهَادَةَ ۚ وَمَن يَكْتُمْهَا فَإِنَّهُ آثِمٌ قَلْبُهُ ۗ"[1].

ويجدر القول، أن المشرع الفلسطيني نص على سماع الشهود في قانون الإجراءات الجزائية، وذلك في المادة رقم (77) منه والتي جاء في معرضها " لوكيل النيابة أو المحقق المفوض إستدعاء جميع الأشخاص الذين يرى إمكانية الإستفادة من شهادتهم في كشف الحقيقة، سواء وردت أسماؤهم في التبليغات أو الشكاوي أو لم ترد، وله الإستماع الى أقوال أي شاهد يحضر من تلقاء نفسه، وفي هذه الحالة يُثبت ذلك في المحضر"[2]، وتقابلها المادة (111) من قانون الإجراءات الجنائية المصري[3].

كما أن المشرع أعفى بعض الشهود من حلف اليمين، وذلك في المادة رقم (2/83) من قانون الإجراءات الجزائية والتي نصت على أنه "يُعفى أصول المتهم وفروعه وزوجه من حلف اليمين ما لم تكن الجريمة قد وقعت على أي منهم "[4].

---

[1] سورة البقرة، الآية (283).

[2] قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة (77).

[3] نصت المادة رقم (111) من قانون الإجراءات الجنائية المصري على أنه "تقوم النيابة العامة بإعلان الشهود الذين يقرر قاضي التحقيق سماعهم ويكون تكليفهم بالحضور بواسطة المحضرين أو بواسطة السلطة العامة، ولقاضي التحقيق أن يسمع شهادة أي شاهد يحضر من تلقاء نفسه وفي هذه الحالة يُثبت ذلك في المحضر".

[4] قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة رقم (83).

وبما أن للشهادة أهمية بالغة في مجال الإجراءات الجنائية، فلا يجوز الإمتناع عن أداءها دون عذر مقبول، وهو ما ذهبت إليه المادة (88) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 والتي نصت على أنه " إذا حضر الشاهد وإمتنع عن أداء الشهادة، أو عن حلف اليمين بدون عذر مقبول، يُعاقب من قِبل المحكمة المختصة بغرامة لا تقل عن خمسين ديناراً ولا تزيد على مائه دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً، أو الحبس مدة أُسبوع أو بِكلتا العقوبتين، فإذا عدَّل الشاهد عن إمتناعه قبل إنتهاء المحاكمة جاز إعفاؤه من العقوبة "[1].

وتكمن أهمية الشهادة في الجرائم الإلكترونية، في صعوبة إدراك الجريمة بأحد الحواس أثناء إرتكابها كما في الجرائم التقليدية، فلا يستطيع الشخص معرفة ما يقوم به شخص آخر أثناء إستخدام جهازه الإلكتروني، وعليه فالشاهد في الجرائم الإلكترونية هو شخص فني لديه خبرة كبيرة يقوم من خلالها بمعرفة ما قام به الجاني.

الفرع الثاني: صعوبة الشهادة في الجرائم الإلكترونية.

إن الشاهد في الجرائم الإلكترونية هو الفني صاحب التخصص في تقنيه الكمبيوتر والشبكات، وهو الذي يملك معلومات جوهرية هامة للدخول إلى نظام معالجة البيانات، متى كانت مصلحة التحقيق تقتضي ذلك[2].

هذا ويشمل الشاهد الإلكتروني العديد من الطوائف ومنها:

---

[1] قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة (88).

[2] هلالي عبد اللاه أحمد: التزامات الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، 1997، ص. 23.

1. القائم على تشغيل الحاسب الآلي:

وهو الشخص المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتعلقة به، ويجب أن يكون لديه معرفة كبيرة في تشغيل الجهاز ومعلومات عن قواعد كتابة البرامج[1].

2. المبرمجون:

وهم المتخصصون في كتابة أوامر البرامج ومنهم كاتبوا برامج التطبيقات وكاتبوا برامج النظم.

3. المحللون:

وهم الذين يقومون بتحليل البيانات ودراستها وذلك بتقسيم النظام إلى وحدات، وإستنتاج العلاقات الوظيفية من تلك الوحدات.

4. مهندسون الصيانة والاتصالات:

وهم الأشخاص المسؤلين عن أعمال الصيانة الخاصة بتقنيات الحاسب، بمكوناتها وشبكات الإتصال المتعلقة بها[2].

ويجدر القول، أن الشاهد الإلكتروني والذي يملك معلومات جوهرية لازمة للبحث عن الأدلة التي تتطلبها مصلحة التحقيق، فإنه يكون مطالباً بأن يُقدمها للقائم بالتحقيق في سبيل المساعدة للوصول إلى الحقيقة، وإلا فإنه يتعرض للعقوبة المقررة للإمتناع عن الشهادة[3].

ولعل من الأسلم عند تقديم المعلومات من قِبل الشاهد، أن يُقدمها بإسلوب سهل ومفهوم، حتى يتسنى للقائم بالتحقيق فهم وإدراك تلك المعلومات، وكذلك عليه أن يكون صادق وأمين في تلك المعلومات، فلا يُقدم معلومات كاذبة أو مستند مزور من شأنه خداع أو تضليل القائم بالتحقيق.

---

[1] محمد فتحي: الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع الكتاب المصري الحديث، 1991، ص. 23.

[2] علي عدنان الفيل: إجراء التحقيق الإبتدائي في الجريمة المعلوماتية، مرجع سابق، ص. 48.

[3] هلال عبد اللاه أحمد: التزامات الشاهد بالإعلام في الجرائم المعلوماتية، مرجع سابق، ص. 25.

وعليه، يجب أن يكون القائمين بالتحقيق في الجرائم الإلكترونية مدربين ومؤهلين للتعامل مع الأنظمة الإلكترونية، وذلك حتى يتم إجراء التحقيق بشكل أسهل وأسرع، وهنا تظهر صعوبة الشهادة في تلك الجرائم.

المبحث الثاني: خصوصية في إجراءات التحقيق الإستثنائية.

يُعتبر إجراء التحقيق في الجرائم الإلكترونية ذات طبيعة خاصة، فكما ذكرنا سابقاً تختص النيابة العامة بإجراء التحقيق، ويكون التفويض لمأموري الضبط القضائي في الغالبية العظمى من الجرائم، نظراً للخبرة والمعرفة المتوافرة لديهم، فتحتاج الجرائم الإلكترونية إلى إجراءات تحقيق أصلية تم الحديث عنها سابقاً، وكذلك إجراءات إستثنائية تتلخص في خصوصية ندب الخبراء (المطلب الأول) والتنصت والمراقبة (المطلب الثاني)، والتسرب والإختراق (المطلب الثالث).

المطلب الأول: خصوصية في ندب الخبراء.

يقوم قاضي التحقيق في سبيل الكشف عن الجرائم ومرتكبيها، بإتخاذ العديد من الإجراءات والوسائل المتنوعة اللازمة لتحقيق مُبتغاه، وعِندما كان ذلك يحتاج إلى جهد كبير لا يستطيع القيام به بمفرده، فإن الأمر يقتضي الإستعانة بأهل الخبرة والإستفادة منهم[1].

"والخبرة هي إبداء رأي فني من شخص مختص فنياً، في شأن واقعة ذات أهمية في الدعوى الجنائية"[2]، فهي تتطلب معرفة فنية خاصة تتجاوز إختصاص المحقق أو القاضي

---

[1] خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 282.

[2] محمود نجيب حسني: شرح قانون الإجراءات الجنائية، دار النهضة العربية، 1988م، الطبعة الثانية، ص. 474.

وعليه فلا يجوز لأي منهما أن يضع نفسه محل الخبير، وإلا كان الحُكم الصادر بناءً على ذلك باطلاً[1].

كما عُرفت الخبرة بأنها الإستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات، لمساعدته على تقدير مسألة فنية يحتاج تقديرها إلى معرفة فنية أو دراية علمية[2].

ولعل العنصر الذي يميز الخبرة عن غيرها من إجراءات التحقيق،[3] كالتفتيش، والمعانية والشهادة، هو الرأي الفني الذي يُبديه الخبير في كشف الدليل، والذي يتطلب معرفة علمية أو فنية خاصة لا تتوافر لدى القائم بالتحقيق.

وعلى ما تقدم، فالخِبرة تُعتبر وقفاً على الأخصائيين من أهل العلم والتكنولوجيا, وليس على مجرد ما تم سماعه أو مشاهدته، ولذلك يجوز إستبدال الخبير في الدعوى بغيره من الخبراء[4].

ويتبين، أن رأي الخبير هو محض تقرير فني لواقعه معينة، أي أنه وصف يضعه الخبير على الواقعة من خلال هذا التقرير، والقاضي بدوره يلمس هذا الوصف، أي أنه لا يستطيع أن يستنتج الوصف من تلقاء نفسه، فلا بد أن يستعين بالخبير الفني لتوضيح الأمور لديه[5].

---

[1] فوزية عبد الستار علي: شرح قانون الإجراءات الجنائية، دار النهضة العربية، 1986، ص. 28.

[2] آمال عبد الرحيم عثمان: الخبرة في المسائل الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964، ص.3، وبنفس المعنى، عادل حافظ غانم: الخبرة في مجال الإثبات الجنائي، مجلة الأمن العام المصرية، العدد. 43، 1968، ص. 20.

[3] الخبرة إجراء من إجراءات التحقيق، وقد نصت على ذلك المادة (491) تعليمات النيابة العامة، التعليمات القضائية، مصر من أن "إنتداب الخبراء من إجراءات التحقيق الابتدائي وإذا إفتتحت به النيابة الدعوى فإنه يُعتبر تحريكاً لها".

[4] آمال عبد الرحيم عثمان: الخبرة في المسائل الجنائية، مرجع سابق، ص. 36.

[5] أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص. 588، مأمون محمد سلامة: قانون الإجراءات الجنائية معلقاً عليه بالفقه وأحكام النقض، مرجع سابق، ص. 589.

وندب الخبراء في الجرائم الإلكترونية له طابع خاص ومميز، فالغالبية العظمى من تلك الجرائم تحتاج لخبرة فنية لأجل إثباتها ونسبتها إلى المتهم، فنجد أن أحد الأشخاص قد يتحدث عبر حسابة الشخصي على الفيس بوك ويرتكب جريمة بحق شخص آخر، وعند تقديم شكوى ضده، يتم سماع أقواله فينفي إرتكابه الجريمة وعلاقته بالحساب، وهو ما يجعل دور الخبير مهماً في إثبات عكس ذلك.

الفرع الأول: تعريف الخبرة:

يُعرف الخبير بأنه "المعاون الفني للمحكمة في المسائل التي تتطلب معرفة فنية خاصة[1] تساعد القاضي على فهم الواقعة بالشكل الصحيح، ومن ثم الفصل في القضية"[2].

ويجدر القول، أن إثبات الواقعة قد يتطلب الحصول على رأي خبير مختص، كالأطباء والمهندسين وخبراء الخطوط[3]، وهو ما نصت عليه المادة (64) من قانون الإجراءات رقم (3) لسنة 2001 على أنه "يستعين وكيل النيابة العامة بالطبيب المختص وغيره من الخبراء لإثبات حالة الجريمة المرتكبة..."[4]، وتقابلها في ذلك أيضاً المادة (85) من قانون الإجراءات الجنائية المصري[5].

---

[1] محمد عبد الخالق عمر: قانون المرافعات، دار النهضة العربية، 1978، ص. 452.

[2] علي الحديدي: دور الخبير الفني في الخصومة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1981، ص. 2.

[3] عمر السعيد رمضان: مرجع سابق، ص. 372.

[4] قانون الإجراءات الجزائية رقم (3) لسنة (2001)، المادة رقم (64).

[5] المادة رقم (85) من قانون الإجراءات الجنائية وفقاً لأحدث التعديلات، 2003، حيث نصت على أنه "إذا إستلزم إثبات الحالة الإستعانة بطبيب أو غيره من الخبراء يجب على قاضي التحقيق الحضور وقت العمل وملاحظته".

ويُستنتج، وفقاً لنص المادة رقم (66) من قانون الإجراءات الجزائية رقم (3) لسنة (2001)[1] والتي ألزمت الخبير بتقديم تقرير فني عن عمله، أن هذا التقرير يُعتبر من الأدلة، أما إجراء ندب الخبير فهو من إجراءات جمع الأدلة، وعليه تُحرك به الدعوى الجنائية حتى لو لم تباشر النيابة العامة قبله أي إجراء، وذلك باعتباره من إجراءات التحقيق.

ويتبين، أن قانون الإجراءات الجزائية كان موفقاً عندما نص في المادة رقم (71)[2] منه على حق الخصوم في أن يطلبوا رد الخبير، وذلك لإمكانية تواجد أسباب قد تُشكك في نزاهة الخبير المنتدب من قبل القائم بالتحقيق، كما لو كان صديقاً أو قريباً لأحد الخصوم[3], وهو ما ذهب إليه أيضاً قانون الإجراءات الجنائية المصري[4].

وبإعتبار أن المشرع قد أفسح أمام المتهم كل طرق الدفاع، فقد منحه الحق في الإستعانة بخبير إستشاري، يودع تقريره في ملف القضية حتى يتسنى للمحكمة النظر إليه عند مناقشة تقرير الخبير المنتدب من قبل القائم بالتحقيق،[5] وهو ما نصت عليه المادة (70) من قانون

---

[1] المادة رقم (66) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 نصت على أنه "يلتزم الخبير بتقديم تقرير فني عن عمله خلال الموعد الذي يحدده وكيل النيابة العامة المحقق...."

[2] لقد نصت المادة (71) من قانون الإجراءات الجزائية رقم (3) لسنة (2001) على أنه "الخصوم رد الخبير إذا وجدت أسباب جدية لذلك، ويقدم طلب الرد إلى وكيل النيابة المحقق.. ويترتب على تقديم هذا الطلب عدم إستمرارية الخبير في عمله ما لم يتقرر غير ذلك، ويتعين أن يكون القرار مسبباً".

[3] جلال ثروت: نُظم الإجراءات الجنائية، دار الجامعة الجديدة، 2003، ص. 427.

[4] كذلك نصت المادة (89) من قانون الإجراءات الجنائية المصري على أنه "للخصوم رد الخبير إذا وجدت أسباب قوية تدعوا لذلك ويقدم طلب الرد إلى قاضي التحقيق للفصل فيه ويجب أن تبين فيه أسباب الرد وعلى القاضي الفصل فيه في مدة ثلاثة أيام من يوم تقديمه.

[5] عبد الفتاح بيومي حجازي: الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، مرجع سابق، ص. 599.

الإجراءات الجزائية رقم (3) لسنة 2001، وكذلك المادة رقم (88) من قانون الإجراءات الجنائية المصري[1].

ورغم أن المشرع الأردني لم يعالج مسألة الخبير الاستشاري، إلا أن محكمة التمييز الأردنية إجتهدت بالأخذ بالخبير الإستشاري، فقضت "إن إتاحة الفرصة للدفاع لتقديم بينه فنية في مقابل البينة الفنية المقدمة من النيابة في معرض الإثبات لا يعني أن المحكمة إستبعدت بينة النيابة كما لا يمنع المحكمة من الموازنة والترجيح بينهما وإعتماد الأولى وترجيحها على الثانية إذا تعارضتا، فإذا لم تتعارضا فإن حق المحكمة في إعتماد بينة النيابة هو من باب أولى، وأنه لا يجوز نقض ما ثُبت بالخبرة الفنية الرسمية الجارية تحت إشراف المحكمة بخبرة عادية غير رسمية من قبل خبير أو خبراء لم تنتخبهم المحكمة ولم يحلفوا اليمين القانونية أمامها[2].

الفرع الثاني: أهمية ندب الخبراء في الجرائم الإلكترونية:

أجاز القانون للقائم بالتحقيق الإستعانة بالخبراء المختصين في مسألة معينة، وذلك عندما يصعب على المحقق فهم الجوانب التقنية أو العلمية للكشف عن غموض تلك المسألة[3].

---

[1] نصت المادة (70) من قانون الإجراءات الجزائية رقم (3) لسنة (2001) على أنه "للمتهم أن يستعين بخبير إستشاري ويطلب تمكينه من الإطلاع على الأوراق.." وفي ذات المعنى نصت المادة (88) قانون الإجراءات الجنائية المصري على أنه "للمتهم أن يستعين بخبير إستشاري ويطلب تمكينه من الإطلاع على الأوراق..".

[2] تمييز جزاء، رقم 86، 1987، تاريخ 1987/2/25م، (هيئة خماسية)، منشورات مركز عدالة.

[3] عبد الرؤوف مهدي: شرح القواعد العامة للإجراءات الجنائية، القاهرة، دار النهضة العربية، طبعة 2000، ص. 447، وفي ذات المعنى علي عدنان الفيل: إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، جامعة الموصل، كلية الحقوق، ص. 26.

ومن الواضح، أنه ليست هناك جرائم تحتاج الى تدخل الخبراء أكثر من الجرائم الإلكترونية، حيث أنها تتميز بطبيعة فنية معقدة، وتتمتع بخاصة التطور السريع والمتلاحق الذي يحتاج إلى درجة عالية من التخصص والإمكانيات الفنية المتميزة[1].

ونجد، أن القرار بقانون بشأن الجرائم الإلكترونية رقم (10) لسنة 2018 قد نص على الإستعانة بأهل الخبرة، وذلك في المادة (4/32) والتي قضت بأنه "لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي، أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات.."[2]

ورغم أن الإستعانة بخبير فني أمر جوازي للقائم بالتحقيق، إلا أن هناك مسائل فنية بحتة لا يستطيع القاضي الفصل فيها دون رأي أهل الخبرة، ففي هذه الحالة يجب عليه أن يستعين بالخبراء لإبداء رأيهم، فإذا فَصل في المسألة دون رأي أهل الخبرة كان حُكمة مُعيباً مستوجباً نقضه، وهذا المبدأ إستقر عليه قَضاء محكمة النقض المصرية[3].

ويجدر القول، أن الجرائم الإلكترونية تتميز بطبيعة معقدة، وتتمتع بخاصية فنية تحتاج للإستعانة بأهل الخبرة للتعامل معها، وعليه فلا بد من تأهيل القائمين بالتحقيق ومأموري الضبط القضائي للتعامل مع هذه الطبيعة الخاصة لتلك الجرائم، بحيث يتم متابعتها وكشف مرتكبيها وعرضهم على العدالة.

---

[1] راشد بشير إبراهيم: التحقيق الجنائي في جرائم تقنية المعلومات، دراسة تطبيقية على إمارة أبو ظبي، تَصدر عن مركز الإمارات للدراسات والبحوث الإستراتيجية، العدد 131، ص. 68.

[2] قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، المادة (33).

[3] أُنظر الأحكام التالية التي وردت مجموعة أحكام محكمة النقض المصرية، الدائرة الجنائية، نقض 1961/6/13، س. 12، رقم 131، ص. 671، نقض 1974/9/15، س. 25، رقم 183، ص. 849، نقض 1983/1/4، س. 34، رقم 5، ص. 52.

الفرع الثالث: الخبرة والشهادة.

هناك أوجه شبه بين كل من الخبرة والشهادة، كما أن هناك أوجه إختلاف كثيرة بينهم، يتم توضيحها كالآتي:

الفقرة الأولى: أوجه الشبه بين الخبرة والشهادة:

أ. من حيث الطبيعة القانونية لكل منهما، فكلاهما وسيلة من وسائل الإثبات المباشرة تهدف لتقديم دليل إثبات وهو أقوال الشاهد و تقرير الخبير[1].

ب. من حيث أن كل منهما يتضمن إقرارات شخصية تتأثر بعوامل مختلفة[2]، فالشاهد يتأثر بحالته النفسية والظروف التي أحاطة بها وقت إرتكاب الجريمة ولغاية الإدلاء بأقواله أمام الجهات المختصة[3]، أما رأي الخبير فيتعلق بمدى كفاءته المهنية وقدراته العلمية[4].

---

[1] حسين محمود إبراهيم: النظرية العامة للإثبات العلمي في قانون الإجراءات الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1401هـ، ص. 92، وكذلك علي عوض حسن: الخبرة في المواد المجنية والتجارية، دار الفكر الجامعي، 2002، ص. 8.

[2] وإن كان هنالك من يرى أن للخبير تفوقاً على الشاهد من ناحية صفاء الإدراك، فالشاهد وقت معاينة الواقعة يتأثر بعنصر المفاجئة بها، في حين أن الخبير لا وجود لعنصر المفاجئة في عمله فهو يُمعن النظر بهدوء وصفاء ذهني، رمسيس بهنان: علم النفس القضائي، منشأة المعارف بالإسكندرية 1997م، ص. 86.

[3] عبد الرحمن محمد عبد الله الحضرمي: سلطات مأمور الضبط القضائي في حالة الجريمة المشهودة، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، 1999، ص. 137، وذات المعنى آمال عثمان: مرجع سابق، ص. 37، وما بعدها.

[4] علياء محمد الكحلاوي: الشهادة دليل للإثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة 1999، ص. 151.

ج. من حيث أن للقاضي سلطة تقدير لكل منهما، فهما يخضعان لمبدأ الإقتناع الذاتي للقاضي[1].

الفقرة الثانية: أوجه الاختلاف بين الخبرة والشهادة:

أ. تقتصر الشهادة على الإدلاء بأقوال بشأن ما رآه الشاهد أو سمعه، وعلى ذلك فالشاهد يعتمد على حواسه وذاكرته بما يدلي به[2]، أما الخبير فيقدم رأيه بناءً على معرفة علمية وأصول فنيه.

ب. يمكن إستبدال الخبير بآخر، بينما لا يمكن إستبدال الشاهد بآخر[3].

ج. "أجازت التشريعات المختلفة للخبراء الحق في إجراء بعض التحقيقات والتحري عن الحقيقة كسماع الشهود، والإطلاع على المحاضر، والإستعانة بخبرة غيرهم، وذلك بخلاف الشهادة، إذ لا يجوز للشاهد إجراء تحقيقات في المسألة التي يُراد إثباتها بالشهادة"[4].

د. يتم ندب الخبير بناءً على أمر من السلطة المختصة بذلك[5]، أما الشاهد فيجوز أن يحضر من تلقاء نفسه دون إبلاغ مسبق[6].

---

[1] وإن كان هناك فرق في هذا الجانب فالمحكمة يمكن أن تعتمد تقرير الخبير وتبني عليه حكمها ولو كان مخالفاً للشهادة المقدمة في ذات الواقعة، ولكن لا يحق لها أن تعتمد على الشهادة في دحض الدليل الفني، محمود نجيب حسني: شرح قانون الإجراءات الجنائية، مرجع سابق، ص. 481، وما بعدها.

[2] حسن صادق المرصفاوي: شرح قانون الإجراءات والمحاكمات الجزائية الكويتي، مكتبة الفلاح، الكويت، الطبعة الثالثة، 2005، ص. 641.

[3] أُنظر المادة رقم (67) من قانون الإجراءات الجزائية رقم (3) لسنة (2001)، وكذلك المادة (71) من قانون أُصول المحاكمات الجزائية الأُردني.

[4] محمد غالب الرحيلي: الخبرة في المسائل الجزائية، مرجع سابق، ص. 35.

[5] أُنظر المادة رقم (64) من قانون الإجراءات الجزائية رقم (3) لسنة (2001).

[6] أنظر المادة رقم (77) من قانون الإجراءات الجزائية رقم (3) لسنة (2001).

المطلب الثاني: التنصت والمراقبة.

إن المراقبة من أهم المصادر التي يتم الإستعانة بها للبحث والتقصي عن الجرائم، سواء الجرائم التقليدية أو الإلكترونية، فلا يُمكن الإستغناء عن المراقبة في أعمال البحث والتحري، إذ تعتبر من أسرع الدروب لكشف الجرائم[1].

ويجدر القول، أن القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية نص على جواز مراقبة الإتصالات والمحادثات الإلكترونية، حيث جاء في المادة رقم (1/34) منه أنه "لقاضي الصُلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الإتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يُعاقب عليها بالحبس مدة لا تقل سنة، وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحد، بناءً على توافر دلائل جدية...".

الفرع الأول: تعريف المراقبة الإلكترونية:

تُعرف المراقبة الإلكترونية بأنها "العمل الذي يقوم به المراقِب بإستخدام التقنية الإلكترونية لجمع بيانات ومعلومات عن المشتبه فيه، سواء أكان شخصاً أو مكاناً أو شيئاً حسب طبيعته مرتبط بالزمن (التاريخ والوقت) لتحقيق غرض أمني أو لأي غرض آخر"[2].

وقد عرفها قانون المراقبة السلكية واللاسلكية الفدرالي الأمريكي بأنها "الإلتقاط السمعي، أو أي إلتقاط لمحتويات أي إتصال سلكي أو إلكتروني أو شفوي بإستخدام أي جهاز آخر"[3].

---

[1] مصطفى محمد موسى: المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكِتاب الخامس، الطُبعة الأولى، دار الكتب والوثاق القومية المصرية، 2003, ص. 30.

[2] نبيله هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، مرجع سابق، ص. 198.

[3] عادل عبد الله خميس المعمري: التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات، بحوث ومقالات، 2013، ص. 270.

ويرى جانب من الفقه، أن المقصود بمراقبة المحادثات التلفونية وتسجيلها " التنصت على الأحاديث الخاصة بشخص أو أكثر مشتبه فيه، ويُعتقد بفائدة محادثاته في الكشف عن الحقيقة، وذلك عن طريق إخضاعها لنوع من الرقابة بقصد التعرف على مضمونها[1].

ويتبين، أن المراقبة الإلكترونية هي وسيلة من وسائل جمع المعلومات والبيانات عن المشتبه فيه، وتتم من خلال التقنية الإلكترونية وعبر شبكة الإنترنت، وذلك بعد الحصول على الإذن من الجهات المختصة حسب القانون، وغالباً ما تُستخدم كإجراء تحقيقي في الجرائم الإلكترونية.

وتبرز خصوصية التنصت والمراقبة الإلكترونية في كونها تتم على المحادثات الإلكترونية، أي أنها تكون على جميع الرسائل الخاصة المتعلقة بالتطبيقات الإجتماعية مثل محادثات الفيس بوك والوتس آب والإنستغرام ...إلى أخ، وهذا لا يتم بسهولة، بل يحتاج إلا جهود أشخاص مختصين لديهم أمكانيات كبيرة قد تمكنهم من إجراء التنصت والمراقبة، وقد لا تمكنهم من ذلك، نظراً لصعوبة الوصول إلى تلك المحادثات.

أما في الجرائم التقليدية، نجد أن التنصت والمراقبة تتم على المحادثات السلكية واللاسلكية، وهو إجراء من السهل القيام به من خلال شركات الإتصالات التي تستطيع تزويد جهات التحقيق بجميع المعلومات والبيانات الخاصه بإتصال أو مكالمة معينة.

وهنا يتبين أن إجراء التنصت والمراقبة الإلكترونية ذات خصوصية منفردة من حيث صعوبة إجراءه والقيام به للوصول إلى الحقيقة.

---

[1] هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص. 217.

الفرع الثاني: ضمانات التنصت والمراقبة الإلكترونية:

من حق الإنسان أن تتم حماية حياته الخاصة من أي إعتداء يمسُها، ولعل من أهم الأُمور المتعلقة بخصوصية الإنسان، حقه في أن يتمتع بحماية مكالماته الهاتفية وتواصله مع الاخرين من أن تخضع للتنصت والمراقبة.

وإذا كانت السُلطات القائمة بالتحقيق تستخدم التنصت والمراقبة لإثبات وقوع الجريمة فلابد من وجود ضمانات تُحيط بهذه الوسيلة، حتى يكون الإجراء صحيح[1].

وأهم ضمانات التنصت والمراقبة الإلكترونية مايلي:

الفقرة الأولى: وجوب صدور الإذن من طرف القضاء:

يُعتبر الحصول على إذن من القضاء بالتنصت والمراقبة، من أهم الضمانات اللازمة لمشروعيتها، وقد نصت المادة رقم (2/51) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 على أنه "كما يجوز له مراقبة المحادثات السلكية واللاسلكية، وإجراء تسجيلات لأحاديث في مكان خاص بناءً على إذن من قاضي الصلح متى كان لذلك فائدة في إظهار الحقيقة في جناية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سنة"[2]، وتقابلها في ذلك أيضاً المادة رقم (95) من قانون الإجراءات الجنائية المصري والتي سَبق ذِكرُها.

ويتضح، أن القضاء هو الحامي للحقوق والحريات العامة، والتنصت والمراقبة يُعد إنتهاكاً خطيراً للحرية وللحق في السرية، فيجب أن يصدر الإذن بها من القضاء، منعاً للتعسف من أي جهة أخرى.

---

[1] جهاد الكسواني: قرينة البراءة، الطُبعة الأولى، 2013، دار وائل للنشر، ص. 270.

[2] قانون الإجراءات الجزائية رقم (3) لسنة (2001)، المادة (51).

الفقرة الثانية: أن تكون المراقبة بصدد جريمة معينة وقعت بالفعل:

إن التنصت والمراقبة الإلكترونية إجراء خطير ينتهك الحق في السرية، ولذلك فقد إستلزم القانون عدم مباشرة هذا الإجراء إلا بصدد جريمة معينة وقعت بالفعل[1].

ونجد، أن القانون الفلسطيني لم يُحدد أنواع الجريمة التي تُبرِر إجراء التنصب والمراقبة، بل إرتكز إلى درجة العقوبة وهي الجناية أو الجنحة التي لا تقل عقوبتها عن الحبس لمدة سنة.

الفقرة الثالثة: أن يكون للمراقبة فائدة في إظهار الحقيقة:

لا يكفي وقوع الجريمة لتبرير إجراء التنصت والمراقبة، بل يجب أن تكون هناك فائدة حقيقية تُرجى من ورائِها كشف الحقيقة، وذلك لأَن هذا الإجراء يتضمن إعتداء جسيم على حُرمة الحياة الخاصة، وحق الإنسان في السرية.

ويصح القول، أن قاضي التحقيق هو الذي يُقدر مدى فائدة إجراء التنصت والمراقبة في كشف الحقيقة، فإذا ظهر أن هذا الإجراء لا تُبرره ضرورة كشف الحقيقة، أصبحت غير مشروعة، وبطّل الدليل المُستمد منها[2].

الفقرة الرابعة: أن يكون الإذن بالتنصت والمراقبة مُسبباً ومحدد المُدة:

لقد نصت المادة رقم (3/51) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 على أنه "يجب أن يكون أمر الضبط أو إذن المراقبة أو التسجيل مُسبباً ..."[3] وتقابلها في ذلك أيضاً المادة رقم (95) من قانون الإجراءات الجنائية المصري.

---

[1] مروان صالح الدروبي: الضوابط القانونية لمراقبة المكالمات الهاتفية، دراسة مقارنة، المملكة الأُردنية الهاشمية، جامعة الإسراء الخاصة، ص. 134.

[2] محمود نجيب حسني: شرح قانون الإجراءات الجنائية، مرجع سابق، ص. 668.

[3] قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة (3/51).

وتَعتبر محكمة النقض أن مُجرد إطلاع القاضي على محضر التحريات وإتخاذ ما جاء به من أسباب، يعد تسبيباً لقرار المراقبة.

ويجدر القول، أنه من الضروري أن يتضمن الإذن تحديد مُدة محددة للمراقبة على نحو يلتزم بها مأمور الضبط الذي يُباشر تنفيذ الأمر[1].

المطلب الثالث: التسرب والإختراق.

تتميز الجرائم الإلكترونية بطابع خاص، فالبحث والتحقيق فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة، وبالتالي حل غموضها والوصول إلى الجاني، وعليه فهي من بين الجرائم التي يُمكن اللجوء فيها لأُسلوب التسرب والإختراق إذا دعت ضرورة التحقيق ذلك.

ويجدر القول أن تقنية التسرب والإختراق أدرجها المشرع الجزائري في قانون الإجراءات الجزائية عندما تقتضي ضرورات التحري والتحقيق ذلك في إحدى الجرائم المذكورة في المادة (65 مكرر5) كما يجوز لوكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب والاختراق ضمن شروط محددة[2].

ويُشترط في عملية التسرب والإختراق حصول الضابط المكلف بذلك على الإذن من وكيل الجمهورية المُختص، ويجب أن تتم العملية تحت إشرافه ومراقبته، فإن قرر قاضي التحقيق

---

[1] محمد أبو العلا عقيدة: مراقبة المحادثات التلفونية، دراسة مقارنة، دار الفكر العربي، سنة 1994م، ص. 186- 193 – 194.

[2] قانون الإجراءات الجزائية الجزائري، المادة (65 مكرر 11) الأمر رقم (66-155) المعدل والمتمم، وقد نصت المادة (66 مكرر 5) على أنه "إذا إقتضت ضرورات التحرى في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المُختص أن يأذن بما يأتي: إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية...".

مباشرة هذا الإجراء، وجب عليه أولاً إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح الإذن مكتوب لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه،[1] وهذا تحت طائلة البطلان المطلق[2]، فيجب أن يكون الإذن مكتوباً يتضمن كل ما يتعلق بعملية التسرب، وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرب.

والتسرب هو قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم[3].

ويتبين، أن التسرب هو قيام المكلف بالتحقيق في الجريمة بمراقبة المشتبه بهم، أو التوغل داخل جماعة إجرامية بإيهامهم أنه شريك لهم مُستخدماً الأسماء والصفات المُستعارة والوهمية من أجل الإيقاع بهم، وقد يرتكب عند الضرورة بعض الجرائم دون مساءلته جزائياً[4].

ويُستنتج، أنه لا يجوز للمكلف بالتسرب والإختراق إظهار هويته الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسباب، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر، وهو ما أكده قانون الإجراءات الجزائية الجزائري لسنة 2007 بموجب المادة (65 مكرر 16)[5] والتي نصت على أنه "لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات".

---

[1] محمد حزيط: قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطُبعة الثانية، الجزائر 2009، ص. 115.

[2] البطلان المطلق: هو البطلان المتعلق بالنظام العام، وهو جزاء مخالفة قاعدة قانونية يُقصد بها حماية مصلحة عامة، أنظر محرك البحث google.

[3] قانون الإجراءات الجزائية الجزائري، المادة (65 مكرر 12) الأمر رقم (66-155) المعدل والمتمم.

[4] أمنة بوزينة أمحمدي: إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، مرجع سابق، ص. 71-72.

[5] قانون الإجراءات الجزائية الجزائري، المادة (65 مكرر رقم 66-155) المعدل والمتمم.

ويصح القول، أنه بالرغم من قيام ضباط الشرطة وأعوانهم بعملية التسرب وإيهام المشتبه فيهم بأنهم شُركاء معهم أو فاعلون، إلا أنه يحُظر عليهم أن يُحرضوا المشتبه فيهم على إرتكاب الجريمة، أي أنه يُمنع عليهم أن يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ودفعه لإرتكاب الجريمة، فهذا الفعل ممنوع تحت طائلة بطلان الإجراء.

ويتضح، أن هناك قصور تشريعي في قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 وكذلك القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية في عدم النص والتطرق إلى أُسلوب التسرب والإختراق للكشف عن الجرائم ومرتكبيها، رغم خصوصية تلك الجرائم وحاجتها الماسة لهذا الإجراء.

الفصل الثاني: معوقات إجراءات التحقيق في الجرائم الإلكترونية.

تتم الجريمة الإلكترونية من خلال تقنيات حديثة متطورة، فقد لاقت إجراءات التحري والتحقيق فيها صعوبات وتحديات كثيرة، تختلف في عدة جوانب عن المشاكل التي تواجه الجرائم التقليدية[1].

ويجدر القول، أن الجرائم الإلكترونية تمتاز بخصوصية من حيث صعوبة إثباتها، وذلك لأسباب قد تعود للجاني أو المجني عليه، أو إلى وسيلة تنفيذها، فضلاً عن إمكانية تدمير الدليل في مدة زمنية قصيرة[2].

ويتبين، أن الجريمة الإلكترونية لها طابعها الخاص، فإجراءات التحقيق فيها تختلف عن إجراءات التحقيق في الجرائم التقليدية، من حيث المعوقات التي تواجه عملية التحقيق، وبالتالي صعوبة إكتشاف هذه الجرائم وجمع الأدلة بشأنِها.

وتُعتبر الجريمة الإلكترونية من الجرائم التي لا تترك آثاراً خارجية مادية، فهي لا تترك بقع دماء كما في جرائم الإيذاء والقتل، ولا إتلاف كما في جرائم السرقة والسطو، وعليه فهي جريمة نظيفة لا تترك آثار مادية ملموسة[3]، وبالتالي يصعب التعامل مع الدليل المعنوي الناتج عنها وضبطه لإثبات الجريمة.

ومن هنا يتم توضيح معوقات متصلة بإجراءات التحقيق في الجرائم الإلكترونية (المبحث الأول)، ومعوقات متصلة بإثبات الجرائم الإلكترونية (المبحث الثاني).

---

[1] عبد الحليم إبن بادرة: إجراءات البحث والتحري عن الجريمة المعلوماتية، الخصوصية والإشكالات، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر2015، ص. 88.

[2] غنية باطلي: الجريمة الإلكترونية، دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر 2015، ص. 32/28.

[3] يوسف خليل يوسف العفيفي: الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة، رسالة ماجستير. الجامعة الإسلامية، غزة 2013، ص. 16.

المبحث الأول: معوقات متصلة بإجراءات التحقيق في الجرائم الإلكترونية.

تُعتبر إجراءات التحقيق في الجرائم الإلكترونية خاصة بطبيعتها، فهناك العديد من الصعوبات التي تعترض الجهات المختصة بالتحقيق، ولعل أهم تلك الصعوبات إرتكاب هذه الجرائم في نطاق الأنظمة المعلوماتية وشبكة الإنترنت، كما أن محلها هو معلومات أو جرائم تتعلق بأشخاص عبر عالم غير متناهي وغير محدود، الشيء الذي يمنحها طابع خاص في طريقة ووسيلة إرتكابها[1].

ويرى العديد من الباحثين أن أهم ما يُميّز الجرائم الإلكترونية صعوبة إكتشافها وإثباتها[2]، وكذلك خصوصية إجراءات جمع الأدلة في هذا النوع من الجرائم.

وتواجه السُلطات المختصة بإجراء التحقيق في الجرائم الإلكترونية العديد من المشاكل فطبيعة هذه الجرائم وخصائصها وسمات مرتكبيها، وضعت الجهات المختصة بمكافحتها أمام تحديات لم تكن مهيأة لها، وليست قادرة على فهما والتعامل معها.

ويجدر القول، أن الجرائم الإلكترونية ما هي إلا نبضات إلكترونية، وبالتالي من الصعب أن يتم تعقب آثارها، وإكتشافها، ومعرفة مرتكبيها[3].

---

[1] عبد الحليم إبن بادرة: إجراءات البحث والتحري عن الجريمة المعلوماتية، مرجع سابق، ص. 88.

[2] أُنظر في ذلك: محمد زكي، الإثبات في المواد الجنائية، ص. 16، محمد محي الدين عوض، مشكلات السياسية الجنائية المعاصرة في جرائم نظم المعلومات، ص. 398–399، هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25–28 أكتوبر 1993، منشورات دار النهضة العربية 1993، ص. 450– 476 – 576، زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأُخرى في مجال التكتيك المعلوماتي، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25–28 أكتوبر 1993، العقيد/ علاء الدين محمد شحاته، رؤية أمنية للجرائم الناشئة عن إستخدام الحاسب الآلى، بحث مقدم للمؤتمر السادس للجهة المصرية للقانون الجنائي، القاهرة، 25–28 أكتوبر 1993.

[3] محمد حماد مرهج الهيتي: جرائم الحاسوب، دراسة تحليلية لواقع الإعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، كلية القانون، جامعة الأنبار حالياً، كلية القانون، جامعة التحدي، ليبيا سابقاً، الطُبعة الأولى، 2006، ص. 211.

كما أن نقص الخِبرة لدى الجهات المُختصة بالتحقيق في الجرائم الإلكترونية، يُعتبر من الصعوبات التي تواجه عملية إستخلاص الدليل في هذه الجرائم .

ومما لا شك فيه، أن الجرائم الإلكترونية تبقى مستورة، ما لم يتم الإبلاغ عنها، وثم جمع الإستدلالات والتحريات، أو تحريك الدعوى الجزائية وفقاً للقانون القائم[1]، وعليه فإن الصعوبات التي تعترض عمل الجهات المختصة بالتحقيق في تلك الجرائم، هو أن هذه الجرائم لا تصل إلى سُلطات التحقيق بالصورة العادية كما في الجرائم التقليدية، وذلك نظراً لصعوبة إكتشافها.

ويتضح، أن الجرائم الإلكترونية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، وبالتالي فهي خطيرة وصعبة الإكتشاف، فلا يُمكن تحديد مكان وقوعها بسهولة بسبب إتساع نطاقها المكاني، وضخامة البيانات[2].

ويتبين، أن الجرائم الإلكترونية تتميز بالعديد من الخصائص التي تجعل التعامل معها وضبطها ذات صعوبة بالغة، سواء على المستوى الوطني، أو على المستوى الدولي[3]، فعدم وجود تنسيق بين الدول، خاصة فيما يتعلق بأعمال الإستدلال والتحقيق، يُشكل عائقاً أمام مكافحة هذه الجرائم.

ومن هنا لا بد أن يتم توضيح صعوبات مرتبطة بالجريمة الإلكترونية والجهات المتضررة منها (المطلب الأول)، صعوبات مرتبطة بالدليل الإلكتروني وسلطات الضبط والتحقيق فيها (المطلب الثاني).

---

[1] عبد الفتاح بيومي حجازي: الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، مرجع سابق، ص. 68 – 81.

[2] خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية 2009، ص. 79.

[3] أيمن عبد الحفيظ: الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، 2005، ص. 2013.

المطلب الأول: صعوبات مرتبطة بالجريمة الإلكترونية والجهات المتضررة منها.

يواجه التحقيق في الجرائم الإلكترونية وملاحقة مرتكبيها العديد من المعوقات التي قد تعرقل عملية التحقيق، بل ويمكن أن تؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق، بفقدانه الثقة في نفسه وفي أداءه، وكذلك على المجتمع بفقدانه الثقة في جهات تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم ومحاسبة مرتكبيها، وقد تنعكس على المجرم نفسه، حيث يشعر أن الجهات الأمنية غير قادرة على إكتشاف أمره، وأن خِبرة القائمين على المكافحة والتحقيق لا تجاري خِبرته وعلمه، الشيء الذي يُعطيه ثقة كبيرة في إرتكاب المزيد من هذه الجرائم، التي قد تكون أكثر فداحة وأشد ضرراً على المجتمع[1].

وقد تتصف الجريمة الإلكترونية بعدة سمات تُشكل صعوبات ومعوقات أمام جهات التحقيق، وقد تكون تلك المعوقات عائدة إلى الجهات المتضررة من الجريمة.

الفرع الأول: النشاط الإجرامي فيها لا يمكن رؤيته (سرعة التخفي):

تتميز الجرائم التي تُرتكب على الحاسبات وشبكات المعلومات، بأنها غير مرئية في الكثير من حالاتها[2]، بحيث لا يُلاحظها المجني عليه غالباً، ولا يُدرك حتى وقوعها.

---

[1] عبد الرحمن بحر: معوقات التحقيق في جرائم الإنترنت (دراسة مسحية على ضباط الشرطة بدولة البحرين)، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض 1999، ص. 51.

[2] إذ تقع هذه النوعية من الجرائم في بيئة لا تعتمد التعاملات فيها أصلاً على الوثائق والمستندات المكتوبة بل على نبضات إلكترونية غير مرئية لا يُمكن قراءتها إلا بواسطة الحاسب الآلى والبيانات التي يُمكن إستخدامها كأدلة ضد الفاعل يُمكن في أقل من الثانية العبث بها أو محوها بالكامل: أُنظر هشام محمد فريد رستم: بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت في الفترة بين 1-3 مايو 2000، بجامعة الإمارات العربية المتحدة بعنوان الجرائم المعلوماتية.

ويمكن القول، أن النشاط الذي يمارسه الجاني هو عبارة عن نبضات إلكترونية تسير عبر أسلاك، وفوق أنها نبضات إلكترونية لا يمكن رؤيتها، فهي غالباً ما تكون مُرمزة ومشفرة، وبالتالي يكون نشاط الجاني الإجرامي مُختفي ولا يمكن رؤيته.

ولابد أن نُبين بأن التشفير يختلف عن الترميز، فالتشفير هو تحويل البيانات أو إرسالها إلى جهة محددة عبر وسط ناقل، بحيث لا يُمكن لأي جهة غير الجهة المُرسل إليها تفسير هذه البيانات المبهمة وإستخلاص المعلومات المفهومة مِنها، أما الترميز فهو تحويل المعلومات من جهة مُعينة إلى جهة أُخرى وفق نظام مُحدد، فلا يُمكن فهمها إلا من خلال نظام يفك هذا الترميز ويحولها إلى معلومات يفهمها القارئ[1].

وتوافر المعرفة والخبرة الفنية لدى الجاني تجعله قادراً على إخفاء سلوكه الإجرامي وتغطيته، عن طريق التلاعب غير المرئي في النبضات الإلكترونية التي تسجل البيانات عن طريقها،[2] وبالتالي لا يعلم الشخص المعتدى عليه بوقوع الجريمة إلا بعد حين، أو عن طريق الصُدفة، ومن هذه الجرائم؛ نجد التجسس عبر الإنترنت وبث الفايروسات عبر البريد الإلكتروني وصفحات الإنترنت وجرائم النصب والإحتيال[3].

ويصح القول، أن الطرق والأساليب التي يستخدمها الجُناة في إرتكاب الجرائم الإلكترونية، لم تعهدها الجِهات المعنية بإنفاذ القانون بشكل كامل، وما تزال وسائل هذه الجهات عاجزة عن الدخول في مواجهة مع مرتكبوا هذا النوع من الجرائم، بالكفاءة والفاعلية المطلوبتين.

---

[1] محمد حماد مرهج الهيتي: جرائم الحاسوب، مرجع سابق، ص. 214.

[2] عبد العال الديربي: محمد صادق إسماعيل: الجرائم الإلكترونية، مرجع سابق، ص. 326.

[3] راشد بشير إبراهيم: التحقيق الجنائي في جرائم تقنية المعلومات، مرجع سابق، ص. 79-80.

الفرع الثاني: الجريمة الإلكترونية لا تتطلب جهد:

تتسم الجرائم الإلكترونية بأنها جرائم سهلة الوقوع، حيث لا يلزم لإرتكابها القيام بأي مجهود عضلي كما في الجرائم التقليدية، مثل القتل والإغتصاب والسرقة، فالجاني الإلكتروني يحتاج إلى القدرة العقلية والذهنية لإرتكاب الجريمة، وكذلك إلمامُه بتقنيات الحاسوب، بحيث تُمكنه هذه الميّزات من إرتكاب الفعل خلال لحظات دون أن يترك أثراً[1].

ويتبين، أن المُجرم الإلكتروني يتميز عن المجرمين العاديين في كونه متخصص في تكنولوجيا المعلومات، بحيث تُمكنه قدرته الفنية في التعامل مع الحاسوب وإرتكاب الجرائم بسهولة، وخلال وقت قصير[2].

كما أن المُجرم الإلكتروني يقوم بالتكرار في هذه الجرائم، حيث يعود مُعظم المجرمين لإرتكاب الجرائم مرة أُخرى في مجال الحاسوب، وذلك إما لشغفهم بالمعلومات[3]، أو لحصولهم على الأرباح، أو لإلحاق الضرر والأذى بالغير.

الفرع الثالث: عدم الإبلاغ عن الجريمة الإلكترونية والتكتم عليها:

يُعد تكتم المجني عليهم وإمتناعهم في الإبلاغ عن الجرائم الإلكترونية، من أكثر الصعوبات التي تواجه عملية التحقيق في الجريمة ومكافحتها.

---

[1] أُسامه أحمد المناعسة: جرائم الحاسي الآلى، دار وائل للنشر والتوزيع، عمان 2001، ص. 107.

[2] عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دراسة قانونية متعمقة في القانون المعلوماتي، دار الفكر الجامعي، 2006، ص83 .

[3] عادل عبد الله خميس المعمري: التفتيش في الجرائم المعلوماتية، مرجع سابق، ص. 253.

ويُلاحظ، أن بعض الأفراد الذين يتعرضون للجرائم الإلكترونية يتجنبون الإبلاغ وخصوصاً إذا كانت تلك الجرائم متعلقة بالأُسرة ومخلة بالآداب العامة، فغالباً ما يتستر المجني عليهم على الجريمة حفاظاً على سمعتهم، وخاصة في مجتمعاتنا المُحافظة.[1]

ومما لا شك فيه، أن بعض المؤسسات والشركات التجارية تتجنب إبلاغ الجهات المختصة عن الجرائم التي تُرتكب بحقهم، وقد يرجع سبب عدم الإبلاغ إلى عدة أُمور وهي:

أ. عدم إدراك المؤسسات والشركات التجارية أن مثل هذه الأفعال والهجمات تُعتبر جرائم يُمكن معاقبة مرتكبيها بموجب القانون.

ب. خوف المؤسسات والشركات التي أُرتكبت الجريمة بحقها من أن يؤثر إنتشار خبر الحادث على سُمعتها، ومصداقيتها وظهورها بمظهر مشين أمام الآخرين، لأن تلك الجرائم أُرتكبت ضدها، مما قد يترك إنطباعاً بإهمالها أو قِلة خبرتها أو عدم وعيها الأمني[2].

ج. خوف المؤسسات والشركات من أن تؤدي أعمال التحقيق إلى إحتجاز حاسباتها أو تعطيل شبكاتها فترة طويلة، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق.

د. شُكوك المؤسسات والشركات حول قدرة الجهات المختصة على التعامل مع هذا النوع المستحدث من الجرائم.

هـ. رغبة المؤسسات والشركات في إخفاء الأُسلوب الذي أُرتكبت به الجريمة لكي لا يتم تقليده من الآخرين مستقبلاً[3].

---

[1] يونس عرب: جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير، الجامعة الأردنية، عمان 1994, ص. 72.

[2] طارق عبد الله الشدي: آلية البناء لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض، 1423هـ، ص. 210.

[3] زكي أمين حسونة جرائم الكمبيوتر والجرائم الأُخرى في مجال التكتيك المعلوماتي، مرجع سابق، ص. 476.

و. قد تكون بعض هذه الجرائم محدودة الأثر، مما يدفع بعدم الإبلاغ عنها.

ي. عدم معرفة المؤسسات والشركات بوجود جريمة أصلاً، وعدم القناعة أنها ممكن أن تحدث في مؤسستها[1].

ويُستنتج، أن الجهات المجني عليها قد لا تقف عند حد الإمتناع عن الإبلاغ عن الجرائم، إنما قد يمتد الأمر إلى إمتناعها عن تقديم الأدلة، أو تقديم أي مساعدة للجهات المختصة حال وقوع الجريمة.

الفرع الرابع: صعوبة تعود لطبيعة النظام الآلي:

لا تترك الجرائم الإلكترونية آثاراً مادية، كالتي تنجم عن جرائم السرقة والإعتداء على الأشخاص، فهي جريمة فنية كونها تتعامل مع بيانات ومعلومات مُخزنة إلكترونياً تأخذ شكل الأرقام والرموز[2].

وعلى ما تقدم، فإن التعامل مع الجريمة الإلكترونية والكشف عنها يُعتبر في غاية الصعوبة، ومما لا شك فيه أن مصدر هذه الصعوبة هو أجهزة الحاسب الآلي ذاتها، لسبب يعود إلى النظم التي تعمل بها، بحيث لا يُمكن إتباع الطريق العكسي لِما يخرج منها.

فإذا قام أحد الأشخاص بطباعة ورق، أو أخرج مستند من الحاسب الآلي بعد أن تم تخزينه، فلا يُمكن معرفة من قام بطباعته والغرض الذي طُبع من أجله، بل أن هذه الإمكانية

---

[1] علي عدنان الفيل: إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، مرجع سابق، ص. 84.

[2] محمد محمد شتا: فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، 2000، ص. 971.

حتى لو وُجِدت فإنها تتطلب من يقوم بالتحليل أن يكون متخصصاً، وعلى مستوى عالي من الدراية في علم الحاسب الآلي[1].

كما أن البيانات المُخزنة في الحاسب الآلي قد يتم التلاعب فيها، دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها، ما قد يؤدي إلى إرتكاب الجرائم الإلكترونية؛ كالإختلاس والتزوير مثلاً، وذلك بإجراء تعديل على البرنامج المخزن في الحاسب الآلي، أو إدخال بيانات غير معتمدة في الحاسب الآلي، الأمر الذي يترتب عليه أن تكون مخرجاته ليس على وفق التعليمات المخزنة، وإنما وفق ما يريد مستعمل الجهاز[2].

المطلب الثاني: صعوبات مرتبطة بالدليل الإلكتروني وسلطات الضبط والتحقيق.

هناك العديد من الصعوبات التي تتعلق بعمل سُلطات التحري والتحقيق والإستدلال، وذلك كون الجريمة الإلكترونية كأي جريمة تقليدية تمر بهذه المراحل، إلا أنها تختلف من حيث كيفية القيام بها، وعادة ما تقوم الشرطة بالتحري عن الجريمة بعد وقوعها، فتحريات الشرطة "هي إجراءات تتخذها للكشف عن الجريمة ومعرفة مرتكبيها، وجمع كل ما يتعلق بها من معلومات لازمة"[3].

ومعوقات التحقيق في الجرائم الإلكترونية قد تعود لطبيعة الدليل الإلكتروني، فنجد قدرة الجاني على تدمير الدليل بسهولة وسرعة فائقة، ويُعتبر الكم الهائل من البيانات والمعلومات التي يجب فحصها وتحليلها من العوائق أمام عملية التحقيق.

---

[1] عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، 2002، ص. 36.

[2] محمد حماد مرهج الهيتي: جرائم الحاسوب، مرجع سابق، ص. 219-220.

[3] كما عرفتها المادة رقم (39) من قانون الإجراءات الكويتي رقم (17) لسنة 1960.

الفرع الأول: قدرة الجاني على تدمير أدلة الإدانة:

تتم الجريمة الإلكترونية من خلال إشارات وأوامر تُعطى من الجاني للحاسب الآلي المُنفذ، عن طريق لوحة المفاتيح، وعليه فإن مسألة التخلص من تلك الأوامر تُصبح في غاية السهولة، وهي مشكلة تؤدي إلى صعوبة تحديد الفاعل وكشفه[1].

ويتمتع مرتكبوا الجرائم الإلكترونية بكونهم محترفون، ولديهم قدرة عالية على إستخدام وسائل الحماية اللازمة للهروب من يد العدالة، وإخفاء ومحو الأدلة، وهذا يؤدي إلى صعوبة في تحديد الجناة وكشفهم، فقد يستخدم الجاني برامج حماية على الجهاز الخاص به، أو فيروسات خاصة تؤدي إلى إتلاف ما لديه حال دخول شخص غيره إلى جهازه[2].

فالجاني يُمكنه أن يمحوا الأدلة التي تكون قائمة ضده أو تدميرها، في زمن قياس لا يتعدى ثواني معدودة[3]، بحيث لا تتمكن السُلطات من كشف الجريمة إذا ما علمت بها، وفي حال علمها فإنه يستهدف المحوا السريع لعدم إقامة الدليل ضده[4].

ومن الوقائع العملية على ذلك، قيام أحد مهربين الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسبة الإلكترونية الذي يستخدمه في تخزين عناوين

---

[1] محمد بن حسن السراء: بحوث ومقالات، مرجع سابق، ص. 41.

[2] وضاح محمود الحمود ونشأت مفضي المجالي: جرائم الإنترنت، مرجع سابق، ص. 117-118.

[3] ما شهدته دولة الإمارات العربية من وقائع، ومنها قيام أحد موظفي القطاع الخاص عام 1996 بتهديد مسؤولي إحدى الشركات بمحو كافة بيانات الشركة المخزنة بأنظمة الحاسب الآلي إن لم تستجب لمطالبه الوظيفية، وما لبث أن قام بتنفيذ تهديده ثم أقدم على الإنتحار، الأمر الذي الحق بالشركة أضراراً كبيرة وصعوبات جمة لإسترجاع هذه البيانات، أُنظر: خالد البستاني: ورقة عمل بعنوان "أمن المعلومات وتحليل المخاطر" مقدمة لندوة فيروسات الحاسب الآلي، والتي عقدها معهد التنمية الإدارية بالمجمع الثقافي بأبوظبي في 23 أيلول/ سبتمبر 1996، وذكرها هشام رستم: بحوث ومقالات، مرجع سابق، ص. 430.

[4] علي عدنان الفيل: إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، مرجع سابق، ص. 80.

عملائه والمتعاملين معه، بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذه الحاسبة من خلال لوحة المفاتيح محوا وتدمير كافة البيانات كاملة[1].

وفي حالة أخرى شهدتها المانيا الإتحادية سابقاً، أدخل الجُناة في نظام الحاسب تعليمات أمنية لحماية البيانات المُخزنة داخله من المحاولات الرامية إلى الوصول إليها، ومن شأنها محوا هذه البيانات بالكامل بواسطة مجال كهربائي، وذلك إذا ما تم إختراقه من قبل شخص غير مرخص له[2].

ويُستنتج، أن الأدلة الرقمية وبِحُكم أنها بيانات مُعبر عنها بلغة الآلة والأرقام، يمكن التلاعب بها وإخفائها بسهولة، حيث يقوم الجاني بمحوا وتدمير أدلة الإدانة التي تكون قائمة ضده في زمن قصير جداً.

الفرع الثاني: ضخامة كم البيانات الإلكترونية:

إذا كانت سُلطات التحقيق في الجرائم التقليدية أمام مسرح جريمة واضح محدد المعالم يُمكنهم بناءاً عليه التحقيق فيه، فإنهم في حالة الجرائم الإلكترونية، سيكونوا أمام عالم إفتراضي لا متناهي متباعد الأطراف متصل ببعضه البعض، من حيث المعلومات والأجهزة، وحتى الكم الهائل والضخم من البيانات، وبالتالي فإن هؤلاء المحققين لن يستطيعوا التحقق والتثبت من كل تلك البيانات والمعلومات الضخمة، لأنه عمل شاق ومُرهق أمام قِلة الإمكانيات المادية والبشرية[3].

---

[1] هشام محمد فريد رستم: الجرائم المعلوماتية، أُصول التحقيق الجنائي الفني، مرجع سابق، ص. 430.

[2] عبد العال الديربي: محمد صادق إسماعيل: الجرائم الإلكترونية، مرجع سابق، ص. 329.

[3] سليمان بن مهجة العنزي: وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2003، ص. 98.

ويتضح، أن كمية المعلومات والبيانات الضخمة التي هي في حاجة الى فحص ودراسة كي يُستخلص منها الدليل على إرتكاب الجريمة، تُعتبر من الصعوبات الكبيرة التي تواجه رجال الضبط والتحقيق في الجرائم الإلكترونية، فيجب أن يتوافر لديهم القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة على الحاسب الآلي أو على ديسكات أو إسطوانات منفصلة[1].

ويُلاحظ، أن ضخامة هذه البيانات والمعلومات، تُعد عائقاً أمام التحقيق في الجرائم الإلكترونية، ذلك أن طباعة كل ما هو موجود على الدعامات الممغنطة لحاسب متوسط العمر يتطلب مئات الآلاف من الصفحات، في الوقت الذي قد لا تُقدم فيه هذه الصفحات شيئاً مفيداً في كشف الجريمة[2]، فقد يجد المحققون أنفسهم في مسار خاطئ ليقوموا بعدها بإعادة التحقيق من جديد في معلومات ومعطيات أُخرى.

الفرع الثالث: نقص الخِبرة الفنية:

"تُواجه عملية إستخلاص الدليل في الجرائم الإلكترونية صعوبات جمّة، مثل نقص الخبرة لِدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لِدى أجهزة العدالة الجنائية مُمثلة في سُلطات الإتهام والتحقيق الجنائي"[3].

---

[1] فعلى سبيل المثال نجد أن قرصاً ضوئياً واحداً لا يتعدي وزنه 150 غرام، وقطره 12 سنتميتر، يمكن أن يحوى المادة الكاملة المدونة بألف كتاب في حجم القرآن الكريم، وهذا لا يمنع من تضاعف هذه السعة، حسب التقدم العلمي، نبيل علي: العرب وعصر المعلومات، الكويت، عالم المعرفة 1994، ص. 91 ومابعدها، وقد زادت هذه السعة في الوقت الحالي بظهور الوسيط الإلكتروني للتخزين والذي يطلق عليه (Flash Memory أي F.M).

[2] عبد الفتاح بيومي حجازي: الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، مرجع سابق، ص. 159.

[3] عبد الحليم إبن بادرة: إجراءات البحث والتحري عن الجريمة المعلوماتية، مرجع سابق، ص. 92.

فالتقنية الإلكترونية دائمة التطور بشكل سريع، حيث أن مُرتكبوا هذه الجرائم يُتابعون كل جديد ويعملون على تطوير سُبل إخفاء أدلة جرائِمهم، ومن هنا يتوجب على المُحقق أن يكون على دراسة تامة ومواكِباً للتطور فيما يتعلق بالجرائم الإلكترونية[1].

ونجد، أن أجهزة الأمن في الكثير من دول العالم إهتمت لمواجهة الجرائم الإلكترونية والتحقيق فيها، فالولايات المتحدة الأمريكية، تُمثل أعلى نسبة من المستخدمين لنُظم المعلومات في العالم، وتعاني بشكل كبير من جرائم الحاسوب والإنترنت، ما دعاها إلى إنشاء وحدة متخصصة للمكافحة والتحقيق في هذه الجرائم من ضمن مكتب التحقيق الفيدرالي، ويكون تدريب عناصر هذه الوحدة مُستمراً ليواكب تطور جرائم الحاسوب والإنترنت[2].

وفي المملكة الأُردنية الهاشمية، أنشأت مديرية الأمن العام قِسماً خاصاً بجرائم الحاسوب والإنترنت منذ عام 1998، بحيث يتولى إجراءات المكافحة والإستدلال والتحقيق في الجرائم المُرتكبة بواسطة الحاسوب[3].

ويجدر القول، أن للعاملين في مجال الحاسب الآلي مصطلحات علمية خاصة، أصبحت تُشكل الطابع المميز لمحادثاتهم وأساليب التفاهم فيما بينهم، كما إختصر العاملون في هذا المجال تِلك المُصطلحات والعبارات بالحروف اللاتينية الأُولى، وذلك لتكوين لغة خاصة بهم تُعرف بلغة المختصرات، وهي لغة خاصة بمستخدمي الحاسب الآلي[4]، ولهذا السبب قامت بعض الجهات الأمنية والقضائية بإستقطاب المتخصصين في الجرائم الإلكترونية ليكونوا ضمن كوادرها.

---

[1] خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، مرجع سابق، ص. 225.

[2] حسين سعيد الغافري: التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب، مرجع سابق، ص. 22.

[3] وضاح محمود الحمود: نشأت مفضي المجالي، جرائم الانترنت، مرجع سابق، ص. 119.

[4] محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي، مرجع سابق، ص. 1073.

ويلاحظ، أن السلطة الوطنية الفلسطينية واكبت التطورات في مجال الجرائم الإلكترونية، إذ أصدر مدير عام الشرطة الفلسطينية تعليماته في مطلع عام 2013 بإنشاء وحدة متخصصة لمكافحة هذا النوع من الجرائم تعمل في إدارة المباحث العامة في محافظة رام الله والبيرة وتسمى (وحدة الجرائم الإلكترونية والإتصالات).

حيث تستقبل هذه الوحدة الشكاوي الواردة لوحدات الجرائم الإلكترونية في باقي المحافظات لمتابعتها فنياً، بحيث تتولى إجراءات المكافحة والإستدلال والتحقيق، إلى جانب دورها في توعية المواطنين من مخاطر هذه الجرائم وكيفية الإستخدام الآمن لشبكة الإنترنت.

فعند حضور أحد المواطنين لوحدة الجرائم الإلكترونية في محافظة معينة لأجل الإبلاغ عن جريمة أُرتكبت بحقه، يتم تحرير محضر شكوى[1]، ويتم الحصول على البيانات والمعلومات اللازمة لمتابعة الإجراءات الفنية، ثم تتم إحالة أوراق الملف لوحدة الجرائم الإلكترونية والإتصالات لإستكمالها ومتابعتها.

ويلاحظ، أن هناك إزدياد في معدل إرتكاب الجرائم الإلكترونية في فلسطين[2]، وعليه فمن الضروري إنشاء محكمة مختصة لمكافحة تلك الجرائم تضم قُضاة لديهم الخبرة الفنية الإلكترونية لمتابعة إجراءات ملف الدعوى والتوصل لإدانة المتهم أو براءته.

وتتكون وحدة الجرائم الإلكترونية والإتصالات من أشخاص مختصين في مجال الحاسوب والقانون، وقد زُودت بما يلزم من معدات وبرمجيات تُساعد في إجراء الإستدلال والتحقيق، ويُعد الباحث مديراً لوحدة الجرائم الإلكترونية في فرع المباحث العامة محافظة بيت لحم لغاية تاريخ اليوم.

---

[1] صورة عن محضر شكوى جريمة إلكترونية، أنظر الملحق رقم (1)، صورة عن محضر إفادة مشتبه به في جريمة إلكترونية، أنظر الملحق رقم (2).

[2] إزدياد معدل إرتكاب الجرائم الإلكترونية في فلسطين منذ عام 2013 لغاية 2018 حسب إحصائية وحدة الجرائم الإلكترونية والإتصالات، أنظر الملحق رقم (3).

الفرع الرابع: إرتكاب الجريمة من الخارج:

لقد ساهمت شبكة الإنترنت في جعل العالم قرية واحدة؛ وذلك من خلال تبادل المعلومات والتواصل بين مختلف جهات المعمورة، ورغم الطابع الإيجابي لذلك إلا أنه قد يتحول إلى جانب سلبي يستغله مجرموا المعلوماتية لإرتكاب أفعالهم الإجرامية، والتي تعدت الحدود الجغرافية التقليدية للدول.

وعادةً ما يتم إرتكاب الجريمة الإلكترونية عن بُعد، بحيث لا يتواجد الفاعل على مسرح الجريمة، ومن ثم تتباعد المسافات بين الفعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة، بل قد تمتد إلى النطاق الإقليمي لدول أُخرى ما يضاعف صعوبة إكتشافها وملاحقتها[1].

ويتضح، أن ما يُزيد من الصعوبات التي تواجه السُلطات في شأن إكتشاف الجرائم الإلكترونية وإثباتها، هو أنها جرائم تُرتكب من مناطق ليست بالقريبة عن مكان المجني عليه، بل أنها بعيدة عنه وعن أجهزة الحاسب الآلي الخاصة به، الأمر الذي يجعل تحديد مكان الجُناة وقت إرتكابهم للجريمة صعباً نوعاً ما، ويترتب على هذا الأمر إشكاليات قانونية تتعلق بقواعد الإختصاص وبنطاق سريان القانون[2].

ومما لا شك فيه، أن إرتكاب الجريمة الإلكترونية من خارج حدود الدولة، أدى بشكل كبير إلى ظهور عِدة صعوبات تواجه التعاون الدولي في ظل مكافحة هذه الجرائم، ومن تلك الصعوبات ما يلي:

---

[1] أُسامة محمد محي الدين عوض: جرائم الكمبيوتر والجرائم الأُخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28 اكتوبر 1993.

[2] محمد حماد مرهج الهيتي: جرائم الحاسوب، مرجع سابق، ص. 228.

الفقرة الأولى: عدم وجود نموذج موحد متفق عليه للنشاط الإجرامي:

إن الأنظمة القانونية في بُلدان العالم قاطبة لم تتفق على صورة مُحددة يندرج في إطارها ما يُسمى "بإساءة إستخدام نظم المعلومات الواجب إتباعها" وكذلك لا يوجد تعريف متفق عليه للنشاط الذي تم تجريمة"[1].

ويُلاحظ، أنه لا يوجد إتفاق عام مُشترك بين الدول، حول نماذج إساءه إستخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مُباحاً في أحد الأنظمة، قد يكون مجرماً وغير مُباح في نظام آخر، ويمكن إرجاع ذلك إلى عدة أسباب وعوامل، كإختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر[2]، وبالتالي إختلاف السياسة التشريعية.

الفقرة الثانية: إختلاف وتنوع النظم القانونية الإجرائية:

إن طُرق التحري والتحقيق والمحاكمة التي تُثبت فائدتها في دولة ما، قد تكون عديمة الفائدة في دولة أُخرى، وقد لا يسُمح بإجرائها، وذلك بسبب إختلاف النُظم القانونية الإجرائية.

ويجدر القول، أنه إذا كانت طريقة من طرق جمع الإستدلالات أو التحقيق قانونية في دولة معينة، فقد تكون ذات الطريقة غير مشروعة في دولة أُخرى، وعليه فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة السُلطات المختصة في الدولة الأخرى على إستخدام ما تعتبره هيّ أداة فعالة، بالإضافة إلى أن السُلطات المختصة في الدولة الثانية، قد لا تسمح بإستخدام أي دليل إثبات جرى الحصول عليه بطرق ترى هذه الدولة أنها طرق غير مشروعة[3].

---

[1] عبد الفتاح بيومي حجازي: الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، مرجع سابق، ص. 104.

[2] جميل عبد الباقي الصغير: الإنترنت والقانون الجنائي، دار النهضة العربية، 2001، ص. 72.

[3] محمد نصر محمد: المسؤولية الجنائية لإنتهاك الخصوصية المعلوماتية، الطُبعة الأولى، 2016، مركز الدراسات العربية للنشر والتوزيع، ص. 112.

الفقرة الثالثة: مشكلة الإختصاص:

إن الجرائم الإلكترونية تُعد من أكثر الجرائم التي تُثير مسألة الإختصاص على المستوى المحلي والدولى، وذلك بسبب التداخل والترابط بين شبكات المعلومات، وعليه فإن هذه المشكلة تُعرقل الحصول على الدليل الإلكتروني[1].

وتُثار مشكلة الإختصاص في الجرائم الإلكترونية على المستوى الدولي نظراً لإختلاف التشريعات والنظم القانونية بين الدول، فقد يحدث أن تُرتكب الجريمة في إقليم دولة معينة من قبل أجنبي، وهنا تكون الجريمة خاضعة للإختصاص الجنائي للدولة الأولى إستناداً إلى مبدأ الإقليمية[2].

كما وتخضع كذلك لإختصاص الدولة الثانية على أساس مبدأ الإختصاص الشخصي وأيضاً قد تكون هذه الجريمة من الجرائم التي تُهدد أمن وسلامة دولة أخرى فتدخل عندئذ في إختصاصها إستناداً إلى مبدأ العينية[3].

وقد يُثار تنازع الإختصاص حال تأسيسة على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي هذه الحالة يُثبَت الإختصاص وفقاً لمبدأ الإقليمية لكل دولة من الدولة التي مستها الجريمة[4].

---

[1] محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي، مرجع سابق، ص. 58.

[2] محمد نصر محمد: المسؤولية الجنائية لإنتهاك الخصوصية، مرجع سابق ص. 113.

[3] جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، 2002، ص. 73.

[4] محمد أبو العلا عقيدة: مواجهة الجرائم الناشئة عن إستخدام الحاسب الآلي، مجموعة أعمال مؤتمر حول الكمبيوتر والقانون المنعقدة بالفيوم من 29 ينار إلى 1 فبراير، 1994، جامعة عين شمس، ص. 119.

ونرى، أن مشكلة الإختصاص في داخل إقليم الدولة يُقضى بها على أساس القانون المحلي[1]، فيتعين الإختصاص بالمكان الذي وقعت فيه الجريمة، أو الذي يقيم فيه المتهم، او الذي يُقبض عليه فيه.

وعلى ما تقدم، فإن بعض الدول قامت بعقد إتفاقيات تعاون ثنائية أو عبر المنظمات الإقليمية والدولية، وذلك من أجل تسهيل القيام بإجراءات التحقيق فيما بينها، كالضبط والتفتيش والقبض والإستجواب وتبادل المعلومات، غير أن الأمر يحتاج إلى مزيد من الإجراءات لمعالجة المشكلات المرتبطة بالإختصاص، وذلك من خلال تعاون دولي أوثق وأشمل يواكب تطور الوسائل التقنية في مجالي الإتصالات ونظم المعلومات، ويتجاوز المحاذير الإقليمية وحساسيتها.

ومما لا شك فيه، أنه بتاريخ 27 سبتمبر من العام 2017 قبلت منظمة الشرطة الجنائية الدولية "الإنتربول" دولة فلسطين عضواً فيها، وهي المنظمة التي تهتم بمكافحة جرائم الكمبيوتر ولديها فرقة خاصة لذلك، كما أنها تقوم بتبادل المعلومات حول كيفية إكتشاف هذا النوع من الجرائم، وكذلك تعزيز الإجراءات الأمنية في شأن معلومات وبيانات الحاسب الآلي.

المبحث الثاني: معوقات متصلة بإثبات الجرائم الإلكترونية.

إن السُلطات المختصة بإجراء الضبط والتحقيق في الجرائم الإلكترونية، تواجه العديد من الصعوبات، لا سيما من حيث إمكانية البحث عن مرتكبوا الجرائم وإقامة دليل الإثبات عليهم وتقديمهم للعدالة للقصاص منهم، خاصة في مجال الإثبات الجنائي والشرعية الإجرائية التي لابد منها حتى يتصف الدليل بالمشروعية[2].

---

[1] قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة رقم 163.

[2] سرحان حسن محمد حسن المعيني: التحقيق في جرائم تقنية المعلومات، مرجع سابق، ص. 32.

ويمكن القول، أن الجريمة بصفة عامة تُعتبر حرب قائمة بين الجاني وأجهزة العدالة فيحاول الجاني طمس معالم الجريمة ومنع ما يتخلف عنها، فيلبس قفازات تمنع ظهور بصمات أصابعه، وقد لا ينتعل حذاءً يُمكن من خلاله الإستدلال عليه، وكذلك تقوم أجهزة العدالة بإستخدام كافة الطرق القانونية لكشف الجرائم وإثباتها والقبض على مرتكبيها[1].

وبشكل عام فإن معنى الإثبات: كل ما يؤدي إلى إظهار الحقيقة[2]، أما المعنى القانوني للإثبات فهو إقامة الدليل على وجود واقعة قانونية تترتب آثارها أمام القضاء بالطرق التي حددها القانون[3].

ويرى جانب من الفقه، أن الإثبات هو إقامة الدليل أمام القضاء على تصرف كالقرض أو واقعة كالسرقة، بوسائل إثبات مُحددة من لَدن الُمشرع[4]، وفي المجال الجنائي، فالإثبات هو الوسيلة التي من خلالها يتم إقرار وقوع الجريمة، وعلاقة المتهم بها، ونسبتها إليه[5]، أو هو الوسيلة الثبوتية التي يتوصل إليها قاضي الموضوع لإثبات التهمة على المتهم ونفيها عنه، ومن ثم الحُكم ببراءته[6].

---

[1] محمد حماد مرهج الهيتي: جرائم الحاسوب، مرجع سابق، ص. 221.

[2] جندي عبد الملك: الموسوعة الجنائية، الجزء الأول، دار الكتب المصرية، القاهرة 1931، ص. 104.

[3] عبد الرزاق السنهوري: الوسيط في شرح القانون المدني، الجزء الثاني، القاهرة 1956، ص. 13.

[4] محمد حبيب التجكاني: النظرية العامة للقضاء والإثبات في الشريعة الإسلامية مع مقارنات بالقانون الوضعي، دار النشر المغربية، الدار البيضاء 1985، ص. 205.

[5] فاروق الكيلاني: محاضرات في قانون أُصول المحاكمات الجزائية الأُردني والمقارن، الجزء الثاني، الطُبعة الثانية، 1985، ص. 105.

[6] علي السماك: الموسوعة الجنائية في القضاء الجنائي العراقي، الجزء الأول، مطبعة الجاحظ، 1990، ص. 165.

ومن هنا نجد، أن الإثبات يحتوي في جوهره على كل ما يؤدي إلى ثبوت إجرام المجرم وما يؤدي إلى براءته، لأن المُقرر في نطاق الفقه الجنائي، أنه لا يمكن مساءلة شخص عن جريمة ما لم تُسند إليه مادياً ومعنوياً[1].

ويجدر القول، أن عِبء الإثبات يقع على النيابة العامة بإعتبار أنها تُمثل الحق العام وذلك وفقاً للقواعد العامة التي تَقضي بأن عِبء الإثبات يقع على المدعى، كما وهناك سند آخر تستند إليه هذه القاعدة وهو قرينة البراءة والتي تقضي بأن المتهم بريء حتى تثبت إدانته، وهو ما نصت عليه المادة (1/147) من قانون أُصول المحاكمات الجزائية الأُردني[2] والتي جاء فيها أن "المتهم بريء حتى تثبت إدانته" وتقابلها في ذلك أيضاً المادة (2/206) من قانون الإجراءات الجزائية رقم (3) لسنة 2001[3] والتي نصت على أنه "إذا لم تقم البينة على المتهم قضت المحكمة ببراءته".

ومما لا شك فيه، أن الآثار الناتجة عن الجرائم التقليدية، دائماً ما تكون كيانات مادية أما الجرائم الإلكترونية، نجد خصوصيتها في الكيانات المعنوية الناتجة عنها، وذلك إضافةً للكيانات المادية أيضاً، وعليه لا بد من الحديث عن صعوبات تعترض إثبات الجرائم الإلكترونية (المطلب الأول) وصعوبات نتائج التحقيق في الجرائم الإلكترونية (المطلب الثاني).

---

[1] سعيد حسب الله عبد الله: شرح قانون أُصول المحاكمات الجزائية، دار الحكمة للطباعة والنشر، الموصل 1990، ص. 165.

[2] قانون أُصول المحاكمات الجزائية الأُردني، المادة (1/147).

[3] قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة (2/206).

المطلب الأول: صعوبات تعترض إثبات الجرائم الإلكترونية.

إن الأدلة المادية كبصمات الأصابع وغيرها، والأدلة المعنوية كالشهادة، هي التي تُرجح كفة الإدانة على البراءة في الجرائم التقليدية، وبالتالي يتم إثبات الجريمة من خلال تلك الأدلة أما الجرائم الإلكترونية فإن إثباتها يُعتبر محلاً للإشكال لصعوبة وجود أدلة الإثبات[1].

"ومن ناحية جمع عناصر الإثبات، فقد إعتادت سُلطات الضبط والتحقيق جمع عناصر الإثبات الجنائي بطرق تقليدية، عن طريق الضبط والتفتيش المادي والملموس، بيّد أن هذه الإجراءات التقليدية يصعب القيام بها في حالات جرائم تقنية المعلومات"[2].

وتواجه الجرائم الإلكترونية صعوبات أكبر من حيث إمكانية إثباتها، وذلك نظراً لطبيعة هذه الجرائم التي تكون خافية المعالم على أجهزة العدالة بجميع طوائفها وإخصاصاتها.

ومن خلال تعرضنا سابقاً لمعوقات التحقيق في الجرائم الإلكترونية، سواء الذي يتعلق منها بقدرة الجاني على تدمير أدلة الإدانة التي تتخلف عن إرتكاب الجريمة، أو منها الذي يتعلق بسرعة تخفي تلك الجرائم، أو ما يتعلق بنقص الخبرات الفنية لسُلطات التحقيق والإمكانيات التي تمكنهم من إكتشاف الجريمة، أو التي تعود إلى طبيعة النظام الآلي، فإن النتيجة المنطقية التي تترتب على ذلك هي صعوبة إثبات تلك الجرائم، وهذه الصعوبات هي:

الفرع الأول: عدم تخلف آثار مادية في الجرائم الإلكترونية:

غالباً ما تكون الأدلة المتخلفة عن الجرائم الإلكترونية بيانات غير مرئية، لا يُستدل مِنها على شخص معين، وهذه البيانات مُسجلة إلكترونياً بكثافة بالغة وبصورة مُرمزة، وبالتالي يتم

---

[1] محمد حماد مرهج الهيتي: جرائم الحاسوب، مرجع سابق، ص. 225.

[2] سرحان حسن محمد حسن المعيني: التحقيق في جرائم تقنية المعلومات، مرجع سابق، ص. 35,

قراءتها من قبل الآلة نفسها، ولا يَترك التلاعب فيها أو التعديل أي أثر، وهو ما يؤدي إلى قطع الصلة بين المجرم وجريمته ويحول دون الكشف عنه[1].

ويتضح، أن كون الجرائم الإلكترونية عبارة عن نبضات إلكترونية تملأ جميع أنحاء الكون، وتنساب كالأشعة التي تخترق كل الحواجز، ويمكن إرسالها وإستقبالها من قبل الجاني عن طريق محطات طرفية، فهي بالتالي تختلف عن الجرائم التقليدية من حيث الأدلة المتخلفة عنها[2].

غير أن هذا لا يعني أن الجرائم الإلكترونية لا يتخلف عنها آثار مادية مطلقاً، فقد يتخلف عن بعض الجرائم أثر مادي يكون على شكل ورقة حاول الجاني أن يُجرب نتيجة التلاعب الذي أجراه على البرنامج عليها، أو تسقط منه ورقة كان قد نسخ عليها معلومات المجني عليه.

الفرع الثاني: إتخاذ الجُناة لتدابير أمنية:

يُمكن للمجرم الإلكتروني أن يُزيد من صعوبة الوصول إلى الدليل أو إستنساخه، وذلك من خلال إحاطة البيانات المنقولة عبر شبكات الإتصال بجدار من الحماية الفنية[3]، فقد يتم وضع كلمات سر تزيد من صعوبة إجراءات التفتيش التي يتوقع حدوثها للبحث عن أدلة الادانة[4].

---

[1] عبد العال الديربي: أ. محمد صادق إسماعيل: الجرائم الإلكترونية، مرجع سابق، ص. 327.

[2] محمد حماد مرهج: الهيتي، جرائم الحاسوب، مرجع سابق، ص. 225-226.

[3] تواجه عملية جمع الأدلة الإلكترونية وإستعمالها بعض التحديات الرئيسية ومنها:

- صعوبة الوصول إلى الملفات المحذوفة أو المخبأة أو المحمية بموجب كلمات مرور.
- صعوبة إستعادة البيانات من بعض الوسائل أو الوسائط القديمة.

[4] أُسامة بن غانم العبيدي: التفتيش عن الدليل في الجرائم المعلوماتية، مرجع سابق، ص. 124.

وقد يقوم المُجرم الإلكتروني بإخفاء جريمته، وذلك بالتمويه على أنها أخطاء أو أعطال في أنظمة التشغيل، كما قد يقوم بإزالة آثار الجريمة عن طريق التلاعب في قواعد البيانات والبرامج الخاصة بجهاز الحاسوب[1].

ويمكن اللجوء إلى دَس تعليمات خفية بين هذه البيانات، أو إستخدام التشفير بالنسبة لها بحيث يستحيل على غيرهم الإطلاع عليها، وبالتالي يتعذر على جهاز الضبط والتحقيق كشف أفعالهم[2].

"وقد شهدت ألمانيا الإتحادية حالة واقعية لذلك؛ حيث تتلخص وقائعها في أن الجُناة في إحدى جرائم الحاسب الآلي عمدوا إلى إدخال تعليمات أمنية إلى الحاسب الآلي لحماية البيانات المخزنة داخله من أية محاولة ترمي إلى الوصول إليها، ومن شأن هذه التعليمات الأمنية محوا البيانات المخزنة بالداخل كلياً بواسطة مجال كهربائي، وذلك إذا ما تم إختراقه من قبل شخص آخر غير مصرح له بالدخول"[3].

ويجدر القول، أن غالبية الجُناة في دولة فلسطين لا يستخدمون عند دخولهم إلى شبكة الإنترنت أجهزتهم الخاصة، وإنما يلجؤون إلى مقاهي الإنترنت التي لا تتقيد بأي ضوابط أو أنظمة أمنية يمكن من خلالها التعرف على مستخدموا أجهزة الحاسب الآلي، كما أنهم قد يستخدمون الإنترنت من خلال شرائح الإتصال الإسرائيلية، والتي لا يُمكن التوصل إليها ومعرفة مستخدمها.

---

[1] عبد الحليم إبن بادرة: إجراءات البحث والتحري عن الجريمة المعلوماتية، مرجع سابق، ص. 90

[2] حسين سعيد الغافري: السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة 2009م، ص. 527.

[3] وضاح محمود الحمود: نشأت مفضي المجالي، جرائم الإنترنت، مرجع سابق، ص. 118.

الفرع الثالث: إثبات الجرائم الإلكترونية بالأدلة العلمية:

إن إختلاف الجرائم المعلوماتية عن الجرائم التقليدية، في كونها تُرتكب عن طريق نبضات إلكترونية يُرسلها الجاني إلى جهاز الضحية فيسيطر عليه بعد إختراقه، أدى إلى إثارة فكرة إثبات الجرائم الإلكترونية بالإستناد إلى الدليل العلمي[1].

ويجدر القول، أنه إذا كانت الجرائم الإلكترونية لا تُرتكب بالطرق التقليدية، فإن من شأن ذلك أن تكون طرق إستخلاص الأدلة غير تقليدية، الأمر الذي يُثير أيضاً فكرة الدليل العلمي في مسألة الإثبات[2].

والدليل العلمي، هو الذي ينبعث من رأي الخبير، أي الرجل الفني أو التقني حول تقديم دليل مادي أو معنوي قائم في الدعوى الجنائية، وهذا الدليل يخضع للفحص العلمي ويُستخرج بواسطة أساليب وفنيات علمية حديثة يتقيد بها الخبير الفني[3].

ويرى البعض، أن الخبرة العلمية لا تُعتبر دليلاً، وإنما هي تنقيب عن قرائن ودراستها وإستخلاص دلالتها، وبالتالي فهي من القرائن التي تُعتبر من طرق الإثبات، الأمر الذي يترتب عليه أنها لا تصلح كدليل وحيد للإثبات.

وهناك من يرى، أنه في كثير من الحالات يتم تطبيق القوانين العلمية التي تفترضها الخبرة تطبيقاً مباشراً لكي يُستخلص منها ثبوت الواقعة، وذلك كفحص الحالة العقلية للمتهم لتحديد مسؤوليته، ما يؤدي إلى إعتبار الخبرة دليل للإثبات[4].

---

[1] محمد حماد مرهج الهيتي: جرائم الحاسوب، مرجع سابق، ص. 231.

[2] عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص. 49.

[3] الموقع الإلكتروني (https://www.mohamah.net)، تم الولوج يوم الثلاثاء الموافق 2018/12/18 الساعة PM19:00

[4] محمود نجيب حسني: شرح قانون الإجراءات الجنائية، مرجع سابق، ص. 475.

ونؤيد الرأي الأول الرامي إلى إعتبار الدليل العلمي قرينة يتم الإستناد إليها للوصول إلى الدليل، سواء كان ذلك بالإعتماد على قرائن أخرى، أو إستخلاصاً لما يراه القاضي مناسباً في الدعوى المنظورة أمامه.

المطلب الثاني: صعوبات نتائج التحقيق في الجرائم الإلكترونية.

مما لا شك فيه، أن الهدف من إجراء التفتيش هو ضبط الأدلة المادية التي تُفيد في كشف الحقيقة، فالضبط هو الأثر المباشر الناتج عن التفتيش[1].

ويتضح، أن الغاية من التفتيش هي ضبط الأشياء التي تُساعد في كشف الحقيقة، سواء الأشياء التي تُعد الدليل على الجريمة، أو الأشياء التي يمكن أن يظهر منها هذا الدليل، أو الأشياء التي أُستخدمت في إرتكاب الجريمة، وقد تكون هذه الأشياء السبب الذي وقعت الجريمة من أجله[2].

ويجدر القول، أنه ليس معنى ذلك أن الضبط لا يقع إلا نتيجة للتفتيش، فقد يكون نتيجة لمعاينة، وكذلك يجوز أن تُضبط أشياء قدمها المتهمون أو الشهود بإرادتهم، كما يجوز للقائم بالتحقيق أن يُطالب أي شخص بتقديم شيء موجود في حيازته إليه ويلزمه بذلك، وهو ما نصت عليه المادة رقم (99) من قانون الإجراءات الجنائية المصري والتي جاء فيها[3] "لقاضي التحقيق أن يأمر الحائز لشيء يرى ضبطه أو الإطلاع عليه بتقديمه ..." وللقائم بالتحقيق ضبط الشيء

---

[1] سامي حسني الحسيني: النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، جامعة القاهرة، ط.1، دار النهضة العربية، القاهرة 1972م، ص. 303.

[2] محمود نجيب حسني: شرح قانون الإجراءات الجنائية، مرجع سابق، ص. 481.

[3] قانون الإجراءات الجنائية المصري، المادة (284/99).

بعد تقديمه، ويُعتبر الإمتناع عن تقديم الشيء مُعاقب عليه بعقوبة الإمتناع عن الشهادة، والمنصوص عليها في المادة رقم (284) من ذات القانون.

ومما لا شك فيه أن نتائج التحقيق في الجرائم الإلكترونية يتم التوصل إليها بشكل أصعب من الجرائم التقليدية، وهذا يقودنا للحديث عن ضبط الكيانات المادية والمعنوية والشبكات الإلكترونية.

الفرع الأول: ضبط الكيان المادي والمعنوي للدليل الالكتروني:

لقد ألزمت المادة (1/34) من قانون أُصول المحاكمات الجزائية الأُردني القائم بالتحقيق أن يضبط الأشياء التي أُستعملت في إرتكاب الجريمة، أو التي أُعدت لهذا العرض، كما عليه أن يضبط الأشياء التي تخلفت عن إرتكاب الجريمة وتساعد في إظهار الحقيقة، وإذا وجد في مسكن المشتكى عليه أوراق أو أشياء تؤيد التهمة أو البراءة، فعليه أن يضبطها وينظم بها محضراً[1].

ويتبين، أن الضبط في الجرائم الإلكترونية يقع على الأشياء التي أُستخدمت في إرتكاب الجريمة، أو التي أُعدت لذلك، وهو ما يشمل أجهزة الربط مع الشبكات الإلكترونية، وأجهزة النسخ وتسجيل برامج الحاسب الآلي، وأجهزة إختراق الإتصالات وتحليل الشيفرات وكلمات السر، وكذلك الملفات المعنوية التي تُعتبر وسيلة لإرتكاب الجريمة[2].

ويجدر القول، أنه من السهل الحديث عن إجراء الضبط على الأدلة المادية لمكونات الحاسوب في الجرائم الإلكترونية، بينما تكمن المشكلة عند الحديث عن إجراء الضبط على مكونات الحاسوب المعنوية، وهو ما أثار جدلاً فقهياً كبيراً إذ يرى بعض الفقهاء؛ عدم إمكانية

---

[1] قانون أُصول المحاكمات الجزائية الأُردني، المادة (1/34).

[2] أُسامة أحمد المناعسة: والقاضي جلال محمد: جرائم نظم المعلومات الإلكترونية، عمان، دار الثقافة للنشر والتوزيع، ط.1، 2009، ص. 285.

إجراء الضبط على مكونات الحاسوب المعنوية، بينما يرى آخرون، أنه لا مانع من إجراء الضبط على تلك المكونات[1].

الفقرة الأولى: الدليل والضبط في الجرائم الإلكترونية:

أجازت بعض القوانين ضبط الأدلة الإلكترونية المتعلقة بجرائم الحاسوب والإنترنت وبالتالي ضبط المكونات المعنوية التي يجري تبادلها في نطاق شبكة المعلومات[2].

ونجد أن المادة رقم (487) من القانون الكندي أجازت إصدار أمر قضائي لتفتيش وضبط أي شيء تتوافر بشأنه أُسس ومبررات معقولة تدعوا للإعتقاد بأن جريمة قد وقعت، أو يُشتبه في وقوعها، أو أن هناك نية لإستخدامه في جريمة، وتفسير الفقه الكندي لهذه المادة يوسع من نطاقها إلى حد يسمح بتفتيش وضبط بيانات الحاسوب غير المحسوسة[3].

أ. تعريف الدليل الإلكتروني:

يُعرف الدليل الإلكتروني بأنه "الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، يُمكن تجميعها وتحليلها بإستخدام برامج وتطبيقات وتكنولوجيا خاصة" وهو مُكون رقمي لتقديم معلومات في أشكال متنوعة، مثل النصوص المكتوبة

---

[1] محمد كاسب خطار الشموط: الإثبات في الجرائم الإلكترونية، رسالة دكتوراه، جامعة العلوم الإسلامية العالمية، عمان، ص. 88.

[2] خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، مرجع سابق، ص. 173.

[3] على الطوالبة: مشروعية الدليل الإلكتروني المُستمد من التفتيش الجنائي، بحث منشور علي شبكة الإنترنت على الموقع (www.policemc.gov.bh)، ص. 129، تم الولوج بتاريخ 2019/1/3.

أو الصور أو الأصوات أو الأشكال أو الرسوم وذلك من أجل إعتماده أمام القضاء والأجهزة المعنية في تطبيق القانون[1].

ويتميز الدليل الإلكتروني عن الدليل التقليدي في عدة خصائص:

1. يُعتبر الدليل الإلكتروني من الأدلة العلمية والفنية المأخوذة من أجهزة الحاسوب، فهو دليل تخيّلي سواء في الشكل أو الحجم أو مكان تواجده، وعليه فهو ليس من الأدلة المادية ويتطلب لإدراكه وجود أجهزة الكترونية تعمل وفق برامج خاصة بذلك[2].
2. يأخذ الدليل الإلكتروني شكل المجال المغناطيسي أو الكهربائي، وعليه فإن وضع الدليل الإلكتروني في شكل مادي ملموس لا يعني أنه أصبح دليل مادي، فالقاضي يبني قناعته لإثبات الجريمة الإلكترونية إستناداً على المجال المغناطيسي أو الكهربائي الموجود على الشكل المادي الملموس[3].
3. يَسهل الحصول على الدليل الإلكتروني دون الحاجة إلى وقت أو جهد كبير، وذلك كونه عبارة عن معلومات وبيانات غير مادية تنتقل بسرعة عبر نبض شبكة الإنترنت[4].
4. إن المتخصصين في مجال الجرائم الإلكترونية لديهم القدرة على إستعادة الدليل الإلكتروني بعد إخفاءه من قبل المجرمين، وذلك كون الدليل عبارة عن بيانات ومعلومات مُعبر عنها بلغة أو أرقام أو رموز.

---

[1] محمد كاسب خطار الشموط: الإثبات في الجرائم الإلكترونية، مرجع سابق، ص. 56-57.

[2] محمد البشري: التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية 2004، ص. 237.

[3] علي محمود حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 2003، ص. 22.

[4] محمد كاسب خطار الشموط: الإثبات في الجرائم الإلكترونية، مرجع سابق، ص. 58.

ب. تعريف الضبط في الجرائم الإلكترونية:

يُمكن تعريف الضبط بشكل عام بأنه وضع اليد على شيء يتصل بجريمة وقعت ويُفيد في كشف الحقيقة عنها وعن مقترفيها[1]، وهو جائز سواء أكان الشيء مملوكاً للمتهم أو لغيره من الأشخاص[2].

ويُعرف الضبط أيضاً بأنه "وضع اليد على الشيء وحبسه والمحافظة عليه لمصلحة التحقيق"[3]

وقد إختلف الفقهاء من حيث الطبيعة القانونية للضبط، فيرى البعض، أن الضبط لا يُعتبر من إجراءات التحقيق رغم أنه يترتب على التفتيش الذي يُعد في جوهره من إجراءات التحقيق، بينما يرى البعض الآخر؛ أن الضبط لا يُعتبر من إجراءات الإستدلال إلا إذا تم في مكان يجوز لمأمور الضبط دخوله، مثل الأشياء التي يتم العثور عليها خارج المسكن، أو في الطريق العام، أو في الحقول، أما إذا تم نتيجة تفتيش المتهم أو مسكنه، فيُعد في هذه الحالة من إجراءات التحقيق لا الإستدلال[4]، ونؤيد ما جاء في الرأي الثاني والمتعلق بتكييف الضبط بحسب الجهة التي قامت به.

ويجدر القول، أن الإنقلاب في مفهوم الجريمة، والإنتقال من مسرح الجريمة التقليدي إلى مسرح الجريمة المعنوي في الجرائم الإلكترونية، ساهم في إيجاد قاعدة مناسبة للحديث عن الضبط المعنوي التقني[5].

---

[1] إبراهيم حامد طنطاوي: سلطات مأمور الضبط القضائي، مرجع سابق، ص 578.

[2] عبد المهيمن بكر: إجراءات الأدلة الجنائية، مرجع سابق، ص. 306.

[3] توفيق الشاوي: فقه الإجراءات الجنائية، القاهرة، دار الكتاب العربي، 1954، ص. 363.

[4] عفيفي كامل عفيفي: جرائم الكمبيوتر، مرجع سابق، ص. 350.

[5] فيصل عايش المطيري: مدى مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، دراسة مقارنة، جامعة عمان العربية 2013، ص. 119.

وعلى ما تقدم، يُمكن تعريف الضبط في الجرائم الإلكترونية بأنه "وضع اليد على الدعائم المادية المُخزنة فيها البيانات الإلكترونية أو المعلومات التي تتصل بالجريمة المعلوماتية التي وقعت وتُفيد في كشف الحقيقة عنها وعن مرتكبها"[1].

ووفقاً للقواعد العامة فإن الضبط يقع على الأشياء المادية فقط، مثل المنقولات والعقارات[2]، وبالتالي لا بد من توضيح المقصود بالمنقولات والعقارات في الجرائم الإلكترونية:

1. المقصود بالأشياء المنقولة في الجرائم الإلكترونية:

يُقصد بالمنقول، الشيء الذي يُمكن نقله من مكان إلى مكان آخر دون تلف[3]، ومثال ذلك الهاتف النقال وأثاث مقهى الإنترنت، والحاسب الآلي وملحقاته من طابعات وتصوير، وكذلك الأشياء الثانية التي يُمكن نزعها من أصلها المثبتة به مثل كابلات الحاسب الآلي.

ويلاحظ، أن قانون الإجراءات الجنائية المصري نص على المنقولات التي يقع عليها الضبط على سبيل المثال لا الحصر، فذكرت المادتان (55) و(2/91) أنه "... الأوراق والأسلحة وكل ما يحتمل أن يكون قد أُستعمل في إرتكاب الجريمة أو نتج عن إرتكابها أو ما وقعت عليها الجريمة وكل ما يُفيد كشف الحقيقة[4]، وتقابلهما في ذلك أيضاً المادة (2/50) من قانون الإجراءات الجزائية رقم(3) لسنة 2001[5].

---

(1) نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، مرجع سابق، ص. 66.

(2) لا يجوز ضبط الأشخاص، لأن الشخص ليس شيء وإنما يجوز القبض عليه، والقبض يمس حرية الشخص الفردية، أما الضبط فيقع على الأشياء، ويمس الملكية أو الحيازة أنظر، سامي حسني الحسيني: النظرية العامة للتفتيش في القانون المصري والمقارن، مرجع سابق، ص. 305.

(3) عبد المهيمن بكر: إجراءات الأدلة الجنائية، مرجع سابق، ص. 310.

(4) قانون الإجراءات الجنائية المصري، المادة (55)، المادة (2/91).

(5) قانون الإجراءات الجزائية رقم (3) لسنة 2001، المادة (2/50).

ويتبين، أن الأشياء التي تُساعد وتفيد في كشف الحقيقة، قد تتواجد في مسرح الجريمة، أو في مكان آخر لدى المتهم أو غيره، وهذه الأشياء قد تكون من القرائن القضائية التي يصل القاضي من خلالها إلى الحقيقة[1].

وهو ما ينطبق على الجرائم الإلكترونية، التي كغيرها من الجرائم تَمُر في مرحلة التفكير والتخطيط والتنفيذ، وثم إخفاء المعالم والآثار، ويمكن إثباتها بالأدلة المعروفة، كالإعتراف وشهادة الشهود والقرائن[2].

2. المقصود بالعقار في الجرائم الإلكترونية:

يُقصد بالعقار في الجرائم الإلكترونية، المكان الذي يوجد فيه آثار لجريمة إلكترونية تُساعد على كشف الحقيقة، كالآثار الموجودة في مقهى للإنترنت، وهو ما يستدعي التحفظ على المكان لمصلحة التحقيق.

وقد نص قانون الإجراءات الجنائية المصري على ذلك في المادة رقم (53) والتي جاء في معرضها "لمأموري الضبط القضائي أن يضعوا الأختام على الأماكن التي بها آثار وأشياء تساعد في كشف الحقيقة، ولهم أن يقيموا حُراساً عليها، ويجب عليهم إخطار النيابة العامة بذلك في الحال، وعلى النيابة إذا ما رأت ضرورة ذلك الإجراء أن ترفع الأمر إلى القاضي الجزئي لإقراره"[3].

---

[1] سامي حسني الحسيني: النظرية العامة للتفتيش في القانون المصري والمقارن، مرجع سابق، ص. 330-331.

[2] مصطفى محمد موسى: التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 221.

[3] قانون الإجراءات الجنائية المصري، المادة (53).

ويُستنتج، أنه إذا ما وقعت جريمة إلكترونية من داخل مكان مُعين وتخلف عنها آثار مادية أو معنوية، جاز لمأمور الضبط القضائي ضبط العقار وفقاً للإجراءات القانونية وخوفاً من ضياع الأدلة.

الفقرة الثانية: ضبط الكيان المادي في الجرائم الإلكترونية:

كما ذكرنا سابقاً، فإن الهدف من التفتيش هو ضبط كل الأشياء التي يُعتقد أنها قد أُستعملت في إرتكاب الجريمة، أو نتجة عنها، أو وقعت عليها سواء كان ذلك أوراق، أو أسلحة، أو الآت، وبالتالي ضبط الأدلة المادية التي تُفيد في كشف الحقيقة، بما في ذلك أدلة الإدانة، أو أدلة البراءة[1].

وعلى ذلك يُصبح التفتيش تحكمياً، إذا ما تم بخصوص جريمة لا يتخلف عنها آثار مادية، كما في جرائم الذم والقدح، وإختلاق الجرائم والإفتراء[2].

ويصح القول، أن ضبط الكيانات المادية في الجرائم الإلكترونية لا يُثير أي خلاف في الفقه، وبالتالي يُمكن ضبط جميع الأدلة بحسب القواعد التقليدية للتفتيش[3]، فلا يوجد خلاف في الفقه حول إمكانية ضبط هذه المكونات.

وقد نص قانون أُصول المحاكمات الجزائية الأُردني على ذلك، حيث جاء في معرض المادة (32) منه أنه "يضبط المدعي العام الأسلحة وكل ما يظهر أنه أُستعمل في إرتكاب الجريمة أو أُعد لهذا الغرض، كما يضبط كل ما يرى من آثار الجريمة وسائر الأشياء التي

---

[1] علي حسن محمد الطوالبة: التفتيش الجنائي على نظم الحاسوب والإنترنت، مرجع سابق، ص. 137-138.

[2] أحمد عوض بلال: قاعدة إستبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنه، دار النهضة العربية، القاهرة 1994م، ص. 392.

[3] أُسامة بن غانم العبيدي: التفتيش عن الدليل في الجرائم المعلوماتية، مرجع سابق، ص. 107.

تُساعد على إظهار الحقيقة ويستجوب المدعي العام المشتكى عليه عن الأشياء المضبوطة بعد عرضها عليه ثم يُنظم محضراً يوقعه والمشتكى عليه وإذا تمنع هذا الأخير عن التوقيع صرح بذلك في المحضر"[1].

أ. ضبط جهاز الحاسوب ومكوناته الرئيسية والفرعية:

عند وقوع جريمة إلكترونية، لا بد من وجود جهاز حاسب آلي له علاقة بمسرح الجريمة، أو بمرتكبها، ويجدر القول، أن أجهزة الحاسب الآلي تختلف من حيث السرعة والدقة في الحصول على النتائج، ولكن قد يتمكن الخُبراء حال ضبط هذه الأجهزة من تمييز نوع الحاسب وسرعته والأسلوب الأمثل للتعامل معه[2].

وأجازت بعض التشريعات إتخاذ أي إجراء لازم لجمع الأدلة والحفاظ عليها، وهو ما يشمل مكونات الحاسوب المادية[3]، ومنها على سبيل المثال قانون الإجراءات الجنائية اليوناني المادة (251) منه، وقانون الإجراءات الجنائية الكندي المادة (487) منه، وكذلك القانون اللوكسومبرجي الذي إعتبر أن الضبط "يشمل كل الأشياء التي تكون مفيدة في إطار الحقيقة".

بينما نصت بعض التشريعات صراحةً على التفتيش وضبط مكونات الحاسوب المادية ومنها قانون إساءة إستخدام الحاسوب في إنكلترا الصادر عام 1990م، وكذلك القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية والذي نص في المادة (3/32) منه على أنه "إذا أسفر التفتيش في الفقرة (2) من هذه المادة عن ضبط أجهزة، أو أدوات، أو وسائل ذات صلة

---

[1] قانون أُصول المحاكمات الجزائية الأردني، المادة (32).

[2] عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص. 18.

[3] هشام محمد فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص. 64.

بالجريمة يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات وعرضها على النيابة العامة لإتخاذ ما يلزم بشأنها[1].

ويُستنتج، أن ضبط الكيانات المادية للحاسب الآلي في الجرائم الإلكترونية، لا يُثير مشاكل في الفقه المقارن، وبالتالي لا يوجد خلاف حول إمكانية ضبط هذه المكونات وتقديمها إلى الجهات المختصة، ومنها على سبيل المثال، الورق، وجهاز الحاسب الإلكتروني وملحقاته، ولوحة المفاتيح والشاشة، والطابعات.

ب. القواعد العامة في ضبط مكونات الحاسوب والإنترنت:

لقد سبق الحديث عن إمكانية ضبط مكونات الحاسب الآلي وملحقاته الرئيسية والفرعية التي تُساعد في كشف الحقيقة، وكذلك التحفظ على العقارات التي تحتوي على آثار للجريمة الإلكترونية، أو أشياء يتعذر نقلها[2].

ويصح القول، أن القائم بالتفتيش يُقدر مدى فائدة ضبط الشيء في كشف الحقيقة، وعليه فهو لا يضبط إلا الأشياء التي تُساعد في إظهار الحقيقة.

وأجازت التشريعات الإجرائية للقائم بالتفتيش ضبط الأشياء التي تظهر عرضاً، والتي تُعد حيازتها جريمة بحد ذاتها، أو التي تُساعد في الكشف عن حقيقة جريمة أُخرى، وهو ما نصت

---

[1] قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، المادة (32).

[2] لا يُعد هذا الإجراء ضبطاً للمكان، وإنما هو إجراء تحفظي قد تقتضية مصلحة التحقيق للتحفظ على الآثار والأشياء التي تُفيد في كشف الحقيقة، خصوصاً إذا ما إقتضى الكشف عنها الإستعانة بالخبراء حتى لا يتم العبث بالأدلة الجرمية في هذا المكان إلى أن تفرغ سلطة التحقيق من إستكمال معاينة مسرح الجريمة، سامي حسني الحسيني: النظرية العامة للتفتيش في القانون المصري والمقارن، مرجع سابق، ص. 331.

عليه المادة (50) من قانون الإجراءات الجزائية رقم (3) لسنة 2001[1]، ويجب على المحكمة التأكد من ظهور الشيء عرضاً، وبالتالي عدم التعسف في تنفيذ إذن التفتيش.

ومنعت بعض التشريعات ضبط الأوراق، أو المستندات، أو الرسائل المتبادلة بين المتهم والمُدافِع عنه في القضية، فقد نصت المادة رقم (211) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 على أنه "لا يجوز إثبات واقعة بالرسائل والأحاديث المتبادلة بين المتهم ومحاميه"[2].

ونرى، أن منع الضبط يمكن أن يشمل كذلك المحادثات التي تتم بين المشتكى عليه ومحاميه إذا تمت عبر الإنترنت أو حتى بالبريد الإلكتروني.

الفقرة الثالثة: ضبط الكيان المعنوي في الجرائم الإلكترونية:

لقد ذكرنا سابقاً، أن الضبط يقع بشكل عام على الأشياء المادية، سواء المنقولات أو العقارات، ونظراً لكون محل الضبط في الجرائم الإلكترونية هو البيانات المعالجة إلكترونياً، فيثور التساؤل الآتي: هل يقع الضبط على الأشياء المعنوية ...؟ أي هل يمكن أن ينطبق على الكيانات المنطقية للحاسوب والإنترنت...؟

لقد إختلفت الإتجاهات الفقهية في مسألة ضبط الكيانات المنطقية للحاسوب والإنترنت والتي لا يمكن وضع اليد عليها[3].

---

[1] لقد نصت المادة (50) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 على ضبط كل ما يظهر عرضاً أثناء التفتيش من أشياء تُعد حيازتها جريمة أو ما يفيد في كشف حقيقة جريمة أُخرى.

[2] تقابلها بالتشريعات العربية المواد: المادة (96) من القانون المصري، المادة (152) من القانون الأُردني، المادة (77) من القانون الإماراتي، المادة (80) من القانون الليبي.

[3] محمد زكي أبو عامر: الإجراءات الجنائية، مرجع سابق، ص. 629.

ويرى جانب من الفقه، أن بيانات الحاسوب ليست أشياء مادية محسوسة، وعليه لا يمكن تصور إجراء الضبط عليها لإنتفاء الكيان المادي عنها[1]، وهو ما نص عليه التشريع الألماني في قانون الإجراءات الجنائية، حيث إعتبرت المادة (94) أن الضبط لا يقع إلا على الأشياء المادية الملموسة أو المحسوسة، ويُفِسر الفقه الألماني ذلك؛ بأن البيانات المعالجة إلكترونياً لا يُمكن ضبطها مجردة، إلا عند تحويلها أو إضافتها إلى كيان مادي مثل طباعتها على ورق، ومن ثم يمكن التعامل معها[2].

وكذلك الأمر فإن الضبط وفقاً للتشريع الروماني يقع على الدعامة المادية الموجود عليها بيانات الحاسوب، كالأقراص والأشرطة المغناطيسية، وليست على الكيان غير المادي[3].

وفي اليابان، تُعتبر السجلات الإلكترومغناطيسية غير مرئية في حد ذاتها، فلا يُمكن ضبطها، وعليه يجب تحويلها إلى صورة مادية ملموسة يمكن قراءتها بعد طباعتها[4].

ويرى جانب آخر، أنه إذا كان الهدف من التفتيش هو ضبط الأدلة المادية التي تُساعد في كشف الحقيقة، فلا يوجد ما يمنع من وقوع الضبط على البيانات الإلكترونية، وهو ما نص عليه قانون الإجراءات الجنائية اليوناني في المادة رقم (251) والتي أعطت سلطة التحقيق إجازة القيام بأي شيء، وهو ما يعني أن التحقيق يشمل ضبط البيانات المخزنة أو المعالجة إلكترونياً، وبالتالي لا يوجد مشكلة في ضبط البيانات الإلكترونية في التشريع اليوناني[5].

---

[1] هشام محمد فريد رستم: الجوانب الإجرائية للجرائم المعلومات، مرجع سابق، ص. 93.

[2] هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص. 85.

[3] علي حسن محمد الطوالبة: التفتيش الجنائي على نظم الحاسوب والإنترنت، مرجع سابق، ص. 146.

[4] هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ص. 85.

[5] أحمد السمدان: النظام القانوني لحماية برامج الكمبيوتر، مجلة الحقوق، العدد. 4، جامعة الكويت، الكويت، ديسمبر، 1987، ص. 35.

وكذلك أعطت المادة رقم (487) من القانون الكندي سُلطة إصدار إذن لضبط أي شيء طالما توافرت أُسس معقولة للإعتقاد أن الجُرم قد أُرتكِب، أو يشُتبه بإرتكابه، أو أن هناك نية في إستخدامه لإرتكاب جريمة، أو سيُعطي دليلاً على إقتراف جريمة[1].

كما إعترف بعض الفقهاء في فرنسا أن للبرنامج كيان مادي ملموس يتمثل في إشارات إلكترونية مغناطيسية أو ممغنطة[2]، وقد نص التشريع الأمريكي الخاص بما قبل المحاكمة لسنة 1975م على أنه "إلا إذا حظر في أي ضبط أي أدلة أو معلومات تتعلق بالجريمة المرتكبة أو أي جريمة أخرى وذلك بإستثناء المعلومات المحضة"[3].

ويجدر القول، أن القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية توافق مع الرأي الثاني، فقد نصت المادة رقم (2/33) منه على أنه[4] "للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تُساعد على كشف الحقيقة" وكذلك نصت المادة (3/33) على أنه "إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً أو تعذر إجراؤه تُنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات".

---

[1] وبالإضافة إلى ما تقدم، فقد نصت المادة (79) من قانون الإثبات الكندي على أنه "ما لم يرد ما يخالف ذلك في أمر التفتيش، فإن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية (كالبنك مثلاً) يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخ من المواد المكتوبة"، وينطبق النص سواء أكانت السجلات مكتوبة أم كانت في شكل سجلات الحاسوب. أنظر، هشام محمد فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص. 96.

[2] هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص. 83.

[3] عفيفي كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، مرجع سابق، ص. 359.

[4] قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، المادة (3,2/33).

ويُستنتج، أنه يمكن أن يقع الضبط على مكونات الحاسب الآلي المعنوية، ما دام ذلك يُحقق مصلحة عامة تتمثل في الكشف عن الجرائم، وإذا تعذر ذلك يمكن تحويل المكونات المعنوية إلى كيانات مادية عن طريق طباعتها على ورق، أو أقراص مضغوطة، وثم ضبطها حسب الأصول.

الفرع الثاني: ضبط الشبكات والمراسلات الإلكترونية وموقف القضاء من إجراء الضبط:

يُقصد بالمراسلات بصفة عامة، جميع الرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد، وجميع البرقيات لدى مكاتب البرق، والمحادثات السلكية واللاسلكية، وهو ما بينه قانون الإجراءات الجزائية رقم (3) لسنة 2001 في المادة (1/51) منه والتي نصت على أنه "للنائب العام أو أحد مساعديه أن يضبط لدى مكاتب البرق والبريد الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات المتعلقة بالجريمة وشخص مرتكبها"[1].

ونجد، أن المادة رقم (18) من الدستور الأُردني نصت على أنه "تُعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية سرية، فلا تخضع للمراقبة أو التوقيف إلا في الأحوال المعينة في القانون"[2].

أما الشبكات الإلكترونية، فهي إرتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها، بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية (الإنترنت).[3]

---

[1] وتقابلها المادة رقم (95) من قانون الإجراءات الجنائية المصري والتي نصت على أنه "لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق...".

[2] الدستور الأُردني المعدل، المادة رقم (18).

[3] قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، المادة (1).

ويتبين، أن إجراء ضبط الشبكات والمراسلات الإلكترونية له طبيعة خاصة، فقد يقوم الجاني بإخفاء تلك الشبكات والمراسلات، أو وضعها تحت جدار حماية وكلمة مرور لا يمكن كسرها، وبالتالي يُصبح إجراء ضبطها ذات صعوبة واضحة.

وفي موقف القضاء من إجراء الضبط، نجد أن القانون الفلسطيني والقانون الأُردني أجاز كل منهما وقوع الضبط على المكونات المادية والمعنوية للحاسب الآلي، حال كان لذلك الضبط دور في كشف الحقيقة[1].

أما الفقه اليوناني والكندي، فقد أجاز كل منهما ضبط الكيانات المادية وكذلك الكيانات المعنوية للحاسب الآلي، وهذا هو الواقع التطبيقي والعملي في هذه الدول[2].

وبالنسبة للفقه الألماني، فقد جعل الضبط يقع على الأشياء المادية المحسوسة، أما البيانات المعالجة إلكترونياً فلا يمكن ضبطها مجردة إلا بعد تحويلها إلى كيان مادي، مثل طباعتها على ورق أو عن طريق التصوير الفوتوغرافي[3].

---

[1] قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، قانون الجرائم الإلكترونية الأُردني رقم (27) لسنة 2015.

[2] يوسف عرب: جرائم الكمبيوتر والإنترنت، إتحاد المصارف العربية 2002، ص. 520.

[3] خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، مرجع سابق، ص. 175.

الخاتمة:

مما لا ريب فيه، أن هُناك إختلاف بين الجريمة التقليدية والجريمة الإلكترونية، فَنجد أن الجريمة التقليدية ظاهرة إجتماعية وإقتصادية وأخلاقية قديمة قِدم الإنسان، ويُعاقِب عليها القانون وفقاً لتشريعات جزائية مُحددة، والجريمة التقليدية يُحددها مكان وزمان وطريقة تنفيذ، ويكون للفاعل وجود فيزيائي فيها، وكذلك فإن نتائِجها ملموسة، وهي الأدلة المادية أو المعنوية التي تخلفة عنها.

أما الجريمة الإلكترونية، فهي ظاهرة مُعقدة ومُركبة تفوق الجريمة التقليدية لإختلاف ظروفها وأدواتها، وطرق تنفيذها ونتائجها، وكذلك صعوبة الكشف عنها وتحديد مُرتكبيها، وغالباً ما يكون هناك بُعد جغرافي بين الجاني والمجني عليه.

وقد أصبحت الجريمة الإلكترونية خطراً يُهدد العالم، سواء على مستوى الأفراد أو الدول، أو على المستوى الإقتصادي أو الإجتماعي والأمني، وهناك العديد من الخسائر التي نجمت عن هذه الجريمة، وعليه كان لابد من وجود إجراءات خاصة للتحقيق من قبل السُلطات القائمة بمكافحة هذه الجرائم.

ويُمكن القول، أن التفتيش في الجرائم الإلكترونية إجراء قانوني شُرع لتحقيق مصلحة عامة، فهو إجراء خطير لأَنه يَمس أدق حقوق الإنسان في حُريته ومسكنه والوسائل الإلكترونية الخاصة به، وهذا الحق مكفول بحماية القانون، وتتمثل هذه الحماية في الضمانات التي تتوفر للمتهم.

ولأَن المساس بهذا الحق قد شُرع من أجل غاية مهمة وهي كشف الحقيقة وتحقيق العدالة، كان لابد من وجود شروط لتحقيق التوازي بين حق الفرد وحق المجتمع، ولعل أهم تلك

الشروط هو أن التفتيش يؤذَن به من قبل سُلطة مختصة وفي جرائم الجنايات والجنح التي يكون المُراد تفتيشه متهماً بها، أو شريكاً، أو يحوز على مواد تتعلق بها.

ويُلاحظ، أن مرتكبوا الجرائم الإلكترونية قاموا بإستغلال وإستخدام كافة وسائل الإتصال، سواء لتنفيذ الجريمة، أو لمحاولة الفِرار من أيدي العدالة، وعليه كان لابد من تسخير التقدم العلمي وإجراء ما هو لازم من عمليات مراقبة للمكالمات الهاتفية في سبيل الوصول إلى الجُناة وتقديمها للعدالة وفقاً للأُطر القانونية الصحيحة.

ومما لا شك فيه، أن إرتفاع معدل إرتكاب الجريمة الإلكترونية وتجاوزها لحدود الدولة الجغرافية، أدى إلى زيادة الإشكاليات القانونية من حيث وجود بعض المعوقات التي تواجه إكتشاف وإثبات هذه الجرائم، وذلك بإعتبارها لا تترك آثاراً مادية ملموسة كما في الجرائم التقليدية.

وتُعتبر النيابة العامة هي صاحِبة الإختصاص الأصيل بإجراء التحقيق في الجرائم الإلكترونية، وكذلك الإشراف على مأموري الضبط القضائي أثناء قيامهم بعملهم في سبيل كشف الحقيقة والوصول للفاعلين.

نتائج هذه الدراسة:

* إتسعت ثورة تقنية نظم المعلومات والإتصالات، بحيث شملت كافة مناحي الحياة، ما أدى إلى ظهور نوع جديد من الجرائم عرُف بالجرائم الإلكترونية.

* إمتازت الجرائم الإلكترونية عن الجرائم التقليدية في عِدة أُمور، منها أُسلوب إرتكاب الجريمة وطرق البحث عن الدليل وضبطه، بالإضافة إلى طبيعة مسرح الجريمة، وكذلك إجراء التفتيش والضبط فيها.

* إن الحق في حُرمة التنصت على المكالمات الهاتفية ليس مطلقاً، فهو كغيره من الحقوق والحريات الفردية، إذ يجوز المساس به إذا كانت مصلحة المجتمع في حِفظ الأمن والنظام العام أولى بالرعاية من حق الفرد في الخصوصية.

* إن تفتيش الوسائل الإلكترونية يُثير العديد من المسائل، كمدى صلاحية تفتيش الكيانات المعنوية، وكذلك حُكم تفتيش الوسائل المتصلة ببعضها البعض، والتي تقع في أماكن عامة أو خاصة داخل أو خارج الدولة.

* لا تترك الجرائم الإلكترونية غالباً أثراً مادياً في مسرح الجريمة كما في الجرائم التقليدية، كما أن مرتكبيها لديهم القدرة على إتلاف وتشويه أو إضاعة الدليل في فترة قصيرة.

* يتم إجراء التفتيش والضبط في الجرائم الإلكترونية من خلال مجموعة من الإجراءات التقنية الفنية، والتي تحتاج إلى كوادر متخصصة قادرة على تحقيق أهداف التفتيش، وضبط الأدلة القانونية الإلكترونية.

* يُواجه التحقيق في الجرائم الإلكترونية العديد من الصعوبات، وذلك كونها جريمة عابرة للحدود يُمكن إرتكابها من خارج إطار الدولة.

* تم إقرار القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، وذلك لمواكبة تطور الجريمة وإنتشارها بشكل سريع.

التوصيات:

* نَظراً لزيادة معدل إرتكاب الجريمة الإلكترونية، نرى ضرورة إنشاء وحدات متخصصة للشرطة في جميع المحافظات، ويكون دورها أيضاً زيادة الوعي للمواطنين من خلال إعطاء محاضرات توعوية.

* ضرورة إعداد مأموري ضبط قضائي وأعضاء نيابة عامة وقُضاة لديهم القدرة الفنية على البحث والتحقيق والمحاكمة في مجال الجرائم الإلكترونية.

* عَقد ندوات بين مأموري الضبط القضائي وأعضاء النيابة العامة والقُضاة حول كيفية إتباع الإجراءات السليمة القانونية لمكافحة الجرائم الإلكترونية.

* إقرار مادة علمية حول مخاطر الجرائم الإلكترونية ومكافحتها في المدارس والكليات والجامعات.

* إبرام إتفاقيات دولية شاملة لتنظيم إجراءات مكافحة الجرائم الإلكترونية.

* التعاون بين دول العالم المختلفة والدول العربية على وجه الخصوص، وذلك بتبادل المعلومات والخبرات في مجال الجرائم الإلكترونية.

* التوعية الإعلامية المستمرة للمخاطر الناجمة عن سوء إستخدام الإنترنت وما قد يترتب على ذلك من أضرار جسيمة على أمن وإقتصاد المجتمع.

* يجب على وزارة الإتصالات وتكنولوجيا المعلومات حجب وحظر المواقع الإلكترونية الغير أمنة (مواقع غير أخلاقية) والتي من شأنها مساعدة الجُناة على التسرب والإختراق وإرتكاب الجرائم.

* نأمل من المشرع إعادة النظر في القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، وذلك بالتطرق بشكل أدق وأوسع إلى إجراءات التحقيق في الجرائم الإلكترونية.

قائمة المصادر

أولاً: القرآن الكريم.

- سورة البقرة.
- سورة النور.

ثانياً: المؤلفات الفقهية.

1. المراجع المتخصصة

- أحمد السمدان، النظام القانوني لحماية برامج الكمبيوتر, مجلة الحقوق, العدد4, جامعة الكويت, الكويت, ديسمبر, 1987
- إبراهيم راسخ، التحقيق الجنائي العملي، الطبعة الأولى، 1991، مطبعة البيان التجارية، دبي.
- أيمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، 2005.
- أُسامة أحمد المناعسة، جرائم الحاسب الآلي، دار وائل للنشر والتوزيع، عمان، 2001.
- أُسامة أحمد المناعسة، القاضي جلال محمد، جرائم نظم المعلومات الإلكترونية، عمان، دار الثقافة للنشر والتوزيع، ط1، 2009.
- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، 2011.
- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، 2002.

- حنان ريحان مبارك المُضحكي، الجرائم المعلوماتية، منشورات الحلبي الحقوقية.
- حسين سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 200.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، 2009.
- خالد ممدوح إبراهيم, الجرائم المعلوماتية, دار الفكر الجامعي, الإسكندرية, 2009.
- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، دار النهضة العربية، الطبعة الأولى، 2009.
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، 2006.
- عبد الفتاح بيومي حجازي, مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي, دراسة قانونية متعمقة في القانون المعلوماتي, دار الفكر الجامعي, 2006.

عبد الفتاح بيومي حجازي, الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت, دار الكتب القانونية, 2002.

- عبد المهيمن بكر, إجراءات الأدلة الجنائية, الجزء الأول في التفتيش, الطبعة الأولى, دار النهضة العربية, القاهرة, 1996.
- عبد العال الديربي, محمد صادق إسماعيل, الجرائم الإلكترونية, دراسة قانونية قضائية مقارنة, القاهرة, الطبعة الأولى, 2012.
- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، جامعة الموصل، كلية الحقوق.

- علي محمود علي حمودة، الجوانب القانونية الأمنية للعمليات الإلكترونية، مجلد رقم (1) محور القانون الجنائي.
- غنية باطلي، الجريمة الإلكترونية، دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، المجلة الكبرى، 2006.
- محمد أبو العلا عقيدة، مراقبة المحادثات التلفونية، داراسة مقارنة، دار الفكر العربي، سنة 1994م.
- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، 2000.
- محمد نصر محمد، المسؤولية الجنائية لإنتهاك الخصوصية المعلوماتية، الطبعة الأولى، 2016، مركز الدراسات العربية للنشر والتوزيع.
- محمد البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، 2004.
- مصطفى محمد موسى, المراقبة الإلكترونية عبر شبكة الإنترنت, دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية, الكتاب الخامس, الطبعة الأولى, دار الكتب والوثائق القومية المصرية, 2003.
- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007م.

- هلالي عبد اللاه أحمد، التزامات الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، 1997.
- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، 1997.
- هشام فريد رستم, الجوانب الإجرائية للجرائم المعلوماتية, القاهرة, النسر الذهبي, 2007.

2. المراجع العامة

- أحمد وهدان، الإنعكاسات الأمنية للعولمة، القاهرة، المجلة الجنائية القومية، مجلد 44، 2001.
- أحمد فتحي سرور, الوسيط في قانون الإجراءات الجنائية, دار النهضة العربية, القاهرة, 1996.
- أحمد عمر شوقي أبو خطوة, شرح قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة, الطبعة الأولى, 1990.
- أحمد عوض بلال, قاعدة إستبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة, دار النهضة العربية, القاهرة, 1994.
- إبراهيم حامد طنطاوي, سُلطات مأمور الضبط القضائي, المكتبة القانونية, الطبعة الثانية, القاهرة, 197.
- إدوارد غالي الدهبي، الإجراءات الجنائية، مكتبة غريب.
- إلهام محمد العاقل، التفتيش في قانون الإجراءات الجزائية، دراسة مقارنة، الطبعة الأولى، جامعة صنعاء، 2003.

- توفيق الشاوي، حُرمة الحياة الخاصة، نظرية التفتيش، 2006.
- توفيق الشاوي, فقه الإجراءات الجنائية, القاهرة, دار الكتاب العربي, 1954.
- جودة حسين جهاد، قانون الإجراءات الجنائية الإتحادي في دولة الإمارات العربية المتحدة، أكاديمية الشرطة دبي، 1994.
- جندي عبد الملك, الموسوعة الجنائية, الجزء الأول, دار الكتب المصرية, القاهرة, 1931.
- جهاد الكسواني, قرينة البراءة, الطبعة الأولى, 2013, دار وائل للنشر.
- جلال ثروت، نظم الإجراءات الجنائية، دار الجامعة الجديدة، 2003.
- جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، 2001.
- حسن صادق المرصفاوي، شرح قانون الإجراءات والمحاكمات الجزائية الكويتي، مكتبة الفلاح، الكويت، الطبعة الثالثة، 2005.
- رؤوف عبيد، مبادئ الإجراءات الجنائية، دار الفكر العربي، القاهرة، دون سنة نشر.
- رمسيس بهنان، علم النفس القضائي، منشأة المعارف بالإسكندرية، 1997.
- سامي صادق الملا، إعتراف المتهم، دار الفكر العربي، الطبعة الأولى، 1998.
- سامي الحسيني, النظرية العامة للتفتيش, دار النهضة العربية, 1972.
- سردار علي عزيز، ضمانات المتهم أثناء الإستجواب، الطبعة الأولى، 2014، شارع عبد الخالق ثروت، وسط البلد، القاهرة.
- سعيد حسب الله عبد الله، شرح قانون أُصول المحاكمات الجزائية، دار الحكمة للطباعة والنشر، الموصل، 1990.

- طارق عبد الله الشدي، آلية البناء لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض، 1423هـ.
- طه أحمد طه متولي, التحقيق الجنائي وفن إستنطاق مسرح الجريمة, منشأة المعارف, الإسكندرية, 2000.
- عبد الرؤوف مهدي, شرح القواعد العامة للإجراءات الجنائية, القاهرة, دار النهضة العربية, الطبعة الأولى, 2000.
- عبد الرزاق السنهوري, الوسيط في شرح القانون المدني, الجزء الثاني, القاهرة, 1956.
- عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1984.
- علي حسن عوض، الخبرة في المواد المدنية والتجارية، دار الفكر الجامعي، 2002.
- علي السماك، الموسوعة الجنائية في القضاء الجنائي العراقي، الجزء الأول، مطبعة الجاحظ، 1990.
- عفيفي كامل عفيفي, جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية, مكتبة الأهرام, 2000.
- فاروق الكيلاني, محاضرات في قانون أُصول المحاكمات الجزائية الأُردني والمقارن, الجزء الثاني, الطبعة الثانية, 1985.
- فوزية عبد الستار علي, شرح قانون الإجراءات الجنائية, دار النهضة العربية, 1986.
- قدري عبد الفتاح الشهاوي، مناط مشروعية العمل الشُرطي، دار النهضة العربية، القاهرة، 2007.

- مأمون محمد سلامة, قانون الإجراءات الجناية, مُعلقاً عليه بالفقه وأحكام النقض, دار الفكر العربي, القاهرة, 1980.
- ممدوح إبراهيم السبكي, حدود سُلطات مأمور الضبط القضائي في التحقيق, دار النهضة العربية القاهرة, 1998.
- محمد زكي أبو عامر، الإجراءات الجنائية، منشأة المعارف، الإسكندرية، 1994.
- محمد فتحي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع الكتاب المصري الحديث، 1991.
- محمد صبحي نجم، الوجيز في قانون أُصول المحاكمات الجزائية، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2000.
- محمد الحلبي، شرح قانون الإجراءات الجزائية الفلسطيني، دار الفكر، 2002.
- محمد سامي الشوا، ثورة المعلومات وإنعكاساتها على قانون العقوبات، دار النهضة العربية، الطبعة الثانية، 1998.
- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2009.
- محمد حماد مرهج الهيتي، جرائم الحاسوب، دراسة تحليلية لواقع الإعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، كلية القانون، جامعة الأنبار حالياً، كلية القانون، جامعة التحدي، ليبيا سابقاً، الطبعة الأولى، 2006.
- محمد حبيب التجكاني، النظرية العامة للقضاء والإثبات في الشريعة الإسلامية مع مقارنات بالقانون الوضعي، دار النشر المغربية، الدار البيضاء، 1985.

- محمود نجيب حسني, شرح قانون الإجراءات الجنائية, دار النهضة العربية, 1988م, الطبعة الثانية.
- محمود محمد مصطفى, الإثبات في المواد الجنائية في القانون المقارن, التفتيش والضبط, جامعة القاهرة, القاهرة, 1987م.
- نبيل علي، العرب وعصر المعلومات، الكويت، عالم المعرفة، 1994.
- نبيه صالح، الوسيط في شرح مبادئ الإجراءات الجزائية، منشأة دار المعارف، الجزء الأول، 2004.
- يونس عرب، جرائم الكمبيوتر والإنترنت، إتحاد المصارف العربية، 2002.

ثالثاً: الرسائل والأطروحات:

- آمال عبد الرحيم عُثمان، الخبرة في المسائل الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964.
- حسين محمود إبراهيم، النظرية العامة للإثبات العلمي في قانون الإجراءات الجنائية، رسالة كتوراه، كلية الحقوق، جامعة القاهرة، 1401هـ، 1981م.
- رُهام سائد أحمد جبر، جريمة الإحتيال الإلكترونية وإجراءات الضبط والتحقيق المتعلق بها، رسالة ماجستير. جامعة القدس، فلسطين، 2015.
- سامي حسني الحسيني, النظرية العامة للتفتيش في القانون المصري والمقارن, رسالة دكتوراه, جامعة القاهرة, ط1, دار النهضة العربية, القاهرة, 1972م.

- سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003.
- عبد الرحمن محمد عبد الله الحضرمي، سُلطات مأمور الضبط القضائي في حالة الجريمة المشهورة، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، 1999.
- عبد الرحمن بحر, معوقات التحقيق في جرائم الإنترنت, دراسة مسحية على ضباط الشرطة لدولة البحرين, رسالة ماجستير, جامعة نايف العربية للعلوم الأمنية الرياض, 1999.
- علياء محمد الكحلاوي, الشهادة دليل للإثبات في المواد الجنائية, رسالة دكتوراه, كلية الحقوق, جامعة القاهرة, 1999.
- علي الحديدي, دور الخبير الفني في الخصومة, رسالة دكتوراه, كلية الحقوق, جامعة القاهرة, 1981.
- عمر محمد أبو بكر بن يونس, الجرائم الناشئة عن إستخدام الإنترنت, رسالة دكتوراه, حقوق عين شمس, 2004.
- فيصل عايش المطيري، مدى مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، دراسة مقارنة، جامعة عمان العربية، 2013.
- محمد سامي النبراوي، إستجواب المتهم، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1968.
- محمد غالب الرحيلي، الخبرة في المسائل الجزائية، رسالة ماجستير، جامعة الشرق الأوسط، 2017.

- محمد علي مصطفى غانم، تفتيش المسكن في قانون الإجراءات الجزائية الفلسطيني، رسالة ماجستير، جامعة النجاح الوطنية، 2008.
- محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات.
- محمد كاسب خطار الشموط، الإثبات في الجرائم الإلكترونية، رسالة دكتوراه، جامعة العلوم الإسلامية العالمية، عمان.
- مروان صالح الدروبي, الضوابط القانونية لمراقبة المكالمات الهاتفية, دراسة مقارنة, المملكة الأُردنية الهاشمية, جامعة الإسراء الخاصة.
- مفيد إرزيقات, رسالة ماجستير, محاضر الضابطة القضائية, جامعة القدس, 2010.
- يوسف خليل يوسف العفيفي, الجرائم الإلكترونية في التشريع الفلسطيني, دراسة تحليلية مقارنة, رسالة ماجستير, الجامعة الإسلامية, غزة, 2013.
- يونس عرب، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير، الجامعة الأُردنية، عمان، 1994.

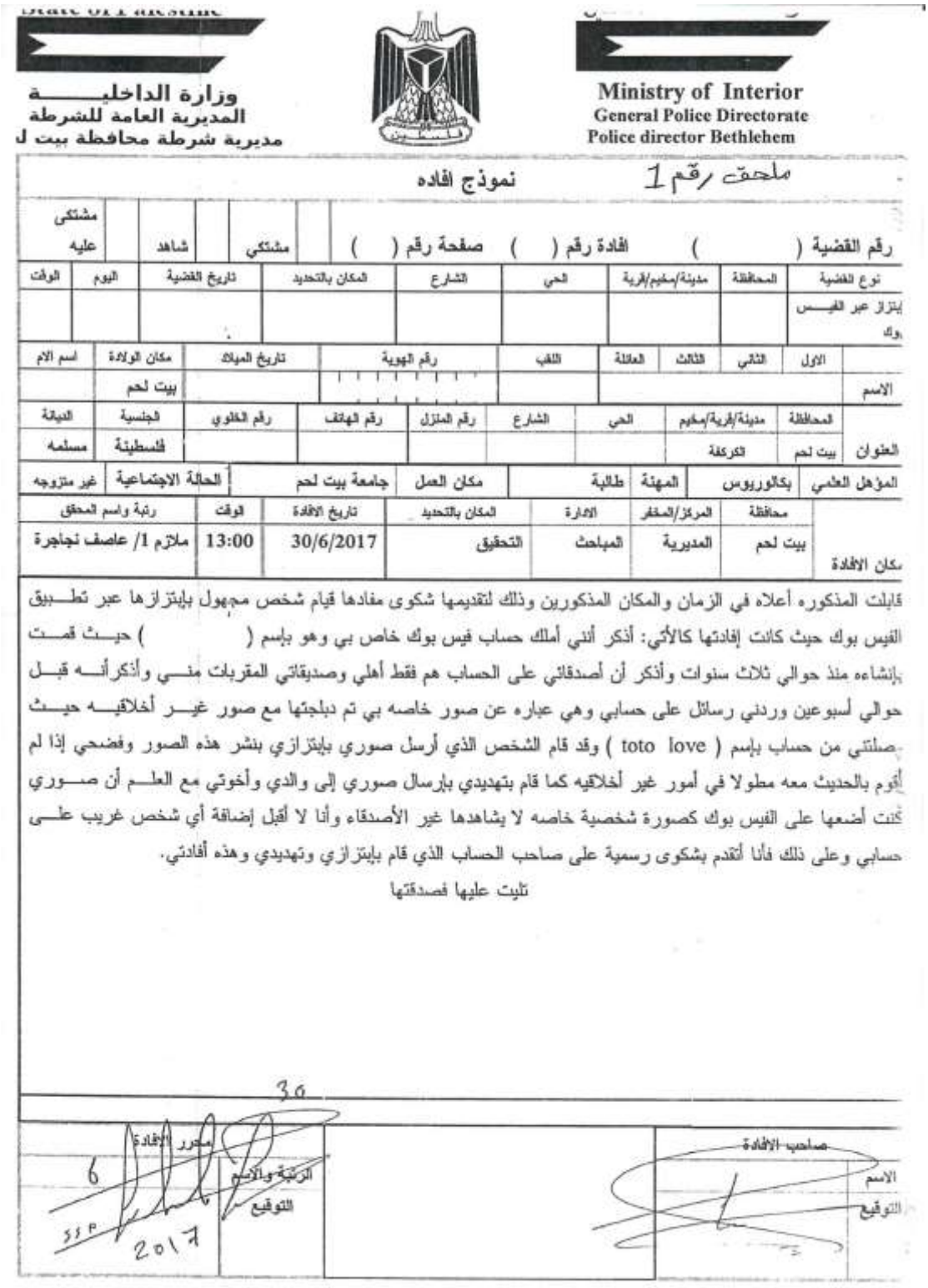
رابعاً: المقالات والأبحاث:

- أمنة بوزية أمحمدي، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام، 2017.
- أُسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب (السعودية)، 2013.

- أُسامة محمد محي الدين عوض, جرائم الكمبيوتر والجرائم الأُخرى في مجال تكنولوجيا المعلومات, بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي, القاهرة, 1993.
- العقيد علاء الدين محمد شحاته، رؤية أمينة للجرائم الناشئة عن إستخدام الحاسب الآلي، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993.
- حسين سعيد الغافري، التحقيق والأدلة في الجرائم المتعلقة بشبكة الإنترنت.
- راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقنية المعلومات، دراسة تطبيقية على إمارة أبوظبي، تُصدر عن مركز الإمارات للدراسات والبحوث الإستراتيجية، العدد 131.
- زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأُخرى في مجال التكتيك المعلوماتي، بحث مُقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993.
- سرحان حسن محمد حسن المعيني، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات، 2011.
- طارق إبراهيم الدسوقي عطية، إجراءات البحث الجنائي في ضبط الجريمة الإلكترونية في ضوء إتفاقية بودابست الموقعة في 23 نوفمبر سنة 2001م.
- عادل حافظ غانم، الخبرة في مجال الإثبات الجنائي، مجلة الأمن العام المصرية، العدد 43، 1968.
- عادل عبد الله خميس المعمري, التفتيش في الجرائم المعلوماتية, مجلة الفكر الشرطي, مركز بحوث الشرطة, القيادة العامة لشرطة الشارقة, الإمارات, بحوث ومقالات, 2013.

- عبد الحليم إبن بادرة, إجراءات البحث والتحري عن الجريمة العلوماتية, الخصوصية والإشكاليات, مجلة الحقوق والعلوم الإنسانية, جامعة زيان عاشور بالجلفة, الجزائر, 2015.
- علي عدنان الفيل، إجراء التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، مجلة البحوث والدراسات العربية، مصر، 2010.
- محمد بن حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات، مج21، ع 81، 2012.
- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب (السعودية)، العدد 30، 2000.
- محمد أبو العلا عقيدة، مواجهة الجرائم الناشئة عن إستخدام الحاسب الآلي، مجموعة أعمال مؤتمر الكمبيوتر والقانون المنعقدة بالفيوم، 1994، جامعة عين شمس.
- هشام محمد فريد رُستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت في الفترة بين 1-3 مايو 2000، جامعة الإمارات العربية المتحدة بعنوان الجرائم المعلوماتية.
- هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأُخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، منشورات دار النهضة العربية، 1993.
- يسر أنور, الإثبات الجنائي ووسائل التحقيق العلمية, محاضرات أُلقيت على طلبة دبلوم العلوم الجنائية بكلية الحقوق جامعة عين شمس, سنة 1979.

الملاحق:



وزارة الداخليـــــة
المديرية العامة للشرطة
مديرية شرطة محافظة بيت ل

Ministry of Interior
General Police Directorate
Police director Bethlehem

ملحق رقم 1

نموذج افاده

رقم القضية ( ) افادة رقم ( ) صفحة رقم ( ) مشتكي شاهد مشتكى عليه

نوع القضية	المحافظة	مدينة/مخيم/قرية	الحي	الشارع	المكان بالتحديد	تاريخ القضية	اليوم	الوقت
ابتزاز عبر الفيس بوك								

	الاول	الثاني	الثالث	العائلة	اللقب	رقم الهوية	تاريخ الميلاد	مكان الولادة	اسم الام
الاسم								بيت لحم	

	المحافظة	مدينة/قرية/مخيم	الحي	الشارع	رقم المنزل	رقم الهاتف	رقم الخلوي	الجنسية	الديانة
العنوان	بيت لحم	الكركفة						فلسطينية	مسلمه

المؤهل العلمي	المهنة	مكان العمل	الحالة الاجتماعية
بكالوريوس	طالبة	جامعة بيت لحم	غير متزوجه

مكان الافادة	محافظة	المركز/المخفر	الادارة	المكان بالتحديد	تاريخ الافادة	الوقت	رتبة واسم المحقق
	بيت لحم	المديرية	المباحث	التحقيق	30/6/2017	13:00	ملازم 1/ عاصف نجاجرة

قابلت المذكوره أعلاه في الزمان والمكان المذكورين وذلك لتقديمها شكوى مفادها قيام شخص مجهول بإبتزازها عبر تطبيق الفيس بوك حيث كانت إفادتها كالأتي: أذكر أنني أملك حساب فيس بوك خاص بي وهو بإسم ( ) حيث قمت بإنشاءه منذ حوالي ثلاث سنوات وأذكر أن أصدقائي على الحساب هم فقط أهلي وصديقاتي المقربات مني وأذكر أنه قبل حوالي أسبوعين وردني رسائل على حسابي وهي عباره عن صور خاصه بي تم دبلجتها مع صور غير أخلاقيه حيث صلتني من حساب بإسم (toto love) وقد قام الشخص الذي أرسل صوري بإبتزازي بنشر هذه الصور وفضحي إذا لم أقوم بالحديث معه مطولا في أمور غير أخلاقيه كما قام بتهديدي بإرسال صوري إلى والدي وأخوتي مع العلم أن صوري كانت أضعها على الفيس بوك كصورة شخصية خاصه لا يشاهدها غير الأصدقاء وأنا لا أقبل إضافة أي شخص غريب على حسابي وعلى ذلك فأنا أتقدم بشكوى رسمية على صاحب الحساب الذي قام بإبتزازي وتهديدي وهذه أفادتي.

تليت عليها فصدقتها

30

محرر الافادة
الرتبة والاسم
التوقيع
6
2017

صاحب الافادة
الاسم
التوقيع

State of Palestine

وزارة الداخليـــــة
المديرية العامة للشرطة
مديرية شرطة محافظة بيت ل

Ministry of Interior
General Police Directorate
Police director Bethlehem

ملحق رقم 2

نموذج افاده

رقم القضية ( ) افادة رقم ( ) صفحة رقم ( ) مشتكي شاهد مشتكى عليه

نوع القضية	المحافظة	مدينة/مخيم/قرية	الحي	الشارع	المكان بالتحديد	تاريخ القضية	اليوم	الوقت
إبتزاز عبر الفيـــس بوك								

	الاول	الثاني	الثالث	العائلة	اللقب	رقم الهوية	تاريخ الميلاد	مكان الولادة	اسم الام
الاسم								الكويت	

	المحافظة	مدينة/قرية/مخيم	الحي	الشارع	رقم المنزل	رقم الهاتف	رقم الخلوي	الجنسية	الديانة
العنوان	بيت لحم	الخضر						فلسطيني	مسلم

المؤهل العلمي	توجيهي	المهنة	عامل	مكان العمل	القدس	الحالة الاجتماعية	اعزب

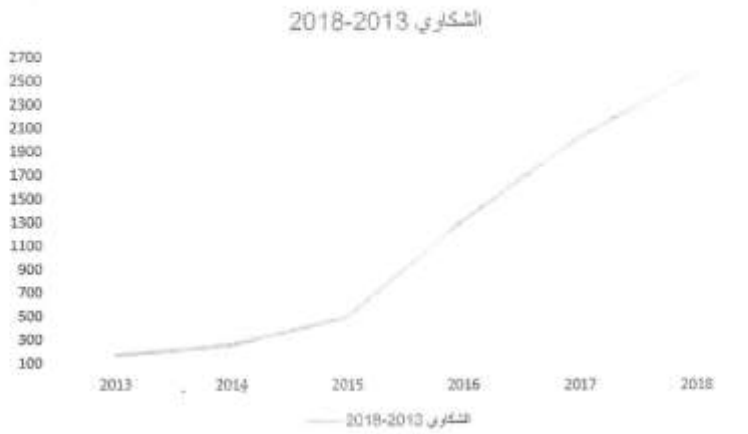
مكان الافادة	محافظة	المركز/السفارة	الادارة	المكان بالتحديد	تاريخ الافادة	الوقت	رتبة واسم المحقق
	بيت لحم	المديرية	المباحث	التحقيق	17/8/2017	19:30	ملازم 1/ عاصف نجاجرة

قابلت المذكور أعلاه في الزمان والمكان المذكورين وذلك لسماع أقواله حول قضية إبتزاز عبر الفيس بوك حيث أفاد بالأتي:
أذكر أنني أسكن في منزل والدي في بلدة الخضر وأملك جهاز بلفون نوع سامسونج دوس لون أسود وقد قمت قبل حوالي عام بإنشاء حساب فيس بوك وهمي بإسم (toto love) حيث قمت من خلاله بإرسال طلب صداقه إلى صديقة أختي في الجامعه وتدعى/ وذلك على حسابها وهو ( ) حيث أنها قبلت طلب الصداقه وكنت أدخل إلى حسابها وأقـــوم بالاطلاع على صورها الخاصه التي تقوم بنشرها على حسابها وقد قمت بإخذ صورتين لها ووضعها مـــع صـــور جنســـيه أحضرتها من الإنترنت وقمت بعد ذلك بإرسال الصور لها قبل حوالي شهرين وطلبت منها أن تتحدث معي في الجنس وحال عدم موافقتها سوف أقوم بفضحها ونشر صورها وأنا أقوم بإستخدام الإنترنت الخاص بمنزل والدي وهو تابع لشركة حضاره ورقم هاتف منزل والدي هو ( ) وأنا أعترف أنني قمت بواسطة جهاز البلفون الخاص بي بأبتزاز
هذه افادتي أوقع عليها بمحض أرادتي.

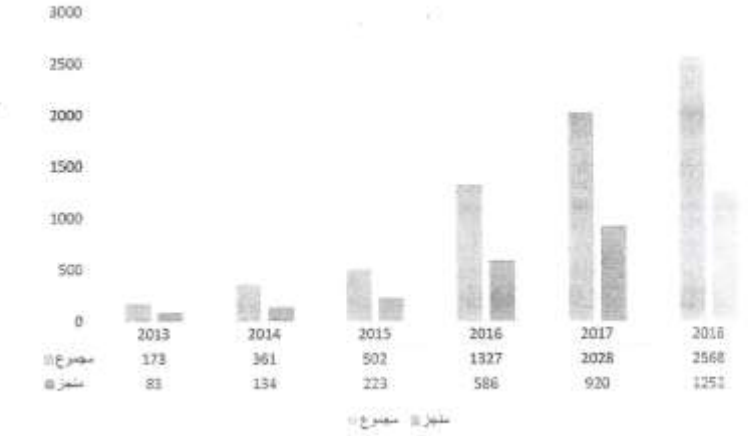
تليت عليه فصدقها

محرر الافادة		صاحب الافادة
الرتبة والاسم		الاسم
التوقيع		التوقيع

ملحق رقم 3



- منحنى طبيعي يوضح الزيادة في عدد القضايا المنجزة في الوحدة خلال اخر 6 سنوات



- القطاع الدائري التالي يوضح نسبة الشكاوي المقدمة حسب جنس مقدم الشكوى:

فهرس المحتويات