

عمادة الدراسات العليا

جامعة القدس

الأحكام الموضوعية والإجرائية للجرائم الإلكترونية بفلسطين  
دراسة تحليلية تأصيلية مقارنة

نسرين جورج عيسى زينة/ ر شماوي

القدس-فلسطين

1441هـ/2020م

الأحكام الموضوعية والإجرائية للجرائم الإلكترونية بفلسطين  
دراسة تحليلية تأصيلية مقارنة

إعداد:

نسرین جورج عیسی زینة / رشماوی

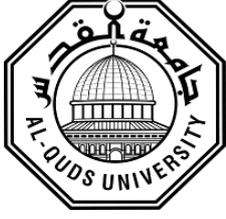
بكالوريوس قانون من جامعة القدس / فلسطين

المشرف: د. أحمد البراك

قدمت هذه الرسالة استكمالاً لمتطلبات درجة الماجستير في القانون الجنائي/

كلية الحقوق - جامعة القدس

1441هـ/2020م



جامعة القدس  
عمادة الدراسات العليا  
برنامج القانون الجنائي

## إجازة الرسالة

الأحكام الموضوعية والإجرائية للجرائم الإلكترونية بفلسطين  
دراسة تحليلية تأصيلية مقارنة

اسم الطالبة: نسرين جورج عيسى زينة/ رشماوي

الرقم الجامعي: 21420357

المشرف: د. أحمد البراك

نوقشت هذه الرسالة واجيزت بتاريخ: 2020/2/1 من أعضاء لجنة المناقشة المدرجة أسماؤهم  
وتوقيعاتهم أدناه:

التوقيع: .....	د. أحمد البراك	1- رئيس لجنة المناقشة :
التوقيع: .....	د. عبد الله ناجرة	2- ممتحناً داخلياً:
التوقيع: .....	د. عبد اللطيف ربايعة	3- ممتحناً خارجياً:

القدس - فلسطين

1441هـ/2020م

## الإهداء

إلى من أحمل اسمه بكل فخرٍ واعتزاز، الذي علمني الوفاء والإخلاص والانتماء والإنحناء تواضعاً للعلم والكبرياء.

إلى من ترمي سهام الحب والحنان والعطاء بعبيرٍ يفوه منه ريحة الريحان أُمي.

إلى روح الروح أولادي المشاغبين ديمتري، زين، ريان كنزي وارثي في الدنيا امل الحياة.

إلى سندي وقوتي وشموخي إخوتي الأعزاء نجوماً تلالأت في السماء.

إلى من دفعني وساندني للوصول، إلى النجاح زوجي الحبيب حب الحياة.

إلى الجميلة المفعمة بالحيوية خالتي رندة والتي سهرت معي لإتهاء هذا الجهد العلمي.

إلى زملائي واخواتي محمد حجوج ومازن لحام رهام جبر وإياد ارفاعي الذين رافقوني في طريق العلم والمعرفة.

إلى من رافقتني لمواجهة الصعاب والكفاح والرقى والنضج رفقاتي نجوى والهام ووفاء.

إلى روح والدة زوجي وجداتي العصميات الشامخات.

إلى الساهرين على تحقيق الأمن والأمان للمواطنين إلى إسرة الشرطة والأجهزة الأمنية.

إلى كل من وقف بجانبني من قريب أو بعيد للوصول الى النجاح أقبائني وأصدقائني وزملائي.

أهدي ثمرة جهدي

## إقرار

أقر أنا معدة هذه الرسالة بأنها قدمت لجامعة القدس؛ لنيل درجة الماجستير وأنها نتيجة أبحاثي الخاصة، باستثناء ما تم الإشارة له حيثما ورد، وأنّ هذه الدّراسة، أو أي جزء منها، لم يقدم لنيل أي درجة عليا لأي جامعة أو معهد آخر.

التوقيع:

الاسم: نسرین جورج عيسى زينة/ رشموي

التاريخ: 2020 / 2 / 1 م

## الشكر والتقدير

"العلم زين فكن للعلم مكتسباً وَكُنْ لَهُ طالبا ما عشتَ مُقْتَنِباً"

أول شكري لمالك السماوات والأرض وما عليها عز جلاله الذي توجني هذا العقل، وسقاه بماء العلم شُكْرًا لِلَّهِ الَّذِي يُفُودُنَا فِي مَوَكِبِ نُصْرَتِهِ فِي كُلِّ حِينٍ، وَيُظْهِرُ بِنَا رَائِحَةَ مَعْرِفَتِهِ فِي كُلِّ مَكَانٍ. ويطيب لي أن أتقدم بوافر الشكر والتقدير والعرفان لمعالي المستشار الدكتور أحمد براك رئيس هيئة الفساد بدولة فلسطين الذي تفضل بداية بقبول الإشراف على موضوع الرسالة عرفاناً له لما بذله من جهد ملحوظ ومشكور لإشرافه معلماً وموجهاً ومرشداً، والذي كان لأرائه السديدة وتوجيهاته القيمة الأثر الكبير في إنجاز هذه الرسالة كما أتوجه بجزيل الشكر والتقدير لأعضاء لجنة المناقشة والحكم على هذه الرسالة الذين ستؤدي ملاحظاتهم بدون شك إلى إثرائها.

ويملي علي واجب الاعتراف بالفضل أن أشكر الأساتذة الأفاضل الدكتور محمد خلف، والدكتور نبيه صالح، والدكتور محمد فهد الشلالدة، والدكتور عبدالله ناجرة والدكتور أشرف الاعور والدكتور محمد عمارنة الذين كان لي شرف نهل العلم على أيديهم. كما أتوجه بالشكر الجزيل لكل من ساهم في إتمام هذه الرسالة ولكل من كان سبباً في تعليمي وتوجيهي ومساعدتي وتشجعي للوقوف وراء هذا العمل المتواضع.

الباحث

## الملخص:

تعتبر الجريمة الإلكترونية من أكثر الجرائم تعقيداً وتحدياً للإجهزة الأمنية والنيابة العامة والقضاء، وذلك لما تتمتع به من خصائص تميزها عن الجريمة التقليدية مما جعلها تتمتع بخصوصية ذاتية وخاصة من حيث الإجراءات وطبيعة الأحكام التي تخضع لها فلم تعد التشريعات التقليدية مؤهلة لهذا النوع من الجرائم المستحدثة والمتطورة والمتجددة لارتباطها بالتطور المتسارع لوسائل تكنولوجيا المعلومات، لذلك أصدر المشرع الفلسطيني قرار بقانون رقم 10 لسنة 2018 لتصدي لهذا النوع من الجرائم، إن إصدار النائب العام الفلسطيني قرار بإنشاء نيابة متخصصة تعمل على مكافحة الجريمة هو أيضاً من أهم الركائز التي تساعد على مواجهتها، لذلك جاءت هذه الدراسة شاملة للجريمة الإلكترونية بشقيها الموضوعي والإجرائي، وبينت الطبيعة الموضوعية للجريمة الإلكترونية وأركانها وخصائصها.

كما وضحت هذه الدراسة العديد من مواد القرار بقانون رقم 10 لسنة 2018، من حيث التجريم والإجراءات المتبعة، وخاصة أهم إجراءات التحقيق وهو التفتيش؛ والضبط وآلية التعامل مع الدليل الرقمي حتى يكون له قيمة في الإثبات أمام المحكمة المختصة متبعة الأسلوب التحليلي والتأصيلي النسبي للأصول العامة والمقارن للتشريعات الاقليمية والدولية، ومن خلال الدراسة تبين أن هذه الجريمة الإلكترونية ليست بديلاً عن الجريمة التقليدية بل نمطاً حديثاً وشكلاً مستحدثاً، واسع النطاق عابراً للحدود أفرد لها طابع خاص في التعامل معها من الناحية الإجرائية والموضوعية، تختلف عن طبيعة الجريمة التقليدية، إلا إن الإجراءات في مرحلة المحاكمة تكون مماثلة للجرائم المتبعة في الجريمة التقليدية التي نظمتها الأحكام العامة في قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001.

## **A comprehensive study on Cybercrime in both its substantive and procedural types**

**Prepared by: Nisreen George Issa Zienah/Rishmawy**

**Supervisor: Dr.Ahamd Al-Barak**

### **Abstract:**

This study is a comprehensive study on Cybercrime in both its substantive and procedural types. The first Chapter addresses the Legal nature of Cybercrime, its definition, elements, and the special characteristics that distinguish it from traditional crimes as well as the tools used for committing a cybercrime as it requires different tools & a person with special characteristics make him a distinctive from the criminal in traditional crimes. International and national efforts were exerted to combat the cybercrime and to establish a specific mechanism for preventing & reducing the crime by holding international conferences, symposia & conventions, as well as issuing the Decree Law No. 10 of 2018 on cybercrime at a national level and establishing specialized prosecution and specialized unit to combat cybercrime in the police and the rest of the security services also training judiciary officers on how to obtain a valuable evidence with a very high techniques to use it before the competent court. Combating this crime requires regulating procedures by a Palestinian legislature under a special law resolution; however, this regulation is limited to the stages of collecting evidences and preliminary investigation. As for the stage of the trial, it is similar to the procedures used in the traditional crimes which are developed by the general provisions of the Palestinian Criminal Procedure Law No. 3 of 2001.

## مقدمة

أصبحنا في عصرنا الحاضر أمام قوة لا يستهان بها سميت بالثورة المعلوماتية<sup>1</sup>، فقد لعبت وسائل تكنولوجيا المعلومات بوجود الحاسب وشبكة الانترنت العالمية<sup>2</sup> ومقدرتها على معالجة البيانات والمعلومات آلياً، وما يصاحبها من تطور مستمر في عالم التقنيات الذي يشهده قطاعي المعلومات والاتصالات ثورة حقيقة أمام الدول، فكان لا بد من مواجهتها وإحاطتها من عدة نواحي، وأهمها الناحية التشريعية بتنظيم الأحكام الموضوعية والإجرائية، التي تتناسب مع الطبيعة الخاصة التي تتميز به هذه الثورة والتي اجتاحت عصرنا الحالي، ولما قد ينتج من إساءة استعمال هذه الوسائل والبرامج والتطبيقات في الاعتداء على حقوق الأفراد والدول بقطاعيه الخاص والعام، من خلال ملاحقتها ومتابعتها من قبل الجهات المختصة حماية للأفراد وللمجتمع، وتنظيمها إدارياً وتقنياً من قبل وزارة الاتصالات، التي يندرج تحت مظلتها شركات الإتصالات ومزودي الخدمة، وتنظيمها دولياً لما تتسم به من الطابع اللاجغرافي غير الحدودي في التعامل فيها من الناحية الايجابية، ومن الناحية السلبية على حدٍ سواء.

إننا لا ننكر الآثار الايجابية التي أحدثتها هذه الثورة المعلوماتية، فقد شكلت نقلة نوعية وحضارية في حياة الأفراد والدول، ففي وقتنا الحالي أصبحت معظم القطاعات تتركز في أداء عملها على استخدام الأنظمة المعلوماتية والشبكة العالمية المرتبطة بها(الانترنت)، لما توفره من سرعة ودقة في جمع المعلومات وتخزينها ومعالجتها ونقلها وتبادلها بين المؤسسات والشركات والافراد والجهات المختلفة داخل الدولة الواحدة أو بين عدة دول.

وأصبحت هذه الانظمة مستودعاً لأسرار الأشخاص المتعلقة بحياتهم الشخصية، أو بطبيعة أعمالهم المالية والاقتصادية، كذلك أمست مستودعاً لأسرار الدول الحربية والصناعية والاقتصادية، التي تعبر على قدر من الأهمية والسرية.

---

<sup>1</sup> كلمة معلوماتية (informatique) هي اختصار لكلمتي معلومة (information) وكلمة آلي أو آلية (automatique)، وهي تعني المعالجة الآلية للمعلومة (Traitement automatique de L'information)، يُنظر: أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2000، ص270

<sup>2</sup> الانترنت: عبارة عن شبكة تتألف من العديد من الحاسبات الآلية المرتبطة ببعضها البعض، إما عن طريق خطوط التلفون أو عن طريق الأقمار الصناعية، وتمتد عبر العالم لتؤلف في النهاية شبكة هائلة، بحيث يمكن للمستخدم لها (user)الدخول من أي مكان في العالم وفي أي وقت، طالما كان جهاز الحاسب الآلي مزوداً بمودم (modem) يربطه بخط الهاتف لتلقي وإرسال البيانات عبر مزود الخدمة (Service Provider). يُنظر: جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الاحكام الموضوعية للجرائم المتعلقة بالانترنت، الطبعة الاولى، دار النهضة العربية، 2001، ص4.

إلا أنّ هذا الجانب الايجابي المشرق لعصر المعلوماتية لا ينفى الانعكاسات السلبية التي أفرزتها هذه التقنية، والمتمثلة في إساءة الأنظمة المعلوماتية واستغلالها على نحو غير مشروع، وبصورة تضر بمصالح الأفراد والجماعات، وبالتالي بمصلحة المجتمع كله، إذ أدى هذا التطور الهائل إلى ظهور أنماط مستحدثة من الجرائم اصطلح على تسميتها "بالجرائم الإلكترونية"<sup>1</sup>.

وخطورة هذه الظاهرة الاجرامية المستحدثة تتجلى في سهولة ارتكابها، وأنّ تنفيذها لا يستغرق إلا دقائق معدودة، وأحياناً تتم في بضع ثوان، وأنّ محر آثار الجريمة، وإتلاف أدلتها غالباً ما يلجأ إليه عقب ارتكاب الجريمة، فضلاً عن أنّ مرتكبيها يتسمون بالدهاء والذكاء، وغالباً ما يلجؤون إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية داخل دول أجنبية بواسطة شبكة الاتصال عن بعد، مع استخدام شفرات أو رموز سرية لإخفائها عن أعين أجهزة العدالة، مما يثير مشكلات كبيرة في جمع الأدلة الجنائية وإثبات هذه الجرائم من قبل الجهات المختصة<sup>2</sup>.

#### أهمية الدراسة:

1- لموضوع الجرائم الإلكترونية من الناحية الموضوعية والإجرائية أهمية بالغة، كانت دافعاً لاختياره وتناوله بالبحث والدراسة، وتظهر هذه الأهمية من خلال ارتباطه الوثيق والمباشر بظاهرة جديدة انتشار هذه الجريمة في مجتمعنا الفلسطيني، والتي باتت تعد من الموضوعات الشائكة التي بدأت، ومحل جدل فقهي وقضائي واسع، إضافة لاهتمام الدولي والاقليمي بهذا النوع من الظواهر، ولعل خير دليل على ذلك كثرة المؤتمرات الدولية والاتفاقيات التي أبرمت في سبيل مكافحة الجريمة المعلوماتية، سواء على المستوى الدولي أو المحلي<sup>3</sup>.

ولذلك فإذا استطاع الجناة تطوير طرق الإجرام على هذا النحو من التقنية العالية في بيئة تكنولوجيا المعلومات، فإنّه من الضروري تطوير وسائل المكافحة بما يواكب التطور في وسائل الإجرام

<sup>1</sup> - د. عبد الكريم الرائدة، الجرائم المستحدثة واستراتيجية مواجهتها، دار الحامد للنشر والتوزيع، الطبعة الأولى، 2013، ص 27

<sup>2</sup> - نهلة عبد القادر المؤمني، الجرائم المعلوماتية، عمان ، دار الثقافة للنشر والتوزيع ، ط1، ص 45.

<sup>3</sup> المؤتمر الدولي لحقوق الانسان بطهران المنعقد في الفترة الممتدة من 22 ابريل الى 13 مايو عام 1968، والخاص بأثر التقدم التكنولوجي على حقوق الانسان. وفي 28 يناير 1981 تم التوقيع على اتفاقية متعلقة بحماية الاشخاص في مواجهة المعالجة الالكترونية للمعطيات الشخصية، وكانت تحت اشراف المجلس الاوروبي، كما قام هذا الاخير بإصدار التوصية رقم 95 (13) في 11-09-1995، والتي تتعلق بمشكلات الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات. وفي 23 نوفمبر 2001، شهدت العاصمة المجرية بودابست أولى المعاهدات الدولية التي تكافح الجرائم الالكترونية، حيث وقع عليها ثلاثون دولة بما في ذلك الدول الاربعة من غير الأعضاء في المجلس الاوروبي وهي كندا واليابان وجنوب افريقيا والولايات المتحدة الامريكية. وحالياً مازالت المشاورات بشأن تشكيل مجموعة عمل بالاجرام الالكتروني مستمرة وكانت هذه المشاورات قد اخذت شكلا جديدا في اعقاب المرحلة الأولى من القمة الدولية بشأن مجتمع المعلومات (WSIS) في جنيف نهاية ديسمبر 2003، ثم نوقشت باستفاضة في المرحلة الثانية من القمة في تونس نهاية نوفمبر 2005.

المعلوماتي، وأصبح متطلباً من أجهزة العدالة الجنائية أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي، وهذا كان إحدى المسائل المهمة التي تتعرض لها المؤتمرات الدولية، حيث كان الموضوع الرئيسي للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، الذي عقد في ريو دي جانيرو بالبرازيل في الفترة من (4-6 سبتمبر 1994). كما أن هذه المسألة أيضاً كانت محل بحث في (الحلقة التمهيدية) التي عقدت على المستوى الدولي في فيوربخ (Wurzburg) بألمانيا في الفترة من (5-8 أكتوبر 1992)، وفي العام 2000 أصدرت الأمم المتحدة مرشداً عاماً حول مكافحة والحد من الجرائم الإلكترونية<sup>1</sup>.

أما على المستوى العالمي العربي، فلم تكن هناك جهود كبيرة في مجال مكافحة هذه الجرائم المستحدثة، سوى بعض الجهود العلمية، والأمنية بشكل خاص، حيث أصبحت متوالية في مجال رصد وتتبع الظواهر الأمنية المصاحبة لانتشار الحاسبات والانترنت، لعل آخرها المؤتمر العلمي الأول حول العالم الرقمي وجرائم الشبكات الإلكترونية، الذي شهدته العاصمة المصرية- القاهرة- في الفترة من (4-5 مارس 2009) وتناول لأول مرة بالدراسة مسألة الإثبات الجنائي باستخدام الوسائل الإلكترونية ومدى قبول الدليل الإلكتروني في الإثبات الجنائي<sup>2</sup>.

2- وتبرز أهمية الموضوع كذلك، في أنه تناول أحدث الوسائل العلمية، وأكثرها انتشاراً في قضايا الإثبات الجنائي، تلك الوسائل التي جاءت لتلازم التطورات التكنولوجية والتقنية، التي تطور معها الفكر الإجرامي، فكر الجرائم المعلوماتية، مما ألقى على عاتق القائمين على مكافحة الجريمة في

---

<sup>1</sup>International Review of Criminal Policy، United Nation "Manual on the Prevention and Control of computer related Crime 2000". Available at: <http://www.ifs.univie.ac.at/pr2gql/rev434.html>

<sup>2</sup>ناقش المؤتمر العلمي الأول حول العالم الرقمي وجرائم الشبكات الإلكترونية، عدداً من الموضوعات تتعلق بصفة عامة بالمواجهة الموضوعية والاجرائية للجرائم الإلكترونية، وجاء ذلك في ستة محاور تتمثل فيما يلي: المحور الأول، عبارة عن مقدمة تقنية وقانونية عن الجريمة الإلكترونية، حول كيفية اختراق الشبكات مثلاً وغيرها من الأساليب الفنية المستخدمة في ارتكاب الجريمة المعلوماتية، أما المحور الثاني، فجاء عبارة عن رصد لأهم الأنماط التقليدية للجريمة الإلكترونية، كالقذف والسب والاعتداء على حرمة الحياة الخاصة عبر الانترنت، والإرهاب الإلكتروني، أما المحور الثالث، فقد خصص لدراسة الجرائم المتعلقة بالمحتوى، كالاعتداء على الملكية الفكرية والاعتداء على حقوق البث الرقمي للقنوات الفضائية، أما المحور الرابع، فجاء خاصاً بالجرائم المتعلقة بالآداب العامة، كالاستغلال الجنسي للأطفال من خلال شبكة الانترنت وتسهيل الدعارة عبر الانترنت، وخصص المحور الخامس، بالجرائم الماسة بشبكة المعلومات الدولية كالدخول غير المشروع على الشبكة، والاعتداء على قواعد البيانات وبنوك المعلومات. أما المحور السادس والأخير، فخصص للمواجهة الاجرائية لهذه الجرائم المستحدثة، من خلال بيان كيفية تعامل مأموري الضبط القضائي مع الدليل الرقمي بالإضافة إلى مسائل الضبط، التفتيش والمعاينة في البيئة الإلكترونية، ومدى حجية الدليل الرقمي في الإثبات الجنائي.

الدولة الكثير من الأعباء والمهام الجسام تفوق القدرات المتاحة، لهم وفق أسس وقواعد إجراءات البحث الجنائي والإثبات الجنائي التقليدية، نظراً لعدم كفاية، وعدم ملائمة هذه النظم التقليدية في اثبات تلك الجرائم سواء من الناحيتين القانونية أو التقنية، وكان على المشرع حتماً أن يستحدث من التشريعات ما يلائم هذا النوع من الجرائم، فضلاً عن إنشاء أجهزة فنية متخصصة يناط بها عملية الإثبات العلمي الفني لهذه الجرائم.

3- وتكمن أهمية البحث أيضاً في محاولته بيان مدى تأثير طبيعة الدليل على اقناع القاضي الجنائي، حيث أصبح القاضي الجنائي حالياً يستند على الدليل العلمي بما فيه الدليل الإلكتروني الرقمي باعتباره تطبيقاً من تطبيقات الدليل العلمي، مما جعل للخبير الدور الأكبر في السيطرة على العملية الإثباتية.

4- وأخيراً، فإنّ اقناع القاضي في الأمور الجنائية، يأتي كوجاء يحمي من الشطط، التي ترتبت على الوسائل العلمية الحديثة في الإثبات، والتي في كثير من الأحيان تكون في ذاتها اعتداء على الحياة الخاصة للأفراد. ذلك ما سنحاول بيانه في هذه الدراسة.

#### **الصعوبات التي يطرحها موضوع البحث:**

تمثلت الصعوبات التي يطرحها موضوع هذه الرسالة بداية في اختيار موضوع البحث، وذلك كون موضوع البحث: "مكافحة الجرائم الإلكترونية موضوعياً وإجرائياً"، هو موضوع حديث في الفقه والقضاء الجنائي الفلسطيني لم يسبق بحثه بتعمق بالإضافة إلى ذلك، ارتباط الجرائم محل الدراسة بالحاسب الآلي، مما يتطلب الاطاعة بمكونات هذا الأخير وبنظام المعالجة الآلية للمعطيات والشبكات، وبطرق الدخول، وكل ما يتعلق بهذه الجرائم من تقنيات، وهذا يحتاج إلى جهد فني فضلاً عن الجهد القانوني، وخاصة أنّ القرار بقانون المتعلق بالجرائم الإلكترونية حديثاً فهو يحتاج إلى المزيد من الدراسة والتحليل.

## إشكالية الدراسة:

بالنظر إلى الطبيعة الخاصة التي تتميز بها الجرائم الإلكترونية، نجد بأنّها جرائم عابرة للحدود لأنّها تقع بين أكثر من دولة غالباً ما يكون الجاني في بلد والمجني عليه في بلد آخر، وقد يكون الضرر المتحصل في بلد ثالث مما يؤدي إلى صعوبة اثبات هذا النوع من الإجرام والملاحقة القضائية. مما يجعل الجريمة المعلوماتية طبيعة من نوع خاص على خلاف الجرائم الأخرى التقليدية، وقد تستمد هذه الطبيعة الخاصة من المجال الذي يمكن أن ترتكب فيه، أو من المحل الذي يقع عليه الاعتداء، مما يثير العديد من الإشكاليات خاصة وأنّ هذه الجريمة لم تحظ بالدراسة والتحليل في الفقه الجنائي، إلا حديثاً، وفلسطينياً لم يكن لها تنظيم تشريعي خاص إلا في وقت قريب مما أوجد خصوصية ذاتية من حيث وضع هذه الحماية، ومن حيث طبيعة الأحكام التي يجب أن تخضع لها واختلاف أثارها، إضافة إلى ما قد يصاحب الحصول على الأدلة الإلكترونية من خطوات معقدة، وإشكاليات إجرائية في الإثبات كدليل جنائي، وعليه لا بد من طرح العديد من التساؤلات حول ماهية الجريمة الإلكترونية وما أوجه الاختلاف ما بينها وبين الجريمة التقليدية؟ وهل التشريع الخاص بالجرائم الإلكترونية كاف للحد من هذه الجريمة؟ وكيف تم مواجهة الجريمة الإلكترونية على الصعيد الدولي والإقليمي؟ وهل تكفي القواعد الاجرائية المقررة للجرائم التقليدية لمكافحة الجرائم المعلوماتية أم يتوجب النص عليها بقانون خاص؟ وما هي الشروط اللازمة لاعتماد الدليل الإلكتروني كدليل إثبات في الجرائم الإلكترونية؟ وكيف يقتنع القاضي الجنائي بالدليل الإلكتروني؟ ومدى كفاية التشريع الفلسطيني في مكافحة هذه الجريمة المستحدثة من حيث الأحكام الموضوعية والإجرائية ومعوقات مكافحة الجريمة الإلكترونية في فلسطين؟ وهل نحن بحاجة إلى تحليل وتقييم الجريمة الإلكترونية بفلسطين، ومدى ملائمة التشريع الفلسطيني بمكافحتها للتطور المستمر؟ وبعد التعرض للتسؤلات السابقة نصل إلى أن مشكلة الدراسة تتمثل بالتسؤال التالي:

إلى أي مدى تصدى أو لأمس قرار بقانون رقم 10 لسنة 2018 كافة الجوانب الموضوعية والإجرائية في التصدي للجريمة الإلكترونية؟

## خطة الدراسة:

من أجل معالجة الإشكاليات السابق طرحها، ارتأينا تقسيم هذا البحث إلى فصلين، حيث تطرقنا في الفصل الأول لدراسة الطبيعة القانونية للجريمة الإلكترونية، فقمنا بتقسيمه الى مبحثين خصصنا الأول منه للحديث ماهية الجريمة الإلكترونية، وأفردنا المبحث الثاني لدراسة: المواجهة التشريعية للجريمة الإلكترونية، فيما تناولنا في الفصل الثاني الأحكام الإجرائية لمكافحة الجريمة الإلكترونية في التشريع الفلسطيني، وقسمناه هو الآخر إلى مبحثين: مبحث تكلمنا فيه عن الإجراءات التحقيقية في الجريمة الإلكترونية، وآخر لدراسة مرحلة المحاكمة في الجرائم الإلكترونية.

## منهج الدراسة

حرصنا على أن ننتهج في دراستنا هذه سبيلاً منطقياً يسير جنباً إلى جنب مع تسلسل الفكرة حرصاً على بلوغ الغاية من الدراسة، لذلك اتبعنا المنهج التكاملي، فهو منهج تأصيلي، تحليلي ومقارن، منهج تأصيلي أولاً، لأنه يرد النقاط التفصيلية إلى أصولها النظرية، وفي دراستنا هذه نرجعها إلى النظرية العامة للإثبات الجنائي.

وتحليلي ثانياً، من خلال قيامنا بشرح الموضوعات المختلفة التي عالجناها في هذه الدراسة، كتحليل أسباب صعوبة إثبات الجريمة الإلكترونية، وإيراد تطبيقات قضائية عليها واستخلاص النتائج التي تترتب على ذلك التحليل.

أما المنهج المقارن، فيظهر جلياً من خلال مقارنة النظام اللاتيني وعلى قمته دراسة القانون الفرنسي وقوانين أخرى التي تأثرت به كالقانون الجزائري والمصري، مع النظام الانجلو الأمريكي من خلال دراسة القانون الأمريكي والانجليزي، باعتبار هذه القوانين الاخيرة ايقنت بسلامة منطق الادلة الإلكترونية ومنظورها العلمي.

## مخطط الدراسة:

### • الفصل الأول: الطبيعة الموضوعية للجريمة الإلكترونية

المبحث الاول: ماهية الجريمة الإلكترونية

المطلب الاول: مدلول الجريمة الإلكترونية

الفرع الاول: تعريف الجريمة الإلكترونية.

الفرع الثاني: سمات الجريمة الإلكترونية والادوات المستخدمة في ارتكابها

**المطلب الثاني: مفهوم المجرم الالكتروني**

الفرع الاول: تعريف المجرم الالكتروني

الفرع الثاني: خصائص المجرم الالكتروني

**المبحث الثاني: المواجهة التشريعية للجريمة الإلكترونية**

المطلب الاول: الجهود المبذولة للتصدي للجريمة الإلكترونية

الفرع الاول: الجهود الدولية للحدّ من الجرائم الإلكترونية

الفرع الثاني: الجهود التشريعية الفلسطينية لمكافحة الجريمة الإلكترونية

• **الفصل الثاني: الاحكام الاجرائية لمكافحة الجريمة الإلكترونية في التشريع الفلسطيني**

المبحث الاول: الاجراءات التحقيقية في الجريمة الإلكترونية

**المطلب الاول: التحقيق التمهيدي ((البحث والاستدلال))**

الفرع الأول: البحث والاستدلال في الجرائم التقليدية

الفرع الثاني: مرحلة جمع الاستدلالات في الجريمة الإلكترونية

**المطلب الثاني: التحقيق الابتدائي في الجريمة الإلكترونية**

الفرع الأول: الجهة المختصة بالتحقيق في الجرائم الإلكترونية

الفرع الثاني: اثبات الجريمة الإلكترونية

**المبحث الثاني: مرحلة المحاكمة في الجرائم الإلكترونية**

المطلب الاول: المبادئ العامة للاختصاص في الجرائم الإلكترونية

المطلب الثاني: الاجراءات المتبعة في مرحلة المحاكمة في الجرائم الإلكترونية

المطلب الثاني: الآثار المترتبة على عدم مشروعية الاجراءات

### الطبيعة القانونية للجريمة الإلكترونية

تعد الجريمة الإلكترونية من الجرائم التي تندرج ضمن نطاق القسم الخاص في قانون العقوبات الذي يتناول كل جريمة على حدا من حيث أركانها وعناصرها الأساسية وطبيعتها، والنتيجة المترتبة منها والعقوبة المقررة لها<sup>1</sup>، وهذا كله نتج عن استخدام الحواسيب والشبكات الإلكترونية إلى ازدواجية بالمنفعة المتحصلة باستخدامها فهي ذات منفعة ايجابية بالاستفادة منها بالمجالات البحث العلمي والتوثيق المعلومات وتخزينها والحصول على معلومات تسهل تيسير إكمال القطاعين الخاص والعام، وما لبث الأمر إلا أن تحولت هذه المنفعة إلى تغيرات جذرية ونوعية وإجرامية، بمختلف مناحي الحياة بنهاية القرن العشرين لاستغلال هذه التقنيات المتطورة في الارتكاب العديد من الجرائم سواء على الصعيد المحلي والاقليمي أو على الصعيد الدولي محدثاً آثاراً سلبية ومباشرة وخطيرة أوردت القطاعين الخاص والعام.<sup>2</sup>

وتستمد هذه الجرائم طبيعتها الخاصة من قدرة الشبكة المعلوماتية على الاعتداء ونقل وتبادل المعلومات العامة والخاصة في آن واحد، وهذا كله جاء نتيجة لتطور العالم الافتراضي الذي أصبح جزءاً من حياة الانسان الذي رافقه وجود الحواسيب والانترنت والتطور التكنولوجي الهائل، الذي هو من متطلبات العصر الراهن والتعامل مع هذه التقنيات المتطورة سواء في القطاع الخاص كالمؤسسات المالية والجمعيات والبنوك والشركات، أو في القطاع العام الحكومي مثل المستشفيات والوزارات والمطارات، وأصبحت الدول في القرن العشرين تعتمد على حوسبة واتتمة أعمالها ونشاطاتها واتصالاتها وتنظيم إدارتها، والاشراف على حسن سير أعمالها من خلال نظام الكتروني، وأصبحت

<sup>1</sup> محمد زكي ابو عامر، وعلي عبد القادر القهوجي، قانون العقوبات/ القسم الخاص، بدون مكان وسنة نشر، ص9 وما بعدها.

<sup>2</sup> عبد الفتاح مراد، شرح جرائم الحاسوب والانترنت، مصر، دار العرب للنشر والتوزيع، ص33.

هذه التكنولوجيا المتمثلة بالحواسيب والشبكة العالمية جزءاً من الحياة اليومية للأفراد ونشاطه الاجتماعي، وتعامله بحيث أنه لا يمكن الاستغناء عنها لتسهيل تسيير الحياة بشكل عام<sup>1</sup>. ونظراً لتمييز الجريمة الإلكترونية بطبيعة خاصة، أصبح هناك ضرورة لوجود قانون خاص ينظم هذا النوع من الجرائم لاتصالها ببيانات وكلمات ورموز وأرقام، سواء من حيث تجميعها وتخزينها وتجهيزها واسترجاعها وتصحيحها وتعديلها ومحوها وطباعتها ونسخها، فهي تتم من خلال المعالجة الآلية للبيانات بهدف الحصول على المعلومات المرجوة<sup>2</sup>، ومن خلال الطبيعة الخاصة للجريمة الإلكترونية والتي تميزها عن الجريمة التقليدية من حيث نصوصها وطريقة التحقيق بها وتحليلها وربطها والحصول على الدليل الرقمي الذي هو أهم دليل لاكتشاف الجريمة الإلكترونية ومتابعتها من خبراء تكنولوجيا المعلومات فهي تمتاز بطبيعة ازدواجية ما بين الحصول على الدليل، وتحليله واتصاله بالنص القانوني فبذلك الجريمة الإلكترونية بحاجة إلى إجراءات خاصة لمتابعتها بشكل يتواءم ويتمشى مع التقنيات المستخدمة والمستحدثة لارتكاب الجريمة، والتحري عن النظام القانوني الملائم لطبيعة هذه الجرائم ليتوافق والخصوصية التي تتميز بها.

ونتيجة لذلك ظهرت أنماط من الجرائم المستحدثة مرافقاً للتطور المتسارع الذي تمر فيه، وكان لإتساع استخدام الحواسيب ومرافقة من وجود الشبكة العالمية (الانترنت) والمرتبطة مع بعضها البعض ظهور مصطلحات وتعريفات عديدة لهذا النوع من الجرائم المستحدثة الإلكترونية وجعل مفهومها وطبيعتها القانونية غير واضح وغير محدد بشكله الدقيق، مع وجود عدة اتجاهات اختلفت على تعريف الجريمة الإلكترونية المتعلقة باستخدام الحاسوب كوسيلة لارتكاب جريمة أو محلاً لها<sup>3</sup>، وهذا ما أثار الكثير من التساؤلات حول تعريف الجريمة الإلكترونية والعناصر الأساسية التي تقوم عليها، ومدى اختلاف الجريمة الإلكترونية عن باقي الجرائم لا سيما وأنها تتميز بطبيعة خاصة؟

وللإجابة على هذا التساؤل ظهرت هناك عدة معايير لتعريف الجريمة الإلكترونية، وبيان عناصرها واركائها، وقبل الإشارة إليها وبيان هذه المعايير لا بد من الإشارة المكونات، والأدوات المستخدمة في

---

<sup>1</sup> عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية من قانون الجرائم الإلكترونية، عمان، دار الاوائل للنشر والتوزيع، الطبعة 2017، ص21.

<sup>2</sup> احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري (دراسة مقارنة)، دار النهضة العربية، الطبعة الأولى، 2010، ص10.

<sup>3</sup> عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، عمان، دار الحامد للنشر والتوزيع، الطبعة الأولى، 2013، ص28.

ارتكاب الجريمة الإلكترونية وصولاً لتعريفها وخصائصها وأركانها (مبحث أول)، متناولين الجهود المبذولة على الصعيد الدولي والوطني لمكافحة الجريمة الإلكترونية (مبحث ثاني).

### المبحث الأول: ماهية الجريمة الإلكترونية

إنّ لهذا النوع من الجرائم التي اجتاحت العالم بفضل التطور التكنولوجي العالمي الذي كان من المفترض أن يقودنا إلى ثورة علمية تقنية بمفهومها الايجابي، فلم تكن الغاية والهدف من وجود هذه التقنيات إلا لخدمة البشرية بشتى أنواع المجالات الحياتية والإقتصادية والأمنية والعلمية وتبادل هذه المجالات للعالم الأجمع الذي أصبح بفضل هذه التقنيات قرية صغيرة. بيد أنّ هناك من استغل هذه الانجازات لمصالحهم الشخصية سواء أكانت لأهداف تدميرية أو انتقامية أو مالية أو حتى عاطفية وجنسياً لم يكن هذا الواقع سهلاً لرجال الأمن والقضاة في بادئ الأمر وخلق حالة تباينية من الآراء ما بين الفقهاء والقانونيين وهذا ماسوفنوضحه عند البحث عن التعريف القانوني للجريمة الإلكترونية والتي ليس لها لغاية اللحظة تعريفاً متفقاً عليه ولكن أمام هذا الواقع كان لا بد من تكثيف الجهود الدولية والاقليمية والمحلية للحد من هذا النوع من الجرائم فتسارعت الدول بسن تشريعاتها وتدريب كوادرها البشرية وتطوير برامجها، ورفع جدار الحماية لانظمتها، وإنشاء دوائر في كل مؤسساتها الحكومية والمدنية تعنى بالجانب التقني التكنولوجي درءاً للاعتداءات غير المشروعة بشتى أنواعها.

### المطلب الأول: مدلول الجريمة الإلكترونية

#### الفرع الأول: تعريف الجريمة الإلكترونية

وقبل الخوض في الجريمة الإلكترونية لا بد من بيان تعريف الجريمة بشكلها التقليدي العام حيث تطرق الفقهاء القانونيين لتعريف الجريمة فعرّفها الفقيه كارارا: "بأنّها انتهاك حرمان قانون من قوانين الدولة بفعل خارجي صادر عن رجل لا يبرره قيام بواجب ولا ممارسة لحق على أن يكون منصوباً على معاقبته في القانون"<sup>1</sup>، وعرّفها الدكتور محمود نجيب حسني أنّها: "سلوك غير مشروع صادر عن ارادة جنائية يقرر القانون له عقوبة"<sup>2</sup>، وعرّفها جارو "أنّها كل فعل أو ترك يعاقب عليه القانون بعقوبة جنائية ولا يبرره استعمال حق ولا أداء واجب"، وعرّفها كامل السعيد في شرح الأحكام العامة قي قانون

<sup>1</sup> محمد صبحي نجم، قانون العقوبات (القسم العام) النظرية العامة للجريمة، دار الثقافة للنشر، 2012، ص 107.

<sup>2</sup> محمد علي السالم الحلبي، شرح قانون العقوبات (القسم العام)، دار الثقافة للنشر، الطبعة الثالثة، 2011، ص 60.

العقوبات "بأنها سلوك يمثّل بفعل أو امتناع غير مشروع أخل بمصلحة أساسية صادرة عن إرادة جنائية يقرر له القانون عقوبة أو تدبيراً احترازياً"، في حين خلى قانون العقوبات رقم 16 لسنة 1960 المطبق في الأراضي الفلسطينية من تعريف للجريمة بإطارها العام، الجريمة بطبيعتها اثبتت وجودها عن القانون لذلك فإنّ المشرع لا يتدخل بالتعريفات إلا في حدود ضيقة إمّا لحسم خلاف فقهي، أو أنّ التعريف يغير ويوضح ما استقرت عليه تعاريف تحمل نفس المعنى -بصورته الضيقة-، بالقوانين الأخرى أي بمعنى توحيد التعاريف المتبانية لنفس المضمون الذي سعى إليه المشرع<sup>1</sup>

### تعريف مصطلح الإلكترونيّة:

مأخوذ من الكتروني الكترونيات إذ بدأ ينتشر العقل الإلكتروني في كل المكاتب من خلال: آلة الحاسوب التي تعتمد على مادة الالكترن لإجراء أدق العمليات الحسابية، وبأسرع وقت ممكن ويسمى أيضاً كمبيوتر: علم الإلكترونيات: علم يهتم بتركيب الإلكترونيات واستخدامها وتناولها وهو فرع من فروع الفيزياء. بالانجليزي (ELECTRO) (رمزه: e) أو الكهيرب هو جسيم دون ذري كروي الشكل تقريبا مكون للذرة ويحمل شحنة كهربائية سالبة والالكترن لديه كتله تعادل تقريبا (1/1836) من كتلة البروتون.<sup>2</sup>

ويقصد به: جسم دقيق جداً وهو أصغر ملايين المرات من أي شيء يمكن أن تراه العين المجردة، وهو من الصغر بحيث لم يراه إنسان قط، حتى بإستعمال أعظم الميكروسكوبات قوة، ونستطيع أن نتصور صغره إذا علمنا إنّ البلاين منه قد لاتصل إلى وزن أخف ريشة، كما لاتصل في حجمها إلى رأس الدبوس.<sup>3</sup>

### تعريف الجريمة الإلكترونيّة:

سوف نتطرق الى أهم التعريفات الفقهية والتشريعية المتعلقة بالجريمة الإلكترونيّة والتي تتمثل فيما يلي:

#### 1- التعريفات الفقهية:

ولم يتفق الفقه والخبراء التقنين والقانونيين على تعريف موحد شامل جامع للجرائم الكترونية أو السلوك الإجرامي الناتج من استخدام واستغلال وسائل تكنولوجيا المعلومات<sup>4</sup> إلا أنّهم اتفقوا بأنّ الجريمة

<sup>1</sup> كامل السعيد ، شرح الاحكام العامة من قانون العقوبات دراسة، عمان، مقارنة دار الثقافة 2011، ص 38 .

<sup>2</sup> معجم المعاني عربي منشور على الموقع الالكتروني <https://www.almaany.com/ar/dict/ar-ar> تاريخ الدخول 2019/10/1 الساعة 3 صباحاً.

<sup>3</sup> جين بنديك، ترجمة أحمد أبو العباس ، التطور الإلكتروني وأثره في حياتنا، دار المعارف القاهرة، مصر، 1957، ص 9.

<sup>4</sup> عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، 2008، ص 21.

المستحدثة بإطارها الجديد بإزدياد وارتفاع بمعدلات الجريمة الإلكترونية والخسائر والضحايا كنتيجة جرمية وأنّ الجرائم الإلكترونية لم تكن بديلاً للجرائم التقليدية بل اضافت عليها أنماطاً وأشكالاً مستحدثة بل اعتبرها الفقه انها ظاهرة تتراد بمعدلات عالمية كما أنه لم يتم الاتفاق على تسمية واحدة لهذا النوع من الجرائم فبعضهم ما أطلق عليها الجرائم المعلوماتية أو جرائم الانترنت أو الجرائم التي تنتج من استخدام التقنيات الحديثة المتمثلة بالحاسب الآلي والانترنت أو الغش المعلوماتي أو الاحتيال المعلوماتي ولعل ذلك يعود الى الواجهة التي يستندون اليها فمنهم من استند على الزاوية الفنية أو الزاوية القانونية أو الموضوعية لتعريف الجريمة الإلكترونية<sup>1</sup>.

يرى بعض الفقهاء أنّ المعيار في تحديد تعريف الجريمة الإلكترونية مرتبط بالتقدم التكنولوجي المتجدد والمتطور بصورة مستمرة معتبراً أنّ هناك علاقة وثيقة لهذا الترابط وأنّه كلما زاد التطور والتجديد بهذه التقنيات تقترن بظهورها جرائم جديدة بأنماط تتلاءم معها لذلك فإنّه يصعب بمكان حصر الجرائم الإلكترونية وهذا ما أخذ به المشرع الانجليزي بعدم وضع تعريف محدد للجريمة الإلكترونية وجرائم الحاسب الآلي وأنّ تحديد الجرائم الإلكترونية قد يؤدي إلى حصر القاعدة التجريبية وبالتالي عدم مواكبتها التطور التقني الذي قد يظهر بالمستقبل<sup>2</sup>.

ومنهم من اعتمد في تحديد تعريف الجريمة الإلكترونية على الاخذ بمحل الجريمة وموضوعها، ومن انصار هذا الراي الفقيه فيفان والفقيه ليستانك اللذان اعتبرا أنّ "الجريمة المعلوماتية مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب، وعرفه البعض بأنها"سلوك غير مشروع معاقب عليه قانوناً صادراً عن إرادة جرمية محله معطيات الحاسوب، والبعض الآخر عرفها بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"<sup>3</sup>.

ويرى البعض من الفقهاء أنّ المعيار في تحديد تعريف الجريمة الإلكترونية هو الوسيلة المستخدمة في ارتكاب الجريمة، واعتبر أنصار هذا الراي أنّ الحاسوب الاداة الرئيسة لارتكاب وتنفيذ الجريمة الإلكترونية ومن أنصار هذا المعيار الفقيه تاديمان حيث عرف الجرائم الإلكترونية "كل أشكال السلوك

<sup>1</sup> عبد الفتاح بيومي حجازي، نفس المرجع السابق، ص28.

<sup>2</sup> عبد الفتاح بيومي حجازي، نفس المرجع السابق، ص37.

<sup>3</sup> نهلة عبد القادر المؤمني، الجرائم المعلوماتية، عمان، دار الثقافة للنشر، مرجع سابق، ص49.

غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب "وعرفه توم فوريستر الجرائم الإلكترونية" أنها كل فعل إجرامي يتم باستخدام الحاسوب كأداة رئيسية<sup>1</sup> ويعرف الفقيه ديفيد تومبسون الجريمة الإلكترونية "أية جريمة يكون متطلباً لاقتوافها أن تتوافر لدى فاعلها معرفة تقنية الحاسب" وعرفها الفقيه ستين سكيولبييرج "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً"، وهذا المعيار يستند على مستوى المعرفة التقنية للفاعل (الجاني)<sup>2</sup>، وهذا ما حدا إليه المشرع الأردني في قانون الجرائم الإلكترونية رقم (27) لسنة 2015 والذي اعتمد على المعيار الشخصي أي على المعرفة التقنية للفاعل وأن الدخول إلى أي شبكة معلوماتية أو نظام المعلومات بدون إذن أو تجاوز الحدود المقترح بها أو خالفها بأيّة وسيلة يعاقب بالحبس<sup>3</sup>.

يؤيد أنصار المعيار الخامس بالأستناد على الخسائر والريح الناتجة من الجريمة الإلكترونية لتحديد تعريف لها، ومن أنصار هذا المعيار الخبير الأمريكي باركر الذي عرف الجريمة الإلكترونية بأنها "كل فعل إجرامي متعمد أياً كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل"، ويعرفها الفقيه ماس بأنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"<sup>4</sup>.

**وجاء المعيار الاخير في تحديد تعريف الجريمة الإلكترونية مرتكزاً على الاعتداء على الاموال المادية والمعنوية، وهذا المعيار ورد بالاستنبان المعد من قبل منظمة التعاون الاقتصادي برد خبراء**

<sup>1</sup> محمود عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر، الطبعة الأولى، 2009، ص15.

<sup>2</sup> محمود عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر، نفس المرجع السابق، ص16.

<sup>3</sup> المادة (3) من قانون الجرائم الإلكترونية الاردني رقم(27) لسنة 2015 والتي نصت: "أ- يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات باي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة اشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين.

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار.

ج- يعاقب كل من دخل قصداً إلى موقع الكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار".

<sup>4</sup> نهلة عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة للنشر، مرجع سابق، ص 49 .

من بلجيكا حول الغش المعلوماتي بأن الجريمة الكترونية "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية"<sup>1</sup>.

وفقا لما جاء بتعريف المشرع الفلسطيني في الباب الأول من قرار بقانون الجرائم الإلكترونية رقم 10 لسنة 2018<sup>2</sup> فيما يتعلق بتكنولوجيا المعلومات، ومن خلال التعريف يتبين أنّ المشرع الفلسطيني لم يحذو حذو المشرع الأردني باعتماد المعيار الشخصي المتعلق بالمعرفة التقنية للفاعل بل اعتمد على معيار الوسيلة لإرتكاب الجريمة الإلكترونية، وعليه نجد أنّ الجرائم الإلكترونية لا تتم إلا بوجود حاسب آلي أو أداة (شبيهة) شبيها لمكوناته تستخدم لذات الأغراض المنصوص عليها في التعريف السابق وبذلك شمل ما قد يتم استحدثه من تقنيات بالمستقبل وبأية شكل من الاشكال<sup>3</sup>، الأهم هو أنّ ارتكاب الجريمة تم من خلال هذه الوسيلة التقنية المستحدثه قد لا يكون في محله لإثباته ليس بالضرورة أن يلم الفاعل بمعرفة تقنية عالية فهناك أنواع عديدة للمجرم الإلكتروني منهم الحاقدون، الهواه، المخترقون، المتطفلون، صغيري السن، وقليل الخبرة وقد ترتكب جريمة من اشخاص ليسو من ذوي الاختصاص و من باب الصدفة إلا أنّه قد نستفيد من سمات المجرم الإلكتروني عند تقديمه للمحاكمة و صدور حكم قضائي فيه معتمدين على تصنيف المجرم لاتخاذ الحكم المناسب له وفقا لنظرية التفريد العقابي<sup>4</sup> بإعادة تأهيله وإرشاده وعدم استغلال هذه الاجهزة لارتكاب جريمة أو وضع سياسة منهجية من قبل مؤسسات الدولة باستقطابه للعمل لصالح الدولة والمؤسسات لقاء أجر يبعده من ارتكاب الجريمة.

نجد أنّ جميع المعايير المذكورة والتي استند الفقهاء عليها اعترى فيها النقص، حيث لم يتم تعريف الجريمة إلا بناء لما استند عليه الفقهاء ومن وجهة نظرهم أمّا للوسيلة أو المعرفة العالية أو المعلومة

<sup>1</sup> احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري(دراسة مقارنة)، مرجع سابق، ص17.

<sup>2</sup> المنشور في الوقائع الفلسطينية العدد الممتاز رقم(16) بتاريخ 2018/5/3

<sup>3</sup> المادة 1 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية، تعريف تكنولوجيا المعلومات: "تكنولوجيا المعلومات: أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية، أو أي وسيلة أخرى، سواء أكانت مادية أم غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أي قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة

<sup>4</sup> وينقسم التفريد الى ثلاث أنواع وهم:

1- التفريد القانوني(العقابي): يقصد به التفريد الذي يتبناه المشرع نفسه عن طريق إيجاد ضوابط للتفرقة بين الأشخاص مثل المجرم الحدث والمجرم البالغ والمجرم لأول مرة والمجرم المكره.

2- التفريد القضائي: وهو ما يقوم به القاضي نفسه بموجب سلطته التقديرية في اختيار العقاب المناسب لشخص الجاني والمتمثلة بتراوح العقوبة بين حداها الأدنى وحدها الأقصى والاختذ بنظام الظروف المخفظة ويقف تنفيذ العقوبة .

3- التفريد الإداري: هو ما تتمتع به إدارة السجون في اختيار الأسلوب الملائم لكل سجين مثل اطلاق سراح السجناء.

محل الجريمة والمعايير الأخرى لم يتم وضع تعريف يجمع بين هذه المعايير موحد وقد تدارك بعض الفقهاء هذا النقص وخرجوا بتعريف للجريمة الإلكترونية بقولهم: "بأنها كل جريمة يقوم بها الشخص الملم بتقنية الحاسب أياً كان مستوى الالمام وتقع على الحاسب الآلي أو من خلاله سواء كانت الوسيلة في ارتكاب جريمة انترنت أو غيرها، وهي من الجرائم الجديدة ومن غير الجرائم التقليدية المعروفة في الفقه الجنائي"<sup>1</sup>

## 2- التعريفات التشريعية:

بدراسة لأنظمة والتشريعات نجد تفاوتاً بينها، أي أنّ بعض هذه الأنظمة والتشريعات عرف الجريمة الإلكترونية والبعض الآخر لم يتطرق لتعريفها مكتفياً بتسمية الأفعال التي يجرمها ووضع لها الجزاءات المناسبة لها.

القانون السعودي: تضمن نظام مكافحة جرائم المعلومات السعودي تعريف الجريمة الإلكترونية في الفقرة الثامنة من المادة الأولى بأنها: "أي فع ليرتكب متضمناً استخدام الحاسب الآلياً والشبكة المعلوماتية بالمخالفة لاحكام هذا النظام".

- القانون القطري: لقد عرف المشرع القطري الجريمة الإلكترونية في الفقرة العاشرة من المادة الأولى الذي خصص للتعريفات بأنه "أي فعل

- ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون"<sup>2</sup>.

أما المشرع الفلسطيني لم يتطرق لتعريف الجريمة الإلكترونية في قرار بقانون رقم 10 لسنة 2018 ، الا أنه يمكن تعريفها على أنها أي فعل يرتكب باستخدام الحاسب الآلي أو شبكة الانترنت يلحق الضرر والأذى بالغير أو أن يقع على الحاسب الآلي نفسه ويكون هذا الفعل مخالفاً لأحكام القانون.

## الفرع الثاني: خصائص الجريمة الإلكترونية والادوات المستخدمة في ارتكابها.

تتمتع الجريمة الإلكترونية كونها ذات طبيعة خاصة، بخصائص تختلف عما تمتاز به الجرائم التقليدية سواء من حيث الوسيلة والأداة المستخدمة أو من حيث الأسلوب التقني المتطور دائماً وهذا يجعلنا نطرح السؤال والذي سيتم الإجابة عليه في الفصل الثاني، هل هذه الخصائص والسمات تقع حائلاً

<sup>1</sup>نهلا عبد القادر المؤمني، ماجستير في القانون الجنائي المعلوماتي، الجرائم المعلوماتية، عمان، دار الثقافة، 2010، ص50.

<sup>2</sup>انظر إلى المادة الأولى من القانون القطري رقم 14 لسنة 2014.

أمام الحصول على الدليل الذي يربط فاعل الجريمة بها؟ كما هل يمكن الاستفادة من هذه الخصائص من قبل الأجهزة الأمنية المختلفة لملاحقتها ومتابعتها، بتطوير الخبرة التقنية لتواكب ما يستجد من جرائم الكترونية؟ وهل يمكن أن تدفع هذه الخصائص المشرع إلى وضع نصوص قد تكون قاسية على الشركات المصنعة والمنتجة للبرامج التي يمكن استخدامها لإخفاء الجريمة؟

فهناك العديد من الخصائص الخاصة بالجريمة الإلكترونية التي تضي عليها الطبيعة الخاصة بالجرائم الإلكترونية دائماً تكبد خسائر فادحة، وأن اختراق أي من القطاعات الخاصة تحديداً أو نشر فيروسات في شبكتها يكبد هذا القطاع خسائر تقنية عالية يدفعها الى تغيير النظام التقني داخلها والى وضع برامج حماية وأمن للمعلومات والبيانات المدخلة للشبكة الخاصة للقطاع فهذا يكبد المنشأة أموال لم تكن بالحسبان من ضمن ميزانيتها فضلاً على إذا كان الاختراق من أجل سرقة أموال أو احتيال الكتروني فإنه أيضاً من ضمن الخسائر الناتج عن الإعتداء الإلكتروني قد تصل الخسائر إلى الملايين وفي هذا المطلب سنبين الخصائص التي تتميز بها الجريمة الإلكترونية عن غيرها من الجرائم كالآتي:

1

**1-سهولة اخفاء الجريمة وسرعة التطور في ارتكابها،** أي بمعنى أن المجرم يبدأ بالأعمال التحضيرية لارتكابها دون أن يلاحظ الضحية أو يشعر بوجود أي تغيير أو اشارات تنبهه أو تحذره بوجود خطر أو اعتداء واقع عليه، والسبب يعود إلى أن الجريمة الإلكترونية تمتاز بالدقة والسرعة المرتبط بالشخص الجاني الذي يتمتع بقدرات فنية عالية، فقد سمي هذا النوع من الجرائم بالمخادعة الآلية التقنية لأنها لا تترك أثر مادي لمتابعتها ومعرفة فاعلها<sup>2</sup>

**2-جريمة لا عنفية التنفيذ،** يتم ارتكاب الجريمة الإلكترونية بهدوء وبدون أية أعمال عنيفة أو مجهود عضلي كما في الجرائم التقليدية بل يتم الاعتماد فيها على المجهود العقلي فهي جريمة العقل البشري الذي ارتبط بالسلوك الاجرامي الواقع كما هو الحال في جرائم الايذاء والقتل والاختطاف أو الخلع والكسر وجرائم السرقة ، فالجاني يعتزل عنفه بوجود الحاسب الآلي خط لشبكة الانترنت مسخراً معرفته

<sup>1</sup> هيثم عبد الرحمن النقلي، الجرائم الإلكترونية الواقعه على العرض، مصر ، دار العلوم، 2010،ص 22.

<sup>2</sup> حمد أمين رمضان، محمد ايمن رمضان احمد، الحماية الجنائية للتوقيع الالكتروني، رسالة دكتوراة، كلية الحقوق جامعة عين شمس، مصر، 2010،ص 248.

التقنية في ارتكاب افعال غير مشروعة فهي من الجرائم التي لا يوجد لها آثار للعنف أو دماء انما فقط ارقام وحسابات وأنظمة ومعلومات يتم التلاعب فيها .<sup>1</sup>

3- **جريمة عابرة للحدود** وقد ظهرت هذه الخاصية عند التعريف بشبكة الانترنت (العالمية) بأنه لا يوجد مساحة جغرافية تحصر وإنما هي ترابط عدد غير محدود من الحواسيب يصل الى مليارات وهذا يؤكد من خلال هذا الاتصال والترابط الذي يتم فيه نقل المعلومات وتبادلها عبر الأنظمة المختلفة فهي تمر بحدود لدول عدة، فقد ترتكب الجريمة من خلال حاسوب بدولة معينة بينما يتحقق الفعل الاجرامي والنتيجة الجرمية في دولة اخرى دون أي رقابة لحركة تنقل هذه المعلومات التي تخترق بتنقلها الزماني والمكاني وعلى سبيل المثال يستطيع شخص موجود في الولايات المتحدة من ارتكاب جريمة لسرقة بيانات أو احتيال الكتروني مستخدماً جهازه الشخصي المتصل بشبكة الانترنت لشخص طبيعي أو معنوي في دولة أخرى كفرنسا، وهذا يجعلنا أمام التساؤل حول الاختصاص الدولي لهذه الجريمة وفيما إذا كان هناك تباين ما بين القوانين التي تحكم الفعل الإجرامي ما بين المباح والمحرم، وهذا ما يضيف على الجريمة الإلكترونية طابعها التقني والقانوني الدولي ، واعتبرت جريمة الانترنت من الجرائم الدولية التي لا تعترف بالحدود القائمة بين الدول سواء الجغرافية أو السياسية وهذه الخاصية شكلت صعوبة في امكانية مكافحة هذه الجريمة التي تمتد لأكثر من اقليم دولة .<sup>2</sup>

4 - **عدم الإبلاغ من قبل المجني عليهم**، إن الاعتداء الواقع على الشركات والبنوك خاصة من الاعتداءات الخطيرة والتي تمس سمعة الشركة أو البنك والتي هي أساس عمل وتشغيل هذه القطاعات هو ما يتمتعون به من سمعة على صعيد العمل والمعاملة الاقتصادية وبالتالي نتاج هذه السمعة هي الثقة التي يمنحها الافراد لهذه القطاعات فإذا تم اختراق أو سرقة بيانات أو احتيال على هذه الشركات والبنوك الخاصة يؤدي بالنتيجة الى هدم جسر الثقة ، لذلك تفضل هذه القطاعات عدم الافصاح أو الإبلاغ أو الاشتكاء حول هذه الاعتداءات الإلكترونية الواقعة عليهم ليحافظوا على سمعتهم التجارية، ولكن عدم التبليغ لا يقتصر فقط على القطاعات الخاصة بل أيضاً يمتد الى الافراد خاصة التي تتعلق بالابتزاز الالكتروني المصنف بالابتزاز الجنسي الالكتروني وحفاظاً على النسيج الاجتماعي والنواة الأسرية المكونة للمجتمع الفلسطيني فضلاً عن الحفاظ على سمعتهم وعدم التشهير بها كما ويوجد

<sup>1</sup>حمدي سائد، مقابلة في مكتب النائب العام مختص بالتحقيق بالجريمة الالكترونية بمحافظة القدس مباحث ضواحي القدس بتاريخ 2018\10\9.

<sup>2</sup>فرغلي عبد الناصر محمد محمود، الاثبات بالادلة الرقمية من الناحيتين الفنية والقانونية -دراسة تطبيقية -مقارنة،المؤتمر العربي الاول لعلوم الادلة الجنائية والطب الشرعي-جامعة نايف للعلوم الامنية الرياض،2007، ص10.

سبب آخر مرتبط بالخاصية الأولى والثانية بأنها جريمة لا يستخدم فيها العنف وأنه يتم ارتكابها بسهولة وإخفاء أثارها بسهولة وهذا يؤدي بالنتيجة الى عدم ادراك ومعرفة المجني عليه أنه يوجد اعتداء على نظامه الالكتروني سواء بالتزوير أو الاحتيال أو الغش أو الإختراق الالكتروني إلا بعد فترة طويلة وقد لا يعرف المجني عليه أنه تم الاعتداء في حالتين فإن الأمر يتعلق بأمن وحماية المعلومات والبيانات لنظام الشركة الالكتروني فإنه ضعيف مما يزيد خوف الأفراد من التعامل مع القطاعات الخاصة تحديداً<sup>1</sup>.

5 - سرعة اخفاء الدليل الالكتروني، فهي من الجرائم التي لا تترك أثر لمتابعتها وملاحقتها بل زد في ذلك هناك برامج وتطبيقات قد يستخدمها الفاعل تعرقل الوصول او المعرفة التقنية للجريمة المرتكبة اياً كان نوعها، فهناك برامج وأنظمة تباع بالأسواق تسهل اخفاء الجريمة وتجعل عملية البحث والتحري من الدليل الالكتروني من قبل المختبر الجنائي الالكتروني والخبراء المختصين صعباً للغاية<sup>2</sup>، للتركيبية المعقدة للجريمة الأولى استخدام التقنيات لارتكاب الجريمة والثانية استخدام تطبيقات لاخفاء العمليات التقنية التي تم استخدامها لارتكاب الجريمة ،وهذا في حال ان الفاعل من الدرجة العالية من الخبرة والمعرفة وحتى لو كان الفاعل من الدرجة العادية من المعرفة، فإن الجريمة الإلكترونية سهلة الارتكاب وسهلة الاخفاء وقد لا يشعر الضحية بأنّ هناك اعتداء الكتروني واقع عليه فإن هذه المراحل تؤدي الى وجود بعد زمني ما بين ارتكاب الجريمة واخفاؤها ومعرفة الفاعل وقد يؤثر هذا على عملية الحصول على الدليل الرقمي الذي يربط الفاعل بالجريمة المرتكبة<sup>3</sup>

6 - عدم وجود تعريف موحد للجريمة الإلكترونية على الصعيد الدولي . من خلال بحثنا وجدنا أنه يوجد خلاف على الصعيد الدولي حول تعريف الجريمة الإلكترونية وأنه يوجد عدة تسميات لها منها؛ الاحتيال الالكتروني، الغش الالكتروني، جريمة الحاسب الآلي، الجريمة المعلوماتية، الجريمة الإلكترونية، جرائم الحاسب والانترنت، وتعود هذه التسميات نتيجة لتعدد المعايير والأسس التي استند إليها الفقهاء والخبراء القانونيين، مما جعل قرصنة تكنولوجيا المعلومات يستغلون هذا الاختلاف

<sup>1</sup>ابراهيم راشد بشير، التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية -امارة ابو ظبي دراسات استراتيجية، تصدر عن مركز الامارات للدراسات والبحوث الاستراتيجية العدد 131 ،الامارة العربية المتحدة، 2008، ص48-49.

<sup>2</sup>ورشة عمل منظمة من قبل مشروع قطاع العدالة بحضور الخبير الامريكي جيرارد باونيل سيزر بتاريخ 24-25 \4\ 2017.

<sup>3</sup>مقابلة مع مأمور الضبط القضائي سونيا حماد -مختبر الادلة الرقمية وحدة الجرائم الالكترونية الادارة العامة للمباحث العامة الشرطة الفلسطينية رام الله بتاريخ 10\10\2018 الساعة العاشرة وواحد وثلاثين دقيقة .)

واعتباره ارضية خصبة للاستمرار بارتكاب جرائمهم الإلكترونية واعتداءاتهم الغير مشروعة وايضاً الى ابتكار أساليب وتقنيات جديدة لذلك.<sup>1</sup>

7 - جريمة تسبق الخبرة التقنية لدى الجهات القضائية والخبراء الأمنيين لدى الأجهزة الأمنية، حيث أن الجريمة تسبق الخبرة لدى الجهات المختصة بملاحقتها ومتابعتها، كما أنها تسبق التشريع خاصة أنها متطورة ومتقدمة من الناحية التقنية ، فالخبرة المتوفرة لدى الفاعل باستغلال هذه التقنيات وتطويرها لارتكاب الفعل غير المشروع تفوق الخبرات القضائية لذلك يوجد فروقات معرفية وتقنية ما بين مرتكب الجريمة الفاعل وما بين الخبراء الجنائيين والسلطة القضائية بفرعها القضاء والنيابة ، فلا بد من متابعة تدريب هذه الجهات بشكل مستمر لكل تطور جديد ليتمكنوا من الإلمام والقدرة على الربط ما بين الدليل التقني والنص القانوني، فالجريمة الإلكترونية سبقت التشريعات فمنها مازال غير مصنف لكي يتم ملاحقة مرتكبيها. فنصبح أمام ملكين: ملك ابيض وملك اسود شيطاني مستفحل بالجريمة وملك ابيض يحاول أن يكافح ويصد الجريمة من خلال متابعة التقنيات التكنولوجية المتطورة بشكل مستمر وعلى جميع الأصعدة من خلال التنسيق والتعاون الدولي والإقليمي خاصة الجهات المختصة والمخولة بمتابعة الجريمة الإلكترونية وملاحقتها<sup>2</sup>

8 - تلزم لارتكابها الحاسب الآلي وشبكة الإنترنت، كما أسلفنا في بداية الفصل وفي معرض التعريف بالجريمة الإلكترونية التعرف على مكونات هذه الجريمة والأدوات التي تستخدم لإرتكابها والمكونة من الحاسب الآلي والأجهزة التقنية المرتبطة به والشبكة العالمية الانترنت، وما يميزها عن الجريمة التقليدية أن أدوات الجريمة الإلكترونية لا تتغير فهي ليس كمن يقدم على القتل مستخدماً أداة حادة أو سلاح ناري أو غيرها من الأدوات التي تؤدي الى الوفاة. كما وان الادوات التي تستخدم لارتكاب الجريمة هي نفسها الادوات المستخدمة لاكتشافها.<sup>3</sup>

9- صعوبة اكتشافها، فالصدفة في اكتشاف الجريمة الإلكترونية للتقنيات العالية في ارتكابها لها الدور الأكبر وقليلة هي الأفعال الإلكترونية غير المشروعة التي تتم اكتشافها. فأغلبها تبقى بغطاء

<sup>1</sup> لم تعريف الاتفاقية العربية واتفاقية بودابست لمكافحة الجريمة الإلكترونية وايضا قرار بقانون رقم 10 لسنة 2018 الجريمة الإلكترونية في نصوص القرار او الاتفاقات الدولية وبقيت تعريفها محلا لاجتهاد الفقه القانوني .

<sup>2</sup> هروال ونبيلة، الجوانب الاجرائية للجرائم الانترنت في مرحلة الاستدلالات، ماجستير في القانون دراسة مقارنة دار الفكر الجامعي 2007 ص 35 و 40.

<sup>3</sup> زهام جبر، نائب مدير وحده الجرائم الإلكترونية في جهاز الشرطة، مقابلة شخصية في مكتب النائب العام، بتاريخ 2019/2/13.

التضليل وتبقى في الزاوية المعتمة التي لا يمكن لأحد أن يكتشفها، كما ويلعب دور القطاعات الخاصة (من شركات ومصانع وجمعيات ومؤسسات وبنوك وجامعات) ذات السمعة التجارية المرموقة بالتستر على هذه الجريمة، حيث أنهم يفضلون حل المشكلة أو الاعتداء أو التصدي له من خلال موظفي تكنولوجيا المعلومات لدى هذه القطاعات (خاصة المالية منها) وصد الهجمات عليهم، وهذا التستر يساهم في الحد من تطوير قدرات الخبراء الفنيين من مأموري الضبط القضائي في قسم الأدلة الإلكترونية.<sup>1</sup>

فقد بلغ مجموع الجرائم المختلفة التي وردت لجهاز الشرطة المدنية في عام 2017 ما يقارب 2028 جريمة منها وقد تم متابعة وملاحقة 908 جرائم منها<sup>2</sup>.

ووفقاً للإحصائية المذكورة يتضح أن نسبة الإنجاز في الجرائم التقليدية تفوق بكثير نسبة الإنجاز في الجرائم الإلكترونية، إلا أن نسبة الخسائر المادية والمعنوية التي تحدثها الجرائم الإلكترونية تفوق الملايين من نسبة الخسائر المادية والمعنوية للجرائم التقليدية وهذه المفارقة تؤكد وتعزز بعدم الإبلاغ عن الجرائم الإلكترونية لأسباب تم ذكرها سابقاً، كما أصدرت هيئة الأمم المتحدة دراسة تبين فيها أن حوالي 40% من مؤسسات القطاع العام والخاص، تكبدوا خسائر لوقوعهم ضحية الجرائم الإلكترونية<sup>3</sup>.

نلاحظ أن الخصائص التي تتسم فيها الجرائم الإلكترونية، لا يمكن بأي حال من الأحوال أن تشترك بأي من خصائص الجريمة التقليدية الظاهرة للعيان آجلاً أم عاجلاً، لوجود فعل مادي ملموس وظاهر للعالم الخارجي، وأن كان من غير مرائف الأفعال المادية دائماً تترك أثر ورائها بينما في الجرائم الإلكترونية فهي من عالم افتراضي ما بين الواقع والخيال يتم في أصغر زاوية في منزل أو بأي مكان مغلق أو حتى بالشارع دون أن يلاحظ أي شخص أو يشك بان هناك من يرتكب جريمة عبر حاسبة الآلي قد تتفق الجريمة الإلكترونية بأحكامها العامة للجريمة وبضرورة وجود الركن المادي المتمثل بالسلوك الإجرامي والنتيجة الجرمية والعلاقة السببية وبالركن المعنوي سواء بقصد العام أو القصد الخاص الذي يشرعه المشرع إلا أن هذه الأركان بحاجة إلى أسلوب تقني متطور ومتقدم للإثباتها والتحقق منها .

<sup>1</sup> عبد العال الديري، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة، مصر المركز القومي للإصدارات القانونية، 2012، ص165.

<sup>2</sup> الهندي (سامر)، تقرير الشرطة مديروحدة الجرائم الإلكترونية في الشرطة.

## الفرع الثاني: الادوات المستخدمة في ارتكابها

بعد تعريف الجريمة الكترونية وبيان أهم الخصائص التي تتسم بها، لا يمكن التوصل الى غاية مفهوم الجريمة دون التعرف على الادوات والمكونات التي تستخدم لتنفيذ الجريمة سيما ان هذه الجريمة تمتاز عن الجريمة التقليدية من حيث الأدوات المستخدمة لتكوين الركن المادي للجريمة الإلكترونية، فالحاسب الآلي والشبكة العلمية (العنكبوتية) هما الأداة الأساسية في ارتكاب الجريمة الإلكترونية، وهما هدية القرن العشرين قرن المعلومات والتي ايضا تضيف على الجريمة الكترونية الطابع الخاص لها لان ذات الادوات المستخدمة لارتكاب الجريمة الكترونية هي ذاتها الاداة والادوات الوحيدة في تتبعها وملاحقتها ومعرفة مرتكبيها والكشف عنها<sup>1</sup>، سنعمل على بيان الأدوات المستخدمة في ارتكاب هذه الجريمة كالآتي:

### أولا: الاجهزة الإلكترونية

#### 1- الحاسب الآلي :

جهاز الكتروني قادر على القيام بعدد كبير من المهام الحسابية بشكل سريع ودقيق كما يمكن للحاسب الآلي معالجة البيانات وتخزينها واسترجاعها ونقلها منه واليه عند الطلب بذلك. كما عرفها البعض بأن الحاسب الآلي بأنه جهاز الكتروني مقسم إلى جزئين الأول الجزء المادي الملموس المرئي كلوحة المفاتيح والشاشة التي تساعد بإدخال البيانات وحفظها وتخزينها وتنظيمها ومن ثم إخراج المعلومات من الجزء الثاني المعنوي غير الملموس وغير المرئي والذي يثمنل بإشارات كهربائية ومغناطيسية<sup>2</sup>، والحاسب الآلي مبرمج لحل الملايين من العمليات الحسابية والمنطقية بسرعة هائلة وبثواني معدودة، بحيث يقوم بالعمل على البيانات المدخلة لتصبح بيانات ذات قيمة يمكن الاستفادة منها كما يقوم الحاسب الآلي بعملية حفظ البيانات لاسترجاعها عند اللزوم أو الحاجة إليها وللحاسب الآلي القدرة بتشغيل العديد من أنظمة التشغيل والبرامج والتوغل فيها والقدرة للتصفح على الانترنت<sup>3</sup> وقد عرفت التشريعات الأمريكية الحاسب الآلي " بأنه الجهاز الذي يقبل ويعالج ويخزن ويسترجع او ينتج بيانات"<sup>4</sup>، أما الموسوعة الشاملة للمصطلحات عرفت الحاسب الآلي: "بأنه آلة الكترونية تستخدم

<sup>1</sup>نهلا عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة للنشر، الطبعة الثانية، 2010، ص13.

<sup>2</sup>أسامة احمد المناعسة وجمال الزعبي، جرائم تقنية نظم المعلومات الالكترونية، (دراسة مقارنة)، دار الثقافة للنشر، الطبعة الثالثة، 2017، ص29.

<sup>3</sup>حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت(دراسة مقارنة)، دار النهضة العربية، 2009، ص4-5.

<sup>4</sup>احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري(دراسة مقارنة)، مرجع سابق، ص9.

وفق نظام معين لمعالجة وإدارة البيانات والمعلومات الرقمية المدخلة فيه وفق أوامر وتعليمات يختارها المشغل أو طالب الخدمة<sup>1</sup> هذا على الصعيد الدولي، في حين على الصعيد الوطني لم يعرف المشرع الفلسطيني الحاسب الآلي بشكل صريح بل اعتبره من ضمن التعريف الوارد في المادة الأولى من القرار بقانون الخاص بالجرائم الإلكترونية تحت إطار تكنولوجيا المعلومات

وتعرف تكنولوجيا المعلومات "هي أية وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية أو أية وسيلة أخرى سواء أكانت مادية أو غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وإداء المنطق والحساب أو الوظائف التخزينية، ويشمل أية قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة"<sup>2</sup>.

وبهذا يكون المشرع الفلسطيني قد حاول جمع الأدوات التي تعمل بطريقة ذاتية تلقائية دون الاعتماد إلى جهد البشري سواء كانت هذه القدرات كهربائية مثل الحاسب الآلي، أو قدرات رقمية مثل الحاسب الشخصي المحمول، أو قدرات مغناطيسية، أو لاسلكية مثل الهاتف العادي، أو الهاتف المحمول أو بصرية كالكاميرات الرقمية أو أية أجهزة وأدوات لها قدرة على التخزين بيانات أو اتصالات مشابهة بوسيلة تكنولوجيا المعلومات

ومن خلال ما ذكر نستخلص أنّ المشرع الفلسطيني راع اتساع التعريف بحيث يشمل أي شبكات إلكترونية أو أدوات تقنية قد تظهر في المستقبل، ولم يقتصرها على الحاسب الآلي كأداة قد يظهر بديلاً لها أو تقوم بنفس الآلية بالتعامل بالبيانات والمعلومات، وبهذا يكون المشرع قد حذا حذو المشرع العربي ضمن القانون الموحد وبتعريف المشرع لإمارة دبي في قانون المعاملات والتجارة الإلكترونية<sup>3</sup> ويتميز الحاسب الآلي بعدة مميزات أهمها السرعة والدقة المتناهية، والقدرة على التشغيل والعمل لساعات طويلة دون أي تعطيل وسهل التعامل كمايمتاز بقابلية التوسع والتطور متعدد الاستعمالات وله طاقة تخزينية غير محدودة، ولكن كنتيجة للتطور والتقدم المستمر<sup>4</sup> لا يعد الحاسب الآلي الوسيلة الوحيدة التي يمكن استخدامها للوصول إلى أي من البيانات والحصول على المعلومات بل ظهرت

<sup>1</sup>أسامة احمد المناعسة وجمال الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، (دراسة مقارنة)، مرجع سابق، ص28.

<sup>2</sup>المادة (1) من قرار بقانون الخاص بالجرائم الإلكترونية رقم 10 لسنة 2018، المنشور بالوقائع الفلسطينية، العدد الممتاز 16، بتاريخ 2018/5/3

<sup>3</sup>المادة (2) من قانون المعاملات والتجارة الإلكترونية رقم(2) لسنة 2002 لإمارة دبي والتي عرفت الحاسب الآلي: "جهاز إلكتروني يتعامل مع المعلومات والبيانات بتحليلها وبرمجتها وإظهارها وحفظها وإرسالها واستلامها بواسطة برامج وأنظمة معلومات إلكترونية ، ويمكن أن يعمل بشكل مستقل أو بالاتصال مع أجهزة أو أنظمة إلكترونية أخرى".

<sup>4</sup>حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت(دراسة مقارنة)، مرجع سابق، ص13.

أجهزة تقنية ذكية تتيح لمستخدميها الاتصال ومشاركة المعلومات والبيانات بحيث لديها القدرة عرض البيانات وإرسالها واستقبالها مثل أجهزة الهواتف النقالة والمتنوعة كنيحة للتنافس التجاري بين الشركات المصنعة العالمية ولكلاً منها تقنياتها وبرامجها وجمعيتها متصلة بعنوان الكتروني المسمى (IP)<sup>1</sup>، ويرتبط هذا الأخير بالشبكة العنكبوتية.

### الشبكة العنكبوتية (الانترنت):

أو ما تسمى بالشبكة العالمية: وهي عبارة عن مجموعة من الأجهزة التقنية أو الحواسيب والتي تتعامل مع بعضها البعض من خلال اتصالات سلكية ولاسلكية، مكونة من مجموعة من الشبكات المترابطة والمتصلة مع بعضها البعض لتوفير المواقع الإلكترونية والبرامج والتطبيقات التكنولوجية.

وعرفها البعض بأنها أكبر شبكة حاسوبية نظراً للكم الهائل من الحواسيب والخوادم المتصلة بها، لتخلق تواصل معلوماتي فيما بينها، وهي عدة أنواع تصنف حسب الترابط الجغرافي مثل الشبكات الداخلية المحلية المتواجدة في المباني أو موقع محدد أو الشبكة العالمية، لارتباط عدد أجهزة غير محصورة بمساحة جغرافية أو تصنف حسب طريقة الاتصال السلكي واللاسلكي أن يقوم مجموعة من المستخدمين بتجسيد شخصيات افتراضية غير واقعية ضمن بيئة ثنائية أو ثلاثية الأبعاد، يعتمدون على المحاكاة الحاسوبية كوسيلة للتخاطب والتواصل مع الأشخاص الافتراضيين الآخرين الموجودين في هذا العالم، ويسمى بالافتراضي نظراً لكون جميع ما به من أشخاص وبيئة ووسائل تواصل افتراضية وليست واقعية، وينتشر استخدام العالم الافتراضي عادة في ألعاب تقمص أدوار اللاعبين عبر الانترنت (الشبكة العنكبوتية)<sup>2</sup>، وعرف المشرع الفلسطيني الشبكة الإلكترونية أنها "ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية"<sup>3</sup>

وقد تربعت شبكة الانترنت على عرش وسائل الاتصالات لتميزها بعدة مميزات وخصائص أهمها النمو المستمر في مجال الشبكات، وتتطور على يد الأفراد والشركات عبر العالم، كما وأنها الشبكة المتاحة

<sup>1</sup> عنوان بروتوكول الإنترنت بالإنجليزية (IP address): هو المعرف الرقمي لأي جهاز حاسوب، هاتف محمول، آلة طباعة، موجه (مرتبط بشبكة معلوماتية تعمل بحزمة بروتوكولات الإنترنت، سواء أكانت شبكة محلية أو شبكة الشبكات الإنترنت. يقابل عنوان الآي بي مثلا في شبكات الهاتف رقم الهاتف، من الموقع الالكتروني <https://ar.wikipedia.org/wiki>، بتاريخ 2018/10/18، الساعة 5:50 مساء

<sup>2</sup> عبد الله السوداني، مبرمج تكنولوجيا معلومات، مقابلة خاصة، تاريخ 2018/10/21، الساعة 1:00 ظهرا، رام الله.

<sup>3</sup> المادة (1) من قرار بقانونالخاصبالجرائم الكترونية رقم 10 لسنة 2018.

لجميع فأصبح مليارات المستخدمون ينتفعون بهذه الشبكة على مستوى العالم، وتتميز بأنها عابرة للدول، وتسمح لجميع المستخدمين باستخدامها بدون أي تعقيدات أو صعوبات بأقل التكاليف مقارنة بوسائل الاتصال الأخرى كالفاكس والهاتف، كما أنه لا سلطة على هذه الشبكة العالمية سواء من الجهات الحكومية أو غير الحكومية فهي ليست مملوكة لاحد<sup>1</sup>.

ولشبكة الانترنت آثار إيجابية وسلبية، الايجابية منها تسهيل التجارة الالكترونية عبر خدمة البريد الالكتروني، وتحويل أموال أو نقل ملفات والتعلم عبر الإنترنت، وتصفح أخبار العالم اليومية وإجراء الفحوصات الطبية، والتعرف على العمليات الجراحية، والاتصال المباشر بالصوت والصورة، وما أضفته للحكومات من تغيير نمطي بالخدمة التقليدية للمواطنين، وسرعة في انجاز المعاملات بسرعة ودقة<sup>2</sup>، أمّا السلبية منها فتركز بانتشار التجارة الاباحية والارهاب، وترويج المخدرات، وغسل الأموال مُشكلة بيئة خصبة للجرائم المنظم، والعصابات المنظمة، وظهور القرصنة، ونشر الفيروسات والابتزاز بأشكاله المختلفة كالمالي والجنسي والسياسي<sup>3</sup>، وبعد بيان الجريمة الإلكترونية وأهم خصائصها والأدوات المستخدمة في ارتكابها، لا بد من بيان من الشخص القائم على هذه الجريمة وما أهم سماته ومدى خطورته، وهل يتوفر لديه صفات تختلف عن المجرم في الجرائم التقليدية (المطلب الثاني)

---

<sup>1</sup> حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة)، مرجع سابق، ص 26-29.

<sup>2</sup> نهلة عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة للنشر، مرجع سابق، ص 38-41.

<sup>3</sup> حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة)، مرجع سابق، ص 29 و 36.

## المطلب الثاني: مفهوم المجرم الإلكتروني

والمتهم في الجرائم الإلكترونية يطلق عليه اسم المجرم الإلكتروني ويتميز هذا المجرم بخصائص تميزه عن غيره من المجرمين سيما أن الجرائم الإلكترونية تتميز بطبيعة خاصة، وبالتالي ترتكب من أشخاص ذو طبيعة خاصة<sup>1</sup>. التساؤل الذي يثور من هو المجرم الإلكتروني، وبماذا يتميز عن غيره من المجرمين، وما هي الطبيعة التي يظهر بها المجرم الإلكتروني؟

## الفرع الأول: تعريف المجرم الإلكتروني:

### أولاً: تعريف المجرم

1- **التعريف اللغوي:** المجرم لغة حسب تعريف المعجم الجامع هو "الَّذِي ارْتَكَبَ جُرْمًا يَسْتَحِقُّ عَلَيْهِ الْعِقَابَ "

2- **تعريف المجرم اصطلاحاً:** "يعرفه الفقه التقليدي بأنه ذلك الشخص الذي يرتكب جريمة مما نص عليها في قانون العقوبات"<sup>2</sup>، وهذا يعني أن الشخص يجب أن يثبت ارتكابه للجريمة من خلال محاكمته قانوناً، ويتميز هذا التعريف بأنه سهل من خلاله التعرف على المجرم.

المتهم: هو كل انسان طبيعي حياً بالغاً عاقلاً مسؤولاً عن اختياراته مدركاً لتصرفاته يسند إليه الفعل المجرم، ويصدر بحقه اتهام ويخضع للإجراءات المحاكمة المنصوص عليها بالقانون، وصدور حكم المحكمة المختصة بعد سماع البيانات وتقدير الأدلة ببرائته أو إدانته حائزاً لقوة الشيء المقضي به<sup>3</sup>.

تعريف المجرم الإلكتروني، قد بينت من خلال دراستي أنه لا يمكن ارتكاب جريمة الكترونية الا بوجود أداة أو أية وسيلة تكنولوجيا المعلومات مرتبطة بالشبكة العالمية يتمكن المجرم من خلالها من ارتكاب الفعل غير المشروع، وهذا ما يميز الجريمة الإلكترونية عن الجريمة التقليدية، بل أيضاً يعد وجود الحاسوب والانترنت سبباً لتمييز المجرم الإلكتروني عن غيره من المجرمين، وهناك سمات وخصائص من شأنها أن تميزه عن المجرم التقليدي المتعارف عليه لدى فقهاء القانون والقضاء، وسنتعرض لأهم الخصائص التي يجب اتخاذها بعين الاعتبار من قبل أعضاء النيابة المحققين عند التحقيق مع المتهم، ومواجهته بالدليل الإلكتروني، وعلى المحكمة أيضاً اخذها بعين الاعتبار لإصدار الحكم

<sup>1</sup> عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، 2008، ص15.

<sup>2</sup> انظر الى <https://www.almaany.com/ar/dict/ar-ar/%D9%85%D8%AC%D8%B1%D9%85> ، تاريخ الدخول 2019\6\16.

<sup>3</sup> سادار علي عزيز ، ضمانات المتهم اثناء الاستجواب، مصر ، المركز القومي للاصدارات القانونية ، 2014، ط1، ص9.

المناسب لشخصية المجرم الإلكتروني، كما أن للباعث على ارتكاب الجرم من قبل المجرم الإلكتروني أهمية كبيرة تؤكد حقيقة القصد الجرمي المرتكب بالجرائم الإلكترونية. فالباعث بالجريمة لا يعتد به أصولاً ولا يعتبر ركناً من أركان الجريمة، إلا أن الأمر يختلف بالنظر إلى الجريمة الإلكترونية المرتكبة، فعالم الإجرام الجنائي شمل مجموعة جديدة وجيلاً من المجرمين لهم أهداف محددة، وتم تسميته المجرم الإلكتروني استناداً لاهدافه الإجرامية والتي سأوجز أغلبها في هذا الفرع.

### الفرع الثاني: خصائص المجرم الإلكتروني

تنقسم خصائص المجرم الإلكتروني إلى قسمين خصائص عامة وخصائص خاصة

أولاً: الخصائص العامة وهي:

1- المجرم الإلكتروني مجرم متخصص قد تبين في عديد من القضايا أن عدداً من المجرمين لا يرتكبون سوى جرائم الكمبيوتر، أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يبين أن المجرم الذي يرتكب الجريمة الإلكترونية هو مجرم في الغالب متخصص في هذا النوع من الإجرام<sup>1</sup>.

2- المجرم الإلكتروني مجرم عائد إلى الإجرام:

يعود كثير من المجرمين إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقاً من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة، فيدخلون في حالة تحدي الذات والشعور بالانتصار ويؤدى ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم إلى المحاكمة<sup>2</sup>.

3- المجرم الإلكتروني مجرم محترف:

يتمتع المجرم الإلكتروني باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر الذي يقتضى الكثير من المهارة والدقة والتخصص والاحترافية والذكاء الخارق للتغلب

<sup>1</sup> سامر الهندي، مدير وحدة الجرائم الإلكترونية بجهاز الشرطة، مقابلة شخصية، قيادة الشرطة، فلسطين، بتاريخ 15/6/2019.

<sup>2</sup> غادة نصار، الارهاب والجريمة الإلكترونية، مصر، العربي للنشر والتوزيع، ط1، 2017، ص 44.

على العقوبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية والمنشآت الكبيرة<sup>1</sup>.

#### 4- المجرم الإلكتروني مجرم غير عنيف:

المجرم الإلكتروني من المجرمين الذين لا يلجئون إلى العنف بتاتاً في تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام الحيلة فهو لا يلجأ إلى العنف في ارتكاب جرائمه، وهذا النوع من الجرائم لا يستلزم أي قدر من العنف للقيام به. وإلى جانب ما تقدم فالمجرم الإلكتروني إنساناً اجتماعياً متصالح لا يوجد له خلافات مع أيّاً من الأشخاص سواء بمحيطه المهني أو العائلي أو الاجتماعي يتمتع بثقة من حوله، وأحياناً كثيرة على درجة عالية من الثقافة، وهذه الخاصية تشجع المجرم الإلكتروني، وتدفعه لارتكاب الجريمة والتمادي فيها، لآته خارج دائرة الشبهات من المحيطين فيه، كما أنه لا يملك القدرة على مواجهة المجني عليه، وهذا ما اثبتته الدراسات، وما توصل إليه الاستاذ باركر من خلال بحثه وتحليله لشخصية المجرم الإلكتروني<sup>2</sup>.

#### 5- يهemin الخوف على المجرم الإلكتروني

فهو يخشى الفضيحة أو كشف أمره وخاصة إذا تعرض لعوامل لم يضعها بالحسبان أو غير متوقعة تؤدي بالنتيجة إلى كشف جريمته، وينبع الخوف لدى المجرم الإلكتروني لانتسابه إلى وسط اجتماعي مرموق سواء من حيث المستوى التعليمي أو الفكري أو الثقافي أو المهني، وقد يتسبب كشف أمره إلى خسارة مادية أو خلخلت مركزه المهني والوظيفي وفقدان ثقة المحيطين به<sup>3</sup>.

#### ثانياً: خصائص المجرم الإلكتروني الخاصة

يتميز المجرم الإلكتروني كذلك بمجموعة من الخصائص التي تميزه بصفة خاصة عن غيره من المجرمين وهي موضحة كالآتي:

<sup>1</sup> غادة نصار، الارهاب والجريمة الإلكترونية، ص 44 .

<sup>2</sup> نهلا عبد القادر المومني، الجرائم المعلوماتية، ماجستير في القانون الجنائي، دار الثقافة للنشر والتوزيع، عام 2010، ص .

<sup>3</sup> علاء رضوان، اسباب انتشار الجريمة المعلوماتية،

، <http://www.soutalomma.com/Article/842092/%D8%A3%D8%B3%D8%A8%D8%A7%D8%A8-> تاريخ النشر 2018\11\11، تاريخ الزيارة 2019\8\13.

## 1- المجرم الالكتروني على قدر كبير من المعرفة التقنية:

يتمتع المجرم الالكتروني بقدر عالي من المعرفة التقنية والمعالجة الالية للمعلومات للحاسوب ووسائل تكنولوجيا المعلومات والانترنت حيث يستطيع المجرم الالكتروني أن يكون تصويراً كاملاً لجريمته، ويرجع ذلك إلى أنّ المسرح الذي تمارس فيه الجريمة الالكتروني هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة قبل تنفيذ الجريمة تحسباً لأي أمر تقني غير متوقع قد يفشل الهدف المراد تحقيقه<sup>1</sup>.

## 2- المجرم الالكتروني لديه الباعث:

الباعث وهو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة وبظل هو الباعث الأول وراء ارتكاب الجريمة الإلكترونية، ويرى البعض أيضاً ما يخالف ذلك في أن الربح المادي لا يعدّ هو الباعث في أغلب الأحيان على ارتكاب الجرائم الإلكترونية، وإنما هناك أمور عديدة أخرى ، فقد يكون الباعث هو الانتقام من رب العمل، وأيضاً مجرد الرغبة في قهر نظام الحاسب، واختراق حاجزه الأمني، فالمجرم الإلكتروني قد يكون شخص مزدري من القانون أو لديه شعور بأنه فوق القانون واسباب اخرى<sup>2</sup>.

## 3- المجرم الالكتروني لديه حب المخاطرة والتلاعب

فهو دائماً يبهر أفعاله بأنّها مشروعة وان ما يقوم به لا يستوجب العقاب وخاصة اذا كان الهدف هو اثبات المهارة الذاتية بتخطيه جدار الحماية لنظام أو تطبيق الكتروني، وليس سعياً للكسب المادي أو الاضرار بالآخرين، فيسخر تفكيره وقدراته الذهنية لتجاوز الهدف مستبعداً أي تفكير عقلي بأنّ ما يقوم به مخالف للقانون، وهذا لا ينطبق على جميع المجرمين فمنهم يدركون تماماً كُنه أفعالهم لا بل يعتمدون ذلك عن علم وإرادة لتحقيق نواياهم الاجرامية.

<sup>1</sup> رهام جبر، نائب مدير وحدة الجرائم الإلكترونية، جهاز الشرطة، مقابلة شخصية، افاد اثناء المقابلة ان المجرم الإلكتروني هو مجرم ذو خبرة ومعرفة في وسائل تكنولوجيا المعلومات وشبكة الانترنت حيث اخبرنا ان هذه الجريمة لا تتم الا اذا كان المجرم لديه المهارات الخاصة التي تمكنه من اخفاء نفسه عبر الانترنت ووضع العراقيل امام سلطات الاستدلال لتوصل اليه على سبيل المثال استخدام ip متخفي.

<sup>2</sup> الباعث: هو الاحساس أو المصلحة التي دفعت الجاني الى ارادة الوضع الاجرامي.

- انظر الى: سمير داود سليمان، بحوث جنائية، القاهرة، المركز القومي للاصدارات القانونية، ط1، 2015، ص 65.

#### 4- المجرم الإلكتروني شخص مدمن الكترونياً

فهو يمضي معظم وقته وتفكيره في البحث التقني، والاستشكاف في بحر التطور المتسارع للأجهزة التقنية والحواسيب وعالم الشبكات.

#### 5- يتمتع المجرم الإلكتروني بقدر من المهارة:

يتطلب تنفيذ الجريمة الإلكترونية قدراً من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في المجال التكنولوجي، أو بمجرد التفاعل الاجتماعي مع الآخرين، وهذه ليست قاعدة ثابتة في أنه لابد أن يكون المجرم الإلكتروني على قدر كبير من العلم، وهذا ما أثبتته الواقع العملي أن هناك مجرمين لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الإجرام<sup>1</sup>.

#### 5- يمتلك المجرم الإلكتروني الوسيلة:

ويراد بها الإمكانيات التي يحتاجها المجرم الإلكتروني لإتمام جريمته، هذه الوسائل قد تكون في أغلب الأحيان، وسائل بسيطة وسهلة الحصول عليها خصوصاً إذا كان النظام الذي يعمل به الكمبيوتر من الأنظمة الشائعة، أما إذا كان النظام من الأنظمة غير المألوفة، فتكون هذه الوسائل معقدة وعلى قدر من الصعوبة، فلا يستطيع أي شخص ارتكاب جريمة الكترونية بدون استخدام الوسيلة، وهي إحدى وسائل تكنولوجيا المعلومات وشبكة الإنترنت<sup>2</sup>.

#### 6- يمتلك المجرم الإلكتروني السلطة:

يقصد بالسلطة الحقوق والمزايا التي يتمتع بها المجرم الإلكتروني والتي تمكنه من ارتكاب جريمته، فكثير من مجرمين لديهم سلطة مباشرة أو غير مباشرة في اختراق المعلومات. وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوى على المعلومات وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي وإجراء المعاملات، كما أنّ السلطة قد تكون شرعية وقد تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر

<sup>1</sup> محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، مصر، دار الجمهورية للصحافة، ط1، 2010، ص51.

<sup>2</sup> محمد مسعود، مختبر الأدلة الإلكترونية، جهاز الشرطة، وحده الجرائم الإلكترونية، مقابلة شخصية بتاريخ 2019\7\1.

كما أنّ المجرم الإلكتروني يظهر بعدة صور وانماط، والتطور السريع في وسائل تكنولوجيا المعلومات بشتى أشكالها، يخلق جيل يستطيع أن يتماشى مع هذا التسارع التقني بـماهرة عالية كما خلف هذا التطور فجوة كبيرة بين جيل لا يمكن بمكان أن يدرك خطورة هذا الاجتياح الرقمي والتقني، والذي تم استغلاله من قبل المجرمين المتخصصين في المجال الإلكتروني مما أدى إلى ظهور أنماط وصور مختلفة للمجرم الإلكتروني مرتبطة بالأهداف المرجوة من ارتكاب الجريمة الإلكترونية، وسأتناول أبرز الأنماط الشائعة عالمياً في هذا المجال<sup>1</sup>.

ويمكن تصنيف المجرم الإلكتروني إلى ما يلي:<sup>2</sup>

1- المتطفلون أو المخترقون والمتعارف عليهم عالمياً وتقنياً بالهاكرز (hacker's)، وأول من أطلق هذه التسمية مجموعة من الطلاب بالجامعات الأمريكية في أول الستينيات من القرن العشرين، وتتميز هذه الفئة بالذكاء والمهارة التقنية التي تلبي غرورهم واثبات الذات، وأن لديهم قدرة اختراق الحواسيب والوسائل التقنية والشبكات من تلقاء أنفسهم، دون مساعدة أي شخص يفوقهم مهارة ومعرفة، وبعثهم لارتكاب الجريمة هو التطفل والفضول وقهر النظام الإلكتروني، وكشف الثغرات التقنية والأمنية، لاية نظام الكترولني والتعلم، وليس لديهم أية نوايا سئية أو تخريبية قد تضر أطراف اخرى.

2- الملاك الابيض أو ما يسمون أيضاً بالمخترقون ذوي أخلاق حسنة وهم يسعون لتدمير المواقع الإلكترونية التي تعرض المواد الاباحية والالاخلاقية ضد الأطفال، باعثهم هو الحفاظ على المصلحة العامة خاصة الأطفال، وقد انشأت هذه الفئة من المخترقون منظمة تجمعهم بهدف تبادل المعلومات التقنية في مجال الاختراق وأساليبه، وكان لهم الدور بالكشف عن بعض الثغرات التقنية سواء في المجال المالي أو الامني

3- المحترفون والمتعارف عليهم عالمياً وتقنياً بالكراركرز (crackers) يتمتعون بالذكاء الخارق والمعرفة التقنية العالية والدهاء المطقع، والخبرة الواسعة في الحاسوب ووسائل تكنولوجيا المعلومات والشبكات، باعثهم للارتكاب الجريمة هو تدمير والتخريب بهدف الحاق الاضرار بالآخرين، والحصول على أرباح مالية وشخصية، مثل نشر الفيروسات، واطلق على الأنماط التي ذكرت مصطلح القرصنة.

<sup>1</sup>شروق سامي فوزي، تكنولوجيا الإعلام الحديث، مؤسسة طيبة للنشر والتوزيع ، 2015، ص 47 .

<sup>2</sup>منير طيبي، الجريمة الإلكترونية المنظور النفسي والاجتماعي والامني، نشرت بتاريخ 2-4-2017

، تاريخ زياره الموقع <https://m.annabaa.org/arabic/informatics/10453> ، تاريخ زياره الموقع 16\6\2019 .

4-موظفي تكنولوجيا المعلومات في المؤسسات المحلية والحكومية، وهم من يقوموا باستغلال الوظيفة من أجل ارتكاب الجريمة باعثهم هو تحقيق أهداف شخصية أو أرباح مالية أو الانتقام من اصحاب العمل، وبطبيعة الحال من يشغل وظيفة تقنية كمبرمج أو متخصص في أية نظام الكتروني يتمتعون بدرجة كبيرة من المعرفة التقنية والمهارة الفنية في هذا المجال.

5-الجماعات الارهابية وهم مجموعة من الاشخاص يعتقدون أفكار ومعتقدات متطرفة سواء على الصعيد الاجتماعي أو السياسي أو الديني، باعثهم هو فرض معتقداتهم ونشر افكارهم من خلال الاعتداء اللفظي أو المادي على الأشخاص والمؤسسات والبنوك والشركات، لجلب الانتباه لما يتدعون به ولا يسعون لتحقيق ارباح مادية.

6-المنظمات الاجرامية: هم مجموعة من الافراد لهم تنظيم وقانون خاص بهم باعثهم هو تحقيق ارباح مالية ضخمة من خلال غسل الأموال أو الاتجار بالاعضاء البشرية وترويج المخدرات والتجسس على الصعيد التجاري والصناعي وابتزاز القادة والمسؤولين السياسيين أو ذوي المراكز رفيعة المستوى ما يميز هذه الفئة هو ارتكاب جرائمهم من خلال الشبكة العالمية بمختلف انحاء العالم وانهم يتابعون اي تطور تقني متعلق بالحاسوب أو وسائل تكنولوجيا المعلومات والشبكات لهم سياسات ومخططات مدروسة على مستوى عالي من المعرفة والدهاء لهم عالمهم الخاص عليهم التزامات وحقوق داخل المنظمة يمنع عليهم مخالفة اي من قوانين المنظمة والى فرض عقاباً قاسياً على المتمرّد فهو يعتبر بمثابة الخائن.<sup>1</sup>

7-المتجسسون: وهم فئة من الافراد ذات مستوى تقني عالي يتبعون للدول وحكومات باعثهم تنفيذ الاوامر الصادرة لهم من قبل مسؤوليناهم وهذا ما تتبعه الدول الكبرى مثل الولايات المتحدة وروسيا والصين وفرنسا وامريكا للتجسس العسكري والاقتصادي والعلمي والفضائي بسبب التنافس والتسابق فيما بينهم.

8-الهواة أو النوابغ وهم من فئة الشباب صغار السن الذي ابهرتهم التقنيات يتمتعون بالذكاء باعثهم اللهو والتسلية والمغامرة والتحدي وهم أقل الانماط خطراً تكمن الخطورة إذا تم استقطاب هذه الفئة للجماعات منظمة أو ارهابية أو إغرائهم من قبل المحترفين بالكسب المالي بوقت قصير.<sup>2</sup>

وفي نهاية هذا المبحث تطرقنا إلى الجريمة التقليدية وتعريفها، وعرفنا الجريمة الإلكترونية وأهم أركانها وخصائصها، والأدوات التي ترتكب بها ومن ثم انتقلنا الى البحث في المجرم الإلكتروني .

<sup>1</sup>محمد نور خالد الدباس، واقع الجريمة المنظمة في الاردن، عمان ، دار يافا العلمية للنشر والتوزيع، ط1، 2007، ص 18-19

<sup>2</sup>عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية ، السعودية، مكتبة القانون والاقتصاد، 2012، ص

## المبحث الثاني: المواجهة التشريعية للجريمة الإلكترونية

إن رؤية وتوجه المجتمع الدولي والوطني المحلي بالاهتمام وبمواكبة تطور الجريمة المستحدثة ودراستها وتحليلها وتنظيمها والتعاون الدولي جاء متوافقاً للسياسة الجنائية بمكافحة الجريمة. لذلك نرى إن تعزيز قانون خاص بمكافحة الجريمة الإلكترونية أمر في غاية الأهمية، حيث أنه لا يمكن تطبيق قانون العقوبات الذي يجرم الجريمة التقليدية على هذا النوع من الجرائم، وكذلك من خلال متابعتي الحثيثة لنوعية الجرائم الإلكترونية باوصافها البسيطة والمعقدة، أنه بالمستقبل ستتدثر الجريمة التقليدية و/أو تصبح نادرة في عالمنا الواقعي، إضافة إلى أن ملاحقة هذا النوع من الجرائم يحتاج إلى أدوات ومعدات وبرامج خاصة تختلف عن الأدوات والوسائل المستخدمة في الجرائم التقليدية كونها ذات بيئه تقنيه غير مادية.

### المطلب الأول: الجهود المبذولة للتصدي للجريمة الإلكترونية

بعد ظهور الجريمة الإلكترونية وانتشارها في بلدان العالم ومدى خطورتها من حيث ارتكابها والنتائج المترتبة عليها، وخطورة المجرم الإلكتروني الذي يتميز بصفات تجعله في درجة عالية من الخطورة كان لا بد من وضع العديد من الآليات والعمل على العديد من المؤتمرات الدولية والوطنية للحد من هذه الجريمة ومكافحتها بشتى الطرق فكان لا بد من بذل جهود دولية موحدة كون هذه الجريمة تمتاز بانها عابرة للقارات(الفرع الاول) والعمل المتواصل والمنسجم مع الاتفاقيات الدولية على الصعيد الوطني(الفرع الثاني).

### الفرع الاول: الجهود الدولية للحد من الجرائم الإلكترونية

بدأ الاهتمام الدولي بمكافحة الجريمة الإلكترونية بشكل ضئيل جداً لا يذكر، حيث مر تطور استخدام تقنيات الحديثة على مراحل تدريجية تنحصر في إطار الجهود العلمية لضمان بقاء الاتصال<sup>1</sup>، ولم يكن هناك فكر أو توقع من قبل الدول في العالم من استغلال التطور التقني لوجود شبكة الانترنت واستخدامه في الاعتداء على المصلحة المحمية بموجب القانون .

<sup>1</sup>-أسامة احمد المناعسة وجلال الزعبي، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)، دار الثقافة للنشر، الطبعة الثالثة،

حيث كان العالم يتطلع إلى وجود قنوات اتصال سريعة وسهلة بدأت باختراع البريد الإلكتروني الذي يمكن المستخدمين من إرسال واستلام رسائل مكتوبة من خلال الحاسوب<sup>1</sup>، ثم بدأ استخدام الاداتين الرئيسيتين للمعاملات الإلكترونية وهي الحاسب وشبكة الانترنت.

ولم يكن هناك حاجة الى تنظيم قانوني للمعاملات الإلكترونية انما كانت تنظم من خلال بروتوكولات موحدة لضمان تنظيم العملية التبادلية ما بين المعلومات والبيانات والتي تحتوي على عدد لا محصور من الحواسيب المترابطة إلا أنه مع مرور الوقت وظهور شركات عديدة تعني بالمجال الإلكتروني والشبكات سواء من حيث الإدارة والتنظيم والتطوير البرمجي والتقني، والذي رافقه انتشار الحواسيب في مختلف أنحاء العالم<sup>2</sup>، ويؤدي سوء استخدام الكمبيوتر وبالنظر لأهمية المعلومات المخزنة بداخل الحاسب الآلي، والتي يتم تبادلها عبر الشبكة العالمية سواء كانت هذه المعلومات اقتصادية (مالية ومصرفية) سياسية وأمنية، وما قد يتعرض له حقوق الافراد من الخطر التي أوجبت الدساتير والمعاهدات الدولية حمايتها، وهذا ما دفع الدول إلى العمل على إعداد وصياغة قرارات ومعاهدات تهتم بمكافحة الجريمة الإلكترونية<sup>3</sup>، ومن أولى هذه القرارات القرار الصادر من منظمة التعاون الاقتصادي والتنمية في عام 1986، والذي خرج بتوصية تتعلق بوضع مبادئ توجيهية وتشريعة تتعلق بالكمبيوتر وفي عام 1989 تم اعتماد هذه التوصية من قبل اللجنة الوزارية لمجلس أوروبا ثم صدر قرار من قبل الامم المتحدة في مؤتمرها الثامن الذي انعقد في هافانا عام 1990م، بضرورة وضع إطار دولي لمكافحة جرائم الكمبيوتر، وخاصة مع ظهور الجرائم المنظمة المتعلقة بغسيل الأموال والارهاب مع ظهور الجرائم التي تتسم بالبعد الدولي<sup>4</sup>، وفي عام 1994 تم عقد مؤتمر في البرازيل من قبل الجمعية الدولية لقانون العقوبات خصيصاً لمناقشة جرائم الكمبيوتر، والخروج بتصنيفات اعتمدت ليتم على أساسها تجريم الأفعال التي تتم عبر الحاسب الآلي لتجريمها، كما وتضمنت مجموعة من الإجراءات لإعتمادها من أجل الحصول على الدليل المتصل بالبيئة الرقمية واثباتها<sup>5</sup>، وفي عام 2001 تم اعتماد مشروع نظمه اللجنة الأوروبية ولجنة من الخبراء في مجال تكنولوجيا المعلومات على شكل

<sup>1</sup> أسامة احمد المناعسة وجلال الزعبي، ص 36.

<sup>2</sup> أسامة احمد المناعسة وجلال الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، مرجع سابق ص 37؛ ونهلا عبد القادر المومني، الجرائم المعلوماتية، عمان، دار الثقافة، 2010، ص 34.

<sup>3</sup> أسامة احمد المناعسة وجلال الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، مرجع سابق، ص 107.

<sup>4</sup> د. عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، 2008، ص 108.

<sup>5</sup> د. عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، 2008، ص 115.

اتفاقية سميت باتفاقية بودابست (وهي اتفاقية تتعلق بالجرائم الإلكترونية وهي الاتفاقية الوحيدة على الصعيد الدولي) والتي وقعت عليها 191 دولة من ضمنها فلسطين والتي دخلت حيز النفاذ بتاريخ 2001/6/1<sup>1</sup>، وقد شملت الاتفاقية على 48 مادة. شكلت هذه المواد الإطار القانوني الدولي لتعاون الدول بالأمور التي تتعلق بالجرائم الإلكترونية وهذا نابع من أن الجريمة الإلكترونية لا حدود جغرافيا لها فكان لا بد من وضع تنظيم لهذه الجريمة التي تمر بلا تاشيرة دخول وتفقيش الى أي من دول العالم، حيث تكونت الاتفاقية من مقدمة وأربعة فصول شملت المقدمة الأسباب الداعية لوجود الاتفاقية والهدف من تنظيمها على المستوى المحلي والاقليمي والدولي، ومن خلال الاطلاع على هذه الاتفاقية والتي قسمت الجرائم الإلكترونية الى خمسة فئات<sup>2</sup>:

الفئة الأولى :- تتعلق بالجرائم الواقعة على امن المعلومات اي عدم التعرض والولوج والاختراق الغير مسموح به من خلال كسر الحماية التقنية التي تحافظ على سرية وسلامة المعلومات داخل المعالجة الحاسوبية<sup>3</sup>

الفئة الثانية : تتعلق بالجرائم التي يتم استخدام الكمبيوتر لإرتكابها مثل سرقة بيانات وتزوير مستندات

4

الفئة الثالثة :- الجرائم التي ترتكب على ما يحتويه الحاسب الألي مثل جرائم دعارة الاطفال<sup>5</sup>

الفئة الرابعة :- الجرائم المتعلقة والمرتبطة بالملكية الفكرية والتي تشكل اعتداء على حقوق المؤلف الفكرية والادبية والصناعية<sup>6</sup>

الفئة الخامسة :- النصوص التي تتعلق بالشروع والمساهمة والاشتراك والتحريض والعقاب<sup>7</sup>

وقد فرض البعد الدولي للجريمة الإلكترونية على المجتمع الدولي البحث عن وسائل أكثر ملاءمة لطبيعتها، وتضييق الثغرات القانونية التي برع مرتكبوها في استغلالها للتهرب من العقاب ولنشر نشاطهم في مناطق مختلفة من أنحاء العالم ولأن السياسة الجنائية المثلى لن تحقق الغرض المرجو

<sup>1</sup> أسامة احمد المناعسة وجمال الزعبي، جرائم تقنية نظم المعلومات الالكترونية، (دراسة مقارنة)، دار الثقافة للنشر، الطبعة الثالثة، 2017، ص258.

<sup>2</sup> - اتفاقية مجلس اوربا بشأن الجرائم الالكترونية (بودابست) لسنة 2001.

الباب الاول، القسم الاول، الفصل الثاني، اتفاقية مجلس اوربا بشأن الجرائم الالكترونية (بودابست) لسنة 2001 .<sup>3</sup>

الباب الثاني، القسم الاول، الفصل الثاني، اتفاقية مجلس اوربا بشأن الجرائم الالكترونية (بودابست) لسنة 2001 .<sup>4</sup>

الباب الثالث، القسم الاول، الفصل الثاني، اتفاقية مجلس اوربا بشأن الجرائم الالكترونية (بودابست) لسنة 2001 .<sup>5</sup>

الباب الرابع، القسم الاول، الفصل الثاني، اتفاقية مجلس اوربا بشأن الجرائم الالكترونية (بودابست) لسنة 2001 .<sup>6</sup>

<sup>7</sup> -الباب الخامس، القسم الاول، الفصل الثاني، اتفاقية مجلس اوربا بشأن الجرائم الالكترونية (بودابست) لسنة 2001.

منها ما لم تتجانس كافة عناصرها التجريبية والعقابية والوقائية والتنفيذية مع بعضها البعض؛ فقد تم إقرار عدد من الآليات ذات الطبيعة التقنية والإدارية، لمواجهة الجريمة المنظمة، وذلك للاستفادة من التقدم التكنولوجي - مصدر الجريمة الإلكترونية - في مكافحتها، وسنستعرض نموذجين من أعمال التعاون الفني على النحو التالي:

#### أولاً : تبادل المعلومات :

عرف العصر الحالي ثورة في مجال المعلومات مما حتم على المجتمع الدولي أن يولي تبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عموماً، والجريمة الإلكترونية خصوصاً، لما توفره المعلومات الصحيحة و الموثوقة من مساندة لأجهزة تنفيذ القوانين في كافة المجالات، بما في ذلك متابعة نشاط المنظمات الإجرامية. ومصادر الأموال في كافة المجالات، لذلك أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، بتطوير التبادل المنهجي للمعلومات بوصفه عنصراً رئيسياً من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها، وأوصى بأنه على منظمة الأمم المتحدة أن تنشئ قاعدة معلوماتية للإعلام الدول الأطراف بالاتجاهات العالمية في مجال الجريمة.

وهكذا ينبغي للتعاون في المسائل المتعلقة بالجريمة الإلكترونية أن يدعم بتوظيف نظم تبادل المعلومات بين الدول الأعضاء، وتقديم المساعدة التقنية الثنائية والمتعددة الأطراف إلى الدول الأعضاء، باستخدام التدريب على تنفيذ القوانين والمعاهدة المتعلقة بالعدالة الجنائية، على الصعيد الدولي<sup>1</sup>.

ويجب ألا تحول مركزية المعلومات دون نشرها وتبادلها فيما بين الدول، بعد ترتيبها ودراستها ومعالجتها، على النحو يسمح بالإفادة منها في مرحلة التحقيقات والمحاكمة، ولمتابعة الأشخاص المشبوهين سواء أكانوا أشخاصاً أم هيئات، مع كفالة الحريات الشخصية، وتشمل كذلك ما يتعلق بتحركات المجرمين المنظمين في جماعة إجرامية عبر الحدود وما يتعلق بالوثائق المزورة والمسروقة

---

1 علي والي، أصداء مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين ، المرجع السابق ، ص 147 .  
وعلى سبيل المثال قضت المادة الأولى من إتفاقية الرياض العربية للتعاون القضائي - التي وافق عليها مجلس وزراء العدل العرب في المؤتمر العربي الأول بالقرار رقم 1 ، بتاريخ أبريل 1983 ، بشأن ضرورة تبادل المعلومات بين الدول الأطراف فيما يتعلق بالنصوص التشريعية والتنسيق بين الأنظمة القضائية كما قضت المادة الخامسة منها بأن ترسل وزارة العدل في الدول الأطراف آخر بيانات عن الأحكام القضائية النهائية الصادرة ضد المواطنين أو الأشخاص المولودين أو المقيمين في إقليمها ، أنظر مجموعة المعاهدات و الإتفاقيات ، جامعة الدول العربية .

التي قد يلجؤون إلى استخدامها وكافة المعلومات المتصلة بما يرتكبون من أنشطة إجرامية، وهو ما أكده اتفاق شنغان للإتحاد الأوروبي، من خلال صياغته نظاماً متكاملًا لتبادل المعلومات<sup>1</sup>. لذلك تعتبر الوقاية- من خلال المعلومات - عنصراً جوهرياً، وقاعدة الأساسية للكفاح ضد الجريمة الإلكترونية، وضمان خلق نظام فعال للمواجهة من خلال تبادل المعلومات بوصفها آلية وقائية للكفاح ضد هذه الجريمة.

### ثانياً: تبادل الخبرات والمساعدة التقنية:

لتحقيق التكامل مع الاتجاه العام لحوسبة عمليات العدالة الجنائية، وتطوير المعلومات وتحليلها على الوجه الذي يخدم أهداف السياسة الجنائية الحديثة لمكافحة الإجرام عموماً ينبغي تبادل العناصر الإدارية ، والتقنيات الفنية، وتعزيز القدرات لأجهزة العدالة وتحليل ونشر البيانات والمعلومات المتاحة حول الجريمة والسبل والآليات المبتكرة لمكافحة ما هو تقليدي وغير تقليدي منها، ويجب التركيز على الأساليب الجديدة كدعم التعاون الفني، وتقديم الخدمات الإستشارية الواسعة لتشمل كافة المجالات كتلك المتعلقة بإخفاء أثر الأموال، لمواجهة جريمة غسل الأموال بهدف حرمان المنظمات الإجرامية من عائدات الجرائم، لأن السياسة الوقائية ستظل قاصرة، ما لم تضبط كافة عناصر السلوك الإجرامي المفترض. ويمكن تقديم المساعدة التقنية الثنائية والمتعددة الأطراف إلى الدول الأعضاء، باستخدام التدريب وبرامج التبادل الدولي والتدريب على إنفاذ القوانين والمعاهدات المعنية بالعدالة الجنائية على الصعيد الدولي.

بيد أنه في هذه الحالة يتوجب على السلطات التشريعية لأي دولة إحداث تعديل في قوانينها الوطنية، لإضفاء الشرعية على هذه الإجراءات بما يتلاءم وطبيعة الجريمة بأبعادها الجديدة المختلفة، التي تستدعي تشريعاً قانونياً خاصاً للإحاطة بكافة الأوجه القانونية - الموضوعية والإجرائية - دون التقيد بالقواعد العامة التي قد تحول دون أن تحقق العدالة الجنائية أغراضها.

وما تم تفصيله اعلاه يتعلق بالجانب الموضوعي للجريمة الإلكترونية وقد تناولت اتفاقية بودابست النصوص الإجرائية الواجب اتباعها في مرحلة البحث والتحري والاستدلال من الالتزامات المفروضة على مزودي الخدمة والتي تتعلق بالحصول على البيانات المحفوظة لديها أو على محتوى البيانات تاركاً أمر تنظيم هذه الإجراءات لكل دولة موقعة منظمة إلى الاتفاقيات بما يتواءم مع تشريعاتها الداخلية، وقد نظمت الاتفاقية التعاون الدولي بين الدول فيما يتعلق بالجرائم الإلكترونية وما ينتج عنها

---

1MICHEL Quille ،strategies en France par la police conter la crimialitcorganise، 1996. p 199.

من تسليم للمجرمين أو المساعدة القضائية المتبادلة إذا نشأ نزاع بين دول الاطراف وكيفية معالجتها وتسويتها هذا على الصعيد الدولي أما اقليميا.

#### • المواجهة التشريعية على المستوى الإقليمي:

تتجلى مكافحة الجريمة الإلكترونية على المستوى الاقليمي بالاتفاقية العربية لمكافحة تقنية المعلومات لعام 2010<sup>1</sup> ووقعت عليها دولة فلسطين بتاريخ 2010/12/21 وتم التصديق عليها وقبولها بتاريخ 2012/5/21 ووقعت عليه 22 دولة عربية. حيث اشتملت الاتفاقية على ما تحويه من نظرية الاتفاقية الاوروبية بودابست مع إضافة بعض النصوص التي لم تتناولها الاتفاقية الاوروبية مثل الجرائم المتعلقة بالارهاب وترويج المخدرات والاتجار بالبشر والاعضاء البشرية والاتجار غير مشروع بالاسلحة وشملت كل ما يتعلق بالاعمال الاباحية غير مقنصرة على استغلال الاطفال لهذه الغاية. ونصت المادة (21) من الاتفاقية العربية بأنّ الجرائم الإلكترونية تشمل كل جريمة تقليدية تمت بوسيلة الكترونية تقنية وهذا النص لا يوجد له نظير في الاتفاقية الاوروبية بودابست والسبب ان الاتفاقية العربية اخذت بمعيار الوسيلة بارتكاب الجريمة الإلكترونية كما فعل المشرع الفلسطيني. شملت الاتفاقية في متن الديباجة الاسباب الداعية لتنظيمها ولتعزيز التعاون بين الدول العربية فيما يتعلق بتقنية المعلومات وضرورة وجود سياسة جنائية مشتركة وموحدة بين الدول العربية لمكافحة الجريمة الإلكترونية، وقسمت الاتفاقية على اربعة فصول تناول الفصل الاول احكام عامة من المادة (1-4) والتي تتعلق بالتعريفات للمصطلحات التقنية وحدود تطبيق الاتفاقية مع الأخذ بمبدأ السيادة لكل دولة طرف وعدم التدخل في الشؤون الداخلية لكل دولة، في حين تناول الفصل الثاني الافعال المجرمة من المادة (5-21) تتعلق بالجرائم التي يتخذ فيها الحاسب دور أساسي لإرتكابها او الادوات والبرامج والمصممة لمساندة الحاسب الآلي بارتكاب الجريمة، واحتوى الفصل الثالث على الاجراءات الواجب اتباعها من قبل دول الاطراف من المادة (22-29) فيما يتعلق بالضبط والتحفظ والجمع الفوري والتفتيش للبيانات المخزنة وآلية تسليم المعلومات بين دول الاطراف والمساعدة فيما بينهم في مجال تقنية المعلومات، وتضمن الفصل الرابع التعاون القانوني والقضائي من المادة (30-43) المتعلقة بتسليم المجرمين والاجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة واسباب رفضها والطلبات العاجلة والطلبات العرضية والتعاون والمساعدة الثنائية للوصول للمعلومات بين دول

<sup>1</sup> نظمت الاتفاقية العربية بمدينة القاهرة بتاريخ 2010/12/21

الاطراف، وجاء الفصل الاخير الخامس باحكام ختامية تتعلق بالالتزامات الواقعة على الدول الاطراف والواجب اتخاذها من اجل تنفيذ وتطبيق الاتفاقية وفقا للتشريعات كل دولة طرف.

### الفرع الثاني: الجهود التشريعية الفلسطينية لمكافحة الجريمة الإلكترونية:

السلطة الوطنية الفلسطينية، ومنذ اعتلاء سدة الحكم، بناءً على اتفاقيات أوسلو عام 1993، حاولت جاهدة إكمال المنظومة التشريعية اللازمة لبيان دولة- فلسطين- المستقبلية، ومن التشريعات الهامة والأساسية التي أصدرتها السلطة الوطنية الفلسطينية قانون الاتصالات السلكية واللاسلكية رقم 3 لسنة 1996<sup>1</sup>، وفضلاً عن ذلك فقد صدر قانون آخر في شأن سريان أحكام السنوات الأخيرة غير الموقع عليها على وثائق نظام الحاسب الآلي، وفي الوقت ذاته أعد " مشروع قانون الانترنت والمعلوماتية " الذي لم يصدر بعد، وكذلك مشروع قانون المبادلات والتجارة الإلكترونية الفلسطينية، وقرار بقانون الجرائم الإلكترونية رقم 10 لسنة 2018 .

وعلى هدي ما تقدم سوف نسلط الضوء على أهم الجهود المبذولة للتصدي لهذه الظاهرة في القوانين الفلسطينية.

بدأت النيابة العامة محاربة الجريمة الإلكترونية والحاق أفعالها بالتكيف القانوني وفق قانون العقوبات رقم 16 لسنة 1960م، وقانون الاتصالات اللاسلكية رقم 3 لسنة 1996، حيث أنها جرّمت بعض الأفعال التي تتم باستخدام شبكة الانترنت ووسائل تكنولوجيا المعلومات مثل جريمة إساءة الأمانة وإطالة اللسان على المقامات عليا والتحقير والتهديد والتشهير والذم وإفساد الرابطة الزوجية وغيرها من الجرائم، الا أنني أرى أن التكيف القانوني حسب قانون العقوبات غير كافية لمحاربة الجريمة الإلكترونية وهناك العديد من الأفعال لا يمكن تجريمها وفقاً لقانون العقوبات المطبق في فلسطين، ولكن هذا لا يعني أن قبل صدور قرار بقانون يتعلق بالجرائم الإلكترونية لم تقوم النيابة العامة والمحاكم واجزة الأمن الفلسطيني بعدم ملاحقة مجرمي الانترنت .

<sup>2</sup> ويعتبر قانون الاتصالات السلكية واللاسلكية رقم 3 لسنة 1996م، من أهم ركائز محاربة الجريمة الإلكترونية لدى النيابة العامة والمحاكم الفلسطينية قبل صدور قرار بقانون يتعلق بمكافحة الجريمة الإلكترونية في فلسطين.

<sup>1</sup> قانون الاتصالات السلكية و اللاسلكية الفلسطيني رقم 3 لسنة 1996 في 18/1/1996 ميلادية الموافق 28 شعبان 1416 .

<sup>2</sup> النيابة العامة ، التقرير السنوي لعام 2018 .

واحتوى هذا القانون على مائة وخمس مواد تكفل بتنظيم الاتصالات السلكية واللاسلكية - في دولة فلسطين المحتلة - وذلك في خمس عشرة فصلاً كما يلي :-

الفصل الأول : تعاريف وأحكام عامة : وذلك في المواد (1-4) حيث وردت في التعريفات الهامة، والجهة المسؤولة عن تطبيق هذا القانون، وهي وزارة الاتصالات ويشرف عليها وزير الاتصالات والبريد الفلسطيني.

وقد وردت تعريفات أخرى، ذات علاقة بعملية تنظيم الاتصالات خاصة ما يتعلق بمحطات البث . وتعلق الفصل الثاني بعنوان مهام وأهداف الوزارة - في المواد (5-8) تحديد الأهداف والاختصاصات المنوطة بوزارة البريد والاتصالات .

وبأتى الفصل الرابع بعنوان - إدارة الترددات- في المواد(1-18) حيث عهدل وزارة البريد والاتصالات بإدارتها بوصفها ثروة وطنية.

أما الفصل الخامس بعنوان - ترخيص شبكات الاتصالات- فقد ورد في المواد (19-28) حيث صدر الجبهة المختصة بترخيص شبكات الاتصالات والشروط الواجب توافرها لإستكمال هذه الشبكات.

والفصل السادس وعنوانه - تجديد الرخص وتعديلها وإلغائها - ورد في المواد (29-37).

وأما الفصل السابع فقد ورد في شأن المواصفات الفنية وأجهزة الاتصالات - وذلك في المواد (38-41).

وأما الفصل الثامن فهو يتعلق بإنشاء وصيانة خطوط الهاتف وتجهيز الاتصالات واستثمارها- وذلك في المواد (42-57).

والفصل التاسع عنوانه - مراقبة المرخصين وحماية المستفيدين وذلك في المواد (58-66) من القانون وقد كرس الفصل العاشر لموضوع -الخدمات الأساسية المتعلقة بالاتصالات - وذلك في المواد (67-

70).

أما الفصل الحادي عشر، وعنوانه - الشبكات المستقلة - فقد كان في المواد (71-77) من القانون . والفصل الثاني عشر، في المواد (78-81)عالج مسألة الإستملاك .

وأماالفصل الثالث عشر، فقد عالج مسألة الضبط، وذلك في المواد (82- 85) .

وأما الفصل الرابع عشر،وهو عصب هذه الدراسة،حيث يتعلق بالحماية الجنائية لتكنولوجيا الاتصالات في فلسطين، من خلال عرض الجرائم والعقوبات المقررة لها،وذلك في المواد (86-100).

والفصل الخامس عشر، في المواد (101-105) تضمن الأحكام العامة والختامية

والحقيقة أن القانون الفلسطيني في شأن الاتصالات السلكية واللاسلكية هو من القوانين - الحديثة - جداً والتي تتم عن رؤية ثاقبة للمشرع الفلسطيني، سواء فيما يتعلق بمعالجة الجوانب الفنية لعملية الاتصالات ذاتها، أو من حيث الرقابة والمعالجة للمخالفة التي ترتكب إساءة لتقنية الاتصالات الحديثة، وواضح ذلك جيداً من العرض - القادم - للجرائم وعقوباتها في نطاق الحماية الجنائية لتكنولوجيا الاتصالات<sup>1</sup>.

وفي هذا المطاف نخلص ان دولة فلسطين اليوم من الدول التي تتمتع بالاعتراف القانوني لها دولياً وإقليمياً بعد انضمامها للعديد من المنظمات والاتفاقيات والمعاهدات على الصعيدين الدولي والإقليمي مما منح الجهات القضائية والتنفيذية أحقية متابعة وتسيير ما يستجد من جرائم على المستوى المحلي والإقليمي والدولي ومواكبة كافة الطرق المتاحة لمكافحتها. ونظراً للتطور التقني الشامل في هذا العالم المتسارع تغيرت مسارات ارتكاب الجرائم وطبيعة مسرح الجريمة، فأصبح لدينا اختلاط بين مسرح الجريمة الرقمي ومسرح الجريمة الطبيعي؛ مما تطلب من النيابة العامة مواكبة هذا التطور لإحاطة سبل اختراق القانون وضمان سير العدالة على أكمل وجه.

وتبعاً لما سبق اتجهت دولة فلسطين إلى تعزيز سبل أعماق التعاون الدولي عن طريق إبرام اتفاقيات وتوقيع مذكرات تفاهم مع دول عدة، خاصة في الفترة الأخيرة. وقامت النيابة العامة الفلسطينية بإنشاء وحدة الجرائم الإلكترونية وتعزيز وحدة التعاون الدولي وسيتم تعزيز عمل نيابة الجرائم الإلكترونية بالتعاون مع نيابة الجرائم الاقتصادية والنيابات المتخصصة الأخرى، والأهم في الفترة السابقة قبول منظمة الشرطة الجنائية الدولية "الإنتربول"، وبالمصادقة عليه أصبحت فلسطين العضو رقم 191 في هذه المنظمة والتي تعمل على تنسيق وتعزيز الجهد الدولي في مكافحة الجريمة الدولية من خلال التواصل الدائم والمستمر بين مختلف الأجهزة الشرطة في العالم لمواكبة تطور الجريمة وتبادل الخبرات في كيفية مكافحتها والحد منها وخاصة ان بعضها أصبح عابراً للحدود، أن انضمام دولة فلسطين للإنتربول يعد انجاز فلسطيني في سلسلة الانجازات الدبلوماسية والقانونية، ويأتي بعد حصول

---

<sup>1</sup> عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، دار النهضة العربية، مصر، 2009، ص315.

فلسطين على عضوية دولة "مراقب" والتي انضمت بموجبها إلى جملة من المواثيق الدولية، ومؤخراً انضمامها إلى "الانتربول"<sup>1</sup>.

وتماشياً مع هذا القرار تم العمل على مساواة فلسطين بجميع الدول الأعضاء من حيث الحقوق والواجبات والمساهمة في تطبيق القانون على المستوى الدولي وتطوير أجهزة الشرطة، ويمثل هذا التصويت اعترافاً دولياً بأحقية فلسطين لتكون شريكاً حقيقياً في منظومة الأمن الدولية والمساهمة في الجهد الدولي الهادف للوصول لعالم أكثر اماناً، وتمكنها من ممارسة كافة الصلاحيات الممنوحة للدول الاعضاء في تتبع مرتكبي الجرائم والذين يتنقلون بين الدول.

ومن هنا سيقود اندماج دولة فلسطين في السياق الأمني والنيابي والقضائي الدولي إلى تعزيز دور الدولة الفتية بتحديد اتجاهاتها والعمل على مصالحها وموازنة الأمن العام بالتعاون مع الدول المدرجة بالاتفاقية وهذا ما يعزز بدوره السيادة والانتقال تدريجياً إلى الصعيد الدولي والاقليمي، حيث يحقق وجود فلسطين في سياق المراقبة الدولية في الانتربول تطوراً ظاهراً في فرض سيادتها على أراضيها ومحاربة عقبات ومعوقات المحتل الذي فرضها عبر محاصرة فلسطين سياسياً ودولياً، وانطلاقاً من هذه المبادرات والخطوات ستفرض فلسطين سيادتها دولياً في سياق مكافحة الجريمة الإلكترونية على الوجه المنشود.

وعلى الرغم من أنّ المشرع الفلسطيني أصدر قرار لمكافحة الجريمة الإلكترونية، والتصدي إليها والمتمثل بقرار رقم 16 لسنة 2017م، لا أنّ هذا القرار تعرض لجملة من الانتقادات التي ابدتها مؤسسات المجتمع المدني وحقوق الانسان ومن أبرز هذه الانتقادات ما يلي:

- ان القانون يمس و ينتهك الحريات العامة والخصوصية.
- أن القانون ينتهك حرية الرأي والتعبير
- أن القانون يشمل مصطلحات فضفاضة مثل النظام العام والمصلحة العامة والاداب العامة
- أن القرار بقانون يتضمن نصوص عقابية مغلفة وتتناقض مع قانون العقوبات لعام 1960
- أن القرار بقانون يشكل ثقل على الاعلاميين وأهل الفكر، والرأي ليعبروا عن آرائهم السياسية

<sup>1</sup> اصدر النائب العام الدكتور احمد براك قرار بتاريخ 2-1-2017 قرار بإنشاء نيابة متخصصة لمكافحة الجريمة وذلك من اجل التصدي لهذا الجريمة وفق منظور قانوني جديد داخل جسم النيابة العامة، تاريخ زياره الموقه 19-8-

<http://www.radionisaa.ps/article/6211/%D8%A7,2019>

-أن الضمانات المرتبطة بالتفتيش والتحفظ تخالف الضمانات الممنوحة والواردة في قانون الاجراءات الجزائية والقانون الاساسي الفلسطيني

-أن القرار بقانون يخالف نص المادة 3\27 من القانون الأساسي والتي تنص على استقلالية الصحافة والتي تنص يحظر الرقابه على وسائل الاعلام ولا يجوز انذارها أو وقفها أو مصادرتها أو الغاؤها أو فرض قيود عليها الا وفقا للقانون وبموجب حكم قضائي

-ان القرار بقانون وسع من صلاحيات مأموري الضبط القضائي بحيث ان القانون نص على ضرورة وجود مختبر جنائي لدى الشرطة المدنية وقوى الامن بما معناه الاجهزة الامنية التابعة لدورة كلا باختصاصه

على ضوء هذه الاعتراضات وجه مكتب المفوض السامي الحقوق الانسان و المكلف بتعزيز وحماية الحق في حرية الرأي والتعبير في 2017\8\16 خطابا ديفيد كاي للحكومة الفلسطينية جملة الاعتراضات، وانا بالرأي اعتقد ان مؤسسات المجتمع المدني قد بالغت بالاسلوب للاعتراض على قرار بقانون فرار بقانون تم عرضه على دولة رئيس مجلس الوزراء بتاريخ 2016\3\15 من اجل مناقشته وبذات الوقت لعرضه على كافة الوزارات بالدولة لتقدييم ملاحظاتهم وتوثيقها، وفي خلال هذه المدة تم عقد مؤتمر الأول من نوعه في جامعة النجاح الفلسطينية بحضور مؤسسات المجتمع المدني والتي كانت من اهم توصيات المؤتمر ضرورة وجود نص تشريعي يعالج الجرائم الإلكترونية وكان هناك كم هائل من التغطية الإعلامية وخاصة أن مؤسسة النيابة العامة إدراكاً منها لخطورة هذه الجريمة ولأنها وفقا للاحصاءات الواردة لمكتب النائب العام والمنظمة من وحدة التخطيط، والسياسات تبين ان واقع الجريمة الإلكترونية في فلسطين خرجت من انها مشكلة لتصبح ظاهرة تتزايد أعدادها وأرقامها لنجد الفارق ما بين 2015 و 2016 ارتفاعاً ما نسبته 41% من نسبة الجرائم الإلكترونية فقرر عطوفة النائب العام لدولة فلسطين ان يضع وبهياً الارضية الخصبة لدى النيابة العامة من حيث تخصيص نيابة متخصصة للجرائم الإلكترونية تحت اشرافه مباشرة وتخصيص أعضاء نيابة متخصصين للتحقيق في الجرائم الإلكترونية في 2017\1\2، وتدريبهم حول ماهية الجريمة الإلكترونية والية التعامل بها من قبل خبراء محليين ودوليين، ان الفترة التي مرت ما بين عرض القانون واقراره تجاوزت العام وأكثر، وأن مؤسسات المجتمع المدني على علم ودراية بتوجه دولة فلسطين إلى إعداد مشروع قرار بقانون وان ما جرى بداخل دولة فلسطين ليسوا بعيدين عنه كما كان بإمكانه الحصول على مشروع القرار بقانون خلال هذه المدة، إن ما تم الاعتراض عليه من وجهة نظري مخالفا للواقع فقرار بقانون الجرائم

الإلكترونية لما يخاطب الاعلاميين حيث انهم يخضعون لقانون خاص بهم وهو قانون المطبوعات والنشر والذي ايضا تسعى الدولة الى تعديله واضافه الية تنظيم الاعلام المرئي وغير المرئي "الالكتروني" هذا من جانب حرية الصحافة والاعلام والتعبير كما وأنه ان قانون المطبوعات والنشر قد استعرض ما هو مخالف لمهنة الصحافة والاعلام وايضا قانون العقوبات رقم 16 لسنة 1960 قد حدد ما هو مشروع نشره بموجب نص المادة 198.

إن الاعتراض الموجه للمصطلحات الفضفاضة فإن القانون الأساسي المعدل لعام 2003م، وقوانين الدول المجاورة قد نصت ببندوها هذه المصطلحات المتمثلة بالمصلحة العامة والاداب العامة، كما وانها مستمدة ايضا من الاتفاقيات الدولية وخاصة نص المادة 119 من العهد الدولي فقد شملت الفقرة 19 اب القيود الواردة بنص القانون لتعبير المواطنين في ارائهم بأن لا تمس احترام وحقوق الآخرين أو سمعتهم لحماية الامن القومي أو النظام العام أو المصلحة العامة أو الاداب العامة وهذه العبارات ايضا عبارات فضفاضة أن تقدير النظام العام والمصلحة العامة، والاداب العامة أمر نسبي متفاوت بين دولة ودولة وحتى أنه في داخل الدولة الواحدة تختلف الاعراف والتقاليد مثلاً بمنطقة الصعيد المصري في منطقة القاهرة أو شرم الشيخ وتفاوت أيضاً بمدينة رام الله عنها بمدينة الخليل يعود تقدير ذلك للسلطة التقديرية للقائمين على الموضوع فهي تختلف من مكان لمكان ومن زمان لزمان.

وتم تأييد بعض اعتراضات مؤسسات المجتمع المدني في أن بعض العقوبات مغلظة الا أن لا توافق مع ما ابدوه من اعتراضات، وعليه فإن المؤسسات الحقوقية والمجتمع المدني، هي جزء لا يتجزأ من دولة فلسطين وان كان عليها واجب الالتزام والعمل للحفاظ على الشعب و حقوقه فكان لا بد منها ان تسعى وتطالب باقرار قانون مكافحة الجرائم الإلكترونية فهذه المؤسسات ليست بعيدة عن المجتمع وتواكب جميع الاخبار والجرائم الإلكترونية وخاصة بالامور التي تتعرض لها النساء، والتي نتج عنها حالات انتحار وقتل على خلفية الشرف بعد أن أوقفنا هذا النزف بجهود مؤسسات المجتمع المدني لنعود إلى هذه الجرائم بطريقة وأسلوب آخر.

وتعارض الباحثة وجود مختبر فني لدى الشرطة المدنية فقط، فالاجهزة الامنية كافة بالشرطة المدنية، الأمن الوقائي، المخابرات العامة، الاستخبارات، كل له اختصاصه فلا يعقل أن تقع جريمة تعرض أمن الدولة الداخلي أو الخارجي للخطر ومن خلال وسيله تقنية المعلومات، وتحال الى جهة غير مختصه لعدم وجود كوادر متخصصة أو مختبر متخصص في كل جهاز.

واخيراً إن وجود قانون خاص من عدم وجوده حتى لو كان هناك انتقادات بناءة فنلجأ الى التعديل ولكن لا يهاجم وخاصة أن القرار بقانون مكافحة الجرائم الإلكترونية بفلسطين ليس الاول في الدول العربية والغربية ولولا وجود حاجة دولية واقليمية ومحلية لوجود قانون متخصص يتواءم مع طبيعة الجريمة الإلكترونية لما وجدت اتفاقية بودابست 2001م وقانون مكافحة تقنية المعلومات والقوانين المحلية بتونس، الامارات، الكويت، مصر، الاردن، الجزائر ... وفرنسا وامريكا وهولندا ...

تم التصدي للمعوقات القانونية بصدر قرار بقانون رقم (16) لعام 2017م، بشأن الجرائم الإلكترونية<sup>1</sup>، حيث أثار جدل واعتراض من قبل مؤسسات المجتمع المدني الحقوقية؛ ولوجود إدراك عالي لدى مؤسسات الدولة الحكومية وإعطاء مبادئ حقوق الإنسان الأولوية كأساس منسق عليه، تم تعديل قرار بقانون (16) لعام 2017 إلى قرار بقانون (10) لعام 2018م، (أخذاً بعين الاعتبار أهم الاعتبارات والاعتراضات الموجهة من طرف مؤسسات حقوق الإنسان<sup>2</sup> ليصدر بحلته الجديدة القرار بقانون رقم (10) لعام 2018 المتفق مع المبادئ العالمية لحقوق الانسان كما وعالج القرار بقانون الجرائم الإلكترونية رقم (10) لعام 2018، جميع الثغرات القانونية السابقة من حيث تضمين القانون لنصوص قانونية تعاقب وتجرم الجريمة الإلكترونية بجميع أشكالها وتحديد الإجراءات الواجب اتباعها مع رسم آلية المساعدة الدولية والتعاون الدولي في هذا المجال، وفرض التزامات على الشركات المختصة والتي تعمل في نطاق الاتصالات، ويستند الاطار المرجعي للقرار بقانون رقم 10 لسنة 2018 الى :-

1. القانون الاساسي المعدل لسنة 2003 ميلادي.
2. الاتفاقية العربية لمكافحة تقنية المعلومات 2010.
3. العهد الدولي الخاص للحقوق المدنية والسياسية 1966.
4. قانون الإجراءات الجزائية رقم 3 سنة 2001.
5. اتفاقية بودابست 2001 ميلادي.

يشتمل القرار بقانون رقم 10 سنة 2018 الخاص بالجرائم الإلكترونية على أربعة أبواب احتوت بداخلها على (57)، مادة حيث جاء الباب الاول شاملا على التعريفات والاحكام العامة من المادة 1-3، وتناول الباب الثاني الجرائم الإلكترونية من المادة 4-31 سواء الجرائم الواقعة على ما يحتويه الكمبيوتر مثل الاختراق، الدخول غير المصرح به، المحو، التعديل، النسخ، التدمير للبيانات. أو التي ترتكب من خلال الكمبيوتر، ومنها الاتجار بالبشر، والاتجار بالمخدرات، والدخول التعسفي لحياة الخاصة للأفراد، وغسيل الاموال والارهاب، وعرض مواد إباحية للأطفال، ونظم الباب الثالث الاجراءات الواجب اتباعها من قبل مأموري الضبط القضائي في مرحلة الاستدلال والبحث والاجراءات

---

<sup>1</sup> عصام عابدين، جهود مؤسسة الحق في مواجهة قرار بقانون الجرائم الإلكترونية، مؤسسة الحق - القانون من أجل الانسان، 2018 .

التحقيقية الصادرة من قبل النيابة العامة بما تحتوية من قيود وضوابط للجهات القضائية من المادة 32-43.<sup>1</sup>

احتوى هذا القرار بقانون على 57 مادة ونظم قرار بقانون رقم 10 لسنة 2018 عدة موضوعات منها: أولاً: إيراد قواعد خاصة ودقيقة بالتعريفات.

ثانياً: إيراد قواعد موضوعية (أنواع الجرائم والعقوبات المفروضة/ نصوص التجريم والعقوبات) الواردة في تماشياً مع اتفاقية الجرائم الإلكترونية الأوروبية (اتفاقية بودابست 2001م) وجرائم الشبكة الدولية الواردة في القوانين الدولية الناجحة ذات العلاقة ولم ترد في الاتفاقية.

ثالثاً: قواعد ذات صلة بالاحكام العامة للعقوبة والاعفاء منها (القواعد الخاصة بالعقوبات التكميلية والمساهمة الجرمية، والتدابير الخاصة بهذه الجرائم والاعفاء من العقوبة ومضاعفتها).

رابعاً: قواعد ذات طبيعة اجرائية خاصة بصلاحيات الضبطية القضائية

واشتمل القرار بقانون على نصوص التجريم الموضوعية على صورة من الجرائم الإلكترونية ومنها: التوصل بغير وجه حق الى الشبكة المعلوماتية أو وسيلة تقنية المعلومات، الإلغاء أو التعديل أو الافشاء أو النشر للمحتوى الناتج عن التوصل بغير وجه حق؛ تزوير المستندات الإلكترونية الرسمية والخاصة؛ استعمال المستندات الإلكترونية المزورة مع العلم بذلك؛ إعاقة أو تعطيل الوصول للخدمة أو الدخول الى الانظمة؛ ايقاف أو تعطيل عمل الشبكة والانظمة؛التنصت والانتقاط والاعتراض لما هو مرسل عبر الشبكة أو الانظمة؛التهديد والابتزاز والمس باعتبار وكرامة الاشخاص<sup>2</sup>.

وأضاف القرار بقانون رقم 10 لسنة 2018 اجراءات مستحدثة تتواءم مع الصعوبات الاجرائية بالحصول على الدليل الرقمي ابتداء من الاجراءات المتعلقة بالمراقبة والمتابعة الاتصالات على الشبكة الإلكترونية والتي هي على عاتق مزودي خدمة الشبكة الإلكترونية بناءً على طلب من الجهات المختصة قانوناً واعتبرت الاتفاقية أن هناك إجراءات تمهيدية لا تعنى تحريك الدعوى الجزائية، وهذه الاجراءات مقسمة إلى نوعين إما أن تكون عاجلة كالتحفظ العاجل والسريع على مضمون البيانات

<sup>1</sup> انظر الى المادتين 32 و 43 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية في فلسطين.

<sup>2</sup> ومن الجرائم التي تصدى لها قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية في فلسطين الاستيلاء على بيانات البطاقات المالية الإلكترونية واستخدامها والاستيلاء على الاموال بواسطتها؛ انتاج ونشر وترويج مواد تمس الاداب العامة (موجهة للبالغين والاطفال؛ الاساءة للمقدسات والشعائر والتعرض للذات الالهية والانبياء؛ التعدي على المبادئ والقيم العائلية والاسرية والحياة الخاصة والتشهير بالاشخاص بالوسائل الإلكترونية؛ترويج المخدرات الكترونياً؛ التعدي على الملكية الفكرية؛ الاتجار بالاشخاص الكترونياً؛ الترويج لما يمس النظام العام ويهدد الامن القومي والاداب العامة؛ الاستيلاء على البيانات والمعلومات الحكومية السرية او اتلافها او تعديلها او نشرها؛ تجريم من يقوم باستخدام البرمجيات الخبيثة بقصد الاضرار بالانظمة والشبكة؛ فك التشفير وتجاوز اجراءات الامن لارتكاب اية جريمة الكترونية.

- قرار بقانون رقم 10 لسنة 2018 .

المخزنة بأمر صادر للمزودي خدمة الانترنت لتحفظ على البيانات المخزنة لمدة زمنية محددة أو التحفظ العاجل لمضمون البيانات ضمن خط سير البيانات اي بمعنى حفظ الوقت والتاريخ والجهة المرسله والمستقبله أما إذا تعلقت الاجراءات بالتفتيش والضبط أو الحصول على بيانات المخزنة والتحفظ علي نسخة منها بظروف تحفظ سلامة البيانات والمعلومات وتعتبر هذه الإجراءات من الاجراءات التحقيقية للحصول على الدليل الرقمي بالبيئة الرقمية، وشمل الاتفاقية نوعاً جديداً قد يطلق عليه بالمراقبة المعاصرة للاتصال من خلال اعتراض محتوى البيانات بجمعها وتسجيلها كخطوة مستقبلية للاحاطة بما يستجد من جديد حول الاستخدام الغير مشروع لهذه الاجهزة التقنية والشبكة العنكبوتية وما يرافقه من تطورات تقنية، واخيرا الباب الرابع الذي احتوى على احكام ختامية من المادة 44-57.

كما تصنف الجرائم الواردة في قرار بقانون رقم(10) لسنة 2018، اولا جرائم ماسة بخصوصية وامن وسلامة البيانات بداخل النظام الالكتروني مثل الدخول الغير مشروع والاعتراض والتدخل في البيانات، ثانيا جرائم تتعلق بالجهاز الكمبيوتر مثل مجموعة التزوير والاحتيال وانتحال صفة الغير، ثالثا جرائم متعلقة بالانتهاكات الخاصة بحقوق الملكية الفكرية، ويعالج المشرع الفلسطيني ايضا المساهمة الجنائية والعقوبة ومسؤولية الاشخاص المعنوية<sup>1</sup>.

وعلى الرغم من ذلك الا انه تم العمل بجد ومثابرة من اجل مكافحة الجريمة الإلكترونية على الصعيد المحلي الوطني وتبلور ذلك من إنشاء نيابة الجرائم الإلكترونية في 2016/3/20 كنيابة مستقلة، وبالتالي تم توسيع اختصاصها بعد أن كانت تعمل بشكل ضيق ضمن نطاق دائرة متابعة الاتصالات السلكية واللاسلكية، وخلال هذه الفترة تم وضع القاعدة التنظيمية لعمل نيابة الجرائم الإلكترونية من حيث تخصيص أعضاء نيابة وموظفين إداريين متخصصين وتدريبهم بشكل يتواءم مع طبيعة الجريمة

---

<sup>1</sup>نص المادة 28 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية: " كل من حرض أو ساعد أو اتفق مع غيره على ارتكاب جريمة من الجرائم المنصوص عليها بموجب أحكام هذا القرار بقانون، بأي وسيلة إلكترونية، ووقعت الجريمة بناءً على هذا التحريض أو المساعدة أو الاتفاق، يعاقب بالعقوبات المقررة لفاعلها الأصلي.

نص المادة 29 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية: " إذا ارتكب، باسم الشخص المعنوي أو لحسابه، إحدى الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة آلاف دينار أردني، وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات أو أن تقضي بحله في حال كانت الجريمة معاقب عليها بالحبس لمدة لا تقل عن سنة، وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع.

الإلكترونية وآلية متابعتها وتحليل الدليل الرقمي وتحديد الاحتياج الإلكتروني وهذا يعتبر من أهم الإنجازات التي قامت بها نيابة الجرائم الإلكترونية، بالرغم من وجود عدة معوقات منها القانونية تتمثل بعدم وجود قانون متخصص وعدم السيطرة على الشرائح الاسرائيلية؛ من حيث عدم وجود تنظيم لآلية تسجيلها ومتابعتها مما جعل عدد من مرتكبي الجرائم يسعون وراء شراء هذه الشرائح الاسرائيلية التي يهربها الموزعين داخل الأراضي الفلسطينية بشكل مخالف للقانون في المناطق التي تخضع للتنسيق الامني والذي يهدف الاحتلال الى عرقلة العمل القانوني ويسط سيادة القانون فيها، وهذه الافعال تشكل جريمة يعاقب عليها القانون ويتوجب على مأموري الضبط القضائي ومفتشي وزارة الاتصالات متابعتها بشكل حثيث للحد منها وسنوضح هذا من خلال الحديث عن هذه المرحلة في المبحث الثاني من تتبع للجريمة والبحث والاستدلال عنها وبيان اكتشافها في مراحلها الاولى وصولا الى مرحلة التحقيق الابتدائي .

### المطلب الثاني: أركان الجريمة الإلكترونية والتحديات التي تواجه مكافحتها

#### الفرع الاول: أركان الجريمة الإلكترونية

تتحقق الجريمة وتكتمل باكتمال اركانها وعناصرها وهذه الأركان وفق ما هو وارد في الاحكام العامة تكون ركن مادي وركن معنوي والركن الشرعي والذي لا يمكن أن تكون جريمة ولا عقاب بدونه، ولكن التساؤل هنا حول طبيعة الاركان في الجريمة الإلكترونية وهل تتوافق مع الأركان في الجريمة التقليدية ام تختلف عنها؟ للاجابة على ذلك سنوضح اركان الجريمة وفقا للاحكام العامة ومقارنتها مع الجريمة الإلكترونية

## أولاً: الركن الشرعي ( القانوني)

انطلاقاً من مبدأ "لا عقوبة ولا جريمة الا بنص قانوني" يجرم الفعل والامتناع لاثبات الجريمة والركن الشرعي من المشرع وهي النصوص القانونية الواردة في قانون العقوبات أو في أي من القوانين الأخرى<sup>1</sup>مثل قانون الاتصالات السلكي واللاسلكية<sup>2</sup> وقانون الصحة<sup>3</sup> وقانون الخدمة المدنية<sup>4</sup> والقوانين الأخرى ومن ضمنها قرار بقانون الجرائم الإلكترونية الفلسطينية رقم 10 لسنة 2018 الذي صدرت بموجب المادة 43 في حالة الطوارئ من القانون الاساسي الفلسطيني

ومن سمات النص الشرعي الجنائي انه لا يجوز القياس عليه فالمشرع إن أبى سكت، وعليه لايجوز أن يعاقب شخص عن فعل لا يطابقه نص قانوني يجرمه<sup>5</sup>، ولا يمكن بأية حال من الأحوال الاستعانة بنصوص قد تطبق على أفعال مشابهة حتى لو شابها الدوافع أو الفاعلية أو النتائج أو العناصر<sup>6</sup>، والنص القانوني هو النص الذي يحظر السلوك الاجرامي وهو واجب على كل الافراد للحفاظ على امن وكيان المجتمع وان الهدف من وجود الركن الشرعي المتمثل في النص القانوني لغايتين:

الأولى هو الحفاظ على كرامة الأفراد وخصوصيتهم، وحياتهم الخاصة من إساءة استعمال السلطة، وبذات الوقت حماية الأفراد من أنفسهم، وذلك بعلمهم بالمحظورات والعقوبات الرادعة، والثانية هو التقيد بمدلول النص والالتزام به من قبل السلطة القضائية وحماية حقوق الافراد من استبداد القضاء أو أفكاره المبني على العادات والتقاليد التي نشأ عليها، والتقيد بالعقوبة والتدابير الجزائية، والالتزام بحدود العقوبة الأعلى والأدنى المقررة في القانون فضلاً عن العقوبات التبعية مثل المصادرة والتقيد بالأحوال التي تحتوي على أسباب مخفضة، أو الظروف المشددة، والاسباب المشددة، ولا يحق للقاضي الاعفاء من العقوبة إلا في الحالات التي صرح بها المشرع بنص قانوني صريح<sup>7</sup>.

<sup>1</sup> كامل السعيد، شرح الاحكام العامة في قانون العقوبات، مرجع سابق، ص55.

<sup>2</sup> قانون الاتصالات السلكي واللاسلكية رقم 3 لسنة 1996 تاريخ النشر 23 يوليو 1996 في العدد الثاني عشر من الوقائع الفلسطينية.

<sup>3</sup> قانون الصحة العامة رقم 20 لسنة 2004 تاريخ النشر 23 ابريل 2005 في العدد الرابع والخمسون من الوقائع الفلسطينية.

<sup>4</sup> قانون الخدمة المدنية رقم 4 لسنة 1998 تاريخ النشر 1 يوليو 1998 في العدد الرابع والعشرون من الوقائع الفلسطينية .

<sup>5</sup> فخري عبد الرازق الحديثي استاذ القانون الجنائي كلية الحقوق -جامعة جرش والدكتور خالد حميدي الزعبي استاذ القانون الجنائي المساعد في كلية الحقوق جامعة فلادلفيا-دار الثقافة للنشر والتوزيع 2010 م -1431، ص30.

<sup>6</sup> كامل السعيد، شرح الاحكام العامة في قانون العقوبات، مرجع سابق، ص58.

<sup>7</sup> أحمد البراك وعبد القادر جرادة، الجريمة الالكترونية في التشريع الفلسطيني مرجع سابق، ص 35.

ويعد أن تم استعراض الركن الشرعي للجريمة بنظريتها العامة يثور في ذهننا سؤال هل يمكن اسقاط هذه الأركان العامة للجريمة التقليدية لتطبيقها على الجرائم الإلكترونية؟

فما تم استعراضه من معايير في تعريف للجريمة الإلكترونية، والأسس التي اعتمد عليها الفقهاء والخبراء والقانونيين في تعريف الجريمة الإلكترونية، تبين لنا أنها جريمة ذو طبيعة خاصة من حيث السلوك وأسلوب ارتكاب الجريمة، وعليه لا يمكن ان تطبق النص التقليدي ليستوعب الجرائم المستحدثة التي تحتوي مصطلحات وإجراءات تختلف كلياً عن الجرائم التقليدية .

وقد تصدت التشريعات الاجنبية لهذه الظاهرة فقد تدارك وجود وانتشار الجريمة الإلكترونية المستحدثة امام العجز التشريعي الموجود فبادرت الدول باصدار قوانين تتعلق بها ومن الدول السباقة لوضع القوانين المناسبة والملائمة للجرائم الإلكترونية دولة السويد حيث اصدرت قانون البيانات السويدي عام 1973م ثم الولايات المتحدة في عام 1976م أو المملكة المتحدة (بريطانيا) في عام 1981م، وفي الدانمارك في عام 1985م ضمن مواضيع مختلفة كجرائم الدخول الغير مشروع الى انظمة الحاسب الآلي او قانون لحماية انظمة الحاسب الآلي او ضمن قانون لمكافحة التزوير والتكليف الالكتروني وجرائم التلاعب غير المشروع في البيانات والمعلومات ومن الدول من قامت الى تعديل تشريعاتها الجزائية مثل فرنسا 1988م بتعديل عام 1994م، وتناولت مكافحة الجريمة بوجود أيضاً نصوص تشريعية خاصة بقانون خاص يتلائم مع طبيعتها. والسبب في تقدم الدول الغربية باصدار التشريعات المناسبة<sup>1</sup>.

تداركت الدول العربية الموضوع في أواخر الثلاثين سنة من العقد العشرين فقامت بوضع نصوص عقابية لمواجهة هذه الجريمة حيث صدر في تونس عام 2000م، وفي إمارة دبي قانون رقم 2 لسنة 2002م، وفي مصر قانون رقم 15 لسنة 2004م وصدر ايضا قوانين لدى عدة دول عربية منها السعودية والبحرين وقطر ولبنان والكويت والاردن وجميعها كانت تتعلق بالمعاملات الإلكترونية والتجارة الإلكترونية والتوقيع والتزوير الالكتروني وصدرت ايضا قرارات بقوانين مثل فلسطين قرار بقانون الجرائم الإلكترونية رقم 10 سنة 2018م، وقانون مصر سنة 2015م، والاردن سنة 2015م، وجميع هذه التشريعات المتعلقة بتجريم سلوكيات الجريمة الإلكترونية جاءت متفرقة وعلى مراحل

<sup>1</sup> عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، 2008، ص 17.

وبعضها كانت تتعلق بانماط معينة للجرائم الإلكترونية خاصة التي تتعلق بالتقنيات المعقدة لهذه الجريمة.

### ثانياً: الركن المادي

ويعد الركن المادي للجريمة ممثلاً بالسلوك الإجرامي المتكون من الفعل أو الامتناع أي الأفعال المادية المكونة للجريمة أما الركن المعنوي المتمثل وهو العلم والارادة لإتيان القصد الجرمي وسنبحث الأركان المكونة للجريمة بأركانها العامة ومدى تطابقها وضرورة توافرها لارتكاب الجريمة الإلكترونية وقبل بيان هذه الأركان لا بد من توضيح من هو الفاعل في الجريمة الإلكترونية كونه هو من يبرز الركن المادي للجريمة إلى حيز الوجود، وهل يتطابق مع ما جاءت به الأحكام العامة للتجريم والعقاب.

يعرف المشرع الفاعل في الجريمة وفقاً للأحكام العامة هو من أبرز إلى حيز الوجود العناصر التي تكون الجريمة أو ساهم مباشرة في ارتكابها<sup>1</sup>، وتتميز الجريمة الإلكترونية أن الفاعل في الجريمة الإلكترونية هو على معرفة تقنية عالية وبدرجة عالية من الذكاء والخداع وهذا لا يعني أن الجريمة لا ترتكب من شخص ذو مستوى عادي بالمعرفة التقنية أو عن طريق الخطأ وقد يستفاد من نوعية الجريمة المرتكبة ومستوى الفاعل في ارتكابها في معرفته من قبل مأموري الضبط القضائي والمختبر الجنائي وقد يسجل لدى المختبر الجنائي بأسماء الفاعلين المعروفين بتقنية عالية وربطهم عند تقديم أي بلاغ بنوعية الاعتداء واسلوب المعتدي، وقد يتم تأجير الفاعلين بالأحرى المجرم الإلكتروني من قبل أشخاص طبيعيين أو معنويين لغايات الحصول على معلومات تتعلق بشركة أخرى منافسة لها في الأسواق وهي تقع تحت دائرة الحرب الاقتصادية والمنافسة غير المشروعة بالأسواق التجارية، وبالتالي يكون دور الفاعل في إبراز الركن المادي للجريمة من خلال القيام بالسلوك (فعل أو امتناع) عن فعل يشكل على الناحيتين جريمة معاقب عليها بالقانون

ويقوم الركن المادي على مجموعة من العناصر المادية التي تتخذ مظهراً خارجياً تلمسه الحواس ويعرف أيضاً بأنه سلوك إجرامي بارتكاب فعل أو الامتناع عن فعل أمر به القانون، وعاقبه على مخالفته فهو السلوك المادي الخارجي الذي ينص القانون على تجريمه والمعاقبة عليه، ومن خلال التعريفات السابقة للركن المادي نلاحظ أن السلوك المتمثل بالفعل والامتناع له مظهر خارجياً<sup>2</sup>، ومن

<sup>1</sup> -المادة (75) من قانون العقوبات رقم 16 لسنة 1960 والتي نصت على: "فاعل الجريمة هو من أبرز إلى حيز الوجود العناصر التي تؤلف الجريمة أو ساهم مباشرة في تنفيذها."

<sup>2</sup> محمد صبحي نجم، مرجع سابق، ص 208.

خلال ما تم ذكره حول الجريمة الإلكترونية من خصائص يتضح أن الفعل أو الامتناع قد لا يشعر به المجني عليه إلا إذا تسبب بأضرار ملموسة له أي تبينت له، وهذا ما يختلف عن الجريمة التقليدية، والتي تبرز الى حيز الوجود بمجرد ارتكاب الفعل سواء تحققت النتيجة أم لا، مثل إطلاق شخص على آخر النار من مسدسه بقصد القتل، فهنا تحققت نتيجة القتل أم لا نكون بصدد جريمة أمّا مكتملة الاركان او تشكل شروع في الجريمة على خلاف الجريمة الإلكترونية التي تكون ارتكبت وتحققت النتيجة ولا تظهر الى حيز الوجود الا بعد اكتشاف المجني عليه ذلك، وهذا ما يدفعنا للتساءل حول طبيعة تكيف الركن المادي للجريمة الإلكترونية؟

فالركن المادي في الجريمة المكتملة يجب ان يتوافر السلوك (الفعل، الامتناع) والذي احدث النتيجة الجرمية والمرتبط بها بعلاقة سببية<sup>1</sup> من ناحية قانونية لا بد من توافر اركان الجريمة سواء كانت الاركان العامة للجريمة المتمثلة في الركن الشرعي القانوني والركن المادي بعناصر الثلاث فعل أو امتناع عن السلوك الاجرامي، ونتيجة جرمية، وعلاقة سببية تربط بينهما، والركن المعنوي يتمثل بالعلم والارادة بقسمة القصد العام والقصد الخاص لبعض الجرائم التي يتطلبها المشرع في أنواع معينة، وهذه الاركان هي أساس لكل من الجرائم المرتكبة، والمخالفة للقانون، وهي التي تمثل عناصر الجريمة وجوداً وعدماً، أمّا الاركان الخاصة وهي التي ينص الركن الشرعي على توافرها والتي تمثل فيما يتطلبه المشرع مثلاً صفة الموظف العام في جريمة الفساد الوظيفي الاختلاس والرشوة<sup>2</sup>.

### ثانياً: الركن المادي

**1- السلوك الاجرامي** يعد السلوك الاجرامي هو المظهر للفعل أو الامتناع الملموس الذي يتم ادراكه من خلال الرؤيا أو السمع أو الاحساس الجسدي، فإن السلوك الإجرامي ظاهراً لمن حول هذا السلوك باستخدام الحواس والادراك<sup>3</sup>، إنّ السلوك الاجرامي لمرتكب الجريمة هو من الشروط الواجب توافرها في جميع صور وأشكال الجريمة، إلا إن السلوك الاجرامي المتمثل بالفعل الايجابي، أو الامتناع الفعل السلبي إذا اقدم عليه الفاعل، وتحققت النتيجة الجرمية نكون أمام جريمة تامة.

<sup>1</sup> كامل السعيد، شرح الاحكام العامة في قانون العقوبات، عمان ، دار الثقافة للنشر والتوزيع ، 2019 ، ص183.

<sup>2</sup> عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، مصر، دار الكتب القانونية، 2008، ص 132.

<sup>3</sup> كامل السعيد، شرح الاحكام العامة في قانون العقوبات، مرجع سابق، ص183.

وإن لم تتحقق النتيجة الجرمية نكون أمام شروع الفاعل لارتكاب الجريمة، وهي المعاقبة عليها بنص القانون<sup>1</sup>.

وهنا نقف أمام تساؤل هل تعاقب الأعمال التحضيرية في الجرائم الإلكترونية خلافاً لما نص عليه المشرع في الجرائم التقليدية، وهل يعاقب المشرع على شروع التام والناقص بالجريمة الإلكترونية كما فعل بالجرائم التقليدية؟

كما أشرنا أن السلوك الاجرامي هو النشاط المادي الذي يمكن ملاحظته وهو بالنتيجة الذي تسبب في أحداث الاعتداء والضرر، هذا فيما يتعلق بالأركان العامة للجريمة الجنائية التامة أو الشروع فيها أما الركن المادي في الجريمة الإلكترونية حيث يبدأ الركن المادي من الجاني مثلاً في تدمير معلومات، اختراق، نشر فيروسات ويتحقق الركن المادي في الجريمة الإلكترونية في وجود بيئة رقمية اي وجود الوسيلة التقنية(الحاسب الآلي)، والشبكة الإلكترونية وقد يكفي وجود الوسيلة التقنية لتحقيق من وجود ركن مادي ممثلاً بتحضير الحاسب الآلي من خلال وضع برامج لغايات الاختراق أو ضبط الحاسب الآلي، وإعادة لتحميل مواد غير قانونية مثل الصور الاباحية، أو حيازة ألعاب مقامرة، أو الشعوذة أو المخدرات أو إعداد برامج لنشر الفيروسات، فهذه جميعها تعتبر من الأعمال التحضيرية ما قبل التنفيذ بعرض الصور الإباحية أو بالإتجار بالمخدرات، أو بث الفيروسات في حواسيب أخرى من خلال شبكة الانترنت أو حيازة برامج للاختراق وفك التشفير، وعاقب المشرع الفلسطيني على هذه الاعمال على أساس أنّ الفاعل لا يصدر عنه فعل إلا بإرادته الحرة، وتعتبر هذه الاعمال قرينة الفعل المفترضة يمكن إثبات عكسها امام القضاء<sup>2</sup>، حيث أشار لذلك في نص المادة(26)<sup>3</sup>، فنلاحظ أن قرار بقانون مكافحة الجريمة الإلكترونية الفلسطيني قد جرم مجرد الحيازة لهذه الأدوات التي تستخدم ما قبل تنفيذ الجريمة الإلكترونية المتمثلة بالاختراق او فك التشفير بحد ذاتها جريمة.

<sup>1</sup>المادة 68 من قانون العقوبات الاردني رقم 16 لسنة 1960 والتي نصت: " الشروع: هو البدء في تنفيذ فعل من الأفعال الظاهرة المؤدية إلى ارتكاب جناية أو جنحة، فإذا لم يتمكن الفاعل من إتمام الأفعال اللازمة لحصول تلك الجناية أو الجنحة لحيلولة أسباب ال دخل إرادته فيها عوقب على الوجه الآتياإل إذا نص القانون على خلاف ذلك- 1 :الأشغال الشاقة المؤبدة أو المؤقتة من سبع سنوات إلى عشرين سنة إذا كانت عقوبة الجناية التي شرع فيها تستلزم الإعدام، وخمس سنوات من ذات العقوبة على الأقل إذا كانت العقوبة الأشغال الشاقة المؤبدة أو العتقال المؤبد- 2 .أن يحط من أية عقوبة أخرى مؤقتة من النصف إلى الثلثين"

<sup>2</sup>كامل السعيد، شرح الاحكام العامة في قانون العقوبات،مرجع سابق، ص184.

<sup>3</sup>نصت المادة (26) من قرار بقانون رقم 10 لسنة 2018 على: "كل من حاز بغرض الاستخدام جهازاً أو برنامجاً أو أي بيانات إلكترونية معدة او كلمة سر أو ترميز دول أو قدمها أو انتجها أو وزعها أو استوردها أو صدرها او روج لها . وذلك بغرض اختراق أي من الجرائم المنصوص عليها في هذا القرار بقانون يعاقب بالسجن مده لا تزيد على خمس سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار اردني ولا تزيد على خمسة آلاف دينار اردني او ما يعادلها بالعملة المتداولة قانونياً".

2- العنصر الثاني لركن الجريمة المادي النتيجة الجرمية: وهو الضرر الذي وقع ووفقاً لتقسيمات القانونيين والفقهاء فقد قسم القانونيين النتيجة الجرمية الى مدلولين الاول مادي وهي الاثار الظاهرة للعالم الخارجي والآخر قانوني، وهو العقوبة المنصوص عليها بنص القانوني عند حصول الاثار المادية والتي شملت الجرائم الناتجة عن الامتناع مثل امتناع الام عن ارضاع طفلها وبذلك تشمل الحماية القانونية للمصالح المحمية بنص القانون وسواء السلوك الجرمي بإتيان فعل أو عدمه فهو بالنتيجة افعال تمس منظومة المجتمع وامنه واستقراره، والنظام فيه باعتماد على الحق الذي يحميه القانون<sup>1</sup>، ومن وجهة نظر بعض الفقهاء بأن الجرائم أما أن تكون جرائم مادية والتي تكون نتيجتها محددة بنص القانون مثل الاغتصاب، القتل، الايذاء وأما أن تكون جرائم شكلية أي بمعنى يلزم لتحقيقها سلوك معين بدون أن تحصل النتيجة الضارة مثل حيازة سلاح بدون ترخيص، حيازة مخدرات أي أنها تشكل بحد ذاتها خطر، وتحقيق النتيجة الجرمية سواء كانت مقصودة أم بالخطأ وضع المشرع في قانون العقوبات رقم 16 لسنة 1960 العقاب الجزائي في حال تحقق النتيجة الجرمية أو كانت عند حد الشروع التام أو الناقص<sup>2</sup>.

تعد النتيجة الجرمية الحاصلة والمرتبطة بالنشاط المادي الذي اقترفه الفاعل، فهي النتيجة التي تعكس الجانب الملموس من الجريمة الإلكترونية لأنّ بتحقيق النتيجة الجرمية تظهر الجريمة الإلكترونية الى العالم الخارجي إلا ان هناك صعوبات قد تواجه المحققين فيها من حيث تحديد مكان وزمان الجريمة، فمثلاً ان يرتكب شخص من داخل فلسطين اختراق لشركة موجودة في سويسرا من خلال جهاز الخادم التابع للشركة فكيف لنا أن نحدد وقت ارتكاب الجريمة هل هي بتوقيت فلسطين بلد الفاعل، أو بتوقيت بلد المجني عليه سويسرا أو بتوقيت المنظم والمبرمج على الخادم المرتبط بحواسيب الشركة، وأي قانون واجب التطبيق في هذه الحالة، ومثال آخر لتحقيق النتيجة الجرمية في الجرائم الإلكترونية، والتي قد تؤدي إلى أضرار مادية اختراق حواسيب لبنك مصرفي، فإنّ نتيجة الاختراق هو الأثر الذي يحدثه بإحداث أضرار مادية في بيانات البنك سواء كان بحذفها وتغييرها أو محوها أو تعديلها، أو إلى ما غير ذلك أو اختراق مصنع أدوية لتغيير معايير ومواصفات دواء معين قد ينتج أثر مادياً بوقوع إصابات جسدية لمتناوليها، وقد تؤدي الجريمة الإلكترونية إلى إحداث أضرار معنوية يحققها شخص

<sup>1</sup> كامل السعيد، شرح الاحكام العامة في قانون العقوبات، مرجع سابق، ص 188-189.

<sup>2</sup> أحمد البراك وعبد القادر جرادة، الجريمة الإلكترونية في التشريع الفلسطيني دراسة تحليلية تأصيلية مقارنة، دار الشروق للنشر والتوزيع، رام الله، فلسطين، 2018، ص 62.

من خلال شبكة الانترنت، أو عرض سلوكيات تؤثر على فئة دينية معينة، مثل صور مشينة للرسول محمد صلى الله عليه وسلم اولسيدنا عيسى ابن مريم عليه السلام فهي تحدث أضراراً معنوياً .

### ثالثاً- الركن الثالث للجريمة هو(المعنوي)

هو الركن المرتبط بشخصية الجاني المتعلق بإرادة الجاني لتحقيق الفعل أو الامتناع ومسؤوليته من هذا السلوك الاجرامي الصادر عن ارادة حرة فيمثل الركن المعنوي بالعلم والارادة وللركن المعنوي صورتين الاولى تتمثل بالقصد الجنائي والثانية تتمثل على صورة الخطأ أو الإهمال وقلة الاحتراز فالركن المعنوي العلاقة التي تربط الركن المادي بعناصره الثلاث وشخصية الفاعل والتي تسمى بالقصد الجنائي وقد عرف القانون القصد الجنائي بأنه " العلم بعناصر الجريمة، واردة متجهة الى تحقيق هذه العناصر أو قبولها، وقد يتحقق الركن المعنوي في جريمة تحتوي بطاقة ائتمان، واستخدامها وسحب نقود غير مملوك للفاعل، وعرف الدكتور محمود نجيب حسني الركن المعنوي بأنه " العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني وهذه العلاقة هي محل الجريمة التي تستوجب العقاب وتوجيه لوم قانون من اجل معاقبته"<sup>1</sup>.

والقصد الجرمي له دور مهم بالتكليف القانوني السليم للجرائم الإلكترونية، والتعرف على شخصية الفاعل الجاني وتحديد النص القانوني الواجب التطبيق والذي يتناسب مع الجريمة المرتكبة، فالعلاقة السببية مثلاً من قام بالتعرف على فتاة واستدراجها واخذ صور لها ليقوم بابتزازها الكترونياً وجلب منفعة غير مشروعة سواء مادية أو جنسية ثم يقوم بنشر هذه الصور على مواقع التواصل الاجتماعي. فهنا قد ثبتت ان لسلوك الفاعل ضرر على المجني عليها بنشر صورها، والحاق ضرراً جسدياً فقد تقتل أو ضرراً معنوياً يمس سمعتها وكرامتها، وهذا ما يتمثل بالقصد الخاص من حصوله على الصور، وذلك لغايات قيام بفعل آخر سواء جنسياً أو مادياً(ابتزاز)<sup>2</sup>.

كما يوجد حالات لا يتوفر فيها القصد الخاص للجريمة مثلاً سرقة معلومات للاطلاع وليس بنية التملك والحيازة والتصرف فيها وليس للفاعل نية بحرمان المجني عليه من المعلومات الموجودة بداخل

<sup>1</sup> احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري(دراسة مقارنة)، دار النهضة العربية، الطبعة الأولى، 2010، ص116.

<sup>2</sup> احمد البراك وعبد القادر جرادة، الجريمة الالكترونية في التشريع الفلسطيني(دراسة تحليلية تأصيلية مقارنة)، دار الشروق للنشر والتوزيع ، رام الله ، فلسطين، سنة 2018،ص65.

جهازه الحاسوبي كما لم تتجه ارادته لتصرف بهذه المعلومات مهما بلغت قيمتها. ويرتبط القصد الجنائي والركن المعنوي بنسبة الضرر أي نية السرقة والتملك، أو نية الاطلاع دون الاضرار فالفاعل يعلم انه يخترق جهاز المجني عليه من أجل الحصول على معلومات، أو بيانات ذات قيمة لدى المجني عليه ولكن قصد الجاني فقط الاطلاع وليس استخدامها، وهذا يختلف فيما لو توجهت نية الفاعل الى اختراق جهاز المجني عليه من اجل محو أو إلغاء أو تعديل أو إعاقة أو تغيير بالمعلومات المملوكة للمجني عليه محدثاً أضرار.<sup>1</sup>

**الفرع الثاني: التحديات والصعوبات التي تواجه التصدي للجريمة الإلكترونية في التشريع الفلسطيني:**  
ومع تطور التكنولوجيا بمعدل لم يسبق له مثيل، أصبحت الجريمة الإلكترونية واسعة النطاق وكلما أصبحت حياتنا أكثر تكاملاً مع العالم الرقمي، ستكون هناك زيادة مقابلة في الأدلة الرقمية؛ لذلك يعد الدليل الرقمي أمراً أساسياً في التحقيقات التي يتم إجراؤها للكشف عن مرتكب الجريمة الإلكترونية وهذا يصاحبه العديد من التحديات منها، نجد ان هناك صعوبات وتحديات تعيق عمل سلطة التحقيق في الحصول على الدليل وتؤثر بشكل ملموس في السير باجراءات الملف التحقيقي، وهذه التحديات لا تنحصر بجانب بل هناك العديد من التحديات فمنها على الصعيد القانوني والتقني والموارد وصولاً الى التحديات على الصعيد السياسي

#### أولاً: التحديات التقنية<sup>2</sup> :-

وهي التحديات التي تعوق قدرة فرض القانون على العثور على المجرمين والمنظمات الإجرامية التي تعمل عبر الإنترنت وملاحقتهم قضائياً، وتتمثل التحديات التقنية ب:-

- 1- نوع الأجهزة الإلكترونية المتاحة وتطورها السريع الذي يؤثر على نوع البيانات التي يمكن استخراجها منها .
- 2- زيادة كمية البيانات المخزنة على الأجهزة المحمولة يجعل عملية استخراجها واستعادة المحذوف منها واستعراضها وتحليلها مهمة بحاجة إلى وقت كثير من الخبراء الفنيين.
- 3- نقص الممارسات والمبادئ التوجيهية القياسية لتحليل تلك البيانات.

<sup>1</sup> محمود نجيب حسني، النظرية العامة للقصد الجنائي، مصر، دار النهضة العربية، 1981، ص90.

<sup>2</sup> مقابلة شخصية مع مأموري الضبط القضائي الخبراء المختصين بقسم الجرائم الالكترونية في جهاز الشرطة المباحث العامة بتاريخ 2019/9/5 في رام الله-قيادة الشرطة.

4- البنية التحتية اللازمة لدعم تحقيق جنائي، خاصة بالنظر إلى الكم الهائل من البيانات الوصفية وراء هذا الإجرام الجنائي

5- ضعف الجاهزية ومزايا ومخاطر النقود الرقمية والانتشار المتزايد للبرامج الخبيثة والتحقق من هوية المستخدم والتقنيات الحديثة المستخدمة في إخفاء البيانات.

6- ظهور وتنامي الأنشطة الإجرامية الإلكترونية وتوسُّل مرتكبيها بتقنيات جديدة غير مسبوقه في مجال تكنولوجيا المعلومات والاتصالات يسرت لهم ارتكاب هذه الأنشطة داخل حدود الدولة وخارجها.

7- تخزين المعلومات أو البيانات المعالجة إلكترونياً خارج إقليم الدولة وضبط أدلة لإثبات جريمة كانت قد وقعت على أراضيها، وعلى الرغم من ضرورة التعاون الدولي وتضافر الجهود من أجل تفعيله إلا أن هناك العديد من العقبات التي تعترض سبيله من أبرزها: عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية، عدم وجود توافق بين قوانين الإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم، والنقص الظاهر في مجال الخبرة لدى الشرطة وجهات الادعاء والقضاء.

8- صعوبات في جمع الأدلة الرقمية وتتمثل :-

أ- **إخفاء الدليل:** نتيجة ضعف الأنظمة الرقابية يتمكن مرتكبوا الجرائم الإلكترونية من التسلل والعبث في النبضات والذبذبات الإلكترونية التي تسجل عن طريقها المعلومات والبيانات بغرض إحداث تغيرات في البيانات والمعلومات والتلاعب في منظومة الحاسب الآلي ومحتوياته، أو دس برامج خاصة ضمن برنامجه فلا يشعر بها القائمون بالتشغيل، ومن ثم إخفاء ما قاموا به أو محو الدليل عليه، بحيث يتعذر إعادة عرض أعمال التسلل والدخول، وهكذا يستطيع الجناة في الجرائم الإلكترونية إخفاء جرائمهم وطمس آثارها في وقت قياسي من القصر وقبل أن تصل إليه سلطة التحقيق ، الأمر الذي يؤدي إلى صعوبات تعيق إجراءات التحقيق الرامية إلى الوصول إلى دليل.

ب- **غياب الدليل ضد متهم معين:** تختلف الجريمة الإلكترونية عن الجريمة التقليدية، بأن الجريمة الأولى لا تحتاج لارتكابها أي من أنواع العنف إلا فيما ندر، وإنما هي معالجة بواسطة إدخال بيانات معلومات خاطئة أو محظورة ضمن البرامج، أو تحريف أو تعديل البيانات والمعلومات المخزنة أصلا في الحاسب الآلي، أو إرسال برامج تخريبية أو التجسس على البيانات والمعلومات المخزنة ونسخها واستخدام الاساليب اللغوية لاستدراج الضحية مثل ابتزاز واستغلال الاطفال، وإذا ما صادف واكتشفت هذه الأفعال وجمعت الأدلة على وقوعها، فإن هذه الأدلة قد لا تفصح عن صلة شخص معين بالجريمة المرتكبة، نظرا لأن معظم نظم الحاسب الآلي لا تسمح للمراجعين والفنيين بالتتابع العكسي

لمسار مخرجاتها، علاوة على صعوبة تتبع الآثار الإلكترونية ومراجعة وفحص الكم الهائل من البيانات والمعلومات المدرجة بالأنظمة، وتعتمد الجناة إلى إخفاء هويتهم.<sup>1</sup>

ت إعاقة الوصول إلى الدليل: يضع الجاني في بعض الحالات عقبات فنية لمنع كشف جريمته وضبط أدلتها باستخدام تقنيات التشفير أو كلمة السر، وذلك بقصد حجب المعلومة عن التداول العام ، ومنع الغير بما فيه أجهزة الرقابة من الوصول غير المشروع إلى البيانات والمعلومات المخزنة أو التلاعب فيها.<sup>2</sup>

ج-نقص في المعرفة التقنية الحديثة والمتجددة لدى القائمين بالبحث والتحقيق في هذه الجرائم ، مما يجعل منهم غير قادرين على أداء واجبهم على الوجه المطلوب ، إذ إن نقص الخبرة والكفاءة ، سواء في أجهزة الشرطة أو الادعاء يعد من الأسباب الرئيسية في الإخفاق في كشف الجرائم الإلكترونية وجمع أدلتها ، ويظهر ذلك بشكل واضح في الدول التي لا تزال تتعامل مع هذه الجرائم بإجراءات البحث والتحقيق التقليدية وتفترق سلطاتها الضبطية والقضائية للأجهزة التقنية المتطورة في متابعة الجرائم الإلكترونية وضبط أدلتها، ويدهيا أنه في حالة عدم توافر التأهيل والخبرة وشحّ الإمكانيات التقنية على وجه الخصوص، فلا يمكن أن نتصور أي وجه للتعامل مع هذه الجرائم، وبالتالي ستكون النتائج سلبية لا محالة.

#### ثانيا: التحديات القانونية

الصعوبات والتحديات في تطبيق القوانين المتعلقة بالجرائم الإلكترونية حيث واجهت الدول والحكومات الكثير من التحديات لتطبيق القوانين المتعلقة بالجرائم الإلكترونية وذلك لأسباب عديدة منها:

ندرة الإعلان أو الإبلاغ عن الجريمة الإلكترونية نظرا لما يتمتع به المجتمع الفلسطيني من خصوصيه تتعلق بالعادات والتقاليد يجعل أمر الإبلاغ في هذا النوع وخاصة في الجرائم التي تمس بالشرف والسمعة والآداب العامة امر صعبا.

▪ صعوبة العلم بوقوع الجريمة.تعتبر الجريمة الإلكترونية جريمة غير مادية (غير ملموسة) وهذا يعيق جهات التحقيق في ملاحقتها ومتابعتها كونها لا تترك اثار مادية.

<sup>1</sup>سونيا حماد ، وحده الجرائم الإلكترونية ، مختبر الأدلة الإلكترونية ، مقابلة شخصية بتاريخ 20\10\2019 .

<sup>2</sup>لقاء مع الخبير الكندي باترك بورشة عمل نظمت في فندق الجراندي بارك بتاريخ 16\10\2019.

- صعوبة تعيين الجانيون ذلك نظرا لارتكابها من خلال وسيط وهو الأجهزة الإلكترونية وشبكة الإنترنت فالجاني بالنسبة لهذه الجريمة معطيات وبيانات رقمية يتم ترجمتها الى بيانات مقروءة ومفهومة.
- صعوبة القبض على الجاني. وتعقبا على ما سبق (صعوبة تعين الجاني) يجعل أمر تتبع الجاني والقبض عليه أكثر صعوبة من الجريمة التقليدية
- التطور الإلكتروني والتكنولوجي السريع. ان سبب انتشار التكنولوجيا في المجتمع الفلسطيني بشكل سريع أدى الى استخدامها من كافة اعمار وشرائح المجتمع وهذه الشرائح ليس لديها جميعها العلم الكافي بطرق الأمان في استخدام الانترنت مما يسهل على الجاني ارتكاب جريمته.
- بعد الجاني عن مسرح الجريمة الإلكترونية
- تفاوت أعمار ودوافع مرتكبي هذه الجرائم.
- سريان القانون من حيث الزمان والمكان
- عدم وجود لوائح تنفيذه توضح القانون العام لمكافحة الجرائم الإلكترونية في فلسطين. وخاصة أن قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وفيما يتعلق بالأحكام الإجرائية يحتاج الى لوائح تنفيذية تساعد على ضبط الدليل وتقادي بعض الإجراءات التي يمكن ان تؤدي الى محو الدليل أو تدميرها.
- عدم وجود قضاء فلسطيني متخصص لمكافحة هذه الجريمة مما يجعل القضاء الفلسطيني غير قادر على التعامل مع أدلة هذه الجريمة بالشكل المطلوب.

### ثالث: تحديات الموارد

- التحديات المادية والبشرية - قلة عدد الأفراد المؤهلين لإجراء التحقيقات ونقص الموارد لتوفير التدريب المستمر للمحققين وللخبراء الفنيين وتزويدهم بالبرامج المناسبة للاستخراج والتحليل التي تختصر جزء من وقت جمع واستخراج وتحليل الدليل الرقمي.
- ضعف سلم الرواتب الحكومي لمن يمكن توظيفهم مما يؤدي لعدم امكانية استقطابهم حيث انهم يتقاضون رواتب عالية في الشركات الخاصة.
- في كثير من الأحيان الأشخاص الذي يجدون مواجهة هذه الجرائم والتي يمكن توظيفهم هم بالأصل قاموا بارتكاب جرائم إلكترونية ولا يصلح توظيفهم<sup>1</sup>.

<sup>1</sup>مقابلة مع سامر الهندي 2018\2\12 ومقابلة مع خبير الكروني مبرمج عبدالله السوادي بمقر مشروع قطاع العدالة جيسابالماسيون.

## ✓ التحديات السياسية<sup>1</sup>:

والتي تتمثل بانتشار الشرائح الاسرائيلية بشكل واسع واعتماد عدد كبير من مرتكبي الجرائم عليها وسيطرت الاحتلال على مداخل الانترنت في فلسطين .

1. ضعف القدرة على اجبار شركات الاسرائيلية لتقديم المعلومات المطلوبة في مجال مكافحة الجرائم الإلكترونية وتشجيعهم على تطوير التكنولوجيا لديهم للتلاؤم مع المتطلبات الأساسية للسيطرة والتحكم في تلك الجرائم

2. عدم القدرة على السيطرة على الفضاء الالكتروني الفلسطيني بشكل كامل.

3. عدم السيطرة على الحالات التي يكون أحد اطرافها في قطاع غزه أو خارج حدود الدولة الفلسطينية.

4. عدم سماح سلطات الاحتلال على ادخال برامج تحقيقه تساعد على مواجهه هذا الجريمة.

نخلص في هذا الفصل لبيان الطبيعة القانونية للجريمة الإلكترونية من حيث تعريفها وخصائصها ومن هو مرتكبها واهم الخصائص التي يتمتع بها وعن اهم الجهود المبذولة لمكافحة الجريمة الإلكترونية على الصعيد الدولي والوطني، وبعد ذلك لا بد من التساؤل ما هي الاجراءات التي يجب اتباعها لمكافحة الجريمة الإلكترونية وهل تتوافق هذه الاجراءات مع الاحكام العامة في قانون الاجراءات الجزائية؟

للإجابة على ذلك لا بد من بيان الاحكام المتبعة في مكافحة الجريمة الإلكترونية (الفصل الثاني) وبعد ذلك الانتقال لبيان الاحكام الاجائية في مرحلة الاستدلال والتحقيق الابتدائي(مبحث اول) وصولا الى مرحلة المحاكمة (مبحث ثاني)

---

<sup>1</sup> جميع التحديات هي من خلال مقابلات وورشات تم اجراها مع مدراء المختبرات ووحدة الجرائم الالكترونية بالشرطة المدنية وقوى الامن ملخص مؤتمر الامن الوقائي بعنوان الفضاء الالكتروني في ظل تطور الجريمة والارهاب المؤتمر الامني الرابع المنعقد باريجا بالفترة 22-23\4\2019.

### الأحكام الاجرائية لمكافحة الجريمة الإلكترونية في التشريع الفلسطيني

إن الجانب الاجرائي للجريمة الكترونية يعتبر الجزء الاهم في مكافحة هذه الظاهرة الخطيرة التي باتت تهدد كيان المجتمع، فتظهر هذه الأهمية ابتداء من تنظيم محضر تحري واستدلال من قبل مأموري الضبط القضائي المتخصصين تحت إشراف النيابة العامة ومتابعتها، لكل إجراء يتخذ من قبل الضابطة القضائية بقراراً منها في هذا النوع من الجرائم للوصول إلى ما يسمى بالدليل الرقمي المثبتات في العالم الافتراضي الذي أصبحنا نعيش فيه وبذات الوقت الحفاظ على التوازن الاجرائي للمصلحة العامة، والحفاظ على خصوصية الأفراد وحياتهم الخاصة من خلال المواجهة التشريعية للجريمة الكترونية والتخصصية التي فرضها المشرع الفلسطيني لمأموري الضبط القضائي وانشاء مختبرات لمتابعة وملاحقة الجريمة الإلكترونية من خلال عرض اقسام المختبرات الإلكترونية المنشأة بقوى الامن وهي مثماتلة مع كافة دول العالمي لاعتمادها المعايير والمقاييس الدولية من الناحية التقنية الاجرائية، ومن خلال تبني اجراءات خاصة متعلقة بالتحقيق الجنائي، وصولاً الى تحقيق الغاية من متابعة الجرائم الا وهي محاكمة المجرمين .

## المبحث الأول: الاجراءات التحقيقية في الجريمة الإلكترونية

### المطلب الأول: التحقيق التمهيدي ((البحث والاستدلال))

تعد أعمال البحث والاستدلال عن الجرائم التي يقوم بها موظفو الضابطة القضائية من الأعمال المهمة التي يجب النظر إليها بقدر من الاهتمام لا يقل عن ذلك القدر الذي ينظر به إلى بقية أعمالهم، ونظرا لخطورة إجراءات التحري، فإنه ينبغي الالتزام بمجموعة من الشروط والقواعد الإجرائية من قبل مأمورو الضبط القضائي أثناء قيامهم بمهامهم. فمهمة البحث ليست من الأمور السهلة، بل تتطلب من مأموري الضبط القضائي كثير من الجهد والمشاق والخبرة والذكاء في محاولة لانتزاع الحقيقة وذلك في إطار الشرعية القانونية<sup>1</sup>.

يشكل مأموري الضبط القضائي مع النيابة العامة ما يعرف "بالضابطة القضائية" حيث يقومون معا على حفظ النظام العام، والأمن والاستقرار في المجتمع، وملاحقة الجناة وجلبهم أمام القضاء للمحاكمة، من خلال مجموعة من الإجراءات والقواعد التي تحكم الدعوى الجزائية في تحريكها ومباشرتها، والتي يكون أساسها ما يعرف بمرحلة جمع الاستدلالات، والتي يعود الاختصاص فيها لمأموري الضبط القضائي، والتي تعتبر الأساس الذي تبنى عليه الدعوى الجزائية. فمرحلة جمع الاستدلالات لا غنى عنها للتحقيق الابتدائي، حيث تعمل على إعداد عناصر التحقيق، والتي يكون هدفها التأكد من مدى كفايتها في إثبات وقوع الجريمة ونسبتها إلى مرتكبيها بالإضافة إلى التحفظ على الآثار المادية للجريمة وحمايتها من الضياع والعبث بهدف تسهيل مهمة سلطة التحقيق في جمع الأدلة ومعرفة الجناة وتقديمهم للمحاكمة.

نجد ان التشريعات الجزائية في فلسطين خلت من وجود تنظيم خاص ومختص بتنظيم اعمال ومهام مأمورو الضبط القضائي بل ترك المشرع ذلك دون قيد او شرط وهذا ما نصت عليه المادة (19) من قانون الاجراءات الجزائية الفلسطيني في متن فقرتها الثانية والتي نصت في على أن "يتولى مأمورو الضبط القضائي البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى"، ومن هنا لا بد من توضيح المقصود بعملية البحث والاستدلال ومن الاشخاص القائمين عليها وما هي المهام الموكلة لهم وما هي حدود صلاحيتهم المكانية والنوعية، وكيفية تنظيم هذه

1محمد علي الحلبي، الوسيط في شرح قانون المحاكمات الجزائية، عمان ، دار الثقافة للنشر والتوزيع، 1996، ص 189.

المرحلة وسواء بالرجوع الى القواعد العامة والمتمثلة بقانون الاجراءات الجزائية أو التشريعات الجزائية المتخصصة؟

وللإجابة على ذلك سنعمل على بيان المقصود بمرحلة الاستدلال وماهيتها والاشخاص القائمين عليها ومن ثم تفرقتها وفقا لما ورد في الاحكام العامة المطبقة على الجرائم التقليدية(فرع اول)، وبيان المقصود بمرحلة الاستدلال في التشريعات المتخصصة والمطبقة على الجرائم المستحدثة وحيث ان الجريمة الإلكترونية تميزت بوجود تشريع متخصص بها سنعمل على بيان مرحلة الاستدلال بها وما يترتب عليها من اثار (فرع ثاني).

### الفرع الاول: البحث والاستدلال في الجرائم التقليدية

يشكل مأموري الضبط القضائي مع النيابة العامة ما يعرف "بالضابطة القضائية" حيث يقومون معا على حفظ النظام العام والأمن والاستقرار في المجتمع وملاحقة الجناة وجلبهم أمام القضاء للمحاكمة من خلال مجموعة من الإجراءات والقواعد التي تحكم الدعوى الجزائية في تحريكها ومباشرتها والتي يكون أساسها ما يعرف بمرحلة جمع الاستدلالات، والتي يعود الاختصاص فيها لمأموري الضبط القضائي، والتي تعتبر الأساس الذي تبنى عليه الدعوى الجزائية. فمرحلة جمع الاستدلالات لا غنى عنها للتحقيق الابتدائي، حيث تعمل على إعداد عناصر التحقيق، والتي يكون هدفها التأكد من مدى كفايتها في إثبات وقوع الجريمة ونسبتها إلى مرتكبيها بالإضافة إلى التحفظ على الآثار المادية للجريمة وحمايتها من الضياع والعبث بهدف تسهيل مهمة سلطة التحقيق في جمع الأدلة ومعرفة الجناة وتقديمهم للمحاكمة.

تعد أعمال البحث والاستدلال عن الجرائم التي يقوم بها موظفو الضابطة القضائية من الأعمال المهمة التي يجب النظر إليها بقدر من الاهتمام لا يقل عن ذلك القدر الذي ينظر به إلى بقية أعمالهم، ونظرا لخطورة إجراءات التحري، فإنه ينبغي الالتزام بمجموعة من الشروط والقواعد الإجرائية من قبل مأموري الضبط القضائي أثناء قيامهم بمهامهم. فمهمة البحث ليست من الأمور السهلة، بل تتطلب من مأموري الضبط القضائي كثير من الجهد والمشاق والخبرة والذكاء في محاولة لانتزاع الحقيقة وذلك في إطار الشرعية القانونية<sup>1</sup>.

1. محمد علي الحلبي، الوسيط في شرح قانون المحاكمات الجزائية، مرجع سابق، ص 1.

نجد ان التشريعات الجزائية في فلسطين خلت من وجود تنظيم خاص ومختص بتنظيم اعمال ومهام مأمورو الضبط القضائي بل ترك المشرع ذلك دون قيد او شرط وهذا ما نصت عليه المادة (19) من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 في متن فقرتها الثانية والتي نصت في على أن "يتولى مأمورو الضبط القضائي البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى".<sup>1</sup>

تمر الدعوى الجزائية بثلاث مراحل اساسية، الاولى مرحلة البحث والاستدلال والثانية مرحلة التحقيق الابتدائي وصولا الى المرحلة الاخيرة والمتمثلة بمرحلة المحاكمة العادلة، ومرحلة الاستدلال هي أولى تلك المراحل والتي تسبق عادة الدعوى الجنائية وهي تعتبر ممهدة لها. وقد اعتبر بعض الفقهاء بأن البحث والاستدلال لا تعد من مراحل الدعوى الجزائية كون الدعوى الجزائية لا تتحرك الا بالبدهء بسلطة التحقيق وهذه السلطة مخولة للنياحة العامة فقط ، فهذه المرحلة تبدأ بتتبع وتجميع العناصر والأدلة المادية التي تثبت وقوع الفعل الإجرامي من خلال اعضاء مأموري الضبط القضائي، ونصت المادة (21) من قانون الإجراءات الجزائية الفلسطيني:- "يكون من مأموري الضبط القضائي:

1. مدير الشرطة ونوابه ومساعدوه ومديرو شرطة المحافظات والإدارات العامة؛
2. رؤساء المراكب البحرية والجوية.
3. الموظفون الذين خولوا صلاحيات الضبط القضائي بموجب القانون"<sup>2</sup>.

نجد أن هذه الفئات التي منحها المشرع الفلسطيني في قانون الاجراءات الجزائية صفة مأموري الضبط القضائي ولكن بتدقيق الفقرة الرابعة من المادة 21 من قانون الاجراءات والتي جاءت على الاطلاق لا الحصر وبالتالي يمكن تحويل صفة مأموري الضبط القاضي لأشخاص اخرين غير الورادين في المادة 21 من قانون الاجراءات ومثال ذلك، اعضاء جهاز المخابرات العامة<sup>3</sup>، واطعاء جهاز الامن الوقائي<sup>4</sup>،.... وغيرهم من مفتشي الصحة واطعاء الدفاع المدني واطعاء الضابطة الجمركية واطعاء هيئة مكافحة الفساد.

<sup>1</sup> انظر إلى نص المادة (19) من قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001.

<sup>2</sup> المادة (21) من قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001.

<sup>3</sup> المادة (12) من قانون جهاز المخابرات العامة رقم 17 لسنة 2005 .

<sup>4</sup> المادة(7) من قرار بقانون الامن الوقائي رقم 11 لسنة 2007 .

وبناء على كل ما سبق يمكننا تعريف فئة مأموري الضبط القضائي بأنهم: "مجموعة من الموظفين كلفهم المشرع بتنفيذ مهمة الضبط القضائي"<sup>1</sup>.

وقضت المادة (19) من قانون الاجراءات الجزائية رقم 3 لسنة 2001 ما يلي "يتولى اعضاء النيابة العامة مهام الضبط القضائي والاشراف على ماموري الضبط كل في دائرة اختصاصه "

"ويتولى ماموري الضبط القضائي البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم التحقيق "

### صلاحيات مأمور الضبط القضائي في الجرائم التقليدية:

كما ورسمت المادة 22 من ذات القانون المهام المناطة بمأموري الضبط القضائي والتي تعتبر اساسا للاختصاصات الملقاة على مأموري الضبط القضائي بما فيها الواجبات الملقاة على عاتقهم وقد اوضحت المادة 22 ان جمع الاستدلالات يتركز على اجراء الكشف والمعانية والمشاهدة والضبط والتحفظ على الاثار المادية وسماع افادات الشهود والاستعانة بالخبراء المختصين دون حلف يمين وهو ما يميز الاجراءات الاستدلالية المناطة بمأموري الضبط القضائي تمهيدا لبدء بالإجراءات التحقيق الابتدائي لدى اعضاء النيابة العامة. وقد الزمت المادة المذكورة بان يقوم مأموري الضبط القضائي بأثبات جميع الإجراءات الاستدلالية في محاضر رسمية موقعة من منظميها ومن المعنيين بها. فوفقا للتشريعات المعاصرة كان لابد من إسناد مهمة التحري والاستدلال لجهاز الضبط القضائي المتمثل بمأموري الضبط القضائي ليعاون النيابة العامة التي تشرف على أعمالهم الوظيفية للقيام بالبحث والتحري عن الجرائم المرتكبة فالعلاقة بينهما تخضع لمفهوم التبعية الوظيفية وفقا لما نصت عليه المادة 20 فقرة 1 من قانون الاجراءات الجزائية رقم 3 لسنة 2001م.

وتختلف الاختصاصات التي يقوم بها مأموري الضبط القضائي وفقا لما ورد في قانون الإجراءات الجزائية الفلسطيني فالمادة(2/19) جاءت : "يتولى مأمورو الضبط القضائي البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى". وعلى مأمور الضبط القضائي في سبيل القيام بأعمال التحري والبحث، قبول البلاغات والشكاوي التي ترد إليهم بخصوص الجرائم، ويجب عليهم عرضها على النيابة بدون تأخير، وعليهم القيام بالأعمال اللازمة من أجل تسهيل مهمة التحقيق، مثل إجراء المعانية والكشف وكذلك يحق لهم الاستعانة بالخبراء، وسماع الشهود ولكن بدون

<sup>1</sup> معوض عبد التواب، الموسوعة الجنائية الشاملة في التعليق على نصوص قانون الإجراءات الجنائية المصري،(الجزء الأول)، القاهرة، دار الفكر العربي، 1998، ص256.

حلف يمين، واتخاذ ما يلزم من الوسائل للحفاظ على أدلة الجريمة من الضياع أو من العبث بها<sup>1</sup>. وحتى تكتسب إجراءاتهم الحجية يجب أن يتم تثبيتها بمحاضر رسمية وتوقيعها من مأموري الضبط القضائي ومن المعني بها وعملاً بأحكام المادة 212 و213 من قانون الإجراءات الفلسطينية جميع محاضر جمع الاستدلالات التي ينظمها مأموري الضبط القضائي الصحيحة شكلاً وموضوعاً من حيث الاختصاص المكاني والوظيفي منتجا لآثارها القانونية ولها قوة ثبوتية وحجية إلى أن يثبت ما ينفىها ولكن لا تعتبر دليلاً قانونياً كاملاً يمكن استناد قاضي الموضوع عليه في حكم الإدانة ولكنها تلعب دوراً مهماً وأساسياً لإعداد القواعد التي تبنى عليها الإجراءات التحقيقية من قبل النيابة العامة، فالهدف الرئيس من وراء تنظيم محضر جمع الاستدلالات هو للحصول على الإيضاحات والمعلومات اللازمة لبدء أعمال التحقيق، وبناء الملف التحقيقي وفقاً للقانون والأصول من قبل النيابة العامة صاحبة الولاية في تحريك الدعوى الجزائية وممثلة عن الحق العام وفقاً لنص المادة 1 من قانون الإجراءات الجزائية رقم 3 لسنة 2001 .

إذ تكمن أهمية الإجراءات الجدية المتخذة من قبل مأموري الضبط القضائي بمساندة النيابة العامة بالوصول إلى الأدلة القانونية وبناء الملف التحقيقي وإحالته إلى المحكمة المختصة الجهة القضائية والتي بدورها ووفقاً لقناعتها تقدر قوة الإجراءات السابقة للتحقيق والاختصاص بها .

فما سبق تم عرض الإجراءات الإلزامية وكأصل عام لمأموري الضبط القضائي مما يدل على أن هذه الإجراءات ليست خياراً أمام مأمور الضبط القضائي وفقاً لنص المادة 22 من قانون الإجراءات الفلسطينية من تنظيم محضر جمع الاستدلالات من عدمه بل أنه ملزم بإرسال جميع الإجراءات التي قام بها إلى النيابة العامة التي لها سلطة التصرف وتحريك الدعوى العمومية من عدمه وفقاً لسلطتها التقديرية كما ولها أن تكتفي فقط بمحضر التحري والاستدلال وإحالة الملف إلى محكمة الموضوع للبحث

---

1- نص المادة (22) من قانون الإجراءات الجزائية الفلسطينية على أنه: "وفقاً لأحكام القانون على مأموري الضبط القضائي القيام بما يلي: 1. قبول البلاغات والشكاوى التي ترد إليهم بشأن الجرائم وعرضها دون تأخير على النيابة العامة؛ 2. إجراء الكشف والمعينة والحصول على الإيضاحات اللازمة لتسهيل التحقيق، والاستعانة بالخبراء المختصين والشهود دون حلف يمين؛ 3. اتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة؛ 4. إثبات جميع الإجراءات التي يقومون بها في محاضر رسمية بعد توقيعها منهم ومن المعنيين بها".

- وفقاً لأحكام القانون على مأموري الضبط القيام بما يلي: " 1- قبول البلاغات والشكاوى التي ترد إليهم بشأن الجرائم وعرضها دون تأخير على النيابة العامة؛ 2- إجراء الكشف والمعينة والحصول على الإيضاحات اللازمة لتسهيل التحقيق والاستعانة بالخبراء المختصين والشهود دون حلف يمين؛ 3- اتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة؛ 4- إثبات جميع الإجراءات التي يقومون بها في محاضر رسمية بعد توقيعها منهم ومن المعنيين بها".

فيها عملاً بأحكام المادة 53<sup>1</sup> من ذات القانون يعتمد على جدية ودقة ما موري الضبط القضائي. مثل قضايا المرور فإذا عاين مأمور الضبط القضائي مكان الحادث واعد تقرير الحادث وسمع افادة الشهود فان الملف يصبح مكتملاً ونستطيع ان نحيله بلائحة اتهام الى المحكمة المختصة وكذلك الامر فيما يتعلق بالحاق ضرر بمال الغير ما ان قام مأموري الضبط القضائي بالكشف ومعاينة المكان وتنظيم تقرير الواقعة وسماع الشهود وضبط الاداة التي استخدمت مثلاً بتكسير شبابيك منزل المجني عليه والاضرار التي لحقت نكون امام محضر جمع استدلالات وافٍ نستطيع احالته الى المحكمة المختصة الا انه لا يجوز باي حال من الاحوال الاكتفاء في محضر جمع الاستدلالات للجرائم التي تخضع لمحكمة البداية ومحكمة الجنايات الكبرى لخطورتها ولضرورة اجراء التحقيق فيها من قبل اعضاء النيابة العامة<sup>2</sup>.

ويختلف الاختصاص النوعي لمأموري الضبط القضائي وفقاً لما إذا كانوا من ذوي الاختصاص العام أو الخاص.

- **فالاختصاص النوعي الخاص** يمارسه مأمورو الضبط القضائي ذوو الاختصاص الخاص، ويقتصر على جرائم معينة تتعلق بأعمال ووظائفهم، ولهذا يكون لهؤلاء الأشخاص كيان خاص يميزهم عن غيرهم. فمفتش الصحة مثلاً يختص بضبط الجرائم المتعلقة بالصحة العامة ولا يختص بضبط الجرائم الواقعة على امن الدولة ولو وقعت ضمن نطاق اختصاصه، ولو قام بتنظيم محضر فلا تتعدى قيمته سوى أن يكون بلاغ.

- **في حين الاختصاص العام** يمارسه مأموري الضبط القضائي ذوي الاختصاص العام، حيث أن صلاحياتهم تشمل جميع الجرائم، ما دام القانون أضاف عليهم تلك الصفة بدون أي قيد يحد من صلاحيتهم، وعليه يكون لمأموري الضبط القضائي ذوي الاختصاص العام ضبط كافة الجرائم ومن ضمنها الجرائم التي تدخل ضمن صلاحيات مأموري الضبط القضائي ذوي الاختصاص الخاص

- **كما ويكون لمأموري الضبط القضائي اختصاص مكاني** لا يجوز الخروج عنه وهذا ما أكدته المادة (163)<sup>3</sup> من قانون الإجراءات الجزائية، فلا تكون العبرة بمحل الاجراء المتخذ وانما تكون بالنطاق التي أوردتها المادة أعلاه، وبالتالي مباشرة افراد الضابطة القضائية لأي اجراء من اجراءات الضبط القضائي خارج النطاق المكاني وكان هذا الاجراء متصل بجريمة وقعت ضمن نطاق

<sup>1</sup>المادة (53) من قانون الإجراءات الجزائية الفلسطيني والتي نصت: إذا رأت النيابة العامة في مواد المخالفات والجنح أن الدعوى صالحة لإقامتها بناءً على محضر جمع الاستدلالات تكلف المتهم بالحضور مباشرة أمام المحكمة المختصة.

<sup>2</sup>المادة 212 من قانون الإجراءات الجزائية الفلسطيني والتي نصت على: "تعتبر المحاضر التي ينظمها مأمورو الضبط القضائي في الجنح والمخالفات المكلفون بإثباتها بموجب أحكام القوانين حجة بالنسبة للوقائع المثبتة فيها إلى أن يثبت ما ينفيها".

<sup>3</sup>المادة 163 من قانون الإجراءات الجزائية الفلسطيني والتي نصت: "يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة، أو الذي يقيم فيه المتهم، أو الذي يقبض عليه فيه".

اختصاص مأموري الضبط القضائي المكاني ولم يكن المتهم يقيم في هذا النطاق المكاني او لم يقبض عليه فيه، فيعد الاجراء المتخذ من قبل مأموري الضبط القضائي من ضمن اختصاصاتهم الاصلية<sup>1</sup>.  
والتساؤل الذي يثور الآن من هي الجهة المسؤولة عن رقابة صحة أعمال مأموري الضبط القضائي ؟

حدد قانون الاجراءات الجزائية باعتباره الاحكام العامة لصلاحيات واختصاصات مأمورو الضبط القضائي، في مباشرتهم لأعمال الاستدلال والتحقيق، وتخضع أعمال الاستدلالات عموماً ومنها إجراء التحريات لرقابة النيابة العامة بوصفها سلطة تحقيق ثم للمحكمة المختصة، و نصت المادة (1/20) على ان مهمة الاشراف على اعضاء ومأموري الضبط القضائي هي من صلاحية النائب العام<sup>2</sup>، فالتبعية هنا تبعية وظيفية متعلقة بمرحلة الاستدلال ولا تقتصر على الصلاحيات الاصلية لمأموري الضبط القضائي بل تمتد للصلاحيات والاستثنائية

فالأصل قيام مأموري الضبط القضائي اثناء عملهم بالالتزام بمهامهم الموكلة اليهم بموجب احكام القانون ولكن منح المشرع لهذه الفئة صلاحيات استثنائية افصحت المجال لمأموري الضبط القضائي للتوسع في صلاحيتهم وهذا ما نجده في نص المادة(26)<sup>3</sup> والمادة(27)<sup>4</sup> من قانون الاجراءات الجزائية في حالة التلبس بالجرائم والواجبات الموكلة لهم، ولم يقتصر الامر على حالة التلبس باعتبارها من المهام الاستثنائية الممنوحة لمأموري الضبط القضائي بل امتد إلى النذب القضائي في حالات معينة وهذا ما نصت عليه المادة(2/55) من قانون الإجراءات الجزائية الفلسطيني والتي نصت على: "لنائب العام أو وكيل النيابة العامة المختص تفويض أحد أعضاء الضبط القضائي المختص بالقيام بأي من

---

<sup>1</sup> ساهر إبراهيم شكري الوليد، شرح قانون الإجراءات الجزائية الفلسطيني،(الجزء الأول)،فلسطين، مكتبة غزه المركزية ، 2009،ص 268.

<sup>2</sup> المادة1/20 من قانون الإجراءات الجزائية الفلسطيني والتي نصت على: "يشرف النائب العام على مأموري الضبط القضائي وهم يخضعون لمراقبته فيما يتعلق بأعمال وظيفتهم".

<sup>3</sup> المادة 26 من قانون الإجراءات الجزائية والتي نصت على: " تكون الجريمة متلبساً بها في إحدى الحالات التالية :1. حال ارتكابها أو عقب ارتكابها ببرهه وجيزة؛إذا تبع المجني عليه مرتكبها أو تبعته العامة بصخب أو صياح أثر وقوعها؛إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملاً آلات أو أسلحة أو أمتعة أو أوراقاً أو أشياء أخرى يستدل منها على أنه فاعل أو شريك فيها، أو إذا وجدت به في هذا الوقت آثار أو علامات تفيد ذلك".

<sup>4</sup> المادة (27) من قانون الإجراءات الجزائية الفلسطيني والتي نصت على: " يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى مكان الجريمة، ويعاين الآثار المادية لها ويتحفظ عليها، ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، ويسمع أقوال من كان حاضراً أو من يمكن الحصول منه على إيضاحات في شأن الجريمة ومرتكبيها، ويجب عليه أن يخطر النيابة العامة فوراً بانتقاله، ويجب على عضو النيابة المختص بمجرد إخطاره بجناية متلبس بها الانتقال فوراً إلى مكان الجريمة".

أعمال التحقيق في دعوى محددة، وذلك عدا استجواب المتهم في مواد الجنايات" ويشترط ان يكون التفويض خطياً.

### الفرع الثاني: مرحلة جمع الاستدلالات في الجريمة الإلكترونية

رجوعاً الى ذي بدء وبعد بيان التفرقة ما بين مأموري الضبط القضائي من ذوي الاختصاص العام والاختصاص الخاص، وكون ان هذه الدراسة تقوم على البحث في الجريمة الإلكترونية والمراحل التي تمر بها من الاستدلال وصولاً للتحقيق الابتدائي نهاية بالمحاكمة العادلة وكون ان هذه الجرائم قد خصها المشرع بتشريع قانوني خاص بها بموجب قرار بقانون رقم 10 لسنة 2018م، فلا بد من طرح عدة تساؤلات وهي هل اختلفت الإجراءات المتابعة من قبل مأموري الضبط القضائي في الجرائم التقليدية عنها بالجرائم الكترونية؟ وما الذي أضافه قرار بقانون الجرائم الإلكترونية على محضر جمع الاستدلالات المناط بمأموري الضبط القضائي؟

ولإجابة على هذه التساؤلات لا بد من بيان المقصود بمرحلة الاستدلال في الجريمة الإلكترونية، ومن القائمين عليها، وما هي المهام الموكلة لهم، وهل تتفق والصلاحيات الممنوحة بموجب الأحكام العامة لمأموري الضبط القضائي أم تتعدها، وسنوضح ذلك فيما يلي.

نصت المادة 3 من القرار بقانون رقم (10) لسنة 2018 "تتشأ وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية" وتتولى النيابة العامة الإشراف القضائي عليها كل في دائرة اختصاصه" ومن خلال النص المذكور فقط انط المشرع ووجب في ذات الوقت تنشأ وحدة متخصصة وهي التي تتمثل بالمختبر الجنائي الالكتروني وقد اصاب المشرع بالزام الشرطة المدنية وقوى الامن بذلك فاذا عدنا الى اختصاص كلا من الاجهزة الامنية باعتبارهم يتمتعون بصفة الضابطة القضائية وفق ما جاء بالتشريعات الخاصة مثل المخبرات والامن الوقائي وغيرهم من يتمتعون بصفة الضابطة القضائية فهي مختلفة وفقاً للقوانين الخاصة لكل جهاز، فقيام جهاز مثل المخبرات العامة والتي حددت مهامه بموجب احكام المواد(9 و10) من قانون رقم 17 لسنة 2005 الخاص بالمخبرات العامة والمختص بالحفظ على الامن الداخلي والخارجي للدولة ان يحقق بجريمة ابتزاز الكتروني لسيدة مثلاً فهو من اختصاص وحدة حماية الاسرة بالتعاون مع وحدة الجرائم الإلكترونية ولا يكون من اختصاص المخبرات العامة، وفق لقانون المخبرات العامة، وهذا الدور الذي تقوم به وحدة حماية الاسرة الوقائي والحماية التي تحيطها بالمجني عليها خوفاً من قتلها مثلاً من قبل أهلها تحت ذريعة الشرف بالاضافة الى إعادة تأهيلها ودمجها في المجتمع لتمارس

حياتها الطبيعية، وتأخذ وحدة الجرائم الإلكترونية دورها بالبحث والتحري والاستدلال للدليل الرقمي، وصولاً إلى الجاني ورفع الملف إلى النيابة العامة، لاتخاذ المقتضى القانوني بملاحقة الجاني، وتقديمه للعدالة والحصول على الحكم المناسب، كما لا يعقل أن يقع تهديد للامن القومي للدولة، وأن تقوم الشرطة المدنية بمتابعتها أصولاً حيث أن الاختصاصات الامنية لكل جهاز بالدولة تختلف عن الاخر، كما ولا يعقل أن يتم تشتيت محضر جمع الاستدلال بين جهاز واخر ونستنتج من النص المذكور أنّ المشرع لصعوبة بمكان أن يباشر مأموري الضبط القضائي إجراءاتهم بمحضر التحري والاستدلال بالجرائم التقليدية، وتطبيقها على هذا النوع من الجرائم، وإن كانت بعض الاجراءات هي ذاتها تطبق على الجريمة الإلكترونية، إلا أنها بداية تختلف ببعض الجزئيات حماية لخصوصيتها وخصوصية الافراد المصانة بموجب القانون الاسمي بالدولة القانون الاساسي الفلسطيني

#### - انشاء المختبر الجنائي الالكتروني:

يقسم المختبر الجنائي الالكتروني في الشرطة المدنية وقوى الامنالى عدة اقسام على النحو التالي :

- قسم مكافحة الجريمة الإلكترونية على الشبكة العالمية قسم تحقيقات الانترنت: مهمتها مباشرة الاجراءات الخاصة بتعقب مرتكبي جرائم الانترنت من اختراق وقرصنة ونشر برمجيات خبيثة واختراق البريد الالكتروني وشبكات التواصل الاجتماعي وانتحال الشخصية وفبركة الاخبار والاساءة والتشهير وغيرها من الجرائم التي تمس أمن المواطن عبر ارتكاب نشاطات غير قانونية من خلال الشبكة العالمية، ومتابعة الجرائم التي يستخدم فيها التقنيات كجرائم تطبيقات الاتصالات والجرائم الواقعة على الاشخاص والاموال والتزوير الالكتروني والاحتيال الالكتروني والابتزاز الالكتروني سواء ارتكبت من داخل الدولة أو خارجها، ومتابعة الاشاعات التي تمس أمن الدولة واستقرارها والعمل على تحديد مطلقها ومنعهم، أو الحد من هذه الإشاعات قدر الامكان. من خلال مراقبة وتعقب المواقع الإلكترونية وصفحات التواصل الاجتماعي التي من شأنها المساس بالأمن العام والنظام العام والاداب العامة.<sup>1</sup>

- قسم التحقيق الجنائي الرقمي **digital forensics**: يختص هذا القسم في ايجاد وتحليل الادلة الكترونية ومعالجتها للقضايا والجرائم المختلفة والتي تتعلق باستخدام وسائل تكنولوجيا المعلومات في اعمال خارج نطاق القانون الفلسطيني واستخدام المخرجات الرقمية كادلة والتي تساعد المحققين في اتخاذ القرارات الصحيحة فيها واحالتها بنقير منظم الى جهة التحقيق النيابة العامة. ومن اختصاصات الدائرة فحص المضبوطات من اجهزة تقنية مثل الحاسب الالي والاجهزة المحمولة واجراء التحقيق

<sup>1</sup> محمد مسعود، وحدة الجرائم الإلكترونية ، مختبر الادلة الإلكترونية ، مقابلة شخصية بتاريخ 16-8-2019.

الجنائي لقواعد البيانات وللشبكات وحفظ المضبوطات بما يحفظ سلامتها وعدم إحداث أي عطب أو تلف فيها ضمن بيئة مناخية مناسبة لها، ومن مهام القسم هو استرجاع الأدلة الرقمية من الأجهزة والمعدات التقنية سواء بداخل المختبر الإلكتروني الجنائي، أو خارج المختبر لأسباب تقنية تمنع من نقل الأجهزة والمعدات التكنولوجية إلى المختبر من أجل توثيقها وتحليلها وتقديم الدعم الفني للافرع في كل محافظة وفقا للاختصاص كل جهاز أمني .

تتجلى جميع هذه الاعمال في إعداد تقارير خبرة فنية تقدم إلى جهات الاختصاص سواء النيابة العامة إن كنا في صدد إعداد ملف تحقيقي أو للمحكمة المختصة بناءً على طلبها في ملف دعوى منظور أمامها كما يتابع فريق قسم الأدلة إعداد التقارير الاحصائية الخاصة، والمتعلقة بالأدلة الرقمية وتقديم وإجراء الخبرة الفنية في نظام التشغيل وقواعد البيانات والتطبيقات والشبكات تحت إشراف مدير الوحدة او من ينوب مكانه

- **قسم دائرة الاتصالات:** تكون مسؤولية الدائرة أمام مدير وحدة عن كافة ما يوكل لهم من مهام التي تشمل متابعة الاحتياجات الواردة من أفرع المباحث العامة أو قوى الأمن المخولين وفقا لقرار بقانون الجرائم الإلكترونية والمتعلقة بحركة الاتصالات وخط سيرها ومتابعة الاحتياجات المتعلقة بسرقة الاجهزة التقنية الخلوية او الجرائم المتضمنة اجهزة خلوية وتحليل الكشوفات وتزويدها الى جهة التحقيق بتقرير مفصل حولها حيث لا يتم الحصول على أية حركة اتصال او خط سير لها دون أن يكون هناك طلب مقدم الى عطوفة النائب العام لتدقيقه، وإعطاء الأمر الى شركات الاتصال السلكية واللاسلكية ضمن الاجراءات القانونية.<sup>1</sup>

- **قسم اختبار الاختراق penetration testing :**

وهو يختص بالقيام بعمليات اختبار الاختراق لنظم الشبكات والاتصالات وقواعد البيانات واكتشاف الثغرات التقنية واصدار الحلول لها وايجاد السبل لمعالجتها واكتشاف القائمين عليها والتأكد من سلامة البرمجيات التي يتم برمجتها بالمؤسسات الحكومية والاقتصادية، وعمل الفحص الدوري للاجهزة الحاسوبية والهواتف النقالة للتأكد من سلامتها من أي اختراقات وتهديدات كما ويختص القسم بتحليل ودراسة الفيروسات والبرمجيات الخبيثة لمعرفة مصدرها، وعمل قاعدة معلومات للجهات التي تستهدف

<sup>1</sup>رهام جبر، نائب مدير وحدة الجرائم الإلكترونية ، مقابلة شخصية .

القطاعات الحكومية والخاصة وإيجاد الحلول للتخلص من هذه الفيروسات والبرمجيات الخبيثة، وتتم جميع هذه المهام من قبل فريق مختص يسمى **computer emergency response team**.<sup>1</sup>

- **قسم التشفير:** ويختص هذا القسم من التأكد من سلامة نقل المعلومة من مكان الى اخر من خلال المهام التالية:

• كتابة الجورثيمات للتشفير encryption algorithms وبرمجتها من إيجاد أفضل الوسائل لضمان نقل المعلومة بشكل آمن.

• تشفير وسائل نقل البيانات بين في داخل القطاعات منعا لاختراقها.

• إيجاد وكتابة البرمجيات حتى يتم من خلالها تخزين البيانات بشكل آمن وسليم.

• العمل على تطوير علم التشفير وفك التشفير المواكب للتطور التكنولوجي.

- **قسم التوعية والإرشاد:** يقسم إلى قسمان على النحو الآتي:

**القسم الأول** يتعلق بالمواطنين وتكون مسؤولية القسم أمام مدير الوحدة عن جميع اعمالهم التي تتضمن نشر الوعي الثقافي والمجتمعي الإلكتروني وكيفية الحفاظ على امن معلومات ومتابعتها والية تامين الحسابات الشخصية منعا لاختراقها وإعداد المواد والمطبوعات حول مخاطر الانترنت الشبكة العالمية، وكيفية التصدي لها وإعداد البرامج التوعية والإرشادية التي تناسب القطاعات المجتمعية المختلفة

**القسم الثاني:** ويختص باصدار النشرات التوعية للأشخاص العاملين داخل المؤسسات الامنية في كيفية التعامل وحماية اجهزتهم التقنية من أي تهديد الكتروني، إعداد نشرات تتعلق بالاساليب التي يتبعها المخترقون واعداد دراسات تتعلق بإهداف ودوافع المجرم الإلكتروني حفاظا على امن المعلومات داخل المؤسسات الامنية والحكومية

- **قسم التحقيقات المتعلقة بالفيديوهات والكاميرات:** يختص القسم بالحصول على DVR وهو الجهاز الذي يتم ضبطه بموافقة النيابة من أجل تفرغ التسجيلات والصور المتعلقة بارتكاب جريمة جنائية بمكان ما وتحليل هذه البيانات على أنظمة تسمى فلترة دقيقة ضمن أقسام المختبر مجهز بانظمة عالمية للحصول على ادلة لارتكاب الجرم وتقديمها للعدالة.

- **قسم المتابعة الفنية:** مختص بتلقي الشكاوي من المواطنين واخذ البيانات اللازمة للبدء بالعمل في القضايا المختلفة وتحديد الحسابات الإلكترونية وتحويل الملف للفرع المختص في الاقسام المختلفة

<sup>1</sup> خالد حبيب ، مختص بالمتابعة الفنية ، مقابلة شخصية ، وحده الجرائم الإلكترونية ، بتاريخ 2019\7\2.

كما وتم تدريب كوادر من مأموري الضبط القضائي مختصين بتلقي الشكاوي والبلاغات المكتوبة والإلكترونية تحت مسمى المستجيب الاول في كل من الاجهزة الامنية على مختلف اختصاصاتها وفي جميع المحافظات

- **قسم التحقيقات الفنية والصيانة:** وهو مختص بالمضبوطات واليات التعامل معها من لحظة التحفظ عليها او ضبطها وتسجيلها وفق القانون من خلال وصولات استلام معتمدة وتخزينها وتحويلها للقسم المختص داخل المختبر لفحصها وفقاً لقرار وكيل النيابة المحقق كما يقوم القسم بصيانة الاجهزة التقنية المضبوطة إذا كانت في حالة تمنع من إجراء الفحص الالكتروني مثلاً أن يقوم المتهم بكسر الجهاز قبل القاء القبض عليه معتقدا انه لن يتم الحصول على اي دليل من الجهاز المكسور ضده

**تتولى وحدة مكافحة الجريمة الإلكترونية على مستوى جهاز الشرطة وقوى الامن المهام التالية:**<sup>1</sup>

- التحقيق في الجرائم الإلكترونية المرتبطة بالانترنت.
- التحقيق بالجرائم الإلكترونية المرتبطة بالتقنية المعلومات والتكنولوجيا.
- استرجاع الادلة الرقمية وثوبيقها وتحليلها وتزويدها الى جهة التحقيق .
- اعداد تقرير فني قضائي للجهات القضائية.
- نشر التوعية والثقافة اللازمة للمجتمع في مجال الجرائم الإلكترونية.
- المساهمة في تنفيذ الاتفاقيات الدولية والاقليمية التي تم اقرارها من دولة فلسطين.
- تلقي الشكاوي في القضايا التي تحال اليها من النيابة العامة والقضاية المتعلقة في الشؤون الداخلة داخل كل جهاز .
- ضبط الادلة الرقمية والتحفظ عليها واعداد التقارير اللازمة حتى احوالها الى النيابة العامة.
- اعداد ارشيف وسجلات خاصة بكافة القضايا والجرائم الرقمية والإلكترونية من حيث انواعها والمعلومات المتعلقة باسم المشتكي وعنوانه ورقم هويته مكان عمله وسكانه وتاريخ الشكوى او الاحالة والمعلومات المتعلقة بالمضبوطات من وصفها تفصيليا ونوعها بالاضافة الى اعداد كشوفات واحصائيات بالادلة والادوات المضبوطة .
- المساعدة الفنية للدارات والافرع في المحافظات.

<sup>1</sup> سامر الهندي، مدير وحدة الجرائم الإلكترونية ، مقابلة شخصية حول اختصاص عمل وحدة الجرائم الإلكترونية بجهاز الشرطة ، فلسطين ، رام الله ، بتاريخ 16-9-2019.

- تدريب المنتسبين الجدد للوحدة بمختلف أقسامها ووفقاً لتخصصاتهم التقنية.
- التنسيق مع مكتب النائب العام نيابة الجرائم الإلكترونية بكل ما يتعلق بالدليل الإلكتروني والاحتياجات الإلكترونية العادية والمستعجلة.
- معاينة مسرح الجريمة الإلكتروني أو تنفيذ أمر التفتيش الصادر من النيابة العامة.
- يقدم البلاغ الى مأموري الضبط القضائي لدى المحافظات والتي بدورها تقوم بالاتصال بوكيل نيابة الجرائم الإلكترونية المختص بالمحافظة الذي يقيم الاحتياج الإلكتروني ورفع من خلال رئيس النيابة الى النائب العام الذي يعطي تعليماته لرئيس النيابة المركزي والخول بقرار من عطوفته بمتابعة الاحتياجات الإلكترونية<sup>1</sup>.

### السمات التي يتميز بها الاشخاص المختصين في مكافحة الجريمة الالكترونية

إن مأموري الضبط القضائي الذين يتعاملون بالجرائم الإلكترونية يتمتعون بنوعية وكفاءة في التعامل مع هذه الجرائم، فنصت المادة (32) فقرة 5 "يشترط في مأموري الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية" وهذا شرط الزامي وهذا يؤكد صعوبة الاجراءات المتخذة في الجرائم الإلكترونية وطبيعتها الخاصة من قبل مأموري الضبط القضائي وجديتها ودقتها فانه لا يستطيع مأموري الضبط القضائي في الجرائم التقليدية متابعتها، لا بل بالعكس قد يؤدي الى ضياع الدليل الإلكتروني بمجرد وجود أي شخص من غير ذوي الاختصاص في مسرح الجريمة وأن يقوم بضبط جهاز حاسوبي وفكه وقطع الشبكة عنه بطريقة عشوائية يؤدي لضياع الدليل الإلكتروني للجريمة المرتكبة. لذا يجب أن يتمتع الخبير الإلكتروني من مأموري الضبط القضائي بالمعرفة الفنية والتقنية والعلمية العالية ومواكبت التطورات التقنية لرفع القدرات الفنية للبحث والتقيب والتحري، بالافعال غير المشروعة الكترونياً،<sup>2</sup> فعليه أن يقوم بتجسيد الدليل الرقمي المستخرج من البنية الرقمية على شكل صور وأرقام ورموز وإشارات، والمخزنة ضمن برامج وتطبيقات وايقونات الكترونية، وتحويلها الى صور مادية يتم تفريغها واستخراجها على شكل حروف مكتوبة ومفهومة للمحقق والقاضي المختص كدليل بالتحقيق والمواجهة ودليل إدانة للمحكمة.

<sup>1</sup>قامت وحده الجرائم الإلكترونية بإنشاء قسم الجرائم الإلكترونية في جميع افرع المباحث في المحافظات ومهتهم تكمن في متابعة الشكوى واستقبالها والتنسيق مع وحده الجرائم الإلكترونية في الاداره العامة للمباحث.

- رهام جبر، نائب مدير وحده الجرائم الإلكترونية في جهاز الشرطه ، مقابلة شخصية بتاريخ، 2019\9\22 .

<sup>2</sup>حمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري(دراسة مقارنة)، دار النهضة العربية، الطبعة الأولى، 2010،ص151.

ويؤكد النصيين المذكورين على خصوصية الجريمة بداية بأنه يجب أن يكون هناك تخصيصية بالتعامل بالجرائم المرتكبة عبر الوسائل الإلكترونية أو على ما تحتويه من معلومات، وبيانات تم معالجتها إلكترونياً.

وبالرغم من ذلك لم يتطرق المشرع في قرار بقانون الجرائم الإلكترونية لمحضر جمع الاستدلالات وبذلك يكون احوال تنظيم هذا الجزء فيما يتعلق بمحاضر الاستدلال إلى الأحكام العامة في قانون الاجراءات الجزائية الفلسطينية رقم 3 لسنة 2001، حيث جاءت النصوص الاجرائية كاستثناء والمتعلقة بالاجراءات التحقيقية لخصوصيتها في المواد (32) و(33) و(34) و(35) و(36) لانها اجراءات تشترك بها النيابة العامة بصفتها التحقيقية وبصفتها المشرفة على أعمال مأموري الضبط القضائي من خلال العلاقة التبعية الوظيفية وتشترك بها أيضاً المحكمة المختصة في مرحلة ما قبل المحاكمة. هذه الاجراءات وضعت لوضع التوازن ما بين الخصوصية واحترام الحريات العامة للأشخاص والحفاظ على المصلحة العليا للدولة بالحفاظ على نظامها الداخلي وامنها ولما يخدم مصلحة التحقيق فهذه الضوابط والقيود التي وضعت على مأموري الضبط القضائي والنيابة العامة والتي تتفق مع القانون الاساسي والاتفاقيات الدولية.<sup>1</sup>

وبما ان المشرع الفلسطيني في قرار بقانون رقم 10 لسنة 2018 وضع الاجراءات الخاصة التي يجب ان يتقيد بها كلا من مأموري الضبط القضائي والنيابة العامة وهو استثناء عن الاصل في متابعة اي جريمة جنائية تقليدية لمتابعة الجرائم الالكترونية فان محضر جمع الاستدلال في الجرائم الالكترونية يتم بالاجراءات التالية :

### 1- المعاينة في البيئة الإلكترونية

المعاينة قد تعد إجراءً تحقيقياً أو استدلالياً مرتبطاً بمدى مساهمة بخصوصية الأفراد وفقد عرفها الفقهاء انها "رؤية بالعين لمكان أو شخص أو شيء لاثبات حالته، وضبط ما يلزم لكشف الحقيقة ومن خلال التعريف نستطيع أن نجزم انه لا يمكن أن يتم اجراء المعاينة دون أن ينتقل مأمور الضبط القضائي إلى مسرح الجريمة لاثباتها وضبط الاشياء، والادوات التي تؤكد وقوعها وتحليلها للوصول الى الفاعل إلى وان كانت المعاينة من الاجراءات المهمة، والتي بالنتيجة تكشف الغموض في الجرائم التقليدية الا أنّها لا تنتج ذات الدور في الجرائم الإلكترونية لعدة أسباب لا يمكن معاينة ما يحتويه الجهاز الحاسوبي من معالجة الية للبيانات والمعلومات الغير مرئية بمجرد الرؤية ولوجود فترة زمنية ما بين

<sup>1</sup>لمزيد حول ذلك انظر إلى نص المواد المذكوره في قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001.

ارتكاب الجريمة واكتشافها مما يؤدي الى تغيير مسرح الجريمة والعبث فيه واندثار الاثار المادية سواء بفعل المجرم نفسه او بفعل الاشخاص المترددين للمكان كما وأن خطورة المجرم الالكتروني حتى وإن ترك أثراً له قد يستطيع ان يقوم بمحو الدليل واتلافه عن بعد، لذلك فإن الدليل المتحصل من المعاينة قد يثير الريبة والشك، لدى السلطة القضائية، وتتحصّر المعاينة بالجرائم الكترونية بتدوين المكونات المادية التي تؤكد وجود بنية رقمية برؤية مسرح الجريمة، وما يحتويه من أجهزة وأدوات تقنية مادية كوجود حاسوب وإثبات وجود وصلات وكوابل متصلة بنظام الحاسوبي وطابعات واقرص صلبة وممغنطة وغيرها من الادوات الإلكترونية التي تشير الى وجود بيئة رقمية وهنا تختلف الية التعامل مع مسرح الجريمة الالكتروني.<sup>1</sup>

وتتميز المعاينة الكترونية بوجود قواعد وإرشادات فنية على مأمور الضبط القضائي اتباعها حتى يقبل الدليل المتحصل منها في اجراءات المحاكمة.

فتصنف الجريمة حسب المسرح الواقعة فيه، ويختلف مسرح الجريمة في السياق الرقمي أصولاً عن السياق المادي أو الطبيعي، حيث يمكن تصنيف تبعية مسارح الجريمة من حيث الطبيعة إلى مسرح جريمة طبيعي(مادي) ومسرح جريمة رقمي ومسرح جريمة مختلط.

حيث يسهل حصر مسرح الجريمة المادي بسبب طبيعته الفيزيائية التي يمكن حصرها بمكان وأدوات من شأنها التواجد في سياق تنفيذ الجريمة، ولكن حياّل مسرح الجريمة الرقمي فالأمر أصعب من ذلك فهو عادة ذو طبيعة مختلطة، حيث يوجد هناك أدوات لها طبيعة فيزيائية يمكن حصرها وهناك الجانب الأخر من الأداة ألا وهو النطاق الإلكتروني، وهذا ما يفتح الباب لعالم غير قابل للحصر من حيث احتياجات الأدلة والتفتيش.

**فعاصر الجريمة الإلكترونية** هي الفعل والوسط الالكتروني الدائر فيه الفعل والأداة المستخدمة في الولوج إلى ذلك الوسط؛ مما يصعب حصر دائرة التفتيش المكانية والزمانية لهذا الفعل، فهو لا يحتاج تواجد فيزيائي في موقع الجريمة الفعلي أو حتى في قطرها الإقليمي، مما يمكن أشخاص في نطاق إقليمي معين بإلحاق الضرر بمصالح لأشخاص متواجدين في نطاق إقليمي آخر، وهذا ما يحول حول سياق التفتيش الإلكتروني، فهل يمكن لسلطة ضبط تفتيش شبكة غير خاضعة لنطاقها الإقليمي؟

<sup>1</sup> احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري(دراسة مقارنة)، دار النهضة العربية، الطبعة الأولى، 2010، ص 135.

وماهي الاجراءات المنصوصة بقرار بقانون رقم 10 لسنة 2018 لتمكين ماموري الضبط القضائي من ذلك؟

يفتح تداخل نطاق الجريمة الإلكترونية من ناحية طبيعية ورقمية الباب لتضارب المصالح والشؤون، حيث يجب اختيار الدقة في نطاق طلب الاحتياجات الإلكترونية المطلوبة كدليل الكتروني، ومن جانب آخر توسع نطاق الجريمة الإلكترونية وانتشارها المكاني، ونقلها الزمني حيث أنّ الجريمة الإلكترونية ذو طبيعة مستمرة في الغالب مثلاً في جريمة التصيد عبر الانترنت<sup>1</sup> (phishing) تفتح تلك الثغرة عدداً لا محدود من الأبواب والموانئ الإلكترونية لتنفيذ الجريمة، وهي عادة ما تكون جريمة مستمرة زمنياً وممتدة مكانياً، وهنا يجب توفير جدار ناري الكتروني لوقف الثغرات، ولكن مع وجود ثغرات ما العمل حيال ذلك، وكيف لسلطة الضبط القضائي التعامل مع تلك الثغرات؟

إن الشبكة الإلكترونية بالاشتراك مع شبكة الاتصال السلكي واللاسلكي متصلة ببعضها البعض ولا يمكن فصلها، حيث أن معظم شبكات الاتصال السلكي واللاسلكي والشبكة العنكبوتية تستخدم مقاسم وخوادم مشتركة بشكل أو بآخر، وعادة ما تستهدف الهجمات الإلكترونية تلك المقاسم والخوادم لتنفيذ الجرائم، وهذا يدل على أن مسرح الجريمة قد يكون رقمي بحت، وهو من اختصاص وحدة الجرائم الكترونية التي تعمل على الولوج داخل الانظمة والتطبيقات للوصول إلى الفاعل، وقد يكون مختلط بين معاينة لمسرح الجريمة كتوافر بيئية رقمية، وبذات الوقت توافر الادوات الإلكترونية التي تؤكد وجودها في مكان لارتكاب الجريمة الكترونية هذا من جانب ومن جانب آخر قد تقع الجريمة لهذا القطاعات الاقتصادية أو المالية مثل البنوك، فإنّ انتقال ماموري الضبط القضائي الى مركز الخوادم والسيرفيرات للبنك لمعاينته كبيئة رقمية والتحفظ عليه لمنع وصول والولوج إلى أي من البيانات والمعلومات المخزنة به لحين اتخاذ الاجراء المناسب بمعرفة النيابة العامة، مثل نسخ البيانات والمعلومات التي لها علاقة بالجريمة المرتكبة، والتي تساعد بكشف الحقيقية، وهذا ما نصت عليه المادة (33) فقرة 2 و3 و4 فنلاحظ أن ما قام به ماموري الضبط القضائي يدخل ضمن إجراءات جمع الاستدلال من معاينة والضبط إلا أن المشرع أوجب أن تكون هذه الاجراءات تحت اشراف واذن من النيابة العامة باصدار

---

1تعريف التصيد الإلكتروني: هو نوع من أنواع الجرائم الإلكترونية الأكثر إنتشار. يعد التصيد الإلكتروني أحد أساليب الإحتيال عبر الإنترنت وذلك لمحاولة الحصول على معلومات شخصية أو مالية عن طريق رسائل البريد الإلكتروني أو من خلال مواقع الإنترنت. مأخوذ من الموقع الالكتروني <http://www.phishingaware.com> بتاريخ 2018/11/23 الساعة 5:00 مساءً

أمر الضبط والتحفظ من قبلها وقيده سلطة واختصاص مأموري الضبط القضائي من مباشرة الاجراءات دون وجود اذن قانوني وهو الغطاء التشريعي لسلامة الاجراءات المتخذة من قبل مأموري الضبط المختصين.

ومن مهام مأموري الضبط القضائي "قبول البلاغات والشكاوي التي ترد إليهم بشأن الجرائم وعرضها دون تاخير على النيابة العامة"<sup>1</sup> وهذا ما هو جاري العمل عليه في جميع الجرائم التقليدية وما قبل ظهور الجرائم الإلكترونية التي ادركها المجتمع الفلسطيني مؤخراً وأدركتها النيابة العامة منذ عام 2007م، حيث تم انشاء وحدة لمتابعة الاتصالات السلكية واللاسلكية، والتي كان عملها محصوراً على متابعة الاتصالات عملاً بنص المادة 51 من قانون الاجراءات الجزائية الفلسطيني<sup>2</sup>، حيث كانت الوحدة تتلقى شكاوي من المواطنين بقضايا بسيطة كالتهديد عبر الهاتف عملاً بأحكام المادة 91 من قانون الاتصالات السلكية واللاسلكية رقم 3 لسنة 1996م<sup>3</sup>، وإحداث ازعاج من قبل مجهولين بشكل متكرر والذم عبر وسائل الاتصال، وفي بعض القضايا التحقيقية يتم مخاطبة النائب العام لمتابعة حركة الاتصالات لقضية جنائية مثل سرقة احد المنازل او المحلات التجارية او تقديم بلاغ لمأموري الضبط القضائي حول سرقة هاتف نقال ليتم متابعة الفاعل من خلال طلب تقدمه قسم التحقيق الشرطي لنيابة العامة في المحافظات والتي بدورها ترفعه لنائب العام المخول والمختص باصدار الامر لشركات الاتصال وتزويد النيابة العامة بالبيانات المحفوظة لديهم بموجب نص المادة 51 من قانون الاجراءات الجزائية الفلسطيني وبموجب نص المادة 4 من قانون الاتصالات السلكية واللاسلكية رقم 3 لسنة 1996 وفي عام 2013م إدراكاً من قيادة الشرطة المدنية بأننا أمام جريمة متطورة سواء اباشكالها واساليبها ووسائلها بدأت قيادة الشرطة بتدريب طاقم للمختبر الجنائي تقنيا حتى يواكب تطور الجريمة

<sup>1</sup> المادة 22 فقرة 1 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001

<sup>2</sup> المادة 51 من قانون الاجراءات الجزائية الفلسطيني والتي نصت على: "1- للنائب العام أو أحد مساعديه أن يضبط لدى مكاتب البرق والبريد الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات المتعلقة بالجريمة وشخص مرتكبها. 2- 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 جنائية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سنة.

3- يجب أن يكون أمر الضبط أو إذن المراقبة أو التسجيل مسبباً، ولمدة لا تتجاوز خمسة عشر يوماً قابلة للتجديد لمرة واحدة"<sup>3</sup> المادة 91 من قانون الاتصالات السلكية واللاسلكية رقم 3 لسنة 1996 والتي نصت على: (أ) كل من قام بتهديد أي شخص أو إهانته أو نقل خبراً مختلفاً بأي وسيلة من وسائل الاتصالات بقصد إثارة الفزع يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد عن سنة أو بغرامة لا تقل عن 50 دينار ولا تزيد على (200) دينار أو بكلتا العقوبتين. (ب) كل من قام أو ساهم بتقديم خدمات اتصالات مخالفة لنظام العام أو الآداب العامة يعاقب بالعقوبات المنصوص عليها في الفقرة (أ) من هذه المادة بالإضافة إلى تطبيق الأحكام المنصوص عليها في المادة (31) من هذا القانون."

بالتسيق مع وحدة النيابة العامة، 2016\3\20 تم انشاء نيابة الجرائم الإلكترونية في مكتب النائب العام كنيابة متخصصة بمتابعة جميع القضايا للالكترونية سواء كانت الاداة التكنولوجيا أداة مستخدمة لارتكاب الجريمة أو واقعة على إحدى وسائل تكنولوجيا المعلومات مثل الاختراقات واعتراض الاتصالات والتصنت وهذا جاء إدراكاً من قبل النائب العام أننا أصبحنا أمام ظاهرة خطيرة تهدد أمن واستقرار المجتمع الفلسطيني سياسيا واجتماعيا واقتصاديا وأنا لسنا امام مشكلة عابرة كما ان عدد الاحتياجات الواردة لنيابة العامة الإلكترونية في تزايد كبير ففي 2015م وحتى 2017م كان عدد الشكاوي الواردة لجهاز الشرطة المدنية، بلغت عدد الشكاوي في عام 2013م (174) شكوى، وفي عام 2014م بلغ العدد (361) شكوى، وفي عام 2015 بلغ العدد (502) شكوى، وفي عام 2016 بلغ العدد (540) شكوى، وفي عام 2017 م<sup>1</sup> وفي عام 2018م ومن خلال الاحصاءات نجد أنّ عدد الشكاوي التي تبلغت بها الشرطة المدنية وحدها دون احتساب عدد الشكاوي التي وصلت الى النيابة الجزئية والشكاوي والبلاغات الواردة للاجهزة الامنية الاخرى بالتزايد وبالرغم أن هذه الاحصاءات لاتعكس معدل ارتفاع الجريمة الإلكترونية في المجتمع الفلسطيني والسبب يعود كما ذكرنا سابقا الى أن عدد من الشركات والبنوك والمنشات لها نظامها الامني لحماية قاعدة البيانات والمعلومات الالكتروني الخاص بها بوضع جدار الناري ومتابعته من قبل كل شركة كما وان تعرضت أية منشأة أو شركة وما في حكمهم الى اي اختراق أو اعتداء الكتروني لا يتم تقديم بلاغ أو شكوى للجهات المختصة بصرحيها الضابطة القضائية أو النيابة العامة خوفا عل التأثير على سمعتهم التجارية والاقتصادية كما أن عدداً كبيراً من المواطنين الذين يتعرضون الى الابتزاز الكتروني باشكاله الجنسي والمادي ايضا لا يبادرون الى تقديم شكوى إلا إذا فقدوا السيطرة على الموضوع وخرج من بين ايديهم بنشر فيديو اباحي لاحد المواطنين والمواطنات فليجأون الى تقديم بلاغ أو شكوى كملاذ أخير، من خلال ما تقدم نجد أن تقديم الشكوى والبلاغ الالكتروني لمأموري الضبط القضائي سيان في جميع انواع الجرائم المرتكبة سواء المعاقب عليها بموجب قانون العقوبات والتشريعات الخاصة الأخرى مثل قانون المخدرات وقانون الاسلحة وقانون الصحة بالمجتمع الفلسطيني وبموجب قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م.

**تقديم الشكاوي والبلاغات** هي من المهام الرئيسية الملقاة على مأموري الضبط القضائي وفقا لنص المادة 22 من قانون الاجراءات الجزائية الفلسطيني وايضاً ما نص عليه قانون الاجراءات الجنائية

<sup>1</sup>- تقرير الاحصائيات الصادر من قيادة الشرطة المدنية عام 2018

المصري حيث نصت المادة 24 "يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوي التي ترد اليهم بشأن الجرائم، وان يبعثوا بها فوراً الى النيابة العامة، ويجب عليهم وعلى مرؤسيهم ان يحصلوا على جميع الايضاحات ويجروا جميع المعاينات اللازمة لتسهيل تحقيق الوقائع التي تبلغ اليهم، أو التي يعلنون بها باية كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على إدلة الجريمة. ويجب ان تثبت جميع الاجراءات التي يقوم بها مأموري الضبط القضائي في محاضر موقع عليها يبين بها وقت اتخاذ الاجراء ومكان حصوله، ويجب ان يشتمل تلك المحاضر زيادة على ما تقدم توقيع الشهود والخبراء الذين سمعوا، وترسل المحاضر الى النيابة العامة مع الاوراق والاشياء المضبوطة"، وتنص المادة(7) من قانون اصول المحاكمات الجزائية الاردني<sup>1</sup> على أن "موظفو الضابطة العدلية مكلفون باستقصاء الجرائم وجمع ادلتها والقبض على فاعليها واحالتهم على المحاكم الموكل اليها أمر معاقبتهم". وتنص المادة (49) من قانون أصول المحاكمات الجزائية الأردني "على موظفي الضابطة العدلية مساعدي المدعي العام ان يودعوا الى المدعي العام بلا ابطاء الاخبارات ومحاضر الضبط التي ينظمونها في الاحوال المرخص لهم فيها مع بقية الاوراق "

حددت النصوص السابقة الاجراءات ابتداءً بعلم مأموري الضبط القضائي بوقوع الجريمة فبمجرد علم مأموري الضبط القضائي بالجريمة سواء عن طريق شكوى مكتوبة أو بلاغ بأي طريقة كانت شفويًا مكتوبة أو اتصال هاتفي من شخص أو بالبريد يياشر مأموري الضبط القضائي صلاحياتهم باجراء التحريات وتنظيم محضر بحث واستدلال والزم المشرع أن يتم ارسال المحضر الى النيابة العامة صاحبة الاختصاص بمباشرة الدعوى العمومية وهنا الفارق أن مأموري الضبط القضائي يتلقون البلاغات والشكاوي ومتابعتها كاختصاص أصيل لهم في جميع الجرائم التقليدية والإلكترونية مع الاخذ بعين الاعتبار أن هناك امور تفصيلية تقنية يجب أن يركز عليها مأمور الضبط القضائي.

### التفتيش في البيئة الإلكترونية

أما الاجراءات التي تبنى على البلاغات والشكاوي اصبحت اختصاصاً استثنائياً في الجرائم الإلكترونية لمأموري الضبط القضائي حيث أن محضر البحث والتحري والتفتيش بالجرائم الإلكترونية للحصول على دليل رقمي ببيئة رقمية وهو محضر ينظم في المساحة الافتراضية للجريمة مثلا التفتيش في اي جريمة على حدا سواء بطلب من النيابة العامة سواءالملف تحقيقي منظور أمامها أو بناءً لمحضر جمع الاستدلالات المنظم من الضابطة القضائية وطلب مرفق بإصدار أمر التفتيش وفقا لما نص

<sup>1</sup>قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961 .

عليه قانون الاجراءات الفلسطينية حيث يتمحور التفتيش حول مكان له حرمة ومصان وفقا للقانون الاساسي الفلسطيني والتساؤل هنا كيف نظم المشرع الفلسطيني اجراء التفتيش في الجرائم الالكترونية وخاصة انها تقع اما على المكونات المادية للحاسب او لاي وسيلة تقنية معلومات او على ما تحتوته هذه الوسائل من مكونات معنوية تتمثل بالبيانات والمعلومات ؟

عرفت محكمة النقض المصرية التفتيش بانه "التفتيش كما هو معروف في القانون هو ذلك الاجراء الذي رخص به الشارع التعرض لحرمة الشخص بسبب جريمة وقعت او ترجح وقوعها منه ذلك تغليبا للمصلحة العامة على مصالح الافراد الخاصة واحتمال الوصول الى دليل مادي يكشف الحقيقة".<sup>1</sup> لم يتطرق المشرع الفلسطيني في قرار بقانون رقم 10 لسنة 2018 الى تعريف التفتيش الإلكتروني لذلك فنرى انه يمكت تعريفه هو احدى اجراءات التحقيق التي تتولاها النيابة العامة بهدف الوصول الى الدليل بهدف اثبات الإدانة أو البراءة فهو قد يقع على المكونات المادية للحاسب الإلكتروني او المكونات الغير مادية.

#### اليات التفتيش الالكتروني:

وقد نصت المادة 32 من قرار بقانون الجرائم الإلكترونية رقم 10 لسنة 2018م، على آلية التفتيش الالكتروني سواء لمسرح الجريمة الالكتروني أو التفتيش المتضمن الأجهزة ووسائل تكنولوجيا المعلومات بالولوج من قبل مأموري الضبط القضائي المتخصصين الى داخل النظام الالكتروني للبحث والتحري في المعالجة الالية للبيانات والمعلومات المثبتة بداخله والحصول على الدليل الرقمي لربط الفاعل بالجريمة المرتكبة من خلال إصدار أمر النفاذ المباشر الذي يخولهم بذلك، لذلك فالتفتيش في الجرائم الإلكترونية نوعان الأول واقعي القصد منه ضبط ماديات الجريمة والادوات المستخدمة وهنا يجب أن أقف إلى أن عملية الضبط يجب أن تنفذ من قبل مأمور ضبط قضائي متخصصاً بعلم تكنولوجيا المعلومات بحيث اذا تم ضبط مثلا الحاسوب بشكل تلقائي دون فصل الكهرباء منه أو اغلاقه بالطريقة التقنية الصحيحة فقد يهدر الدليل الالكتروني ولن يعد بامكان المختبر الجنائي الالكتروني من اثبات الجريمة والحصول على الدليل الرقمي والنوع الاخر للتفتيش هو التفتيش

---

<sup>1</sup> احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري(دراسة مقارنة)، دار النهضة العربية، الطبعة الأولى، 2010،ص 136.

الافتراضي المعنوي والذي يعتبر محضر التحري والاستدلال لمأموري الضبط القضائي بالبحث بمكونات الجهاز من ارقام ورموز وصور واشارات وتحليلها للحصول على الدليل الرقمي وربط الفاعل به من قبل المختبر الجنائي الالكتروني بتقرير فني تقني وفقاً للقانون والاصول والذي يقدم الى النيابة العامة من اجل ان تستكمل إجراءاتها التحقيقية بدمج الدليل الرقمي بالنص التشريعي واحالة الملف الى المحكمة المختصة.<sup>1</sup>

وفي جميع انماط الجريمة الإلكترونية لا يستطيع مأموري الضبط القضائي ان ينظم محضر تحري واستدلال دون الرجوع الى النيابة العامة سواء باخذ اذن التفتيش أو الاذن المباشر أو الحصول على كشوفات اتصال أو معرفة صاحب البريد الالكتروني أو العنوان الالكتروني أو رقم شصي الجهاز دون ان يكون عبر القناة الرسمية وهي النيابة العامة، وهذا حرصاً من المشرع الفلسطيني للحفاظ على الحريات الخاصة والحياة الخصوصية للأفراد.

عليه نجد أنّ المشرع الفلسطيني قد نظم تفتيش الاشخاص والاماكن ووسائل تكنولوجيا المعلومات من خلال أمر التفتيش أو الندب لمأمور الضبط القضائي المؤهل فنياً وقانونياً للتعامل مع هذه الأجهزة والوسائل بضبطها ابتداءً كمكون مادي، ومن ثم الحصول على اذن تفتيش آخر قد اسماه المشرع بالاذن المباشر للولوج وتفتيش المكونات المعنوية بداخل الاجهزة المضبوطة ونظمت المادة 33 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية.<sup>2</sup>

حيث عالج المشرع الفلسطيني الية الحصول على البيانات والمعلومات وكلمات المرور وبيانات المشترك من خلال متابعة حركات الاتصال أو نسخ المعلومات والبيانات المرتبطة بالجريمة

---

<sup>1</sup> انظر إلى نص المادة (32) من قانون الجرائم الإلكترونية رقم 10 لسنة 2018 .

<sup>2</sup> نص المادة 33 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية: "1. للنيابة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات أو بمستعملها أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية. 2. للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة. 3. إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً أو تعذر إجراؤه، تنتسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات. 4. إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفوذ إلى البيانات المخزنة بنظام المعلومات. 5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها. 6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف أو مغلف مختوم، ويكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية".

الإلكترونية وبذلك هذا المشرع الفلسطيني راي الفقهاء الذين اعتبروا أن التفتيش يشمل البيانات والمعلومات الملموسة وغير ملموسة من خلال تحليلها وترجمتها بالمعالجة الآلية للبيانات وتحويلها الي بيانات مقروءة أو مرئية أو مسموعة فيتم تفتيشها من قبل مامور الضبط القضائي المختص تقنيا وفنيا ومن التشريعات التي اخذت بهذا الرأي التشريع الفرنسي، والانجلترى، والامريكي والياباني.<sup>1</sup> أما تشريعات اخرى مثل التشريع اليوناني اعتبر مسالة التفتيش وجوبية على المكونات المادية وجوازية التفتيش على ما يحتويه الحاسوب من معلومات وبيانات.

وراي اخر ذهب الى عدم اعتبار بوجود مكونات مادية بل اعتمدوا على ان كل ما يتم معالجته داخل الحاسوب من معلومات وبيانات فهي تترجم الى رموز وصور وارقام واشارات تمر خلال اسلاك مادية وبالتالي لا يمكن اعتبارها مكونا معنويا لانها في نهاية المطاف تظهر مكون مادي يرى بالعين.<sup>2</sup> ونخلص ان التفتيش يجب ان يشمل اية معالجة الية داخل وسائل تقنية المعلومات باشكالها فالجريمة الإلكترونية اما ان تقع على الاجزاء المادية إلا أنّ اغلبية الجرائم الإلكترونية تقع من خلال استخدام التقنيات والتطبيقات والبرامج والمعالجات الآلية الحاسوبية وبالتالي اذا وقعت عملية اختراق كيف بامكان الخبراء والمختصين تكنولوجيا المعلومات من ماموري الضبط القضائي من الحصول على الدليل الالكتروني وربطة بالفاعل اذا لم يتمكنوا من التفتيش التقني بداخل الحاسوب لذا اعتقدوا بان جميع التشريعات المعاصرة يجب ان تشمل تشريعاتها بما يتضمن التفتيش الخارجي والمادي والتفتيش الفني الغير مرئي حيث ان الجرعة تقع على ما يحتويه الحاسوب من معلومات وبيانات.

وبصعوبة بامكان ان نفصل مهام ماموري الضبط القضائي في الجرائم الكترونية حيث ان جميعها ومنذ اللحظة الاولى يتصل بها عضو النيابة المختص الذي يقوم بدوره اما باعطاء امر التفتيش او الانتداب لتفتيش الاماكن والاشخاص ووسائل تكنولوجيا المعلومات ذات صلة بالجريمة والضبط والتحفيز الالكتروني لفريق البحث الجنائي الالكتروني وخبير البصمات وعرضها على النيابة العامة لاتخاذ المقتضى القانوني باصدار الاذن المباشر لتفتيش الكتروني الذي يتمحور حوله بما يسمى بالاحتياجات الكترونية اي الحصول على المعلومات والبيانات المحفوظة بقاعدة بيانات شركات الاتصالات ومزويدي خدمة الانترنت وفقا لنص المادة 31 من قرار بقانون الجرائم الإلكترونية رقم 10 لسنة 2018 حيث نصت "تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة

<sup>1</sup> احمد مصطفى ، مرجع سابق، ص137.

<sup>2</sup> المرجع السابق ، ص 137 و138.

،وبناء على طلب النيابة او المحكمة المختصة "لما تتسم به هذه المعلومات من الصفة السرية المتلازمة لها لذلك وضع المشرع الامر بيد النيابة العامة والمحكمة المختصة للحصول على هذه المعلومات وحركتها في اشخاص محددين ملزمة بها الجهات الشريكة كشركات الاتصال ومزودي خدمة الانترنت وليس الامر سيان في الجرائم التقليدية التي لا تتصل مباشرة بالحياة الخاصة والحريات الخصوصية.<sup>1</sup>

وفيما يتعلق بالتفتيش على الصعيد الاقليمي اي خارج حدود وسيادة الدولة حتى لو كان المراد تفتيشه من وسائل تقنية وحاسوبية غير موجودة داخل منزل المتهم او اي مكان ينتسب اليه الاشكالية تظهر اذا ارتكب المتهم جريمته من خلال حاسوب متصل بالشبكة العالمية ومرتبطة بجهاز اخر خارج حدود المساحة الجغرافية للدولة اي مرتبط بدولة اخرى وبالتالي لا يستطيع المحقق التعدي باجراءاته التحقيقية على سيادة دولة اخرى للحصول على ما هو مخزن بشبكات الاتصال وتم معالجته من خلال الشبكة التابعة للدولة الاخرى ومن التشريعات ما نصت على ان التفتيش يمتد الى الاجهزة الإلكترونية حتى لو كان فيها تعدي على سيادة دولة اخرى ما دام ان جهاز المتهم متصل بها مع وضع ضوابط وقيود اجرائية معللين ذلك ان الهدف هو اظهار الحقيقة وانه اجراء مؤقت مثل التشريع الهولندي والماني<sup>2</sup> وبمراجعة التشريعات والاتفاقيات الدولية نجد ان اتفاقية بودابست الزمت الاطراف الموقعين عليها ان يتخذوا كافة التدابير التشريعية التي تمكن السلطات التحقيق المختصة من الدخول والتفتيش داخل البنية الرقمية لاثبات الجريمة.

وقدالزمت الاتفاقية العربية لمكافحة تقنية المعلومات الدول الاطراف بتبني الاجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش او الوصول الى تقنية معلومات او جزء منها والمعلومات المخزنة فيها او المخزنة عليها والتفتيش بالبيئة الرقمية او اي وسيط تخزين معلومات والذي قد تكون معلومات التقنية مخزنة فيها

ونصت المادة 38 من قرار بقانون الجرائم الالكترونية رقم 10 لسنة 2018 "تعتبر الادلة المتحصل عليها بمعرفة الجهة المختصة او جهات التحقيق من دول اخرى ،من ادلة الاثبات طالما ان الحصول عليها قد تم وفقا للاجراءات القانونية والقضائية للتعاون الدولي "، كما نصت المادة 42 من ذات القانون "تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الاجنبية في اطار

<sup>1</sup> انظر إلى نص المادة (31) من قرار بقانون رقم 10 لسنة 2018 المتعلق بالجرائم الإلكترونية في فلسطين .

<sup>2</sup> احمد مصطفى ، مرجع سابق، ص 160.

الاتفاقيات الدولية والاقليمية والثنائية المصادق عليها ، او طبق المعاملة بالمثل ، بقصد الاسراع في تبادل المعلومات بما من شأنه ان يكفل الانذار المبكر بجرائم انظمة المعلومات والاتصال وتقادي ارتكابها والمساعدة على التحقيق فيها وتتبع مرتكبيها "وتتص الفقرة الثانية من ذات المادة "يتوقف التعاون المشار اليه بالفقرة السابقة على التزام الدولة المعنية بالحفاظ على سرية المعلومات المحالة اليها ، والتزامها بعدم احالتها الى طرف اخر او استغلالها لاغراض اخرى غير مكافحة الجرائم المعنية بهذا القرار "ونصت المادة 43 من ذات القانون ايضا على تقديم المساعدة القانونية وتسليم المجرمين اذا كانت تتعلق بالتحقيقات والاجراءات الجنائية المرتبطة بكل ما جرم بقرار بقانون الجرائم الإلكترونية الفلسطيني .

ومن الاشكاليات التي تواجه مأموري الضبط القضائي في التفتيش اذا وضع المتهم رقم سري او رقم مرور على الجهاز التقني ورفض اعطاء الرقم بصمته او ادعى بنسيانه او بالفعل لم يعد يتذكر رقم المرور او الرقم السري فكيف لجهات التحقيق من اجراء التفتيش التقني الفني والدخول الى جهاز المتهم المضبوط عنوة لتفتيش البيئة الرقمية وكسر باب الحماية والذي يشبه كسر باب منزل احد الاشخاص فوفقا للقانون الاجراءات الجزائية رقم 3 لسنة 2001 حول صمت المهم وعدم الاجابة على الاسئلة الموجهة اليه بالتحقيق من ضمن الحقوق وحريات الفرد بحيث لا يمكن اجبار المتهم بالإفصاح عن كلمة المرور كما لا يعتبر صمته دليلا الكترونيا عليه او الدفع بصمت المتهم اثناء التحقيق من قبل عضو النيابة اثناء تقديم البيئات للمحكمة بيينة لادانته حيث نصت المادة 217 من قانون الاجراءات الجزائية الفلسطيني بانه "للمتهم الحق في الصمت ، ولا يفسر صمته او امتناعه عن الاجابة بانه اعتراف منه "وهذا ما اخذت به اغلب التشريعات العربية الاردني والتونسي والجزائري والكويتي واللبناني . اذا كان الصمت لا يفسر اعترافا من المتهم فانه بذات الوقت لا يعتبر انه بري فصمته لا يعني برائته والا اصبح الصمت الوسيلة للبراءة للمتهم البري والمذنب على حدا سواء لذلك يجب التنبيه على المتهم ان الصمت لن يفيدك في حال انك بريء لانك لن تستطيع ان تدافع عن حقا امام القضاء

فاذا كان لا يمكن اجبار المتهم بالضغط عليه واكراه وان رفض او التزم الصمت ارى ان ما نص عليه المشرع الفلسطيني باعطاء امر الاذن المباشر وهو الامر الذي يسمح لمأموري الضبط القضائي المتخصصين الكترونيا بالفحص والتفتيش الكتروني بالدخول الى الجهاز والتفتيش بمكوناته الالية وذلك لمصلحة القانون وتحقيق العدالة والاهم من ذلك ان ما قام به المتهم ما هو الى اعتداء على

حقوق آخرين سواء الخاصة او المالية وان تأثير وعواقب الفعل الالكتروني اشد ضررا من الجرائم التقليدية مع هذا وضع المشرع قيود على النيابة العامة ومأموري الضبط القضائي حفاظا للحقوق والحريات الخاصة فما دام التفتيش ضمن الشروط والضوابط القانونية المحددة بالقانون فان التفتيش يقع كإجراء صحيح<sup>1</sup>.

ومن الاجراءات الموكلة لمأموري الضبط القضائي سماع الشهود دون حلف اليمين، الاصل ان يقوم مأموري الضبط القضائي بسماع اقوال الشهود وتدوينها والتوقيع عليها من قبل الطرفين ولكن هل يسمح للمجرم الالكتروني بوجود اي شاهد عليه؟ نجد ان الجريمة الالكترونية مختلفة تماما حيث انه تتم بالخفاء اي في غرف مغلقة لا يدخلها سواء المجرم الالكتروني وان كان ايضا في مكان عام كمقهى اونادي فجريمته ترتكب من خلال جهازه الخاص فينفذ جريمته عبر الضغط على بعض الازرار دون ان يلاحظ اي من الموجودين الافعال التي يقوم بها لذلك الجريمة الالكترونية لا يمكن معها وجود شهود ليستعينوا مأموري الضبط القضائي بهم كشهود على الفاعل والجريمة كما انه يوجد اسباب اخرى تحول بعدم وجود شهود هو انه يوجد فارق زمني ما بين ارتكاب الفعل واحداث النتيجة الجريمة ولا يمكن ربط ساعة ارتكابها وان كان هناك شهود فالفارق الزمني كفيل بان يتعرض الشاهد لعوامل النسيان وانه ايضا حتى لو لاحظ الشاهد على اية اشارات قد تشير الى الفاعل الى انها غير مؤكدة من ان تكون مرتبطة بالفعل المرتكب من ناحية تقنية فالفاعل دائما مجهول بالجرائم الإلكترونية لذلك لا يتم سماع الشهود من قبل مأموري الضبط القضائي الى بعد الحصول على دليل الرقمي وربطه بالفاعل وانما يتم سماع شهود للواقعة اي بمعنى اذا تعرضت احدا الشركات او الجامعات للاختراق فانه يتم سماع الشهود على واقعة الاختراق بان لاحظوا او شاهدوا عدم تمكن المجني عليه من التحكم بحسابه او عدم تمكنهم دخول الموقع المخترق للسيطرة عليه من قبل المخترق وان تباينت وقت ارتكاب الجريمة عن وقت اكتشافها<sup>2</sup>.

وايضاً لتسهيل التحقيق والحصول على ايضاحات اللازمة، فإنّ هذا الاجراء يتم من خلال النيابة العامة فان ما يقومون به مأموري الضبط القضائي والمقصود مأموري الضبط المختصين بالجرائم الإلكترونية يكون من خلال تحديد احتياجات الكترونية والحصول عليها بموافقة النيابة العامة فهذه

<sup>1</sup> اسراء جاسم عمران ، التحقيق الابتدائي ، عمان ، المركز الاكاديمي ، 2014، ص 24.

<sup>2</sup> سامر المصري ، وكيل نيابة الجرائم الإلكترونية في محافظة رام الله ، مقابلة شخصية حول سماع الشهود في الجريمة الإلكترونية ، تمت المقابلة بتاريخ 15\9\2019.

الاجراءات تصبح من ضمن الاجراءات التحقيقية للنيابة، والتي تستخدمها لمواجهة المتهم بها حين معرفته وبناء الملف التحقيقي معتمدين عليها .

كما ويكون لهم الحق في الاستعانة بالخبراء المتخصصين، فإنّ دورهم ينقسم الى قسمين الأول عند الانتقال إلى مسرح الجريمة أو عند الإبلاغ بوقوع جريمة أية كانت جنائية أو الكترونية لا بد من وجود خبير بالجرائم الكترونية، وخبير بصمات والسبب يعود أنّ الخبير المختص أقدر على تحديد الوسائل التقنية الموجودة لتحديد إمكانية الاستفادة منها للكشف عن الجريمة، وخبير بصمات لمنع أي شخص بلمس الوسائل الإلكترونية لحين رفع البصمات عنها، بالإضافة إلى الخبراء الآخرين مثلاً وجود الطبيب الشرعي في مسرح جريمة القتل ووجود كاميرات واجهزة خلوية لمقاة ووجود جهاز لاسلكي لربط على الشبكة العالمية انترنت وهذا ما منحه المشرع في المادة 64 من قانون الاجراءات الجزائية الفلسطيني كصلاحية تتمتع بها النيابة العامة من ندب للخبراء والطبيب الشرعي<sup>1</sup>.

### الضبط في الجريمة الإلكترونية

ويعد الضبط من الإجراءات الأصلية لمأموري الضبط القضائي في الدعاوي الجنائية في الجرائم التقليدية، أمّا بقرار بقانون الجرائم الكترونية أصبح من ضمن الإجراءات المكلف بها من قبل النيابة وبالتالي اصبح الضبط المقصود بالجرائم الإلكترونية من الإجراءات التحقيقية، وقد رسمت المادة 32 فقرة 3 والمادة 33 فقرة 2 و 4 و 6 آلية الضبط والتحفظ على الأجهزة والأدوات والوسائل التقنية، سواء بضبطها بموجب محضر ونقلها إلى مكان حفظ المضبوطات لدى مأموري الضبط القضائي، ويتم تحرير قائمة فيها ورفعها إلى النيابة العامة لاتخاذ المقتضى القانوني كما رسمت المواد المذكورة الإجراء القانوني في حال استحالة إجراء الضبط الفعلي للأدوات والأجهزة، وهذا مثلاً بسبب حجمها أو وجود السيرفرات داخل خزنة مبنية أو محاطة ببناء وحددت المادة 33 فقرة 5 لا بل ألزمت جهات الضبط القضائي بالحفاظ على سلامة المضبوطات والمتحفظ عليها من ناحيتين القانونية بعدم التلاعب بها، ومن ناحية فنية بالية حفظها وعدم تعرضها للكسر مثلاً وهنا يجب أن أنه أحياناً يلزم حفظ المضبوطات في غرفة بدرجة حرارة معينة في حال ابقائها متصلة بالكهرباء وضمن دائرة التشغيل، وحدد المشرع شروط التعامل مع المضبوط الكتروني. ووضعها في حرز مغلق، ويختتم عليه ويكتب عليه شريط بياناتها من تاريخ الضبط ورقم القضية التحقيقية، ومكان الضبط واسم الشخص التي ضبط منه وساعة الضبط، ومكان الضبط، وتودع في مكان حفظ المضبوطات في النيابة العامة أو أي مكان تقرره لحفظها مثلاً في قاصة المختبر الجنائي مع أخذ التدابير اللازمة لسلامة الأجهزة، ويحرر محضر الضبط ويدون فيه اسم منظمه أو من إجره واصحاب العلاقة والضبط نوعان أمّا

<sup>1</sup> انظر على نص المادة 64 من قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 .

مادي أو معنوي بما يسمى بالضبط المعنوي، مثل المعلومات والبرامج والبريد الإلكتروني، والصور والبيانات والتحفظ عليها.<sup>1</sup>

فما تم عرضه حول مهام مأموري الضبط القضائي بموجب قانون الاجراءات الجزائية الفلسطيني، وقرار بقانون الجرائم الإلكترونية رقم 10 لسنة 2018م، فقد شملت الاجراءات الأصيلة والمهام الملقاة عليهم واسقاطها على الجرائم الإلكترونية، وبذات الوقت بينيت بأنّ الاجراءات التقليدية والمنصوص عليها كالاستعانة بخبراء، والحصول على الايضاحات اللازمة لتسهيل التحقيق، والكشف والمعاينة وقبول البلاغات والشكاوي وسماع الشهود، دون حلف اليمين واتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة، وإثبات جميع هذه الاجراءات وفقاً للقواعد الاجرائية القانونية، واقتصرت محاضر جمع الاستدلال بالجرائم الإلكترونية بقبول البلاغات والشكاوي والمعاينة لمسرح الجريمة المادي والمتصل بالجريمة الإلكترونية والاستعانة بخبراء متخصصين أمّا عدا ذلك اعتبره المشرع من ضمن الاجراءات التحقيقية للنياحة العامة والتي لا تتم الا بإذن منها او بقرار صادر منها واطاف قرار بقانون الجرائم الإلكترونية إجراء يتركز عليه تحديد الاحتياج الإلكتروني من قبل مأموري الضبط القضائي والذي يجب أن يتسم بالدقة والخصوصية والسرية والسرعة، وتقديمه على شكل طلب للنياحة العامة التي لها أن تجيبه أو ترفضه أو تعدله، مثل تحديد احتياج بضرورة فحص جهاز المجني عليها لتعرضها للابتزاز الإلكتروني، وحين سماع أقوالها أدلت بأنها هي من صورت نفسها وأرسلت الصور للجاني عبر تطبيق الرسائل الإلكترونية فلا يجوز عند فحص الجهاز أن تتطال مثلاً إلى ملف الصور الخاص بل يتحدد بشكل دقيق وموضح ولا يجوز تجاوزه، والا اعتبر خرقاً لخصوصية المجني عليها.

ومن الإجراءات المهمة والاستثنائية التي نص عليها المشرع الفلسطيني في قرار بقانون الجرائم الإلكترونية هو حجب المواقع الإلكترونية، حيث خولت المادة 39 مأموري الضبط القضائي برصد المواقع الإلكترونية التي من شأنها تهديد النظام العام، والاداب العامة والامن القومي، وتقديم محضر بحث وتحري مرفقاً معه طلب الإذن لحجب الموقع الإلكتروني، ويرفع إلى النائب العام أو أحد مساعديه الذي له قبول الطلب أو رفضه، وفي حال أن الطلب محق يقدم النائب العام مذكرة برأيه الى قاضي الصلح المختص خلال 24 ساعة، الذي ينظر الطلب وله قبوله أو رفضه، وفي حال القبول يتم إعطاء الاذن بحجب الموقع لمدة سنة أشهر قابلة للتجديد وفقاً للمحضر، وفي حال الرفض لم ينص قرار بقانون الجرائم الإلكترونية إجراءات استئناف القرار الصادر، وبما أنه قرار فاصل في الطلب فإنه من الجائز استئنافه بالرجوع إلى الأحكام العامة في قانون الاجراءات الجزائية رقم 3 لسنة 2001.<sup>2</sup>

<sup>1</sup> انظر الى المادة (32) والمادة (33) من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية في فلسطين .

<sup>2</sup> انظر الى نص المادة (39) من قرار بقانون رقم 10 لسنة 2018 المتعلق بالجرائم الإلكترونية في فلسطين .

وذاات الأمر فيما يتعلق بتسجيل ونسخ ومراقبة الاتصالات حيث المادة 36، من قرار بقانون الجرائم الإلكترونية والإجراءات الواجب اتباعها، والتي تتمثل بقيود وضوابط للحفاظ على خصوصية الأفراد وحياتهم الخاصة، وجعلها في حدود ضيقة وبموافقة المحكمة المختصة بناء على محضر يقدم من مأموري الضبط القضائي، ويرفع إلى النائب العام ويقدم بنفس الإجراءات المتبعة بحجب المواقع الإلكترونية وحدد المشرع مدة اعتراض ومراقبة الاتصالات بثلاثة أشهر من تاريخ الاعتراض الفعلي تحت إشراف النيابة العامة لسلامة الاجراءات، والحصول على ما هو مطلوب لتقديمه للمحكمة المختصة اثناء المحاكمة.

### المطلب الثاني : التحقيق الابتدائي في الجريمة الإلكترونية

بعد التطرق لمرحلة جمع الاستدلال التي يقوم بها مأموري الضبط القضائي تحت إشراف النيابة العامة في إطار عملهم الذي نظمه القانون، وبيننا بأنّ الدعوى الجزائية تمر بثلاث مراحل أساسية تبدأ بجمع الاستدلالات ومن ثم يقوم مأموري الضبط القضائي بإحالة الملف مرفقاً بها كافة الاوراق والافادات وكشف الاستدلال المنظم من قبل مأمور الضبط القضائي المختص إلى النيابة العامة بصفتها سلطة التحقيق وذلك لمباشرة عملية التحقيق الابتدائي وتحريك الدعوى العمومية عملاً بأحكام المادة (1) من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م، كونها هي ممثلة الحق المجتمعي سوف نتطرق الى مرحلة التحقيق الابتدائي، بداية من الجهة المختصة في التحقيق(الفرع الأول) وبيان الادلة التي تثبت وقوع الجرائم ونسبتها الى مرتكبيها(الفرع الثاني) .

### الفرع الأول: الجهة المختصة بالتحقيق في الجرائم الإلكترونية

تعد النيابة العامة هي شعبة من شعب السلطة القضائية واحد مكوناتها وتهدف للحفاظ على الأمن وتوفير الحماية المجتمعية، ومكافحة الجريمة ومعاقبة مرتكبيها وفقاً للإجراءات التي رسمها القانون، وذلك ضمن إجراءات تحقيق عادلة مراعية للحقوق والضمانات التي كفلها المشرع للمتهم أثناء مرحلة التحقيق الابتدائي، كما وتعد النيابة وحدة واحدة لا تتجزأ، إذ قيام أحد أعضاء النيابة العامة بمباشرة أي عمل من أعمال التحقيق يعتبر كأنه صادر من النيابة العامة في مجموعها، كما ولا يجوز رد أعضاء النيابة العامة.<sup>1</sup>

تباشر النيابة العامة عملها في الملف التحقيقي وفقاً للصلاحيات المخولة لها في قانون الإجراءات الجزائية بصفة أصلية من لحظة وصول الملف التحقيقي من مأموري الضبط القضائي لا بل وقبل ذلك من لحظة وقوع الجريمة ففي جرائم التلبس في الجنايات والجنح أوجب القانون على النيابة العامة

<sup>1</sup>أشرف رمضان عبد الحميد، النيابة العامة ودورها في المرحلة السابقة على المحاكمة (دراسة تحليلية مقارنة)، الطبعة الاولى، دار النهضة العربية، 2004، ص61.

انتقلت فوراً لمكان الجريمة<sup>1</sup>، وهناك بعض الاجراءات تمنح بصفة استثنائية على سبيل النذب مثل القبض على المتهم، اوالتفتيش، وهناك من الصلاحيات الاستثنائية التي تمنح بقوة القانون مثل تفويض احد اعضاء الضبط القضائي بالقيام باعمال التحقيق في دعوى محددة<sup>2</sup>.

يعد الهدف الاساسي من التحقيق الابتدائي الذي تجريه النيابة العامة ما هو إلا إجراء لكشف الحقيقة والوقوف على مجريات التحقيق وضمان الحقوق والحريات للجاني والمجني عليه على حد سواء، وتعتبر مرحلة التحقيق الابتدائي هي الأساس في اقامة الدعوى الجزائية، واحالتها للمحكمة المختصة سيما أنّ كافة الادلة والبيانات التي تقدم أمام النيابة العامة تكون لها قيمة أساسية في المحكمة المختصة وقد تستخدم كدليل ضد المتهم حتى على صعيد الافادة الشخصية للمتهم أثناء مرحلة الاستجواب<sup>3</sup>.

وفي نهاية مرحلة التحقيق الابتدائي من قبل النيابة العامة يكون الحق للنيابة العامة في التصرف في الدعوى الجزائية اما بالاحالة للمحكمة المختصة بعد تكوين الادلة وتقييمها أو بحفظ الملف الجزائي عملاً بأحكام المادة 149 من قانون الاجراءات الجزائية الفلسطيني<sup>4</sup>، وهناك في مصر ما يسمى بأن لا وجه لاقامة الدعوى الجنائية حيث عرفته محكمة النقض المصرية بأنه "القرار الذي تصدره سلطة

---

1- نصت المادة 27 من قانون الإجراءات الجزائية الفلسطيني والتي نصت على "يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى مكان الجريمة، ويعاين الآثار المادية لها ويتحفظ عليها، ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، ويسمع أقوال من كان حاضراً أو من يمكن الحصول منه على إيضاحات في شأن الجريمة ومرتكبيها، ويجب عليه أن يخطر النيابة العامة فوراً بانتقاله، ويجب على عضو النيابة المختص بمجرد إخطاره بجناية متلبس بها الانتقال فوراً إلى مكان الجريمة.

2- نصت المادة 55 من قانون الإجراءات الجزائية الفلسطيني والتي نصت على " I. تختص النيابة العامة دون غيرها بالتحقيق في الجرائم والتصرف بها؛ للنائب العام أو وكيل النيابة العامة المختص تفويض أحد أعضاء الضبط القضائي المختص بالقيام بأي عمل من أعمال التحقيق في دعوى محددة، وذلك عدا استجواب المتهم في مواد الجنايات؛ لا يجوز أن يكون التفويض عاماً؛ يتمتع التفويض في حدود تفويضه بجميع السلطات المخولة لوكيل النيابة".

3- نصت المادة 96 من قانون الإجراءات الجزائية الفلسطيني والتي نصت على " يجب على وكيل النيابة عند حضور المتهم لأول مرة إلى التحقيق أن يثبت من هويته واسمه وعنوانه ومهنته ويستجوبه بالتهمة المنسوبة إليه وبطالبه بالإجابة عليها، ويخطره أن من حقه الاستعانة بمحام، وان كل ما يقول يجوز تقديمه كدليل ضده في معرض البيئة عند محاكمته؛ يجب إثبات أقوال المتهم في محضر الاستجواب".

4- نصت المادة 149 من قانون الإجراءات الجزائية الفلسطيني والتي نصت على " I. متى انتهى التحقيق ورأى وكيل النيابة أن الفعل لا يعاقب عليه القانون أو أن الدعوى انقضت بالتقدم أو بالوفاة أو العفو العام أو لسبق محاكمة المتهم عن ذات الجريمة أو لأنه غير مسؤول جزئياً لصغر سنه أو بسبب عاهة في عقله أو أن ظروف الدعوى وملابساتها تستوجب حفظها لعدم الأهمية بيدي الأمر ويرسلها للنائب العام للتصرف؛ إذا وجد النائب العام أو احد مساعديه أن رأي وكيل النيابة في محله يصدر قراراً مسبباً بحفظ الدعوى ويأمر بإطلاق سراح المتهم إذا كان موقوفاً؛ إذا كان قرار الحفظ لعدم مسئولية المتهم بسبب عاهة في عقله فللنائب العام مخاطبة جهات الاختصاص لعلاج.

التحقيق بعد فحص التهمة وبعد الموازنة بين الأدلة والترجيح ترجح بأن القضية لا تصلح لان تقام عنها الدعوى الجنائية" وبعد الامر بأن لا وجه لاقامة الدعوى ذو طبيعة قضائية وهو بمثابة قرار صادر عن سلطة التحقيق هذه الاجراءات تمهيداً لمرحلة المحاكمة النهائية امام المحكمة المختصة بعد احالة الملف التحقيقي من قبل النيابة العامة<sup>1</sup>.

إنّ أهم ما يميز هذه المرحلة انها تحت اشراف النيابة العامة وملتصدة مباشرة بعضو النيابة منذ العلم فيها أو اكتشافها أو تقديم شكوى أو بلاغ الى مأموري الضبط القضائي أو بالعكس في حال تم تقديم الشكوى إلى النيابة العامة فالاجراءات التحقيقية التي تقوم بها النيابة العامة من أجل بناء الملف التحقيقي تكلف فيه مأموري الضبط القضائي المختص الكترونياً، أمّا بالتفتيش أو إصدار الإذن المباشر أو الضبط أو التحفظ بنوعه المادي والمعنوي، للحصول على الدليل الرقمي من قبل وحدة الجرائم الإلكترونية وتنظيم تقرير خبرة فني من قبل الخبراء والمختصين بالمختبر الالكتروني، فمثلاً عند الحصول على رقم العنوان الالكتروني من قبل المختبر يتم مخاطبة النيابة العامة من اجل معرفة صاحب الرقم المتصل بالعنوان الالكتروني سواء رقم يعود الى شركة الاتصالات السلكية او اللاسلكية فمعرفة صاحب الرقم من قبل الشركات لا يتم إلا بموجب قرار صادر من النائب العام للجهة المعنية والتي بموجبه يتم تزويد النيابة المركزية بمكتب النائب العام بالبيانات المسجلة في شركة، والمتصلة والمتعلقة بصاحب الرقم، ومن ثم يتم تنظيم تقرير فني بالدليل الرقمي يربط العنوان الالكتروني، وتحليل الواقعة يربطها بالمتهم ورفع التقرير الى عضو النيابة المختص للسير بالاجراءات التحقيقية<sup>2</sup>.

إنّ من مميزات الحصول على الدليل الرقمي تحت إشراف النيابة العامة، واتصاله مباشرة بمأمور الضبط القضائي المختص ما قبل تنظيم محضر تحري واستدلال وفي مرحلة تنظيمه، وما قبل إجراء التحقيق وخلالها وصولاً إلى القرار المناسب أهمية في متابعة وكيل النيابة المحقق إجراءات متابعة الدليل الرقمي وفهمه من ناحية تقنية الى اكتشاف الحقيقة ومواجهة المتهم بالدليل عند الاستجواب .

وقد نصت المواد (1) و(2) من قانون الاجراءات الجزائية رقم 3 لسنة 2001، إن النيابة العامة دون غيرها الحق في اقامة الدعوى الجزائية ومباشرتها اي جعل اختصاص اقامة الدعوى والتحقيق فيها للنيابة العامة<sup>3</sup> كما وحددت المادة (55) من ذات القانون اختصاصات النيابة العامة بمباشرة التحقيق

<sup>1</sup> محمد صلاح الدين بهجت محمد، تصرف النيابة العامة في التحقيق الابتدائي، دار النهضة العربية، ص 90-91.

<sup>2</sup> سامر المصري، وكيل نيابة الجرائم الإلكترونية في محافظة رام الله، مقابلة شخصية.

<sup>3</sup> نصت المادة (1) من قانون الإجراءات الجزائية الفلسطيني على تختص النيابة العامة دون غيرها بإقامة الدعوى الجزائية ومباشرتها ولا تقام من غيرها إلا في الأحوال المبينة في القانون. ولا يجوز وقف الدعوى أو التنازل عنها أو تركها أو تعطيل سيرها أو التصالح معها، إلا في الحالات الواردة في القانون. مادة (2) يباشر النائب العام الدعوى الجزائية بنفسه أو بواسطة احد أعضاء النيابة العامة. تختص النيابة العامة دون غيرها بإقامة الدعوى الجزائية ومباشرتها ولا تقام من غيرها إلا في الأحوال المبينة في القانون.

الجزائي بكافة الجرائم الغير مشروعة والمعاقب عليها بالقانون ولها أيضاً أن تتصرف بالدعوى أما بحفظها وفقاً لما رسمت المادة (149) وأما إحالتها إلى المحكمة المختصة بدرجتها الصلح والبدائية ومن هنا فإنّ النيابة العامة لها سلطة التحقيق، والاتهام بالدعوى الجزائية بصفتها شعبة من شعب السلطة القضائية.

إنّ أهمية التحقيق الابتدائي تكمن في ما تتبعه من الاجراءات منصوص عليها بالقانون الاجراءات الجزائية للكشف عن الحقيقة وبذات الوقت تحافظ على التوازن ما بين المصلحة العامة والحريات الخاصة للأفراد، وعدم المساس بهذه الحريات الا من قبل سلطة قضائية تلتزم الحياد والشفافية والكفاءة والمهنية تدافع عن الحق العام وعن حق المجتمع بالعقاب<sup>1</sup>.

والاجراءات المتبعة في مرحلة التحقيق الابتدائي من قبل النيابة العامة سياتى سواء كنا أمام جريمة تقليدية أو جريمة الكترونية فلم ينص قرار بقانون الجرائم الكترونية أية اجراءات خاصة تتعلق بالتحقيق لذا فإنّ عضو النيابة العامة يتبع الاحكام العامة بمباشرة التحقيق بما يتواءم مع طبيعة الجريمة الكترونية من سماع شهود ندب خبراء والتصرف بالمضبوطات واستجواب المتهم مع مراعاة الضمانات الممنوحة له بموجب القانون التوقيف والحبس الاحتياطي وصولاً الى حق النيابة العامة بالتصرف بالدعوى إما بإحالتها أو حفظها قانونياً أو إدارياً بأن لا وجه لإقامة الدعوى<sup>2</sup>(مباشرة التحقيق قانون الاجراءات الجزائية رقم 3 لسنة 2001 الباب الثالث).

نهجت النيابة العامة في فلسطين نهج التخصصية فتم تخصيص أعضاء نيابة متخصصين أسوة بالدول المتقدمة حيث اصدر النائب العام لدولة فلسطين قرار بتخصيص اعضاء نيابة متخصصين لمتابعة الجرائم الإلكترونية مع اتخاذ سياسة التدريب والتمكين للمتخصصين في هذا المجال بتاريخ 2017\1\2 وهذا يعود إلى أن طبيعة الجريمة الإلكترونية تختلف عن الجريمة التقليدية، فالجريمة المعلوماتية تقم في مسرح وحقل الكتروني ذو طبيعة رقمية فيلزم للمحقق الإلمام بالتكليف القانوني المتصل بمواكبة التطور الالكتروني والمعلوماتي.

---

ولا يجوز وقف الدعوى أو التنازل عنها أو تركها أو تعطيل سيرها أو التصالح معها، إلا في الحالات الواردة في القانون.

مادة (2)

يباشر النائب العام الدعوى الجزائية بنفسه أو بواسطة احد أعضاء النيابة العامة.

<sup>1</sup>ايمن ظاهر، شرح الاجراءات الجزائية الفلسطيني، فلسطين، 2014، جزء 2، ص 7.

<sup>2</sup>-مباشرة التحقيق في قانون الاجراءات الجزائية رقم 3 لسنة 2001، الباب الثالث، ص23

## الخصائص التي يتميز بها ممثل (النيابة العامة) للتحقيق بالجرائم الإلكترونية:

لم ينص المشرع الفلسطيني على سمات خاصة بوكيل النيابة العامة في ممارسة عمله الا انه وضع الضوابط والحدود الممنوحة لوكيل النيابة في مباشرة عمله ضمن الشرعية الاجرائية، ولم تنص أي تشريعات حديثة على صفات الزامية الوجود في المحقق الذي يتولى الشق الالكتروني من القضية أو القضايا ذات الطبيعة الرقمية ولكن حسب الإحصائيات الواردة في مجال القضايا الإلكترونية فإن من يباشر التحقيق هو محقق ملم وعلى دراية بمعلومات متقدمة عن الحقل الالكتروني، وهو ما يعطي مأموري الضبط القضائي والتحقيق القدرة على تقييم عمل الخبير المنتدب لإصدار تقرير الخبرة عند تحريك الدعوى؛ وهذا بدوره يحمي المحقق من التصديق الأعمى للخبير المنتدب. في ضوء ما ورد ذكره سابقاً في هذا الجزء من الرسالة فإن عضو النيابة المختص بالتحقيق بالجرائم الإلكترونية يجب أن يتسم بالسمات التالية على سبيل المثال لا الحصر، تبعاً للتنوع الهائل بطبيعة الجرائم الإلكترونية ومنها (رسالة ماجستير السعودية) وهذه السمات تتمثل بالمهارات الفنية والمعرفة التقنية التي يجب ان يكتسبها عضو النيابة وهي:

- القدرة على التعامل مع الأجهزة الرقمية الحديثة. وفهم عناصرها المادية الملموسة والمرئية اي يجب على عضو النيابة العامة المام بانواع الاجهزة التقنية ومعرفة اشكالها ومكوناتها ومسمياتها والادوات المتصلة بها من طابعة وماسح ضوئي وميكروفون وشاشة وكاميرا وغيرها من الادوات التقنية والقدرة على التعامل مع هذه الاجهزة والادوات وهذا يساعد عضو النيابة العامة عند تطبيق وقائع الجريمة معرفة الاداة المستخدمة والية استخدامها لارتكاب الجرم الالكتروني، وهذا ما تتبعه الدول المتحضرة من خلال تدريب المحققين من مأموري ضبط قضائي ونيابة عامة بالجرائم الكترونية<sup>1</sup>.

- الإلمام بأنظمة الاتصالات السلكية واللاسلكية والية عمل الشبكة العالمية وادراك المصطلحات المستخدمة مثل البريد الالكتروني (e-mail) العنوان الالكتروني (ip) اندرويد اي كلاود وهذا يساعد عضو النيابة العامة بالتعرف على الية ارتكاب الجرم الالكتروني من خلال العالم الافتراضي وخاصة في قضايا الاختراق والتجسس واعتراض البيانات المتنقلة من خلال شبكة الاتصالات العالمية والية متابعتها من عدمه<sup>2</sup>

<sup>1</sup> حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة)، دار النهضة العربية، 2009، ص506.

<sup>2</sup> حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة)، دار النهضة العربية، 2009، ص507.

- دراسة خوارزميات التطبيقات المالية والتعاملات البنكية.اي معرفة الجانب النظري لالية عمل هذه الخوارزميات وهي عبارة عن تعليمات محددة لاداء مهمة معينة والية تنفيذها وخوارزميات الحاسوب متنوعة ويعنى كل نوع فيها لوظيفة ما مما يساعد عضو النيابة العامة بتحديد النطاق الخوازمي المحدد للجريمة المرتكبة

- متابعة التحديثات التي تتم على النطاق الرقمي.

- الدقة في العمل.

- العدالة وعدم التحيز والحياد التام.الدقةبالعملحيث تتميز الجرائم الإلكترونية بالمبادق التفاصيل وذلك يعود الى الجزئيات المعقدة والمستخدمه بارتكاب الفعل الالكتروني الغير مشروع

- المعرفة المبدئية بانظمة تشغيل الحاسوب وخاصة الاكثر انتشارا مثل انظمة ويندوز،انظمة يونيكس،والينكس ونظام ماكنتوش مما يساعد وكيل النيابة العامة المحقق بمتابعة الفعل مع مأموري الضبط القضائي قسم المختبر الجنائي الالكتروني واتخاذ القرار الفني الملائم لطبيعة الجريمة المرتكبة والمشاركة بعملية الفحص والتفتيش المعنوي لمسرح الجريمة الرقمي ومن دون ذلك سيتم اتخاذ كافة الامور الفنية والتقنية بمنأى عن مشاركة ومشاورة عضو النيابة المختص متخذًا الخبير المختص من مأموري الضبط القضائي كافة القرارات المتعلقة من الناحية الفنية

- متابعة الاطلاع والقراءة من عضو النيابة المختص لكل ما يتعلق بجرائم الشبكة العالمية من خلال قراءة ودراسة وتحليل للجرائم والقضايا الإلكترونية والية التعامل فيها من قبل سلطة انفاذ القانون والية مواجهتها والاستفادة من تجارب الدول الاخرى والاطلاع على جميع الاتفاقيات والمعاهدات الدولية والاقليمية المتعلقة بالجريمة الإلكترونية للامام بالية متابعتها دوليا لتمييزهاالجريمةبانهاعابرة للحدود ولها ابعاد دولية والاطلاع على التشريعات الاجنبية والعربية والاتجاهات القانونية لهذا النوع من الجرائم ومعرفة الانماط المختلفة للمجرم الالكتروني فعلى عضو النيابة مواكبة تطورات الجريمة الإلكترونية وادراك واقعها الانبي والمستقبلي

- مواكبة جميع الجرائم الإلكترونية وما يستجد منها والمساهمة ببناء خطة وقائية من خلال التوعية المستمرة لهذه الاجرائم ودراستها وتحليلها من خلال محاضرات ونشرات توعية وهذا يساعد عضو النيابة بالوقوف على جميع انواع الجرائم ويساهم في الية متابعتها ومكافحتها بالمجتمع الفلسطيني والتصدي لها

- المهارة في استجواب المتهم ومناقشة الشهود وذلك من خلال معرفة الادوات والاساليب المستخدمة بارتكاب الجريمة الإلكترونية وهذا يمكن عضو النيابة العامة ببناء الملف التحقيقي بشكل المتفق مع طبيعة الجريمة الإلكترونية من خلال توجيه الاسئلة المناسبة بهذا المجال وبذات الوقت فهم الدليل المستخرج من قبل الخبير الالكتروني ومواجهة المتهم به

- المام بجميع التطبيقات المتاحة على الاجهزة التقنية وهذا يساعد عضو النيابة بتوجيه التحقيق الى الهدف المراد منه استخراج الدليل الرقمي والحصول على المعلومات المهمة من قبل المجني عليهم فكثير من الاحيان يغفل المجنى عليه من ذكرها ويجهل اهمية تقديم المعلومة الدقيقة لما يخدم مصلحة لمصلحة التحقيق

- النشاط والمتابعة.

- احترام حرية الدفاع.

- الهدوء ورباطة الجأش.

- تقوم الدول الحديثة حاليا باستخدام محققين لديهم إلمام ومعرفة بأساليب القرصنة والتتبع لحل بعض القضايا، مما يسهل عمل أجهزة المباحث والنيابة العامة للتوصل للفاعل. هذا ما يتعلق باهم السمات التي يجب ان تتوفر في المحقق في الجرائم الإلكترونية لكي يقوم بعمله في استنباط الادلة الإلكترونية لتكوين الملف التحقيقي

يحكم النيابة العامة في مباشرة التحقيق الابتدائي مبادئ دستورية وضمانات قانونية يتوجب على النيابة العامة الالتزام بها<sup>1</sup>، وهذا ما اكد عليه المشرع في القانون الاساسي الفلسطيني في الباب الثاني الذي نظم الحقوق والحريات، حيث اكد على الكرامة الانسانية وعلى تجريم التعذيب بكافة صورته وكفالة الحرية الشخصية والحفاظ على الحياة الخاصة للأفراد في الدولة وكذلك اكد المشرع في هذا الباب على مبدا الشرعية الموضوعية والاجرائية وكفالة حق الدفاع للمتهم وحقه في توكيل محام

والتحقيق الابتدائي يمتاز بالسرية في الاجراءات حرصا على سرية التحقيقات واسرار الافراد وعدم التشهير بأي شخص كان تطبيقا لمبدا الشرعية الاجرائية القائلة "المتهم بريء حتى تثبت ادانته"، وايضا يتسم التحقيق الابتدائي بعدة ضمانات نظمها المشرع في قانون الاجراءات الجزائية توافقا مع المبادئ الدستورية وهذا ما جاء في الفصل الخامس من الباب الثالث في قانون الاجراءات الجزائية تحت مسمى الاستجواب حيث اكد المشرع على ضمانات المتهم اثناء التحقيق ومنها الحق في الصمت

<sup>1</sup> محمد صلاح الدين بهجت محمد، تصرف النيابة العامة في التحقيق الابتدائي، مصر، دار النهضة العربية، 2018، ص60.

والحق في المعاينة والكشف على المتهم والحق في توكيل محام والحق في تدوين التحقيق والحق في ابداء اي دفوع لعدم قبول الدعوى عملاً باحكام المادة 104 من قانون الاجراءات الجزائية<sup>1</sup>.

### الفرع الثاني: اثبات الجريمة الالكترونية

لقد عجزت الأدلة الجنائية التقليدية في شكلها المادي الملموس من اثبات وقع الجريمة ونسبتها الى فاعلها وأصطدمت جهات التحقيق وانقاذ القانون بنوع جديد من الأدلة لم يكن معهوداً من قبل إلا وهي الأدلة الجنائية الإلكترونية فما كان على الدولة إلا ان تتماشى مع التحول الجذري والعالمي في مجال اثبات الجريمة الإلكترونية سواء من حيث سن التشريعات واعداد جيشاً من الخبراء المختصين فيناً في هذا المجال .

فالدليل الإلكتروني يضم في طياته جوانب عدة تتعلق الشق القانوني والشق الإجرائي والشق الفني ولقد عالجنا الجريمة الإلكترونية من خلال الرسالة الشق الإجرائي والشق القانوني إلا ان الجانب الفني هو في غاية الأهمية إذ يحتوي على الدليل الوحيد في اثبات الجريمة الإلكترونية والذي يترتب على عدم مراعاة هذا الجانب إلى ابطال الدليل المستخرج وبالتالي لا يمكن القضاء قبول الدليل الاعتماد عليه في إصدار الحكم المتفق عليه واحكام القانوني.

يعتبر الدليل الإلكتروني الدليل الوحيد العلمي الذي يمكن استخراجه من نفس الوسائل التي استخدمها الفاعل لارتكاب الجريمة الكترونية فكما ان الفاعل يقوم باقتحام الحاسب الالي والشبكة العالمية لارتكاب الفعل الغير مشروع هي ذاتها الادوات التي يتم استخدامها من قبل الخبراء التقنيين من الضابطة العدلية لاكتشافها والحصول على الدليل الفني وتقديمه للعدلة وذلك من خلال مرحلة التحقيق الابتدائي لتكوين الملف التحقيقي وحالته للمحكمة المختصة ولذلك لا بد من توافر اسس وتعريف تقوم عليها مرحلة التحقيق الابتدائي في الجرائم الإلكترونية وذلك لما تتمتع به الجرائم الإلكترونية من سمات تميزها عن غيرها من الجرائم وتضفي عليها الطبيعة الخاصة، وهذه الاسس والتعاريفتكنم في بيان المجرم الالكتروني وبيان ماهو الدليل الالكتروني الذي يعتمد عليه في مرحلة التحقيق الابتدائي كبينة ضد المتهم وبيان خصائص الدليل ومدى مشروعيته ، وقد يراود القارئ عدة تساؤلات تتعلق بالدليل الالكتروني فبعد ان تم عرض خصائص الجريمة الإلكترونية تبين بشكل جلي ان سهولة اخفاء

<sup>1</sup> نصت المادة 104 من قانون الإجراءات الجزائية الفلسطيني والتي نصت على " إذا دفع المتهم بعدم الاختصاص أو بعدم القبول أو بانقضاء لدعوى وجب عرض الدفع على النائب العام أو احد مساعديه للفصل فيه خلال أربع وعشرين ساعة بموجب قرار قابل للاستئناف أما محاكم البداية.

الدليل الالكتروني ومحو اثارها بالكامل قبل اكتشاف الجريمة امر وارد ويؤدي الي عدم تمكن اعضاء النيابة بتعاون مع الخبراء المختصين من تعقب فاعلها فاي نوع من الدليل الذي قد يتحصل عليه المختبر الجنائي الالكتروني وكيف يتم استخراجة وثوثيقه؟ وبماذا يتسم الدليل الالكتروني لكي يتم اعتماده امام القضاء؟ ومدى تاثير تطور الادوات الكترونية في نوعية الدليل وقيمتة القانونية؟ فالدليل الالكتروني يعتبر من اخطر التحديات التي يواجهها رجال الامن والبحث الجنائي فهو كما يلاحق الخيال في الظل لذا يتعين علينا بيان ما هو الدليل الالكتروني من خلال تعريفه وتبيان خصائصه؟ فالدليل الجنائي كما اتفق على تعريفه فقهاء القانون هو "كل واقعة مادية أو معنوية تؤدي الى اثبات وقع الجريمة، او تحديد الشخصية مرتكبها، أو إثبات ارتكابه لها سواء تم ذلك مباشرة او عن طريق غير مباشر بهذا الحجة والبرهان لإثبات الفعل او نفيه".<sup>1</sup>

ويعرف الدليل الجنائي هو "الحجة والبرهان وما يستدل به من صحة الواقعة" وبتعريف اخر هو "كل واقعة مادية او معنوية تؤدي الى اثبات وقوع جريمة او تحديد شخصية مرتكبها، او اثبات ارتكابها لها سواء تم ذلك مباشرة او عن طريق غير مباشر"<sup>2</sup>، فالدليل هو الوسيلة التي تتأكد فيها النيابة العامة والقضاء بشكل يقيني على ارتكاب الجريمة والتي على اساسها تتكون قناعة الادانة او البراءة . وينقسم الدليل الجنائي الى قسمين :-<sup>3</sup>

الأول مادي مثل ضبط أداة الجريمة المحسوس او أداة حادة أو اخذ بصمات الفاعل والثاني المعنوي مثل سماع شهوداً على الواقعة أو اعتراف الفاعل . فالدليل في القضاية الجنائية قد يكون دليل مادي مثل وجود الاداة الجرمية او بصمة العين القدم واليدين للجاني او عينة من فصيلة دم الجاني بمسرح الجريمة وقد يكون الدليل معنوي كشهادة شهود

---

<sup>1</sup> محمد فاروق عبد الحميد كامل، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، اكااديمية نايف العربية للعلوم الأمنية الطبعة الأولى ، ، السعودية 1999، ص185

<sup>2</sup> طاهري عبد المطلب ، الاثبات الجنائي بالادلة الرقمية ، مذكرة مكملة لنيل شهادة الماجستير في الحقوق تخصص قانون جنائي السنة الجامعية 2014-2015 ، ص 3.

<sup>3</sup> طاهري عبد المطلب ، الاثبات الجنائي بالادلة الرقمية ، رسالة ماجستير، - جامعة المسيلة - كلية الحقوق والعلوم السياسية قسم الحقوق ، السنة الجامعية 2014-2015 - ، ص3.

او اعتراف متهم او تسجيل كاميرات يختلف الامر عند الحصول على الدليل الرقمي المستخرج من الوسط الافتراضي الغير ملموس.<sup>1</sup>

اما الدليل الجنائي الرقمي (الالكتروني) :عرفه فقهاء القانون الجنائي بانه "الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الإلكترونية من معطيات الحاسوب وشبكة الانترنت ،والاجهزة الإلكترونية الملحقة والمتصلة به وشبكات الاتصال ،من خلال اجراءات قانونية لتقديمها للقضاء كدليل الكتروني جنائي يصلح لاثبات الجريمة"<sup>2</sup>

وقد عرفته مجموعة العمل العلمية للدلالة الرقمية بانه "مجموعة المعلومات القيمة التي تخزن او ترسل في شكل رقمي"<sup>3</sup> وعرفته المنظمة الدولية لدليل الحاسوب بانه " المعلومات التي جرى تخزينها او ارسالها والتي يمكن ان تعتمد عليها المحكمة .

ومن التعريفات للدليل الرقمي "بانه الدليل الماخوذ من اجهزة الكمبيوتر ويكون في شكل مجالات اونبضات مغناطيسية او كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا خاصة ،وهي مكون رقمي لتقديم معلومات في اشكال متنوعة مثل النصوص المكتوبة او الصور او الاصوات او الاشكال او الرسوم وذلك من اجل اعتماده امام اجهزة انفاذ وتطبيق القانون "ومن خلال التعريفات نجد انها مختلفة وهذا يعود الى المعيار الذي اعتمده الفقهاء القانونيين للدليل الرقمي ما بين المعيار الشكلي المتمركز على استخلاص الدليل فقط من خلال الحاسب الالي وشبكة الاتصال العالمية او المعيار الاجرائي والذي يتمثل باجراءات استخراج الدليل الكتروني والية متابعتها مع التطور التقني الذي يلزمها وتحليلها وربطها بالجريمة<sup>4</sup>.

لم تشمل التعريفات المذكورة اي دليل رقمي قد يتم الحصول عليه من اي جهاز تقني اخر غير الحاسوب وبوجود التطور التكنولوجي التقني قد نستخلص الدليل الرقمي من الاجهزة الذكية او اجهزة

---

<sup>1</sup> احمد ابو القاسم ،الدليل الجنائي المادي ودوره في اثبات جرائم الحدود والقصاص، الجزء الاول، دار النشر بالمركز العربي للدراسات الامنية والتدريب، السعودية، 1993 ،ص185.

<sup>2</sup> خالد عياد حليبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة والنشر والتوزيع ،الاردن 2011 ،ص 230.

<sup>3</sup> - published by Elsevier inc ،third edition،eoghancasey<digitalevidence and computercrime 2011 p7،London ،

<sup>4</sup> نور الهدى محمودي، حجية الدليل الرقمي في إثبات المعلوماتية، جامعة باتنة، ص 911-912 [mahmmoudidroit@yahoo.com](mailto:mahmmoudidroit@yahoo.com)

تحديد الاماكن او من اي جهاز له خصائص ومميزات الحاسب الالي اهمها خاصية التخزين المعلومات والمعالجة الالية للبيانات.

زنظرا لعدم قيام المشرع الفلسطيني بتعرف الدليل الإلكتروني بقرار بقانون رقم 10 لسنة 2018 فإنني اتوافق مع تعريف الدكتورة نور الهدى محمودي بتعريفها للدليل الرقمي بانه "الدليل المشتق من او بواسطة النظم البرمجية المعلوماتية الحاسوبية ، واجهزة وادوات الحاسب الالي ، او شبكات الاتصال من خلال اجراءات قانونية وفنية لتقديمها الى القضاء بعد تحليلها علميا وفنيا باستخدام برامج وتطبيقات خاصة او تفسيرها في شكل نصوص مكتوبة ، او رسومات او صور او اشكال واصوات لاثبات وقوع الجريمة ولتقرير البراءة او الادانة فيها مما يضيف عليه طابع وسيلة اثبات جنائي "

- وبالتعريف المذكور نجد ان الدليل الالكتروني لم يقتصر استخراجها من الحاسب الالي فقد شمل وسائل تكنولوجيا المعلومات بكافة تطبيقاتها ووسائلها كما انه ضم شبكات الاتصال التي من خلالها تنتقل الجريمة مكانيا وزمانيا متعددة الحدود الجغرافيا وبذلت الوقت اخذا بالاعتبار التطور التقني بالبيئة الرقمية المستمر. المتلازمة للتطور التكنولوجي لغايات الحصول على دليل الاثبات الرقمي بالجريمة الالكترونية .

### سمات الدليل الالكتروني

كما ذكرنا فان الدليل الالكتروني يتكون ببيئة افتراضية وينتمي لهذا الواقع الغير ملموس من خلال المكونات المادية والمعنوية لوسائل تكنولوجيا المعلومات اهمها الحاسب الالي و البرامج الحاسوبية التي تحتويها وما يدور بالبيئة الرقمية مرتبط بالدليل المستخرج مما يجعل الاخير يتسم بخصائص نتيجة ارتباطه بالعالم الافتراضي وهذا ما يميز الدليل الرقمي عن الدليل الجنائي التقليدي وساتناول اهمها هذه الخصائص<sup>1</sup>:

- 1- الدليل الالكتروني ذات طبيعة فنية اي ان الدليل يتم استخلاصه بطرق واساليب تقنية مرتكزة على ارقام وحروف واشارات وصور وعبر تطبيقات وبرامج ذات ميزة فنية وهذا يشير بانه ليس من الصعب العبث بالدليل بتعديله او حذفه او الغاءه دون ان يتم اكتشاف هذا العبث الذي يؤدي الى زوال الدليل .
- 2- الدليل الالكتروني غير مؤكد اي ان احتمالية وجود خطأ في الحصول على الدليل الالكتروني ممكنة وخاصة اذا لم يتم اتباع اجراءات تقنية اثناء البحث عن الدليل وقد اثارث هذه السمة عدة

<sup>1</sup>محمد رزق ، الدليل الإلكتروني في الجريمة المعلوماتية ، <https://www.mohamah.net/law/> ، تاريخ الزيارة 2019\10\25.

اشكاليات في اعتماد الدليل واعتباره حجة بالاثبات لحين التأكد من سلامة الاجراءات المتبعة لاستخراج الدليل من قبل خبراء فنيين وتقنيين معتمدين .

3- الدليل الالكتروني ذات طبيعة مزدوجة علمية وقضائية والتي تتمثل في ربط الدليل الرقمي بالنص القانوني وذلك من خلال تحليل الدليل واسناده للفاعل وتطبيق صحيح القانون للاصدار الحكم القضائي مجسدا حقيقة الدليل الالكتروني لذا يجب ان يواكب الخبراء والمحقيقين والقضاة هذه الحقيقة العلمية ما يلزمها من التطورات التقنية التي تؤدي الى التنوع بالدليل الرقمي . فكلما تطورت الوسائل التقنية كلما تنوع الدليل المتحصل منها وكلما تطورت الاساليب والوسائل الفنية للحصول على الدليل

4- الدليل الالكتروني دليل غير ملموس مما يجعل صعوبة بالغة في الحصول عليه ولا يمكن باي حال من الاحوال استخدام الوسائل والاساليب التقليدية لاستخراج الدليل ولا يستطيع الانسان العادي من ذلك ايضا فلا بد من توافر مختبرات تقنية وخبراء متخصصين في مجال تكنولوجيا المعلومات والشبكات .

5- الدليل الالكتروني قابل للتلف بسهولة فما على ماموري الضبط القضائي امتصاصيين اتخاذ التدابير اللازمة لسلامة الاجهزة المضبوطة قانونيا واتخاذ كافة وسائل الحماية للحفاظ على الدليل الالكتروني المتحصل من الاجهزة التقنية المضبوطة بمسرح الجريمة .<sup>1</sup>

6- الدليل الرقمي يمتاز بطبيعة ديناميكية فهو متنقل بسرعة فائقة من خلال شبكات الاتصال العابرة للحدود الجغرافيا والزمانيا

7- الدليل الرقمي يتطور بشكل عشوائي وهذا يعود لطبيعة التطور التقني والفني لوسائل تكنولوجيا المعلومات ونظم الاتصالات المتغيرة من حين الى اخر

8- الدليل الالكتروني ذو طبيعة معقدة وصعبة لانه يعتمد على تطبيقات وبرامج ذات تقنية عالية كما وان المكونات المادية للوسائل تكنولوجيا المعلومات بشتى انواعها ذات تركيبية معقدة

كما اجاز المشرع الفلسطيني بنص المادة 2/33 من قرار بقانون بشأن الجرائم الإلكترونية ان للنيابة العامة الإذن بالضبط والتحفيز على كامل نظام المعلومات او جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها ان تساعد على كشف الحقيقة. أي ان المشرع الفلسطيني اعتبر ان كل ما يتم ضبطه او التحفظ عليه من وسائل الإلكترونية بجميع اشكالها الهواتف الذكية او أجهزة

<sup>1</sup>سونيا حماد ، مخبر الادلة الإلكترونية ، وحده الجرائم الإلكترونية ، مقابلة شخصية .

تحديد المواقع أو الروتات أو أي جهاز تقني يمتاز بمعالجته البيانات وتخزينها مصدراً لدليل جنائي إلكتروني<sup>1</sup>.

وبالتالي فإنما يتم استخراجها من هذه الرسائل التقنية دليلاً إلكترونياً قد يستخدم للثبات الجنائي وكشف الحقيقة ومن خلال ما تم عرضه من التعريفات المتعلقة بالدليل الجنائي الإلكتروني إلا أننا نستطيع أن نستخلص أن الدليل الإلكتروني يستخرج من وسائل تكنولوجيا المعلومات التي تشمل أجهزة الحاسوب وملحقاته والأجزاء المتصلة وأي جهاز إلكتروني له نفس قوام الحاسب الآلي من حيث معالجة البيانات وتخزين المعلومات يستخرج من الشبكة العنكبوتية من خلال تناقل نبضات مغناطيسية كهروكيميائية والتي يتم ضبطها واستخراجها وتحليلها لتصبح دليلاً يعتمد عليه من قبل جهات التحقيق أو القضاء .

وعليه فإن الدليل الإلكتروني أهمية بالغة المتعلقة ابتداءً بمسألة فنية تساعد جهات التحقيق من التكيف القانوني السليم والمتفق مع الواقعة المرتكبة وأهمية يرتكزون القضية عليه لإصدار الحكم المتفق وأحكام القانون من خلال فهم الحقيقة والوصول إلى العلم اليقيني البعيد عن الشك بعقيدة مبنية حول البراءة أو الإدانة في الملف المعروض عليها<sup>2</sup>.

يتميز الدليل الجنائي الإلكتروني بعدة صور وأشكاله فأصدرت وزارة العدل الأمريكية سنة 2002 قراراً يتضمن أشكال الدليل الإلكتروني مقسمة على 3 صور

1. المستندات والوثائق المكتوبة والمخزنة بالحاسب الآلي على شكل سجلات مثل البريد الإلكتروني وغرفة الدردشة عبر الإنترنت أي الدليل المرتبط بالشبكة العنكبوتية الإنترنت<sup>3</sup>

2. السجلات التي قام الحاسوب بإنشائها وتنظيمها دون التدخل البشري مثل سجلات الهاتف واي أدلة مرتبطة بحاسب الآلي وأعداداته<sup>4</sup>.

3. الملفات والسجلات التي اشترك في إعدادها وأنشؤها الإنسان بإدخال المعلومات والبيانات والجزء الآخر تم إنشاؤه من خلال جهاز الحاسوب مثل ترتيب وتنظيم البيانات والمعلومات المدخلة ومعالجتها

---

<sup>1</sup> للمزيد حول ذلك انظر إلى نص المادة 33 من قرار بقانون رقم 10 لسنة 2018 المتعلق بالجرائم الإلكترونية في فلسطين .  
<sup>2</sup> ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر 2006 ص88.

<sup>3</sup> ممدوح حسن مانع العدوان ضمانات المتهم في مرحلة البحث الأولي أو الاستدلال دراسة مقارنة ، جامعة العلوم الإسلامية كلية الشريعة والقانون، الأردن ، رسالة ماجستير ، 2011، ص69

<sup>4</sup> ممدوح حسن مانع ، مرجع السابق، ص69.

تلقائياً من قبل الحاسب كتقارير المالية على نظام اكسل أي الادلة المرتبطة بأجهزة الحاسب الآلي وشبكاتها<sup>1</sup>.

بالرغم من اعتماد التقسيمات المذكورة للدليل الرقمي إلا انه قد يتطور بحسب الطبيعة التقنية المتطورة وقد تظهر انواع اخرى مما يؤكد ان الجريمة الإلكترونية مستمرة ومتطورة وفي تزايد وتتنوع بتعدد واشكال الدليل بالرجوع الى تعدد المصادر المستخرجة منه<sup>2</sup>

وكان لا بد من وضع احكام خاصة متفقة مع الدليل المستخرج من الجرائم الإلكترونية تتعلق بآلية الإثبات للوسائل المستحدثة والتي ظهرت بظهور التقنيات التكنولوجية حتى تحدث نتيجة قانونية تمكن القضاء وسلطات التحقيق من الارتكاز عليها لكشف عن الجرائم واثباتها .

مما لا شك فيه ان الدليل الرقمي هو الدليل الوحيد الموجود لاثبات الجريمة الإلكترونية بشكل يقين وقد يرافقه دليل اثبات آخر (مساند) تقليدي يدعم ويؤكد ارتكاب الفعل الغير مشروع والمخالف للقانون اتجاه المتهم الفاعل وهنا تكمن اهمية البحث في الدليل الإلكتروني في مجال الاثبات الجزائي .

فالدليل الإلكتروني هو الوسيلة التي يتم ترجمتها في المجال الكهربائي على شكل نبضات كهرومغناطيسية او نبضات كهربائية وتسخيرها للإثبات لمعرفة مرتكب الجريمة<sup>3</sup>. فالدليل الإلكتروني هو الذي يثبت العلاقة ما بين الجاني والجريمة والمتضرر منها ان الدليل الرقمي لا يحصر فقط في اجهزة الكمبيوتر وشبكات الإنترنت بل ايضا موجود في جميع التقنيات الإلكترونية كالكاميرا والهاتف و GPS، واجهزة الاستدلال على الموقع الجغرافي ، واجهزة التسجيل الصوتية والمرئية .

لقد نص المشرع الفلسطيني في نص المادة 37 من قرار بقانون بشأن الجرائم الإلكترونية رقم 10 لسنة 2018 نصاً واضحاً وصريحة بالأخذ بالدليل الإلكتروني حيث نصت المادة: "يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات".

يمر الدليل في عدة مراحل تبدأ بالضبط المعنون أو الضبط المادي ثم التحليل ثم التقييم الى النيابة العامة القضاء ثم عرض جميع هذه المراحل امام المحكمة المختصة لتتظر في صحة الإجراءات

<sup>1</sup>عمش زهية ،غانم نسيمه ، الاثبات الجنائي في الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في الحقوق قسم القانون الخاص جامعة عبد الرحمن ميرة -جاية السنة الجامعية 2012-2013 ،ص48 و ص47 .

<sup>2</sup>خالد ممدوح ابراهيم ،التقاضي الإلكتروني ،دار الفكر الجامعي ،ط1، مصر، 2007، ص80

<sup>3</sup> - المربع السابق، ص272 .

المتعلقة بالتفتيش والضبط وربط التحليل المتفرغ في تقرير فني الكتروني من الخبراء التقنيين بالواقعة المعروضة لإصدار الحكم والمتفق مع النص القانون<sup>1</sup>

احيانا يتم الحصول على الدليل الإلكتروني دون الوصول الى مقترف الجريمة وهذه مشكلة وتحدي للمحققين والخبراء في مجال اثبات الجريمة الإلكترونية، وبعد بيان تعريف الحجية وما دور الدليل في الثبات لا بد من بيان شروط قبوله امام القضاء وبيان اهم الشروط الواجب توافرها في الدليل الرقمي حتى يتم قبول الدليل الإلكتروني المستخرج من البيئة الرقيمة الافتراضية امام القضاء يجب ان تتوافر الشروط التالية من ان الدليل لم يتعرض لأي من التزييف او التلاعب او التحريف او أي خطأ قد يؤثر على عدم صحة الدليل لم يشترط المشرع الفلسطيني والاردني والجزائري على شروط معينة للدليل الإلكتروني بيد ان تقدير صحة الدليل يعود الى القاضي المختص .

#### الشروط الواجب توافرها بالدليل الرقمي

1. ان يكون دليل يؤكد ويعكس الحقيقة والواقعة المنظورة امام القاضي يقين لا يعتريه أي شك فلا يعقل ان يقدم دليل افتراضيا تخمينيا للواقعة .
2. ان يكون دليل تقني بما ان الدليل الإلكتروني هو لاثبات جريمة الكترونية تمت بوسيلة تقنية فلا بد من ان يكون الدليل متوافق مع الاسلوب التي استخدمت لإرتكابها كما اشرت سالفاً ان الادوات المستخدمة لإرتكاب الجريمة الإلكترونية تتحصر باحدى وسائل تكنولوجيا المعلومات كالحاسوب ولايتوب والهاتف الذكي وغيرها من الادوات التكنولوجية المبتكرة وشبكة الانترنت فهي نفس الادوات التي يتم اكتشاف الجريمة من خلالها بنفس الاسلوب التقني .
3. ان يكون دليل سلبي متفقاً مع المبدأ المشروعية الإجرائية والقانونية أي ان يستخرج الدليل وفقاً للإجراءات المنصوص عليها من قبل المشرع بوجود إذن تفتيش وإذن للنفذ المباشر الذي يمكن مأموري الضبط القضائي من الحصول على الدليل بالإجراءات القانونية وأتباع إجراءات التحفظ وسلامة الاجهزة حين الضبط حفاظا على مصداقية الدليل<sup>2</sup>.
4. ان يكون دليلاً موثقاً.
5. ان يكون الدليل محددًا مرتبطًا بالواقعة المطلوب إثباتها او نفيها .
6. ان يكون دليلاً قوياً ومؤثراً منظمًا من قبل خبير مختص .

<sup>1</sup>نور الهدى محمودي، مجلة الباحث للدراسات الأكاديمية جامعة بائنة - العدد الحادي عشر - جوان 2017، ص913.

<sup>2</sup>نور الهدى محمودي، مرجع السابق، ص920.

7. ان يكون دليلاً علمياً أي أن الدليل بحقيقته العلمياً يجب ان يكون متفقاً مع الحقيقة القضائية للواقعة .

8. ان يكون الدليل مقبولاً من حيث المنطق والعقل .

9. مناقشة الدليل امام القاضي فنص القانون الإجراءات على ذلك بنص المادة ظهرت بجانب الأدلة الجنائية المصنفة على النحو التالي :-

- الدليل القانوني والذي حدده المشرع يص القانون مثل .
  - الدليل الفني مثل تقرير الطب الشرعي "التشريح" تقرير الخبرة والمضاهاة للخطوط.
  - الأدلة المادية لضبط اداة التي استخدمت بالقتل كالمسدس او السكين .
  - الأدلة القولية كشهادة الشهود.
  - الأدلة الرقمية المستخرجة من وسائل تكنولوجيا المعلومات .
- المشرع الفلسطيني ومعظم التشريعات المعاصرة اعتمد على نظام الأدلة الاقتناعية فقد نصت المادة 206 من قانون الإجراءات الجزائية الفلسطيني (تقام البنية من الدعاوي الجزائية بجميع طرق الإثبات ، إلا إذا نص القانون على طريقة معينة للإثبات فالنظام المتبع للإثبات هو النظام الحر والذي يعود ال سلطة تقدير او اقتناع القاضي بالدليل والنظام المقيد من قبل المشرع ويحق للقاضي قبول أية دليل رافقه اقتناعه به وقد نص قرار بقانون رقم 10 لسنة 2018 على حجية الدليل المستخرج من الوسائل تكنولوجيا المعلومات واعتبرها المشرع ادلة اثبات. المادة (37) يعتبر الدليل الناتج باي وسيلة من وسائل تكنولوجيا المعلومات او انظمة المعلومات او شبكات المعلومات او المواقع الإلكترونية او البيانات والمعلومات الإلكترونية من ادلة الاثبات).

إلا ان القاضي بالرغم من حريته بقبول الدليل وتقدير الاقتناع به لا بد له ان يسبب حكمه خلافاً لاحكام المادة 273 والتي تنص : " تحكم المحكمة في الدعوى حسب قناعتها التي تكونت لديها بكامل حريتها ولا يجوز لها ان تبني حكمها على اي دليل لم يطرح امامها في الجلسة او تم التوصل إليه بطريق غير مشروع".

كما على المحكمة وفق ما نصت عليه المادة 276 من الاجراءات الجزائية ان تبدي الاسباب التي اقتنع بها القاضي المختص بإصدار الحكم سواء بالادانة او البراءة<sup>1</sup>.

وهنا نرى ان المشرع الفلسطيني نص على قبول الدليل الالكتروني المستخرج وعلى حجيته امام المحكمة مقيدا القاضي وفق للاحكام العامة بضرورة تسبب حكمة وبيان الادلة التي اعتمدت عليها لتكوين قناعته، كما ان هناك العديد من الإشكالات التي تواجه رجال الضبط القضائي والنيابة العامة في استخراج الدليل والحصول عليه

تكمن الإشكالات هو ان استخراج الدليل والحصول عليه يرافقه خطوات معقدة ودقيقة وعدم اتباعها قد يؤدي بالنتيجة الى تغييرها والتلاعب بها فهنا على القاضي الخوض في التأكد من صحة ومصداقية الدليل المقدم امامه ليسترح ضميره ووجدانه وعليه تكون عقيدته واقتناعه بالدليل الإلكتروني المعروض عليه والذي يستند عليه لتسبب الحكم .

وقد رسم قرار بقانون الجرائم الإلكترونية الإجراءات الواجب اتباعها من قبل مأموري الضبط القضائي المختصصباشراف وموافقة النيابة العامة في ضبط الادوات الإلكترونية وتفتيش والولوج إليها وتحريرها وحفظها ونسخ المعلومات والبيانات في حال تم وجود صعوبات بذلك.

كما ذكرنا سابقا ان قرار بقانون وضع القواعد والإجراءات الخاصة التي يجب اتباعها في ضبط الدليل وتفتيشه والتحفظ عليه<sup>2</sup>

---

<sup>1</sup> نصت المادة 276 من قانون الإجراءات الجزائية الفلسطيني على :يشتمل الحكم على ملخص الوقائع الواردة في قرار الاتهام والمحاكمة وعلى ملخص طلبات النيابة العامة والمدعي بالحق المدني ودفاع المتهم وعلى الأسباب الموجبة للبراءة أو الإدانة، وعلى المادة القانونية المنطبقة على الفعل في حالة الإدانة، وعلى تحديد العقوبة ومقدار التعويضات المدنية.

<sup>2</sup> نص المادة 32 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية: " 1.للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة. 2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة. 3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها. 4. لوكيل النيابة أن يأذن بالنفذ 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. 5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية.

نص المادة 33 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية: " 1.للنيابة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات أو بمستعملها أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية. 2. للنيابة العامة الإنن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على

وحدد ان من يقوم بهذه الإجراءات شخصاً مؤهلاً له القدرة بالتعامل بالمضبوطات أي انه عليه اتباع القواعد الخاصة عند ضبط الجهاز وفكه وآليه نقله وقطع الكهرباء منه وأخذ الاحتياطات التقنية اثناء اداء المهمة تحسباً لأي خطأ قد يؤدي الى فقدان الدليل او المساس بمحتويات وسائل تكنولوجيا المعلومات .

فالحصول عليه بطريقة مشروعة من قبل الخبراء المتخصصين او مأموري الضبط القضائي المتخصص الالكتروني بطريقة فنياً وعلمياً فإنه يعطي الدليل حجيته الثبوتية ويصعب بينة قانونية ذات تقنية مقبول امام المحكمة المختصة. وبتساءلهل يمكن الاستناد على الدليل الإلكتروني كدليل ذي حجة قانونية امام القضاء؟

عجز القواعد وإجراءات البحث والإثبات الجنائي التقليدي امام الجريمة الإلكترونية فكان لا بد من الدخول الى عالم آخر من الأدلة الاثبات وهي الأدلة الإلكترونية المستنبطة من الاجهزة الإلكترونية بشتى انواعها تتلاءم وتتناسب مع طبيعة الجريمة الإلكترونية من ناحية فنية وتقنية تساعد على ربط الدليل الفني مع النص القانوني للجريمة المرتكبة<sup>1</sup>.

إن الدليل الإلكتروني يوازي الأدلة العلمية الجنائية مثل دليل البصمات ، للعين ، للقدم ، لليدن وتقرير فحص البصمة الوراثية ، تقرير مضاهاة الخطوط (تقريرالتزوير) تقرير خبير زراعي ، تعتبر بنية قانونية مقبول للمحكمة ويستند عليها لإصدار الحكم<sup>2</sup>. ويستبعد الدليل الرقمي من وزن البينة في حالة واحدة وهي إما ان تدحض بدليل رقمي آخر لنفس الواقعة ويقتنع به القاضي أو بطلان في إجراءات الحصول على الدليل .

ونهدف من وراء الاثبات كنشاط اجرائي هو احداث التطابق بين الواقعة المعروضة والتكييف القانوني للجريمة بصورة تقنية الى المحكمة المختصة من خلال نشاط يبذله مأموري الضبط القضائي وجهة

---

كشفت الحقيقة. 3. إذا لم يكن الضبط والتحفيز على نظام المعلومات ضرورياً أو تعذر إجراؤه، تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات. 4. إذا استحال إجراء الضبط والتحفيز بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاد إلى البيانات المخزنة بنظام المعلومات. 5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها. 6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف أو مغلف مختوم، ويكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.

<sup>1</sup>ممدوح حسن مانع العدوان ،حجية الدليل الإلكتروني في الاثبات الجزائي، مرجع سابق ، ص64،

<sup>2</sup>نور الهدى محمودي مجلة الباحث للدراسات الأكاديمية جامعة بائنة- العدد الحادي عشر -جوان 2017، ص923

التحقيق في سبيل اكتشاف حالة او وضع معين يساهم بالحصول على الدليل من اجل إصدار حكم الإدانة أو البراءة من خلال تقديم الدليل على وقوع الجريمة واسنادها الى فاعل معين<sup>1</sup>.

ايضا اعتراف العديد من التشريعات بالمحركات الإلكترونية والتوقيع الإلكتروني واتساع التعامل ببطاقات الصراف الآلي (ATM) يجعلنا ندرك اهمية الدليل الإلكتروني وغيرها من جرائم السرقة والاختلاس والاحتيال والتزوير<sup>2</sup> كما تتنوع الأدلة الإلكترونية التي تقدم للمحكمة فمنها الدليل الذي يساهم الإنسان في انشاءه .

والمقصود بالاوراق والمستندات التي استخدمت من خلال وسائل تكنولوجيا المعلومات وشبكة الانترنت للإرتكاب الجريمة عن طريق انشاء سجلات، ومنها الدليل الورقي المستخرج ويكون اما متوفر بجهاز الحاسب الآلي ذاته<sup>3</sup> او الدليل الذي يعرض امام المحكمة اما ان يستخرج من خلال التفتيش أو الضبط أو من خلال الخبرة الفنية، ونتيجة للتطور في الأدلة واستعمال الأدلة الإلكترونية في الاثبات امام القضاء كان لا بد من تطور أساليب الحصول على الدليل وهي تعد من اهم الإجراءات التي قد يترتب على الخطأ فيها بطلان كافة الاجراءات

تثور المشكلة اذا كان التفتيش والضبط للمكونات المعنوية لوسائل تكنولوجيا المعلومات أي تفتيش وضبط انظمة وسائل تكنولوجيا المعلومات .ومن خلال قرار بقانون فإن أمر التفتيش والإذن المباشر الممنوح من جهة التحقيق تسمح بتفتيش نظام المعلومات والبيانات المخزنة والمحفوظة والبيانات والأقرص الصلبة والاسطوانات والأشرطة الممغنطة ومخرجات الحاسب والمعلومات المخزنة في الوحدة المركزية لنظام الإلكتروني وفي الاطراف المتصلة بجهاز الحاسب كالفاكس والطابعة، وأيضا تعد الخبرة من اهم طرق الحصول على الدليل فمنح المشرع الفلسطيني الحق لوكيل النيابة العامة في نص المادة(64) من قانون الإجراءات الجزائية الفلسطيني الحق بالاستعانة بالخبراء وندبهم للقيام بأعمال الخبرة ان لزم الامر<sup>4</sup>

<sup>1</sup> ممدوح حسن مانع العدوان، حجية الدليل الإلكتروني في الاثبات الجزائي، كلية الشريعة والقانون جامعة العلوم الإسلامية / الأردن،المجلة العالمية للتسويق الإسلامي /المجلد السادس - العدد الاول ، لندن - المملكة المتحدة، ص 67

<sup>2</sup> ممدوح حسن مانع العدوان ، المرجع السابق، ص 68.

<sup>3</sup> - نفس المرجع ، ص 69.

<sup>4</sup> - نص المادة 64 من قانون الإجراءات الجزائية الفلسطيني نصت على :”يستعين وكيل النيابة العامة بالطبيب المختص وغيره من الخبراء لإثبات حالة الجريمة المرتكبة، ويقوم الطبيب المنتدب لذلك وغيره من الخبراء باتخاذ الإجراءات اللازمة تحت إشراف الجهة المختصة بالتحقيق، وللمحقق الحضور أثناء مباشرة أعمال الخبراء، إذا قدر أن مصلحة التحقيق تقتضي ذلك.

تعرف الخبرة بأنها إعطاء الرأي الفني او العلمي من اهل الصفة والفن والاختصاص يندبهم القاضي بخصوص واقعة تتعلق بالإثبات في الدعوى الجزائية ، ويتوقف عليها الفصل في تلك الدعوى والرأي الذي يعطيه الخبير يعد دليلاً يخضع للسلطة التقديرية للقاضي ولقناعته الوجدانية<sup>1</sup> كما يحق للمحكمة انتداب خبير الكترونياً لإي مسألة معروضة عليه في حالة الشك بتقرير الخبير. فتقرير الخبرة يجب ان يتوافق فنياً وعلمياً مع الثورة التي أحدثها التطور التكنولوجي والتقني . ويجب على الخبير ان يكون حاصل على تأهيل علمي وعملي يتمثل بالمهارة والقدرات الذهنية العالية ضرورة ترجمة الدليل الغير مقرأ الى دليل مفهوم ومقروء. ولكن هل يمكن للمحكمة في الجرائم الإلكترونية اصدار حكمها دون الرجوع للخبرة سيما ان الجرائم الإلكترونية قائمة على الأمور الفنية التكنولوجية؟

للمحكمة ان تستعين بالخبير إلا انه لا يمكنها إصدار الحكم في هذا النوع من الجرائم بسبب ارتباطها بمسائل فنية إلا من خلال خبير فني يحلل التقنيات بصورة علمية فنية مفهومة للمحكمة وللنيابة على حد سواء. لذا فالدليل المستخرج من وسائل تكنولوجيا المعلومات يجب ان يخضع الى مناقشة من قبل الخبير وهو أمر وجوبي عندما نكون امام جريمة الكترونية فإننا حتما بحاجة على تقرير خبرة فني فيها لغايات الاثبات الجنائي امام القضاء وقد يكون الخبير هو الشاهد الوحيد لإثبات الواقعة الجرمية فكما عرضها البعض الخبرة هي "الاستشارة الفنية التي يستعين بها القاضي او المحقق لمساعدته في تكون عقيدته نحو المسائل التي يحتاج تقديرها الى معرفة او دارية علميه خاصة لا تتوافر لديه الخبرة الفنية تعتبر إجراء من إجراءات التحقيق " <sup>2</sup>

وبحكم استحداث الدليل داخل مسرح اقتضت الحاجة القانونية الى استحداث نوع جديد من الخبراء فالخبير الإلكتروني هو الخبير المتخصص فنيا في علم البحث الجنائي الإلكتروني يحوز على درجة علميه بعلم في علوم الحاسوب تمنحه الاختصاص العلمي من اجل استخراج البيانات وتشعر الدليل الإلكتروني (ش) وتحليله من خلال محاكاة الدليل والاسترجاع والاستخراج من الواقع المباشر البيئية الإلكترونية (بنسخ) بنسخة تطبيق الاصل والتعامل معها دون اي اجراء قد يعول او يغير بالنسخة الاصلية المحفوظة في وسيلة تكنولوجيا المعلومات مع مراعاة الزمن التي يستغرقه الخبير من لحظة

<sup>1</sup> ممدوح حسن مانع العدوان ، مرجع سابق، ص 72،

<sup>2</sup> أمال عثمان ، الخبرة في المسألة الجنائية، رسالة دكتوراة ،كلية الحقوق ،جامعة القاهرة ، 1964، ص 28 - ص 29.

الضبط والاستلام والاستخراج والتشريح والتحليل وقد يستلزم وجود أكثر من خبير فني (التعدد) لتنظيم تقرير خبرة قضائي إلكتروني لإثبات واقعه معينة .

وهنا تكمن تقرير الخبرة من قبل خبير فني فالقضاء والنيابة العامة موجودة في مرحلة المحاكمة وتقل العلاقة القانونية القضائية بظاهرة التكنولوجيا وشبكة الانترنت، لذا فقد يستعين عضو النيابة المحقق بالخبراء وفقا لنص المادة 64 من قانون الإجراءات الجزائية رقم 3 لسنة 2001 لإثبات واقعة ما او نفيها توثيق النص من خلال خبرته وتوثيقه في تقرير يبرز فيه رؤية الفني اوالعلمي او الطبي وغير ذلك من اوجه الخبرة في قضية تحقيقية معروضة عليه ويساعد تقرير الخبرة القاضي المختص في فالواقعة وتحليلها وربطها بالفاعل وبالتالي تساعد القاضي في تكوين عقيدته الوجدانية بملف الدعوى المعروض امامه .<sup>1</sup>

وقد اوجب القانوني القضاء في الدعاوي الجزائية باتخاذ الدور الإيجابي لإظهار الحقيقة والبحث في الدليل فقد نصت المادة 251"المحكمة في أي حالة كانت عليها الدعوى ان توجه للخصوم اي سؤال ترى لزومه لظهور الحقيقة ، وأن تأذن للخصوم بذلك ويجب عليها ان تمنع عن الشاهد أي كلام بالتصريح او التلميح وأية إشارة قد تؤدي الى اضطراب افكاره او تخويفه ،ولها ان تمتنع عن سماع شهادة شهود عن وقائع ترى أنها واضحة وضوحا كافياً "

ونصت المادة 208 من قانون الإجراءات الجزائية رقم (3) لسنة 2001 " للمحكمة بناء على طلب الخصوم، أو من تلقاء نفسها اثناء سير الدعوى ان تأمر بتقديم أي دليل تراه لازماً لظهور الحقيقة، ولها ان تسمع شهادة من يحضر من تلقاء نفسه لإبداء معلوماته في الدعوى"

الخبرة القضائية الإلكترونية تحمل في طياتها شقين:-

الاول :- وهو الدراية الفنية والعلمية لما هو مكلف به من قبل عضو النيابة العامة أو القاضي المختص وهي ذاتها لا المعرفة العلمية والفنية باباً في العلوم الجنائية سواء المتعلقة بمعرفة سبب الوفاة من خلال التشريح أو تحليل مادة معينة ومكوناتها الكيميائية او المصنفة مثل السموم والمخدرات والمتفجرات<sup>2</sup>

<sup>1</sup>خير عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالإدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلية الجنائية والطب الشرعي ، الرياض 2-4/11/1428هـ الموافق 12-14/11/2007م ص24،

<sup>2</sup>احمد محمد براك ،من مبادئ الإجراءات الجزائية دراسة تحليلية تأهيلية مقارنة الجزء الاول الدعاوي الناشئة في الجريمة- الإجراءات السابقة على المحاكمة.دار الشامل للنشر والتوزيع الطبعة الاولى 2019 ،ص 658 و656.

الشق الثاني:- الطابع القضائي بإصدار قرار انتداب قضائي لإجراء مهمته الفنية والعمامة من قبل عضو النيابة المحقق او القاضي المختص وهو يؤدي عمله تحت مظلة السلطة القضائية واستحداثها<sup>1</sup> وبناءً على ما تقدم فان ما يقوم به الخبير من اعمال الخبرة القائم على معرفة فنية وعلمية واختصاص (مقدم) يعتبر من أدلة الاثبات ويعتبر تقريره ناطقاً بما فيه كما يجوز استدعاه لسماع خبرته كشاهد في الملف التحقيقي او بملف الدعوى وهذا لا يعني انه لاي يجوز الطعن به من قبل المتهم او وكيله والطلب من المحكمة المختصة ببرد الخبير وبتعيين خبير استشاري آخر لتقديم رأيه الفني والعلمي بالواقعة ذاتها فهو حق من حقوق الدفاع وضمانة للمتهم للحصول على محاكمة عادلة<sup>2</sup> وقد نظم قانون الإجراءات الجزائي رقم 3 لسنة 2001 بالفصل الثاني اعمال الخبرة من المواد 64-71 واعتبرها المشرع الفلسطيني اجراءً تحقيقياً وان كان تقريرنا لعضو النيابة العمامة فله حرية الاستعانة بأهل الخبرة سواء من تلقاء نفسه او بناءً على طلب الخصوم وفقاً للمادة 64 إلا انه ضرورياً في ( ) المسائل التي لا يستطيع عضو النيابة العمامة التقرير فيها فالمعرفة القضائية مقتصرة على الجانب القانوني المتعلق بعلم القانون فهو بحاجة الى مساعدة اهل (الخبرة) المعرفة من الفني التقني لاتخاذ القرار المناسب في الملف التحقيقي المنظور امامه .

لم ينظم قرار بقانون رقم 10 لسنة 2018 او يعرف تقرير الخبرة الإلكترونية والخبير المختص إلا انه الزم بوجود مختبرات الكترونية لدى الجهات الامنية<sup>3</sup> كما الزم ان يكون مأموري الضبط القضائي ذات مؤهل المادة 33 وبما اننا امام علم فإنه يلزم ان يكون المختصين ذات معرفة فنية واكاديمية وتقنية بعلم (الجريمة) البحث الجنائي المتعلق بعلم الحاسوب والشبكات وهي مسرح ارتكاب ووجود الجريمة الإلكترونية .

وقد ينقسم الخبراء في مجال الجريمة الإلكترونية الى مجموعات متعدد منها المختص بتشغيل جهاز الحاسوب ومنهم المختص باستخراج مكونات الحاسوب المادية والمعنوية ومنهم المبرمجين ومنهم المحللون ومنهم المختصون بالشبكات الحاسوبية او شبكات الاتصال العالمية وهذا ما يميز تقارير

<sup>1</sup> - نفس المرجع السابق، ص 658

<sup>2</sup> - نفس المرجع السابق ص 657

<sup>3</sup> - نص المادة 3 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية: 1. تنشأ وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية"، وتتولى النيابة العمامة الإشراف القضائي عليها، كل في دائرة اختصاصه. 2. تتولى المحاكم النظامية والنيابة العمامة، وفقاً لاختصاصاتهما، النظر في دعاوى الجرائم الإلكترونية.

الخبرة الإلكترونية انه قد يتم تنظيمه من اكثر من خبير واحد ذات تخصصات فنية وتقنية مختلفة لذات الواقعة<sup>1</sup>

#### شروط تقرير الخبرة الإلكتروني القضائي

- ان يكون الخبير متخصص بالمسألة الفنية المكلف بها .
- ان لا يتجاوز رأي الخبير حدود معرفته الفنية بالواقعة المكلف بها .
- ان لا يقدم رأياً قانونياً بمسألة تدخل باختصاص عضو النيابة والقاضي المختص .
- ان يكون خبيراً معتمداً ومدرجا بسجل العدلي بوزارة العدل .
- ان يكون الخبير ذات سنوات خبرة بالمسائل الفنية والتقنية
- ان يكون الخبير حائزاً على تدريبات فنية وتقنية في علم البحث الجنائي الإلكتروني ، علم الحاسوب، و/او الشبكات .
- ان يكون الخبير ذات كفاءه (خبرة ) ومعرفة عالية
- ان يكون التقرير مسبباً وموقعاً من قبل الخبير .
- ان يكون التقرير مكتوباً .
- ان ينظم الخبير تقريره تحت اداة اليمين القانوني بأداء مهمته بكل صدق وامانه .

ومن حيث حجية تقرير الخبرة هو دليل اثبات فني يخضع لتقرير المحكمة المختصة وقدرتها بربط المسائل الفنية كما هو مستند للمتهم ويكتفها التكيف المثقف واحكام القانون من خلال فهم الواقعة وتقدير الأدلة وصولاً لتكوين القناعة الوجدانية للقاضي المختص ولا يحق للقاضي ان يحكم بعلمة الشخصي بمسألة فنية او ان يفندها من تلقاء نفسه دون اللجوء الى تقرير خبرة فني آخر يساويه في قيمته القانونية والفنية والعلمية.

فبالرغم ان القاضي هو الخبير المختص بفصل الدعوى المعروضة امامه إلا أنه لا يمكن ان تحل المحكمة محل الخبير الفني في المسائل الفنية وهذا ما قضت به محكمة النقض المصرية بحكمها "لا يجوز للمحكمة ان تحل نفسها محل الخبير الفني في مسألة فنية، فاذا كان الحكم قد استند بين ما اسند إليه - في إدانته المتهمين الى ان المجني عليه قد تكلم بعد إصابته وافضى باسماء الجناه الى الشهود

<sup>1</sup>حسين بن سعيد استشاري قانوني هيئة تقنية المعلومات - السياسة الجنائية في مواجهة جرائم الانترنت دراسة مقارنة، سلطنة عُمان دار النهضة العربية 32 شارع عبد الخالق ثروت 2009، ص595.

وكان الدفاع قد طعن في صحة رواية هؤلاء الشهود ونازع في قدرة المجني عليه على التمييز والإدراك بعد إصابته ، فإنه يتعين على المحكمة ان تحققها عن طريق المختص فنياً وهو الطبيب الشرعي أما وهي لم تفعل فإن حكمها يكون معيباً لإخلاله بحق الدفاع مما يتعين نقضه<sup>1</sup>

للمحكمة ان تقرر بأخذ التقرير المنظم من قبل خبير استشاري كما للمحكمة ان تقرر ترجيح تقرير الخبرة الاستشاري على تقارير المنظمة من قبل مأموري الضبط الجنائي المتخصص فنياً بالوحدة الجرائم الإلكترونية فيعود الى تقرير المحكمة المختصة بعد مناقشتها والاعتراض عليها ولها ان تقدر المحكمة تقرير الخبرة كدليل اثبات او العكس صحيح حتى تطمئن المحكمة المختصة لدينا من التقرير المقدمة لها بالمسأل الفنية.<sup>2</sup>

لقد أجاز المشرع الفلسطيني المادة 2/22 فإن من ضمن مهام مأموري الضبط القضائي:-

إجراء الكشف والمعaine والحصول على الايضاحات اللازمة لتسهيل التحقيق والاستعانة بالخبراء المختصين والشهود دون حلف اليمين فقيام مأمور الضبط القضائي المختص بالجرائم الإلكترونية بالمحافظات والمسمى بالمستجيب الاول بالتوجه الى مسرح الجريمة وضبط الادوات الإلكترونية بالطريقة (المدون) الفنية والتقنية وبما يحفظ سلامتها فإنه يعتبر خبيراً إلكترونياً لإن ضبط الادوات الإلكترونية تخضع للاصول فنية للمحافظة عليها.

واستعانة مأموري الضبط القضائي اثناء تفتيش مسكن بعمارة الى شخص فني لتعامل بفك سيرفرات تسجيل الكاميرات المخزنة عليها له صفة الخبير في المحافظة على ما تحتويه هذه السيرفرات من تسجيلات باتباع الاصول الفنية والمتفقة مع طبيعة الأداء الإلكترونية مما يحفظ سلامتها يعتبر خبير بضمان الحصول على التسجيلات المخزنة دون التلاعب بها او فقدانها وحتى ولو لم يكن من مأموري الضبط القضائي المتخصصين.

لقد وصف القاضي (Holmes) أن التسجيل والتنصيب "عمل قدر" فرد الفقيه Silver " لأ احد ينكر أن القتل والاتجار بالمخدرات وابتزاز الاموال وغيرها من الأفعال الاجرامية ليست إلا أعمالاً أشد قذارة،

<sup>1</sup> - طعن رقم 486 لسنة 34 ف لسنة 1964\6\29 ص 30 من المؤتمر العربي.

<sup>2</sup> الدكتور أشرف توفيق شمس الدين، شرح قانون الإجراءات الجزائية الجزء الاول الدعوى الجنائية- الاستدلال والتحقيق الابتدائي - التصرف في الأوراق، القاهرة، دار النهضة العربية، الطبعة الخامسة، 2017، ص 365.

فالجريمة زادت معدلات إرتكابها خاصة الجريمة المنظمة فإذا عزمنا على محاربتها، فيجب ألا نتردد في تمكين رجال الشرطة من حمل سلاح المراقبة التليفونية<sup>1</sup> لم يعالج نص المادة (34) ضبط الرسائل الإلكترونية، وإنما اقتصرنا على مراقبة الاتصالات والمحادثات الإلكترونية، وعليه قد نواجه في بعض القضايا فيما يخص الرسائل تم ارسالها عبر بريد الكتروني E-mail لذلك فإننا نطبق المادة (51) من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 حيث ان سواء كنا أمام رسالة ورقية أو رسالة الكترونية فهي تحمل ذات الصفات بوجودها من حيث الرد عليها أو الاحتفاظ بها أو نقلها إلى شخص آخر، وبنفس الخصائص وهي الكتابة، والإرسال والاستقبال والتخزين والاستعراض من خلال برامج واعدادات حاسوبية، كما الرسائل الإلكترونية يتم استخراجها من النظام الحاسوبي عبر الطابعة المتصلة بالحاسوب لتظهر بشكل الورقي، وعليه فإن إمكانية تطبيق نص المادة 51 من قانون الإجراءات الجزائي لهذا النوع من الرسائل قد أجاز المشرع فضلاً أنه لم يحدد شكل الرسالة التي تم تضبطها إلا أننا هنا، ولسلامة الإجراءات فإنه يجب أن يتم ضبطها والحصول عليها من قبل مأموري الضبط القضائي المؤهلين تقنياً، ومختصين فنياً، بموجب تكليف من النيابة العامة بتحديد الرسالة من وإلى، ضمن محضر موثق فيه كافة الإجراءات من لحظة التكليف والإطلاع والاستخراج بزمان والمكان واسم من قام باستخراج الرسالة الإلكترونية لتصبح بشكلها التقليدي.

المادي أي يجب مراعاة الجوانب التقنية لضبط الرسائل الإلكترونية سلامة للإجراءات وتوثيق مصداقية الاستخراج على اعتبار أن الرسالة الإلكترونية قد تقدم دليل أمام محكمة الموضوع مراقبة وتسجيل الاتصالات والمحادثات الإلكترونية الهاتفية والسلكية واللاسلكية.

لقد نصت المادة 34 من قرار بقانون رقم 10 لسنة 2018<sup>1</sup> - لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل سنة، وذلك لمدة خمسة عشرة يوماً قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جديّة، وعلى من قام بالتفتيش أو المراقبة أو التسجيل ان ينظم محضراً بذلك يقدمه الى النيابة العامه"

<sup>1</sup> الحاج الطاهر زهير، من آليات الوقاية من الجريمة المعلوماتية ومكافحتها، جامعة الجزائر كلية الحقوق مذكرة للحصول على شهادة ماجستير في فرع القانون الجنائي والعلوم الجنائية، 2013، ص178.

وقد نصت المادة 51 ف1 من قانون الإجراءات الجزائية رقم 3 لسنة 2001م بأنّ للنائب العام أو أحد مساعديه أن يضبط لدى مكاتب البرق والبريد الخطابات والرسائل، والجرائد والمطبوعات والطرود والبرقيات المتعلقة بالجريمة وشخص مرتكبها إلا ان المشرع وضع قيوداً للحماية الحق في الحياة الخاصة وخصوصية الافراد، بحيث أنّه لم يعطي الحق في إجراء أي تسجيل، أو مراقبة للمحادثات الهاتفية وتسجيلها إلا بإذن صادر من قاضي الصلح المختص.

"المادة 51 ف2 كما يجوز للنائب العام مراقبة المحادثات السلكية واللاسلكية وإجراء تسجيلات لأحاديث في مكان خاص بناءً على إذن من قاضي الصلح متى كان لذلك فائدة في إظهار الحقيقة من جنائية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سنة حتى 3، يجب أن يكون أمر الضبط أو إذن المراقبة أو التسجيل سبباً ولمدة لا تتجاوز خمسة عشر يوماً قابلة للتجديد لمرة واحدة.

وتعتبر مراقبة الاتصالات والتنصت على المحادثات الإلكترونية التي تشتمل على الاتصالات السلكية واللاسلكية من الإجراءات التحقيقية للجريمة، ولا تقل عقوبتها عن سنة، كون التنصت من أخطر الإجراءات التي تمس الحياة الخاصة للأفراد ولا يلجأ إليها إلا إذا كانت سبباً في إظهار الحقيقة سواء لمصلحة المتهم أو ضده.

ونرى أن المشرع وضع أربعة قيود وضوابط وصولاً (لا) لاتخاذ هذا:

الإجراء الأول :-إذن من قاضي الصلح وقوع جنائية أو جنحة عقوبتها سنة على الأقل، وأن يكون الهدف والفائدة من التنصت، هو إظهار الحقيقة وأن يكون سبباً لإقناع قاضي الموضوع بإجابة الطلب خلال فترة محددة.

والسؤال الذي يتم طرحه إذ لم تسفر التنصت والمراقبة إلى نتيجة، والتسجيل والتنصت لا يتم إتخاذة إلا بعد وقوع جنائية أو جنحة، أي أنّه من ضمن الإجراءات التحقيقية المتخذة من قبل عضو النيابة العامة الذي أصدر قرار اتخاذ هذا الإجراء، وبالتالي يترتب عليه البطلان إذا لم يتم اتخاذ الإجراءات المتفق عليها، وصحيح في القانون، أنه في حال أن التسجيل أو التنصت كان إيجابياً ضد المتهم وي طرح من البيئة اذا كان سلبياً كأن لم يكن، حيث لم يتم الحصول على أي دليل منه سواء لمصلحة المتهم أو ضده، ومن خلال نص المادة أنّ هذا الإجراء الخطير لا يمكن اتخاذه في مرحلة الاستدلال والتحري بموجب قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 .

وأضافت المادة 34 من قرار بقانون الجرائم الإلكترونية قيديين آخرين وهما ان تكون هناك دلائل جديّة وعلى توثيق وتنظيم محضراً من قبل من قام بالتفتيش أو المراقبة أو التسجيل من قبل مأمور ضبط قضائي أو خبير مختص فنياً له اختصاص في تنظيم المحضر، أو توثيقة لتقديمه دليلاً أمام المحكمة. لقد ضيق المشرع الفلسطيني من سلطات جهات التحقيق في اتخاذ هذا الإجراء الخطير حفاظاً على حقوق وضمانات المتهم وحفاظاً على ما نص عليه القانون الأساسي بحرية الحياة والحياة للأفراد إلا في حدود المصلحة العامة حيث انه يجوز مع كلا هذه القيود والضمانات ان يتم التضحية بالحقوق اقل قيمة من اجل انقاذ حقاً ذا قيمة أكبر المتمثل بحق المجتمع وامنه واستقراره<sup>1</sup>. وقد أجازت الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية بودابست بنص المواد 19 و20 إجراء التنصت والاعتراض للدول الموقعة على الاتفاقية بشرطان تتم بموافقة الجهات القضائية وان تقوم الدول بوضع الإجراءات المنظمة لهذا الإجراء الخطير الذي يمس بحقوق الافراد الخاصة<sup>2</sup>.

### الرقابة الإلكترونية

لقد نصت المادة 39 ف 1 لجهات التحري والضبط المختصة إذا ما رصدت قيام مواقع الكترونية مستضافة داخل الدولة او خارجها بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو غيرها من شأنها تهديد الأمن القومي أو النظام العام أو الآداب العامة، وأن تعرض محضراً لذلك للنائب العام أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية أو حجب بعض روابطها من العرض.

فالمراقبة هي الرصيد من قبل مأموري الضبط القضائي المختصين وهو في مرحلة التحري والاستدلال سابق لإجراء الحجب بموجب نص المادة 39 ف2 ويلزم تنظيم محضراً بما تم رصده. وهذا ما اضافة المشرع الفلسطيني لاختصاصات مأموري الضبط القضائي فعملية الرصد هو جمع المعلومات المتعلقة بموقع الكتروني لمراقبة جميع الحركات التي تتم عبر الانترنت لصالح الموقع الإلكتروني وما يتم نشره يهدد الامن والنظام العام والآداب العامة<sup>3</sup>

<sup>1</sup> احمد براك، مبادئ الإجراءات الجزائية دراسة تحليلية تأجيلية مقارنة، الجزء الأول. دار الشامل للنشر والتوزيع الطبعة الأولى 2019. ص 679

<sup>2</sup> بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي. جامعة الجزائر 51- بن يوسف بن خده، كلية الحقوق السنة الجامعية 2017-2018، اطروحة لنيل شهادة دكتوراه علوم تخصص - قانون عام، ص 47.

<sup>3</sup> - نفس المرجع السابق. ص 101

مثال وجود صفحات ومواقع تقوم بالاحتياط على الافراد من خلال نشر دعايات أو إرسال منشور من قبل الفاعل الى المجني عليه تفيد بأنك رحبت معنا رحلة او جائزة نقدية وما عليك ان تقوم ببعض اساليب الاحتياط الإلكتروني المشابهة وقد يتبع الرصد والمراقبة الإلكتروني وجود احتياج الكتروني يُرفع لنيابة المركزية لمخاطبة مزودي الخدمة لتزويد النيابة باسم القنوات المتعلقة بالبريد الإلكتروني لمباشرة الإجراءات ويعتبر إجراء المراقبة والرصد من إجراءات التحري والاستدلال تحت إشراف النيابة العامة ليتبعه اتخاذ الإجراءات اللازمة بحجب الموقع ضمن القيود الواردة بنص المادة 39 ف2 وللمراقبة الإلكترونية فائدتين:-

الاولى: برصد ما يستحدث من جرائم الكترونية والوسائل والاساليب المستخدمة فيها. الثاني: للحفاظ على الجانب الأمني لافراد خاصة والمجتمع عامة.

وقد تميز المشرع الجزائري دونا عن التشريعات الدولية الأخرى بأنه اجاز إجراء المراقبة الإلكترونية والرصد من قبل مأموري الضبط القضائي وأجاز ايضاً إجراء آخر يسمى بإجراء التسرب وهو إجراء من اجراءات التحري والاستدلال يسمح لمأموري الضبط القضائي المختصين الاشتراك مع المشتبه به بالفعل الجرمي وخاصة من الجرائم المنظمة كغسيل الأموال والارهاب الفساد والمخدرات وإيهام المشتبه به انه فاعلاً وشريكاً معهم مستخدماً اسماً مستعاراً، وذلك الهدف من وراء إجازة هذا الإجراء من قبل المشرع الجزائري هو للمعرفة والاسلوب الذي اتبعه المشتبه به للاختراق واقتحام موقع ولم تتطرق اياً من التشريعات العربية والدولية لهذا الإجراء ضمن تشريعاتها<sup>1</sup>.

ونجد أن ضبط وتسجيل ومراقبة الاتصالات والمحادثات هو من الإجراءات التحقيقية والتي نظمها المشرع بإجراءات دقيقة بينما المراقبة الإلكترونية أو ما تسمى الرصد هو إجراء من إجراءات التحري والاستدلال يسبق الحجب الذي هو من الإجراءات التحقيقية بحيث انه مرتبط بحق الدفاع بالطعن بالإجراءات المحجب والدفاع عن الموقع الإلكتروني المحجوب والتمسك بحرية الرأي والتعبير والأمر يعود تقديرة لقاضي الموضوع بنهاية المطاف بإصدار الحكم والمتفق بإحكام القانون<sup>2</sup>.

نصت المادة 36 على ما يلي :-

<sup>1</sup>الحاج الطاهر زهير، من آليات الوقاية من الجريمة المعلوماتية ومكافحتها، جامعة الجزائر كلية الحقوق مذكرة للحصول على شهادة ماجستير في فرع القانون الجنائي والعلوم الجنائية، 2013، ص178

<sup>2</sup>خالد ممدوح ابراهيم، فن التحقيق في الجرائم الإلكترونية، مصر، دار الفكر الجامعي، 2010، ص357.

1. للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبه له ومدته.

2. تكون مدة الاعتراض في الفقرة(1) من هذه المادة لا تزيد على ثلاثة اشهر من بداية تاريخ الشروع الفعلي في انجازه قابلة لتمديد مرة واحدة فقط.

3. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لإنطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها.

لقد شملت المراقبة الاعتراض والتسجيل والالتقاط فجميعها تهدف الى رقابة الشخص لمحيطه السري احاديثه مراسلاته المكتوبة السرية المرئية وهي رقابة مشروعه محاطة بعدة ضمانات وظوابط من اجل حماية حقه الشخصي وحديثه وخصوصيته وعدم المساس بها إلا في حدود القانون فكما ميزان المجتمع اولى بالرعاية من الحقوق الخاصة للأفراد.

لم يتطرق المشرع الفلسطيني لتعريف بالاعتراض الفوري لمحتوى الاتصالات التي تشمل السلوكية واللاسلكية وأية وسيلة اتصالات مكتوبة ايضاً مثل الرسائل عبر تطبيق المواقع، التواصل الاجتماع أو تطبيق المحادثات مثل (الواتس اب) ولكن وفقاً لما جاء بنص المادة 36 لقد نظم المشرع الفلسطيني الإجراءات الواجب اتباعها لإجراء الاعتراض.

وقد عُرف الاعتراض فقهاء بأنه "التتبع السري والمتواصل لمراسلات المشتبه فيه قبل واثناء وبعذارتكابه للجريمة: وقد عُرف بأنه :عملية مراقبة سرية المراسلات السلوكية واللاسلكية وذلك في إطار البحث والتحري في الجريمة وجمع الادلة أو المعلومات حول الاسخاص المشتبه فيهم او في مشاركتهم في ارتكات الجرائم<sup>1</sup>

ومن خلال نص المادة نجد ان المشرع الفلسطيني اجاز الاعتراض على محتوى الاتصالات التي قد يكون مقروءاً او مسموعاً كما واننا نجد ان إجراء الاعتراض قد يكون في مرحلة سابقة لوقوع الجريمة أو اثناءها وبعدها بأذن يمنح من قبل المحكمة المختصة لطلب النائب العام وأهم ما يميز الاعتراض انه يتم دون رضاء المشتبه به وإلا انبثقت الغاية من وجوده فسيتمكن الفاعل من اخفاء كل ما يدور حول بسبب اعتراض مراسلاته واتصالاته وبذلك لن يتمكن المحقق من الحصول على الدليل لإثبات جريمة

<sup>1</sup>غلاباحمد، اعتراض المراسلات السلوكية واللاسلكية في التشريع الجزائري ، مذكرة ماجستير 2014/2016 ، جامعة باجي مختار - عنابة - كلية الحقوق، ص3.

مثلاً الاتجار بالمخدرات وغسيل الاموال ولا يقع الاعتراض إلا على دليل غير مادي يتمثل بالمحتوى المتناقل عبر قنوات الاتصالات السلكية واللاسلكية بجميع اشكالها<sup>1</sup> من قبل جهة متخصصة تقنياً وهذا ما اكدته نص المادة 36 ف3 بأن يتم تكلف جهة بتنفيذ الإذن الاعتراض وإعلام والتنسيق مع النيابة العامة منذ بدء الاعتراض حتى انتهائه، فلا يمكن أن يتم اعتراض دليل غير مادي بوسيلة تقليدية، كما إنه لا يمكن ذلك ايضاً بعدم وجود متخصص تقني لتوثيق الدليل المستخرج من إجراء الاعتراض وحماية مصداقيته لتقديمه لقاضي الموضوع والوصول الى الحقيقة، وبذلك يعتبر الاعتراض إجراءً تحقيقاً يهدف الى الدخول والحصول على نسخة من محتوى الاتصال وتفريغها في محضر خاص، وتقديمها لجهات التحقيق لرفعها للمحكمة المختصة.

كما ويتميز إجراء الاعتراض أنه يتم عن بعد باستخدام برامج وتطبيقات تقنية، بينما التصنت والتسجيل والمراقبة يكون وضع أجهزة تسجيل صوتي وكاميرات التسجيل المرئي في داخل المكان الخاص المراد إجراءه فيه.

وبعد بيان الإجراءات التحقيقية من مرحلة الاستدلال والتحقيق الابتدائي ستكون هناك مرحلة التصرف في الدعوى الجزائية أما بالحفظ او الإحالة إلى المحكمة المختصة وهنا لا بد من بيان مرحلة المحاكمة في الجرائم الإلكترونية (المبحث الثاني) وهل هذه المرحلة تتوافق مع مرحلة المحاكمة في الجرائم التقليدية ؟

---

<sup>1</sup> غلاباحمد، اعتراض المراسلات السلكية واللاسلكية في التشريع الجزائري، المرجع السابق، ص7.

## المبحث الثاني: مرحلة المحاكمة في الجرائم الإلكترونية

تطرق الباحثة في المبحث الأول الاجراءات التحقيقية لدى النيابة العامة، وتناولت للجوانب المهمة التي اعتبرها مفصلية لانجاح بناء الملف التحقيقي بالتكليف القانوني المنفق مع أحكام القانون وصولاً إلى إحالة الملف وفقاً للاجراءات التي رسمها القانون بلائحة اتهام الى المحكمة المختصة فكان لا بد من التطرق الى تعريف الدليل الالكتروني وخصائصه وذلك للاهمية القانونية من ناحية وللاهمية الاجرائية من ناحية اخرى فالدليل الالكتروني له قيمة في الاثبات الجنائي في الجرائم الإلكترونية فلا يمكن أن يقدم دليل تقليدي لاثبات الجنائي في جريمة الكترونية فلم يعد الدليل العادي يجدي نفعاً بالاثبات لهذا النوع من الجرائم فهو لا يتناسب مع طبيعة الجريمة الإلكترونية ولا يتوافق مع البيئة التي كون فيه الدليل وهو العالم الافتراضي غير الملموس وبما ان الدليل الالكتروني هو المحور الاساسي الذي يدور حوله كافة الاجراءات المرسومة لدى النيابة العامة والقضاة وصولاً الى اصدار الحكم والمنفق واحكام القانون ووجدت أن من الامور المهمة التي يجب تناولها هو السمات التي يجب أن يتصف فيها عضو النيابة العامة المختص والقضاة ايضا فالجريمة الإلكترونية بمجملها احدثت تغييرا جوهريا بالمنظومة القانونية والاجرائية على حد سواء وفقا لطبيعتها الخاصة، وهذا ما يجب أن يلم به عضو النيابة العامة من خلال إجراءاته التحقيقية، ويجب أن يلم به القاضي المختص بالدليل الالكتروني سيقدم ويناقش أمام هيئة المحكمة المختصة فلا يعقل أن يصبح القاضي متلقي لما يقدم امامه فهو من عليه تقدير الادلة والاقتناع به ليصدر حكمه السديد وعلى يقينا تام متفقا واحكام القانون وما جذبني من خلال اعداد رسالتي الأهداف وراء ارتكاب هذه الافعال فالجريمة الإلكترونية ترجمة لاحد مظاهر الحياة الانسانية، وما رافقتها من ابتكارات وتطورات تقنية اجتاحت العالم بصورة لا يتصورها العقل وتسارعت في ظهور فئة جديدة من مرتكبيها الذين استطاعوا استغلال هذه الوسائل واستحداث أساليب لاستغلالها في مجال تنفيذ وارتكاب الجريمة الإلكترونية، فالتكنولوجيا انشئت جيلا رقميا بامتياز.

وتسعى الاجهزة الشرطية الى متابعته وملاحقته بمعاونة النيابة العامة للوصول إليه من خلال الدليل الرقمي، وهو دليل الإثبات الوحيد الذي يربط المتهم بالجريمة المرتكبة، وخطورة هذا المتهم إقليمياً ودولياً وفي هذا المبحث سنبين المبادئ العامة لاختصاص المحكمة سواء العيني أو الاقليمي (المطلب الأول) ومن ثم بيان الإجراءات المتبعة أمام المحكمة في الجرائم الإلكترونية ومشروعية الدليل امام القضاء وحجيته في بناء الاحكام وصولاً للطعن بهذه الأحكام (مبحث ثاني).

## المطلب الاول : المبادئ العامة للاختصاص في الجرائم الإلكترونية

نصت الفقرة الثانية من المادة (3) من قرار بقانون بشأن الجرائم الإلكترونية رقم 10 لسنة 2018

"تتولى المحاكم النظامية والنيابة العامة، وفقاً لاختصاصاتهم، النظر في دعاوي الجرائم الإلكترونية"<sup>1</sup>

ونصت المادة (2) من ذات القرار بقانون على: "1-تطبق احكام هذا القرار بقانون على اي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، او امتد أثرها داخل فلسطين، سواء كان الفاعل أصلياً أم شريكاً أم محرصاً أم متدخلاً، على أن تكون الجرائم معاقباً عليها خارج فلسطين مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ.

2-يجوز ملاحقة كل من يرتكب، خارج فلسطين، إحدى الجرائم المنصوص عليها في هذا القرار بقانون في إحدى الحالات التالية:<sup>2</sup>

أ-إذا ارتكبت من مواطن فلسطيني .

ب-إذا ارتكبت ضد أطراف أو مصالح فلسطينية .

ج-إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية، وجد بالاراضي الفلسطينية ولم تتوافر في شأنه شروط التسليم القانونية" .

فالسطة الوحيدة التي منحها القانون صلاحية حل النزاعات وفصلها بين افراد المجتمع هي السلطة القضائية، وهي الجهة الوحيدة المختصة بتحديد القانون الواجب التطبيق، فتصدر أحكامها في الوقائع المعروضة عليها باستقلالية تامة دون أي تدخل من اي من الجهات والسلطات الأخرى وهذا ما اكد عليه القانون الاساسي الفلسطيني في المواد (97- 98)<sup>3</sup> وكذلك ما نص عليه المشرع في المادة 1 و2 من قانون السلطة القضائية رقم (1) لسنة 2002<sup>4</sup>.

وهنا نتسال هل إجراءات المحاكمة أو ما يسميها بعض التشريعات الأخرى مثل التشريع المصري مرحلة التحقيق النهائي في الجرائم الإلكترونية تختلف عن مرحلة المحاكمة في الجرائم الجنائية

<sup>1</sup>انظر إلى المادة (3) قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية في فلسطين .

<sup>2</sup>نصت المادة رقم (2) من قرار بقانون رقم 10 لسنة 2018 على نطاق تطبيق القانون .

<sup>3</sup>- نص المادة 97 من القانون الاساسي الفلسطيني والتي نصت على: "السلطة القضائية مستقلة ،وتتولاها المحاكم على اختلاف انواعها ودرجاتها ،ويحدد القانون طريقة تشكيلها واختصاصاتها وتصدر احكامها وفقا للقانون ،وتعلن الاحكام وتنفذ باسم الشعب العربي الفلسطيني " ونصت المادة 98 من القانون الاساسي الفلسطيني على: "القضاة مستقلون ، لا سلطان عليهم في قضائهم لغير القانون،ولا يجوز لاية سلطة التدخل في القضاء او في شؤون العدالة

<sup>4</sup>- نص المادة 1 من قانون السلطة القضائية والتي نصت على : " السلطة القضائية مستقلة ،ويحظر التدخل في القضاء او في شؤون العدالة" نص المادة 2 من قانون السلطة القضائية والتي نصت على: " والقضاة مستقلون لا سلطان عليهم في قضائهم لغير القانون "

"التقليدية"، وهل خصص القانون الفلسطيني قضاة متخصصين للنظر والفصل في دعاوي الملفات الإلكترونية المعروضة أمام السلطة الحاكمة وخاصة أننا أمام جرائم مستحدثة، وفي غاية التعقيد ترتكب بأعلى درجات الذكاء و الدهاء، وعادة تكون متطورة ومختلفة لما اعتاد عليه القضاة، سواء من ناحية طبيعة الجرم والأدوات والأساليب المستخدمة لارتكابها، فهي ذات طبيعة خاصة مع احتفاظها بأنها قد تستخدم للاعتداء على الأموال والأشخاص على حد سواء .

لقد نصت المادة(2) من قرار بقانون الجرائم الإلكترونية رقم 10 لسنة 2018 بأن الاختصاص للمحاكم والنيابة العامة النظامية، ولم يفرد القانون تخصيصاً سواء للقضاة أو للنيابة العامة للنظر بالدعاوي الإلكترونية، وعليه فإن إجراءات المحاكمة بالقضايا الإلكترونية هي ذاتها الإجراءات المتبعة بالنظر والفصل بالجرائم الجنائية الأخرى، ووفقاً لما نص عليه قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 كاصل عام. فيما نصت المادة (1) من قانون تشكيل المحاكم النظامية بفلسطين رقم 5 لسنة 2001 : "تنظر المحاكم النظامية في فلسطين في المنازعات والجرائم كافة الا ما استثني بنص قانوني خاص، وتمارس سلطة القضاء على جميع الاشخاص،<sup>2</sup>- تحدد قواعد اختصاص المحاكم وتباشر اختصاصها وفقاً للقانون" فالقانون مصدراً لتحديد الاختصاص والولاية القضائية، فلم يرد استثناء في قرار بقانون الجرائم الإلكترونية سواء بتخصيص قضاة وأعضاء نيابة عامة أو بتحديد محكمة معينة للنظر بالدعاوي الإلكترونية، وبذلك نكون أمام ما نصت عليه المادة 163 من قانون الاجراءات الجزائية الفلسطيني<sup>1</sup>، فلا يعقل أن تترك ولاية واختصاص القضاة بالنظر والفصل بجميع أنواع القضايا دون نصوص تقيد من أعماله القضائية، فقد حددت المادة المذكورة القواعد الأساسية التي على أساسها تحدد المحكمة المختصة للنظر والفصل بموضوع الجريمة الإلكترونية فمثلاً عند نشر فيروسات أو اختراق نظام الكتروني يعود للشركة تجارية أو ما يتعلق بالابتزاز الالكتروني فان المحكمة صاحبة الاختصاص هي المكان التي وقعت به الجريمة اي مكان وجود الشركة او الضحية بقضايا الابتزاز الالكتروني التي تضررت من هذه الافعال وفي حال ان قام الفاعل بنشر صور او افلام اباحية خلافا لنص المادة "توثيق مادة القاصرين من قرار بقانون أو ترويج لمستحضر طبي مخالف للمواصفات والمقاييس الطبية وغير مرخص "توثيق المادة من قانون الصحة والقرار بقانون فيعقد الاختصاص بمكان اقامة الفاعل. وإذا ارتكب فاعل الجريمة جرماً معاقب عليه بقرار بقانون

<sup>1</sup>- نص المادة 163 من قانون الاجراءات الجزائية الفلسطينيين والتي نصت على: " يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة، او الذي يقيم فيه المتهم، او الذي يقبض عليه فيه"

الجرائم الإلكترونية وهرب، فمكان إلقاء القبض عليه يحدد اختصاص المحكمة للنظر فيها، وهو ما بينته المادة (1) من القرار بقانون، حيث نص المشرع على حدود الاختصاص للجرائم التي تقع خارج الحدود الجغرافية لدولة فلسطين، أما في جرائم الاعتداء والجرائم المستمرة وحالات الشروع وجرائم المتابعة فقد حدد المشرع الفلسطيني النظر ضمن اختصاص الأماكن التي وقعت فيها أي فعل في نطاق الجريمة.<sup>1</sup>

الجريمة المستمرة يعتبر مكانا للجريمة كل محل تقوم فيه حالة الاستمرار. أما جريمة الاعتداء وجرائم المتابعة يعتبر مكانا للجريمة كل محل يقع فيه أحد الأفعال الداخلة فيها حالة الشروع تعتبر الجريمة أنها وقعت في كل مكان يقع فيه عمل من أعمال البدء بالتنفيذ.

نتطرق للموضوع الاختصاص الدولي أو خارج حدود فلسطين حيث أدرك وعالج المشرع الفلسطيني الخاصة التي تمتاز بها الجرائم الإلكترونية بأنها عابرة للحدود تمر بدون تأشيرة دخول يمكن معها تحديد المحكمة أو الدولة صاحبة الصلاحية للنظر فيها. مثلاً حصان طروادة بنشر الفيروسات إلى عدد من الدول بهدف اتلاف النظام الإلكتروني<sup>2</sup>، قد تُرتكب في دولة ما خارج حدود دولة فلسطين، أو دول أخرى وتنتج آثارها في دولة أخرى مغايرة، أو عدة دول مثل المثل السابق نشر الفيروسات فالاختصاص وفقاً لقرار بقانون المادة 1 فالاختصاص القضائي في الجرائم الإلكترونية كقاعدة عامة في الفقه القانوني الدولي في الجرائم التي ترتكب عبر الشبكة العنكبوتية (الانترنت) هو محل تحقق النتيجة الجرمية سواء كان الفاعل داخل الدولة أو خارجها<sup>3</sup>.

فالاختصاص هو صلاحية القاضي العادي بمباشرة ولايته القضائية في نطاق معين، وتقتصر هذه الصلاحية على نوع معين من الإجراءات وفي حدود معينة، فهي صلاحية تمنح وفقاً للقانون للقاضي لأداء وظيفة قضائية معينة، أما الاختصاص المكاني: فيقصد به وفقاً لما نصت عليه المادة 7 من قانون العقوبات رقم 16 لسنة 1960 الصلاحية الإقليمية من حيث المكان في تطبيق القانون الفلسطيني في حال ارتكاب أي من الجرائم داخل الأراضي الفلسطينية، واعتبر المشرع أن مصطلح الأراضي وفقاً لنص المادة 7 يشمل طبقة الهواء التي تغطي الأراضي الفلسطينية، والبحر الإقليمي إلى مسافة خمسة كيلو مترات من الشاطئ، والمدى الجوي الذي يغطيه البحر الإقليمي، والسفن والمركبات

<sup>1</sup> - ينظر المادة 164 من قانون الإجراءات الجزائية .

<sup>2</sup> - ينظر المادة 166 من قانون الإجراءات الجزائية والمادة 1 من قرار بقانون رقم 10 لسنة 2018 بشأن الجريمة الإلكترونية.

<sup>3</sup> أيمن عبد العال ، الاختصاص القضائي في القانون الاردني، صفحة 135،

الهوائية، واعتبر المشرع أيضاً من ضمن الاختصاص الاقليمي الأراضي الأجنبية التي يحتلها الجيش الوطني<sup>1</sup>.

هذا ما نصت عليه الأحكام العامة في قانون العقوبات النافذ من حيث السريان المكاني لتطبيق القانون في حال ارتكاب أي فعل يعاقب عليه بموجب قانون العقوبات النافذ، كما ونصت المادة(2)من القرار بقانون رقم(10) لسنة 2018 بشأن الجرائم الإلكترونية:(1-تطبق احكام هذا القرار بقانون على اي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء كان الفاعل أصلياً أم شريكاً أم محرصاً أم متدخلًا، على أن تكون الجرائم معاقبا عليها خارج فلسطين مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ؛ 2-يجوز ملاحقة كل من يرتكب، خارج فلسطين، إحدى الجرائم المنصوص عليها في هذا القرار بقانون في إحدى الحالات التالية :

أ-إذا ارتكبت من مواطن فلسطيني.

ب-إذا ارتكبت ضد أطراف أو مصالح فلسطينية.

ج-إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية وجد بالأراضي الفلسطينية ولم تتوافر في شأنه شروط التسليم القانونية).

وهنا يتضح جليا بأنّ الجرائم الإلكترونية ومن أهم الخصائص التي تقوم عليها انها من الجرائم العابرة للقارات وهذا ما أوضحناه في الفصل الأول، حيث يمكن أن تقع جريمة في الاراضي الفلسطينية ويكون المجرم موجود في الخارج وبالتالي يكون هناك تساؤلات حول ما هو القانون الواجب التطبيق هل قانون مكان وقوع الفعل ام قانون اقامة المجرم؟ وهذا التساؤل يقودنا الى بيان الصلاحية الذاتية والشخصية لتطبيق القانون في حال ارتكاب الفعل الذي يعد جريمة .

حيث نصت المادة (9) والمادة(10) من قانون العقوبات رقم 16 لسنة 1960 على مبدأ الصلاحية الذاتية ومبدأ الصلاحية الشخصية لسريان قانون العقوبات والتي بينت حالات انطباق قانون العقوبات

---

<sup>1</sup> - نص المادة 7 من قانون العقوبات رقم 16 لسنة 1960 والتي نصت على: " -1تسري أحكام هذا القانون على كل من يرتكب داخل المملكة جريمة من الجرائم المنصوص عليها فيه.

تعد الجريمة مرتكبة في المملكة، إذا تم على أرض هذه المملكة أحد العناصر التي تؤلف الجريمة أو فعل من أفعال جريمة غير متجزئة أو فعل اشتراك أصلي أو فرعي:

تشمل أراضي المملكة طبقة الهواء التي تغطيها، والبحر الإقليمي إلى مسافة خمسة كيلومترات من الشاطئ والمدى الجوي الذي يغطي البحر الإقليمي والسفن والمركبات الهوائية الأردنية.

والأراضي الأجنبية التي يحتلها الجيش الأردني إذا كانت الجريمة المقترفة تنال من سلامة الجيش أو من مصالحه.

على كل من يرتكب جريمة ومتى ينطبق القانون على المجرم<sup>1</sup>، وبعد بيان حالات سريان القانون لما في ذلك من حفاظ على سيادة الدولة سيما أنّ تطبيق القانون وعلى الأخص قانون العقوبات، والذي يعد قوة الدولة في الحفاظ على سيادتها وكرامتها من المساس بها، وإيقاع العقوبة الرادعة على كل من يمس بها سننقل لبيان الاجراءات اثناء مرحلة المحاكمة وماذا يترتب عليها من آثار.

### المطلب الثاني: الاجراءات المتبعة في مرحلة المحاكمة في الجرائم الإلكترونية

تعد مرحلة المحاكمة من اهم المراحل التي تمر بها الدعوى الجزائية سيما انها تقوم على الرقابة على صحة كافة الاجراءات التي تمت من قبل مأموري الضبط القضائي ومن قبل النيابة العامة في اعداد الملف التحقيقي وايضا تقوم على وزن للبيانات المقدمة من قبل النيابة العامة بصفتها ممثلة للحق العام حيث نصت المادة (207) من قانون الاجراءات الجزائية الفلسطيني على: "لا يبنى الحكم الا على الادلة التي قدمت اثناء المحاكمة والتي تمت مناقشتها في الجلسة بصورة علنة امام الخصوم" يعتبر الدليل هو الاساس الذي يبنى عليه الحكم ولكن قبل الخوض في مدى مشروعية الدليل المقدم امام المحكمة وحجيته في بناء الاحكام القضائية لا بد من بيان الاسس التي تقوم عليها مرحلة المحاكمة والتي تتمثل في الضمانات التي كفلها المشرع في قانون الاجراءات الجزائية الفلسطيني نص قانون الاجراءات الجزائية الفلسطيني على العديد من الضمانات اثناء مرحلة المحاكمة فمنها ما هو يتعلق بالمبادئ العامة للمحاكمة وتتمثل في شفوية المرافعة وعلانية الجلسات وتدوين اجراءات المحاكمة وتقييد المحكمة وفقا لمبدأ عينية الدعوى الجزائية ومبدأ شخصية الدعوى الجزائية(توثيق تعريف عينية وشخصية الدعوى)، وهناك من الضمانات ما يرتبط بالمتهم، وأهمها أن الأصل بالمتهم البراءة مراعاة لمبدأ قرينة البراءة، وحق المتهم بالدفاع عن نفسه وتوكيل محام، وهناك من الضمانات المرتبطة بالمحكمة والقاضي الجزائي تتمثل بالتزام المحكمة بالنصوص القانونية التي يعمل القضاة على تطبيقها لتنظيم إجراءات المحاكمة وصولاً إلى المحاكمة العادلة، ومنها ما يتعلق بالقاضي الجزائي من حياد القاضي وعدم حكمه بعلمه الشخصي عملاً بأحكام المادة(205) من قانون الاجراءات الجزائية<sup>2</sup>.

<sup>1</sup> - نص المادة 9 من قانون العقوبات رقم 16 لسنة 1960 والتي نصت على: " تسري أحكام هذا القانون على كل أردني أو أجنبي - فاعلاً كان أو شريكاً محرصاً أو متدخلاً - ارتكب خارج المملكة جناية أو جنحة مخلة بأمن الدولة أو قلد ختم الدولة أو قلد نقوداً أو زور أوراق النقد أو السندات المصرفية الأردنية أو الأجنبية المتداولة قانوناً أو تعامللاً في المملكة.

<sup>2</sup> - نص المادة 205 من قانون الإجراءات الجزائية الفلسطيني التي نصت: " لا يجوز للقاضي أن يحكم بعلمه الشخصي".

حيث ذكرنا سابقاً بأن الدعوى الجزائية تمر في ثلاث مراحل تبدأ بإحالة لائحة اتهام من قبل وكيل النيابة إلى محكمة الصلح في الجرح و/أو قرار اتهام مصادق عليه من قبل النائب العام إلى محكمة البداية مما يجعل ملف الدعوى بحوزة المحكمة، فالإحالة إجرائياً نقل الملف التحقيقي، وتغيير حالته إلى دعوى وإدخالها بحوزة المحكمة<sup>1</sup>.

وقد صنف المشرع الفلسطيني الجرائم الإلكترونية بقرار بقانون رقم 10 لسنة 2018م، إلى جنح وجنايات حيث تتراوح العقوبات بعدها الأدنى من ثلاثة شهور إلى سبع سنوات كحددها الأقصى وتتراوح الغرامات من مئتان دينار أردني إلى خمسة آلاف دينار أردني، ثوثيق المواد مثل المادة 17 و 19 و 18 و 5 و 6 مثلاً على سبيل المثال:

تتعد العلاقة الاجرائية القضائية بمجرد أن تبلغ المحكمة المختصة الخصوم، وتكليفهم بالمثل أمامها للبدء بالاجراءات التقاضي بصورة علنية، وعلى المحكمة أن تقرر سرية الجلسات حفاظاً على النظام العام أو الأخلاق، ولم تختلف الاجراءات المتبعة أمام المحكمة بالجرائم الإلكترونية عن الجرائم الأخرى، فهي ذات الاجراءات بتلاوة التهمة على المتهم بلغة بسيطة من قبل النيابة العامة، والرد عليها بحضور القاضي من قبل المتهم، والبدء بتقديم البيانات السمعية المتمثلة بسماع الشهود، والورقية والمتمثلة بالمستندات والتقارير وغيرها من الأوراق المتصلة بإثبات الواقعة المنظورة امام القضاة، والتي على ضوءها يصدر القاضي حكمه المبني على علم، ويقين بكامل قناعته الوجدانية والقضائية مصدراً لحكمه، والمتفق مع احكام القانون، وقد نظم قانون الإجراءات الجزائية أصول إجراءات المحاكمة

- 
- 1- نص المادة 53 من قانون الإجراءات الجزائية الفلسطيني والتي نصت : "إذا رأت النيابة العامة في مواد المخالفات و الجرح أن للدعوى الصالحة لإقامتها بناء على محضر جمع الاستدلالات تكلف المتهم بالحضور مباشرة أمام المحكمة المختصة. نص المادة 152 من قانون الاجراءات الجزائية الفلسطيني والتي نصت على : " 1. إذا تبين لوكيل النيابة أن الفعل يشكل جنابة فانه يقرر توجيه الاتهام إلى المتهم ويرسل ملف الدعوى إلى النائب العام أو احد مساعديه.
  2. إذا رأي النائب العام أو أحد مساعديه وجوب إجراء تحقيقات أخرى، يعيد ملف الدعوى إلى وكيل النيابة لاستيفاء هذه التحقيقات.
  3. إذا وجد النائب العام أو أحد مساعديه أن قرار الاتهام صائب يأمر بإحالة المتهم إلى المحكمة المختصة لمحاكمته.
  4. إذا وجد النائب العام أو احد مساعديه أن الفعل لا يشكل جنابة بأمر تعديل وصف التهمة وإعادة ملف الدعوى إلى وكيل النيابة لتقديمها إلى المحكمة المختصة.
  5. إذا وجد النائب العام أو احد مساعديه أن الفعل لا يعاقب عليه القانون، أو أن الدعوى انقضت بالتقادم أو العفو العام أو سبق محاكمة المتهم عن ذات الجريمة، أو انه غير مسؤول جزائياً لصغر سنه أو لعاهة عقلية، أو لعدم وجود أدلة أو إن الفاعل غير معروف أو أن الظروف والملابسات تقتضي حفظ الدعوى لعدم الأهمية يأمر بحفظها.
  6. إذا رأت النيابة العامة حفظ الأوراق عليها أن تعلن أمر الحفظ للمجني عليه والمدعي بالحقوق المدنية، فإذا توفى أحدهما كان الإعلان لورثته في محل إقامتهم.

بالباب الخامس من قانون الاجراءات الجزائية(237- 271)، ولم ينص قرار بقانون بشأن الجرائم الإلكترونية على أية إجراءات خاصة، أو استثنائية أمام المحكمة، وهذا يعيدنا إلى الدائرة المهمة، فليس مهماً ما يقدم أمام القضاء من بينات، والأهم هو صحة استخراج الدليل الإلكتروني ومشروعيته ومناقشته مع ذوي الخبرة المختصين، وهذا ما يثير العديد من التساؤلات حول الدليل وتعريفه، ومدى مشروعيته وحجيته، سيما أن الدليل هو الأساس في بناء الحكم سواء بالإدانة أو البراءة؟

من خلال دراستي المتعلقة بالجريمة الإلكترونية تبين لي ظهور جريمة مستحدثة جديدة مترابطة بالتقدم العلمي والتكنولوجيا وابتكار واختراع اجهزة الكترونية لم تكن البشرية شاهدة عليها من قبل وحدثت تغيير جوهرى في خلق بيئة جرمية متغايرة ومتطورة لم نعهدها من قبل ادت بالنتيجة الى تغيير في المفاهيم الجرمية وآلية ملاحقتها سواء على الصعيد العمل الشرطي او العمل التحقيقي للنيابة العامة والعمل القضائي وصولاً الى إصدار الحكم إما ببراءة المتهم، أو إدانته بناءً على الدليل المستخرج من هذا العالم الافتراضي، غير الملموس، فلا مجال لإبقاء المنظومة الإجرائية بوجود دليل مادي في الجريمة الإلكترونية فهو لا يتناسب مع طبيعتها ولا يجدي نفعاً لإثبات الجريمة، واسقاط الحكم المناسب، وتحقيق الردع العام بحق الدولة بالعقاب والحفاظ على المنظومة العامة بحفاظ الأمن والمصلحة العامة والاستقرار العام في الدولة.<sup>1</sup>

تعد مرحلة المحاكمة من أهم مراحل لآنها مرحلة إصدار الحكم من خلال الجزم بتوافر دليل أو أدلة يفتتح القاضي بها سواء بالإدانة أ البراءة .

تعتمد حجية الدليل الإلكتروني على قوة الخبراء التقنيين القضائين الذين يقومون باستخراج الدليل بشكل يقين لا مجال للشك فيه، فالدليل الإلكتروني هو الدليل الوحيد والافضل لإثبات الجريمة الإلكترونية، فلا بد من التأكد من سلامة الدليل من العبث وسلامة استخراجة فنياً وفقاً للإجراءات المتبعه، والتأكد من دقة الأدوات والوسائل المستخدمة.

كما ويخضع الدليل الى مبدأ المناقشة مادة في قانون الإجراءات فلا يجوز ان يعتمد القاضي على دليل لم يتم مناقشته من قبل الخصوم والإطلاع عليه هي ضمانة اكيدة للحصول المتهم على محاكمة عادله ويترتب على عدم مناقشة الدليل بطلانه بالمطلق.

<sup>1</sup>لارك ، (الدليل الإلكتروني في مجال الاثبات الجزائي ) ، العدد السابع والعشرون سنة 2017،ص272.

وهذا ما يجعلنا نتطرق الى تعريف الحجية قانوناً : هي "الوصف الثابت بحكم الشرع يلحق بمضمون الحكم القضائي أو الامر القضائي فيه ويكون غير قابل للمناقشة فيه مرة اخرى". أما فقها: " هي حجية الشيء المحكوم فيه او عدم نقضه ، معناها هو ان القاضي اذا عرضت منازعة امامه في موضوع ما وتنازع الخصوم فيه وفحص القاضي ادلة كل خصم ومستنداته ووزنها ثم قال كلمته الفاصلة في موضوع هذه الدعوى فلا يجوز لأي من الخصوم ان يعيدوا عرض النزاع مرة ثانية لمناقشة ما سبق ان فصل فيه"<sup>1</sup>.

لقد نال الدليل الالكتروني قوة وحجية في الإثبات لتعلقه بمعايير علمية لا مجال للشك فيها مما جعلها تمتاز بالثقة والمصدقية امام المحاكم إلا ان وجود دليل الالكتروني يربط الفاعل "المتهم" بما هو مسند إليه لا يكفي اذا لم يحاط بالقواعد الاثبات القانونية من حيث صحة الإجراءات واتفاقها مت المبادئ القانونية والضمانات الاساسية للمتهم حماية للحقوق وحرمانه إلا في الاحوال التي اجازها المشرع ومراعاة القواعد الموضوعه. فالمشرع الفلسطيني أجاز الاثبات بجميع طرق الاثبات، واعتمد على نظام الإثبات الحر في الاقتناع بالإدلة.

مخالفة الإجراءات المنصوص عليها من قبل المشرع تؤدي الى بطلان الدليل، وما يستخلص منه مثل إجراء الاعتراض والمراقبة بدون اتخاذ الإجراءات الموضوعية والشكلية والهدف من وراء متطابقة القواعد الموضوعية والإجرائي هي لكي يصيب السهم الهدف ويصل القاضي الى الحقيقة لتمكنه من إصدار الحكم بالبراءة والإدانة.

فيخضع الدليل الى عدة مبادئ اساسية وهي مبدأ تقنية الدليل اي وصول القاضي الى مرحلة اليقين بالدليل .

تؤكد الفعل وحقيقته من خلال معرفة القاضي الحسية والعقلية لدليل وتحليله واستنتاج الحقيقة بجزم ويقين<sup>2</sup>.

التأكد من سلامة الدليل من العبث وسلامة استخراجة فنياً وفقاً للإجراءات المتبعه والتأكد من دقة الادوات والوسائل المستخدمة.

---

<sup>1</sup> نور الهدى محمودي، جامعة بائنة MAHMOUDIDROIT@YAHOO.COM1، مجلة الباحث للدراسات الأكاديمية - العدد الحادي عشر - جوان 2017، ص919.

<sup>2</sup> طاهر عبد المطلب، الإثبات الجنائي بالأدلة الرقمية، جامعة المسيلة - كلية الحقوق والعلوم السياسية - قسم الحقوق - السنة الجامعية 2014-2015، ص52،

كما ويخضع الدليل الى مبدأ المناقشة مادة في قانون الإجراءات، فلا يجوز ان يعتمد القاضي على دليل لم يتم مناقشته من قبل الخصوم والإطلاع عليه هي ضمانات أكيدة للحصول المتهم على محاكمة عادلة ويترتب على عدم مناقشة الدليل بطلانه بالمطلق.

### **المطلب الثالث: الآثار المترتبة على عدم مشروعية الاجراءات**

يترتب على الحكم ببطلان إجراء ما تجريد الإجراء من آثاره القانونية أي تعطيله عن أداء وظيفته في الخصومة الجنائية، ولا يقتصر هذا الأثر على الإجراء الباطل فقط، بل يمتد إلى الإجراءات اللاحقة على الإجراء الباطل.

وبطلان الإجراء لا يقرر بقوة القانون بل لابد من حكم أو قرار يصدر من المحكمة سواء كان بطلان مطلقاً أي متعلقاً بمصلحة عامة أم كان البطلان نسبياً أي متعلقاً بمصلحة خاصة وعلى ذلك فان العمل الإجرائي يكون فعالاً ومنتجاً لآثاره القانونية إلى أن يحكم ببطلانه<sup>1</sup>.

ويترتب على التقرير بالبطلان آثار هامة منها ما يتعلق بالإجراء الباطل ذاته ومنها ما يتعلق بالإجراءات المتصلة به سواء كانت سابقة أو لاحقة فمتى تقرر بطلان إجراء معين وجب استبعاد الدليل المستمد منه وإلا أضحت الضمانات التي يقرها القانون للحفاظ على الحريات عديمة الجدوى .

### **الفرع الأول: آثار البطلان على الإجراء المعيب ذاته**

بمجرد أن يصدر حكم ببطلان إجراء من الإجراءات يترتب عنه زوال آثاره القانونية وفقدان قيمته في الدعوة الجزائية ويتوقف عن أداء وظيفته الأساسية المنوط به، ويصبح الإجراء المعيب منعماً كأنه لم يكن أبداً كما إن بطلان الإجراء يترتب عنه زوال أثره القانوني المؤدي لقطع تقادم الدعوى الجزائية وعليه فان الأحكام والقرارات النهائية أو الصادرة قبل الفصل في الموضوع لا تقطع التقادم إذا صدرت اثر التكليف مباشر صرح ببطلانه كما إن تبليغ حكم مشوب ببطلان لا يمكن اعتباره إجراء من إجراءات المتابعة القاطعة للتقادم .

<sup>1</sup> محمد أمين الخرشنة، مشروعية الصوت والصورة في الإثبات الجنائي، (دراسة مقارنة)، دار الثقافة، عمان، الأردن، 2011.

## الفرع الثاني: آثار البطلان على الإجراءات الأخرى

إذا حكم ببطلان إجراء ما فإن هذا البطلان لا يقتصر تأثيره في الإجراء نفسه بل قد يمتد البطلان إلى الإجراءات اللاحقة عليه أما بنسبة للإجراءات السابقة فقد اختلف الفقهاء بشأن تأثير الإجراء الباطل فيها.<sup>1</sup>

### أولاً - أثر البطلان على الإجراءات السابقة

القاعدة أن الإجراء الباطل لا يمتد بطلانه إلى الإجراءات السابقة عليه، لأن تلك الإجراءات السابقة قد تكون صحيحة قانوناً دون أن تتأثر في وجودها بالإجراء الذي تقرر بطلانه. فقد نصت المادة 477 من قانون الإجراءات الجزائية الفلسطيني على أنه " لا يترتب على بطلان الإجراء بطلان الإجراءات السابقة عليه أو بطلان الإجراءات اللاحقة عليه إذا لم تكن مبنية عليه وإذا كان الإجراء باطلاً في جزء منه فإن هذا الجزء وحده الذي يبطل "

ويتضح من القاعدة القانونية السابقة إن الإجراءات السابقة على الإجراء الباطل تبقى صحيحة، وتنتج جميع أثارها القانونية، فبطلان الحكم مثلاً لعدم التسبب لا يترتب عليه بطلان إجراءات نظر الدعوى والمرافعات التي وقعت صحيحة قبل الإجراء الباطل.<sup>2</sup>

### ثانياً - أثر البطلان على الإجراءات اللاحقة

القاعدة هي إن الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة عليه إذا كانت هذه الإجراءات تترتب عليه مباشرة، وتثير هذه القاعدة مسألة تتعلق بأهمية المعيار الذي يبين مدى العلاقة التي تربط بين العمل الإجرائي الباطل والأعمال التالية له حتى يمتد إليها البطلان أو بعبارة أخرى بيان متى يكون الإجراء مترتباً على ما سبق وقد اختلف الفقه<sup>3</sup>، في تحديد معايير الإجراءات المترتبة على الإجراء الباطل، إلا إن المعيار السائد هو أنه ينبغي توافر علاقة تبعية بين الإجراء السابق والإجراءات اللاحقة عليه، بحيث يعتبر الأجراء السابق المقدمة الضرورية والشرعية لصحة العمل اللاحق فالقانون وحده هو الذي يتولى بيان أهمية الإجراء الباطل بالنسبة لما تلاه من الإجراءات، فإذا أوجب مباشرة إجراء معين قبل آخر فيصبح الإجراء الأول بمثابة السبب الوحيد للإجراء الذي تلاه أي لا يمكن مباشرة الإجراء الأخير دون الإجراء الأول فكان هذا الإجراء الأول شرطاً لصحة الإجراء التالي له فإذا

<sup>1</sup> - لؤي عبد الله نوح، مدى مشروعية المراقبة الالكترونية في الإثبات الجنائي، مركز الدراسات العربية للنشر والتوزيع، مصر، 2017، ص 239.

<sup>2</sup> - محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة، 1998، ص 372.

<sup>3</sup> فتحي والي، نظرية البطلان في قانون المرافعات، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2005، ص 676.

بطل ترتب عليه بطلان الإجراء الذي بنى عليه<sup>1</sup>. لقد عالج المشرع الفلسطيني أثر بطلان الإجراء على الإجراءات اللاحقة عليه في المادة (477) من قانون الإجراءات الجزائية إذ اعتبرت هذه المادة أن الإجراء اللاحق يكون باطلا إذا كان مبنيا على الإجراء الذي سبقه، وقد نصت هذه المادة على أنه " لا يترتب على بطلان الإجراء بطلان الإجراءات السابقة عليه أو بطلان الإجراءات اللاحقة عليه إذا لم تكن مبنية عليه...."

اما بالنسبة لموقف القضاء المصري فرقت محكمة النقض المصرية في هذا الشأن بين أمرين :  
\_إن الإجراء المعيب سبب أو مقدمة شرعية مفترضة لاتخاذ الإجراء اللاحق وفي هذه الحالة لا مناص لمحكمة الموضوع من القضاء بالبطلان في شأن الإجراء اللاحق وإلا كان حكمها مخالفا للقانون  
\_في حالة ما إذا كان الإجراء اللاحق قد تأثر بالإجراء السابق عليه فجاءت نتيجة على وجه معين ويرجع تقدير ذلك لمحكمة الموضوع وتبت فيه على ضوء ظروف كل من الإجراءين<sup>2</sup>..

يتبين مما سبق إن بطلان الإجراء المعيب لا يؤثر على صحة الإجراءات اللاحقة عليه متى كانت هذه الإجراءات مستقلة عن الإجراء المعيب فاستقلال الإجراء اللاحق يعصمه من البطلان الذي شاب ما سبقه من إجراءات وبالتالي فإنّ الحكم ببطلان التفتيش المعيب لا يؤثر على صحة الإجراءات التالية إذا كانت مستقلة عن هذا التفتيش وغير مرتبطة به<sup>3</sup>

كما يستخلص بان الحكم بامتداد اثر بطلان الإجراء المعيب إلى كل أو جزء من الإجراءات اللاحقة له يخضع لتقدير القضاة الذين يلتزمون بتسبب حكمهم وإبراز العلاقة السببية والرابطة المباشرة بين الإجراء الباطل والإجراءات اللاحقة ويخضع قرار قضاة الموضوع لرقابة المحكمة العليا التي تراقب مدى وجود علاقة سببية بين الإجراء الباطل المعيب والإجراءات التالية له<sup>4</sup>.

وقد أكدت المحكمة العليا الجزائرية في عدة قرارات لها إن اثر بطلان الإجراء يمتد إلى الإجراءات اللاحقة له إذا كان العيب يتصل بها وتوجد بينهما علاقة سببية<sup>5</sup>.

<sup>1</sup> - فتحي والي، المرجع السابق، ص 677.

<sup>2</sup> بوسندة عباس، مشروعية الدليل الالكتروني في الإثبات الجنائي، كلية الحقوق والعلوم السياسية جامعة الجيلالي ليايس، سيدي بلعباس، الجزائر، 2013-2014، ص 330..

<sup>3</sup> لؤي عبد الله نوح، المرجع السابق، ص 242،

<sup>4</sup> - أحمد الشافعي، البطلان في قانون الإجراءات دراسة مقارنة، دار هومه، الجزائر 2005، ص 190.

<sup>5</sup> - قرار صادر في 16/12/1986، طعن رقم 45442 عن الغرفة الجنائية الأولى للمحكمة العليا الجزائرية .

ومن اهم الضمانات المتعلقة بتسبيب وتعليل الاحكام والتي نصت عليها المادة (276) من قانون الاجراءات الجزائية الفلسطيني والمادة (2/5) من قانون تشكيل المحاكم النظامية رقم 5 لسنة 2001 والذي اشترط بأن يكون الحكم معلا وموضحا للاسباب الموجبة له سيما ان تعليل الاحكام وتسبيبها من اهم الضمانات كون الحكم يعبر الخلاصة النهائية للاجراءات والذي يتوجب ان يكون معلا ومسببا وذلك لبسط رقابة المحاكم الاعلى درجة على المحاكم الدنيا اضافة لرقابة اطراف الدعوى على الحكم مما يزيد من الثقة بالجهاز القضائي، وايضا يترتب على هذه الضمانة ضمانا ترتبط ارتباطا وثيقا بها تتمثل بحق اطراف الدعوى بالطعن بالاحكام امام المحكمة المختصة، كما وتخضع الاحكام الصادرة من محكمتي الصلح والبداية الى طرق الطعن العادية كالاستئناف والغير عادية كالنقض واعادة محاكمة وفقا لما نص عليه قانون الاجراءات الجزائية رقم 3 لسنة 2001.

## الخاتمة:

تحدثت هذه الدراسة عن الجريمة الإلكترونية ومدى خطورتها على العالم بأسره، وتكمن خطوره هذه الجريمة كونها عابرة للحدود والقارات وهذا ما يمنحها ميزة خاصة عن الجرائم التقليدية ويجعلها على درجة من التعقيد سيما ان الجاني يتحكم بالفعل الجرمي الذي يرتكبه عن بعد ويلحق الضرر بالمجني عليه وهو على درجة عالية من الخبرة، وبالتالي فإن مواجهة المجرم الإلكتروني في معظم الأحيان تكون ذات تعقيد وبحاجة الى الخبرة العالية.

وقد بينت الدراسة تعريف الجريمة الإلكترونية وماهيتها واهم سماتها، ومن خلال ذلك تبين لنا بأن الجريمة الإلكترونية لها أدوات ومكونات تختلف عما هو عليه في الجريمة التقليدية فهي بحاجة الى أدوات خاصة لتظهر الى حيز الوجود ولتكتمل أركانها، وكذلك مرتكبي هذه الجريمة يتميز بخصائص معينة تجعله يختلف نوعا ما عما هو عليه المجرم في الجرائم التقليدية، واستعرضت الدراسة آلية التصدي الى هذه الجريمة لما قد يتسبب عليها من نثار على المجتمع والفرد المجني عليه، وقد تم مكافحة هذه الجريمة دولياً من خلال عقد المؤتمرات، وصياغة الاتفاقيات الخاصة بهذا الشأن، وعلى الصعيد الوطني تم اصدار قرار بقانون خاص بشأن الجريمة الإلكترونية يحتوي على نصوص ناظمة لبيان الجريمة الإلكترونية وادواتها، والية مكافحتها والعقوبات التي تترتب على هذه الجريمة، وهذا ما تم بيانه في الفصل الأول من الدراسة

وفي الفصل الثاني تم الانتقال الى دراسة الشق الاجرائي في مكافحة الجريمة الإلكترونية، حيث تطرقنا الى الإجراءات التحقيقية في مرحلة الاستدلال التي يقوم بها مأموري الضبط القضائي، وفرقنا ما بين مرحلة الاستدلال في الجرائم التقليدية والجرائم الإلكترونية كون ان الجرائم الإلكترونية تمتاز بنوع من الخصوصية، فإن مرحلة الاستدلال تعد من اهم المراحل في هذا النوع من الجرائم وتتطلب درجة عالية من الخبرة، وبعد مرحلة الاستدلال يتم الانتقال الى مرحلة التحقيق الابتدائي امام النيابة العامة والبحث في الدليل الإلكتروني والية استخراج واستعماله امام المحكمة المختصة ذلك ان الدليل الإلكتروني يختلف عن الدليل في الجرائم التقليدية ويتطلب الية معينة ليصبح دليلا صالحا للاستخدام امام المحكمة، وفي نهاية التحقيق الابتدائي يتم التصرف في الملف التحقيقي اما بالاحالة الى المحكمة المختصة او بالحفظ وفي حالة الإحالة لا بد من بيان الإجراءات المتبعة امام المحكمة المختصة سيما ان المشرع الفلسطيني لم ينظم باجراءات خاصة مرحلة المحاكم في الجرائم الإلكترونية واكتفى بما هو

عليه في الاحكام العامة في قانون الإجراءات الجزائية الفلسطيني، وقد ترتب على هذه الدراسة العديد من النتائج والتوصيات التي تؤثر في إيجابا في مكافحة الجريمة الإلكترونية .

### النتائج:

1. إن العصر التكنولوجي الذي اجتاح العالم بايجابياته لم يخلو من سلبيات تمثلت في إساءة استخدام الانظمة ووسائل تكنولوجيا المعلومات مما ادى الى ظهور جرائم الكترونية تتطور بتطور الادوات والوسائل التقنية مما ادى الى ظهور انواع جديدة من هذه الجرائم.
2. تتميز الجريمة الإلكترونية بعدة سمات وخصائص لا نظير لها في الجرائم التقليدية ويتميز المجرم الالكتروني بسمات تجعله مختلفا عن المجرم المتعارف عليه، وهذه ما يجعل اليات التحقيق فيها تتسم بالصعوبة والحاجه الى المعرفة الفنيه. وأن النظم التقليدي غير ملائمة لاثبات الجريمة الإلكترونية سواء من ناحية اجرائية وقانونية وتقنية.
3. ان الجريمة الإلكترونية هي جريمة عابره للحدود ولا تخضع للحدود الجغرافية لذلك فهي تعد من اخطر الجرائم التي تواجهها الجهات المختصة لسهولة ارتكابها واخفاء اثارها فترتكب من قبل اشخاص في غاية الدهاء والذكاء، وعلى قدر عال من المعرفة التقنية والعلمية لذلك فهي تطلب من جهات التحقيق الجريمة الإلكترونية أن يكونوا اشخاص مؤهلين للتحقيق فيها سواء على مستوى جهات انفاذ القانون او جهات تطبيق العدالة النيابة والقضاة.
4. ان الدليل الرقمي وكيفية الحصول عليه واستخراجه والاجراءات الواجب اتباعها تشكل اشكالية حقيقية امام الجهات القضائية تمثل بمشروعية وصحة ومصداقية الحصول على الدليل الرقمي والتي تؤثر على اقتناع القاضي الجنائي به
5. ان الادوات المستخدمة لتنفيذ الجريمة الإلكترونية هي ذاتها الادوات التي تستخدم لاكتشافها من قبل الخبراء المتخصصين
6. ان قرار قانون الجرائم الإلكترونية بدولة فلسطين رقم 10 لسنة 2018 غير كافي لمكافحة الجريمة ولم يتطرق الى تعريف الجريمة الإلكترونية والتفتيش الإلكتروني .
7. ان الجريمة الإلكترونية ليست بديلا عن الجريمة التقليدية بل نمطا حديثا وشكلا مستحدثا للجرائم التقليدية فهي

تتفق باحكامها العامة مع الجريمة التقليدية بضرورة وجود الركن المادي والنتيجة الجرمية والعلاقة السببية وبالركن المعنوي الا انها اختلفت من حيث الاسلوب المستخدم لإثبات هذه الاركان والتحقق منها.

8. اضافة الجريمة الإلكترونية نوع جديد من الادلة والذي يعتبر الدليل الوحيد في الاثبات الجنائي ويعتبر هذا الدليل من اكثر التحديات التي يواجهها رجال الامن والبحث الجنائي والخبراء والسبب يعود الى ان الدليل محله في الوسط الافتراضي الغير ملموس .

9. عدم وجود قضاة و مدربين ومتخصصين بالجريمة الإلكترونية.

### **التوصيات:**

1- ان تنشأ محاكم محايدة دولية كنقطة اتصال مع جميع دول العالم بحيث ان تقوم هذه المحاكم المحايدة بالتحقيق وملاحقة المجرمين وخاصة في الدول المختلفة لحل إشكالية الاختصاص. وكحل الإشكاليات الناتجة من اختلاف القوانين ففي بعض الدول مجرمة أفعال غير مجرمة وفي دولة أخرى مما يؤدي الى افلات الجناة من العقاب

2- ان (تشارك) تتكاثف الجهود الدولية من اجل الوصول الى تعريف موحد للجريمة الإلكترونية من خلال (الجهات) من خلال اشراك الجهات التشريعية والقضائية وجهات انفاذ القانون والمختصين الفنيين لسد جميع الثغرات التي قد تعتري الجريمة الإلكترونية وخاصة فيما يتعلق باثباتها الجنائي من الناحيتين القانونية والفنية

3- رفق الجهات الفنية المختصة بالتدريب المستمر ومواكبة جميع التطورات التكنولوجية والتقنية واطلاعهم على اخر المستجدات بالجريمة الإلكترونية.

4- وضع استراتيجية على مستوى جميع المؤسسات من اجل رفع التوعية وادماج هذه الجرائم في المناهج التعليمية والتوعية و مواكبته.

5- يجب ان يتم تاهيل مأموري الضبط القضائي كاختصاص عام بأهمية دور وسائل تكنولوجيا المعلومات للكشف عن الجريمة سواء كانت جريمة الكترونية بحتة او كالاختراق او أداة تم استخدامها لارتكاب جريمة جنائية وإبلاغ مأموري الضبط القضائي المختصين بموجب القانون بضرورة تواجدهم خاصة باجراءات المعينة والتفتيش

- 6- اعداد وتدريب وتخصيص قضاة متخصصين بالجرائم الإلكترونية وتدريب القضاة لهذا النوع الجديد من الأدلة في الاثبات التي تتميز بالطابع العلمي والتقني والفني ذات الشكل الرقمي وتدريب وتأهيل اعضاء النيابة والشرطة والجهات الاخرى ذات العلاقة للتعامل مع أجهزة الحاسوب والإنترنت.
- 7- تطوير إجراءات إثبات الجريمة الإلكترونية وهذا يتطلب إيجاد قواعد خاصة للتعامل مع الأدلة الجرمية في هذه الجرائم لأن البحث عنها يتم داخل نظام الكتروني معقد، يصعب فيه اثبات هوية الجاني وجمع الادالة.
- 8- عقد اجتماعات بشكل مستمر ما بين اعضاء النيابة المتخصصين وما بين ماموري الضبط المتخصصين للوقوف على التطورات في مجال الجريمة الإلكترونية
- 9- عقد اجتماعات تنظيمية ما بين النيابة العامة المتخصصين وشركات الاتصالات ومزودي الخدمة والمتعلقة بتلبية الاحتياجات الإلكترونية وما يعترئها من اشكاليات وحلها .
- 10- يجب على جهات التعاون الدولي المسؤولة عن التنسيق بين الدول لتحديد صيغة موافقة على منكرات تفتيش الخوادم بما لا يسيء من الحفاظ على البيانات ولا ينتهك خصوصية الافراد اوالمؤسسات او الدول تماشياً مع مبدأ مصلحة الفرد والمجتمع الدولي من خطر الهجمات الإلكترونية

## قائمة المصادر والمراجع:

### أولاً: المراجع العربية :

- احمد ابو القاسم،الدليل الجنائي المادي ودوره في اثبات جرائم الحدود والقصاص الجزء الاول دار النشر بالمركز العربي للدراسات الامنية والتدريب، السعودية، 1993 .
- أحمد البراك، عبد القادر جرادة، الجريمة الإلكترونية في التشريع الفلسطيني، دراسة تحليلية تأصيلية مقارنة، دار الشروق للنشر والتوزيع ،رام الله ،فلسطين، 2018.
- أحمد الشافعي،البطلان في قانون الإجراءات ،دراسة مقارنة ،دار هومه ،الجزائر 2005.
- احمد براك وعبد القادر جرادة كتاب الجرائم الإلكترونية في التشريع الفلسطيني دراسة تحليلية تأصيلية مقارنة عمان دار الشروق والتوزيع 2018.
- احمد براك، مبادئ الإجراءات الجزائية دراسة تحليلية تأجيلية مقارنة الجزء الأول.دار الشامل للنشر والتوزيع الطبعة الأولى 2019.
- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2000.
- احمد محمد براك ، مبادئ الإجراءات الجزائية دراسة تحليلية تأهيلية مقارنة الجزء الاول الدعاوي الناشئة في الجريمة- الإجراءات السابقة على المحاكمة.دار الشامل للنشر والتوزيع الطبعة الاولى 2019 .
- احمد محمود مصطفى، جرائم الحاسبات الالية في التشريع المصري(دراسة مقارنة)، دار النهضة العربية، الطبعة الأولى، 2010.
- أسامة احمد المناعسة وجلال الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، (دراسة مقارنة)، دار الثقافة للنشر، الطبعة الثالثة، 2017.
- اسراء جاسم عمران ، التحقيق الابتدائي ، عمان ، المركز الاكاديمي ، 2014.
- أشرف توفيق شمس الدين شرح قانون الإجراءات الجزائية الجزء الاول الدعوى الجنائية – الاستدلال والتحقيق الابتدائي – التصرف في الأوراق- دار النهضة العربية الطبعة الخامسة 2017 .
- أمال عثمان ، الخبرة في المسألة الجنائية –رسالة دكتوراة ،كلية الحقوق ،جامعة القاهرة ،1964.
- ايمن ظاهر، شرح الاجراءات الجزائية الفلسطيني، فلسطين ،2014.

- جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الاحكام الموضوعية للجرائم المتعلقة بالانترنت، الطبعة الاولى، دار النهضة العربية، 2001.
- جين بندك، ترجمة أحمد أبو العباس ، الإلكتروني وأثره في حياتنا، دار المعارف القاهرة، مصر، 1957 .
- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة)، دار النهضة العربية، 2009.
- حسين بن سعيد القانوني استشاري قانوني هيئة تقنية المعلومات - السياسة الجنائية في مواجهة جرائم الانترنت دراسة مقارنة سلطنة عُمان دار النهضة العربية 32 شارع عبد الخالق ثروت 2009.
- خالد عياد حلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة والنشر والتوزيع، الاردن 2011 .
- خالد ممدوح ابراهيم، التفاضي الالكتروني، دار الفكر الجامعي ، ط1، مصر، 2007.
- خالد ممدوح ابراهيم، فن التحقيق في الجرائم الإلكترونية، مصر، دار الفكر الجامعي، 2010.
- سادار علي عزيز ، ضمانات المتهم اثناء الاستجواب، مصر ، المركز القومي للاصدارات القانونية ، 2014، ط1.
- ساهر إبراهيم شكري الوليد: شرح قانون الإجراءات الجزائية الفلسطيني، (الجزء الأول)، فلسطين ، مكتبة غزة المركزية ، 2009.
- سمير داود سليمان، بحوث جنائية، القاهرة، المركز القومي للاصدارات القانونية، ط1.
- شروق سامي فوزي، تكنولوجيا الإعلام الحديث، مؤسسة طبية للنشر والتوزيع ، 2015.
- عبد الاله محمد النوايسة، جرائم تكنولوجيا المعلومات شرح الاحكام الموضوعية من قانون الجرائم الإلكترونية، عمان ، دار الاوائل للنشر والتوزيع، الطبعة 2017.
- عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية ، السعودية، مكتبة القانون والاقتصاد، 2012.
- عبد العال الديربي، الجرائم الإلكترونية دراسته قانونية قضائية مقارنة ، مصر المركز القومي للاصدارات القانونية، 2012.
- عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنت، القاهرة، دار الكتب القانونية، 2008.

- عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة ،دار النهضة العربية ،مصر، 2009.
- عبد الفتاح مراد، شرح جرائم الحاسوب والانترنت، مصر ، دار العرب للنشر والتوزيع.
- عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، عمان، دار الحامد للنشر والتوزيع، الطبعة الأولى، 2013.
- غادة نصار، الارهاب والجريمة الإلكترونية ، مصر، العربي للنشر والتوزيع، ط1، 2017.
- كامل السعيد، شرح الاحكام العامة في قانون العقوبات، عمان ، دار الثقافة للنشر والتوزيع ، 2019 .
- لؤي عبد الله نوح،مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي ،مركز الدراسات العربية للنشر والتوزيع ،مصر ، 2017 .
- محمد أمين الخرشة ،مشروعية الصوت والصورة في الإثبات الجنائي ،(دراسة مقارنة)، دار الثقافة ،عمان ،الأردن ، 2011.
- محمد زكي ابو عامر ، و د. علي عبد القادر القهوجي ، قانون العقوبات / القسم الخاص.
- محمد صبحي نجم، قانون العقوبات(القسم العام) النظرية العامة للجريمة، دار الثقافة للنشر، 2012.
- محمد صلاح الدين بهجت محمد، تصرف النيابة العامة في التحقيق الابتدائي، دار النهضة العربية، 2009.
- محمد علي الحلبي، الوسيط في شرح قانون المحاكمات الجزائية، عمان ، دار الثقافة للنشر والتوزيع ، 1996.
- محمد علي السالم الحلبي، شرح قانون العقوبات(القسم العام)، دار الثقافة للنشر، الطبعة الثالثة، 2011.
- محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، مصر ، دار الجمهورية للصحافة، ط1 ، 2010.
- محمد فاروق عبد الحميد كامل، القواعد الفنية الشرطية للتحقيق والبحث الجنائي،اكاديمية نايف العربية للعلوم الأمنية الطبعة الأولى، السعودية 1999.

- محمد نور خالد الدباس، وقاع الجريمة المنظمة في الاردن، عمان ، دار يافا العلمية للنشر والتوزيع، ط1، 2007.
- محمود عباينة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر، الطبعة الأولى، 2009.
- محمود نجيب حسني ،شرح قانون الإجراءات الجنائية، الطبعة الثالثة ،دار النهضة ،1998.
- محمود نجيب حسني النظرية العامة للقصد الجنائي، مصر، دار النهضة العربية ، 1981 .
- معوض عبد التواب، الموسوعة الجنائية الشاملة في التعليق على نصوص قانون الإجراءات الجنائية المصري،(الجزء الأول)، القاهرة ،دار الفكر العربي، 1998.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية ،مصر 2006 .
- نهلا عبد القادر المؤمني، ماجستير في القانون الجنائي المعلوماتي، الجرائم المعلوماتية، عمان، دار الثقافة، 2010.
- نور الهدى محمودي مجلة الباحث للدراسات الأكاديمية جامعة بائنة - العدد الحادي عشر - جوان 2017.
- هيثم عبد الرحمن البقلي، الجرائم الإلكترونية الواقعه على العرض، مصر ، دار العلوم، 2010.

#### ثانياً: المراجع الاجنبية :

- Eoghancasey،digitalevidence and computercrime، third edition، published by Elsevier Inc، London، 2011.
- MICHEL Quille: strategies en France par la police conter la crimialitcorganise، 1996
- ،1968International Review of Criminal Policy، United Nation .“Manual on the Prevention and Control of computer related Crime 2000”

#### ثالثاً: القوانين والاتفاقات الدولية:

- اتفاقية مجلس اوربا بشأن الجرائم الإلكترونية( بودابست) لسنة 2001.
- نظام مكافحة الجرائم المعلوماتية السعودي
- قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961 ،
- قانون الاتصالات السلوكية و اللاسلوكية الفلسطيني رقم3 لسنة 1996

- قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001.
- قانون الخدمة المدنية رقم 4 لسنة 1998
- قانون الصحة العامة رقم 20 لسنة 2004
- القانون القطري رقم 14 لسنة 2014.
- قانون جهاز المخابرات العامة رقم 17 لسنة 2005
- قرار بقانون الامن الوقائي رقم 11 لسنة 2007
- نظمت الاتفاقية العربية بمدينة القاهرة بتاريخ 2010/12/21

#### رابعاً: الرسائل العلمية:

- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي. جامعة الجزائر 51-بن يوسف بن خده، كلية الحقوق السنة الجامعية 2017-2018، اطروحة لنيل شهادة دكتوراه.
- بوسنودة عباس، مشروعية الدليل الالكتروني في الإثبات الجنائي، كلية الحقوق والعلوم السياسية جامعة الجيلالي ليايس، سيدي بلعباس، الجزائر، 2013-2014.
- الحاج الطاهر زهير، من آليات الوقاية من الجريمة المعلوماتية ومكافحتها السنة الجامعية 2012-2013. جامعة الجزائر كلية الحقوق مذكرة للحصول على شهادة ماجستير في فرع القانون الجنائي والعلوم والعلوم الجنائية.
- حمد امين رمضان، محمد ايمن رمضان احمد، الحماية الجنائية للتوقيع الالكتروني، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، مصر، 2010.
- طاهري عبد المطلب، الإثبات الجنائي بالإدلة الرقمية - رسالة ماجستير، - جامعة المسيلة - كلية الحقوق والعلوم السياسية قسم الحقوق، السنة الجامعية 2014-2015 .
- غلاباحمد، اعتراض المراسلات السلوكية واللاسلكية في التشريع الجزائري، مذكرة ماجستير 2014/2016، جامعة باجي مختار - عنابة - كلية الحقوق.
- فتحي والي، نظرية البطلان في قانون المرافعات، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، مصر، 2005.

- فخري عبد الرازق الحديثي استاذ القانون الجنائي كلية الحقوق ،جامعة جرش والدكتور خالد حميدي الزعبي استاذ القانون الجنائي المساعد في كلية الحقوق جامعة فلادلفيا،دار الثقافة للنشر والتوزيع 2010.
- فرغلي عبد الناصر محمد محمود ، الاثبات بالادلة الرقمية من الناحيتين الفنية والقانونية -دراسة تطبيقية -مقارنة المؤتمر العربي الاول لعلوم الادلة الجنائية والطب الشرعي -جامعة نايف للعلوم الامنية الرياض، 2007 .
- معمش زهية ، غانم نسيمه ، الاثبات الجنائي في الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في الحقوق قسم القانون الخاص جامعة عبد الرحمن ميرة -بجاية السنة الجامعية 2012-2013 .
- ممدوح حسن مانع العدوان، ضمانات المتهم في مرحلة البحث الأولي او الاستدلال دراسة مقارنة ، جامعة العلوم الاسلامية كلية الشريعة والقانون، الاردن، رسالة ماجستير ،
- هروال نبيلة، الجوانب الاجرائية للجرائم الانترنت في مرحلة الاستدلالات، ماجستير في القانون دراسة مقارنة دار الفكر الجامعي، 2007 .

#### مقابلات شخصية :

- حمدي سائد ،مقابلة في مكتب النائب العام مختص بالتحقيق بالجريمة الإلكترونية بمحافظة القدس مباحث ضواحي القدس .
- رهام جبر، نائب مدير وحده الجرائم الإلكترونية في جهاز الشرطة ، مقابلة شخصية في مكتب النائب العام.
- سامر المصري ، وكيل نيابة الجرائم الإلكترونية في محافظة رام الله ، مقابلة شخصية حول سماع الشهود في الجريمة الإلكترونية .
- سامر الهندي، مدير وحده الجرائم الإلكترونية ، مقابلة شخصية حول اختصاص عمل وحده الجرائم الإلكترونية بجهاز الشرطة ، فلسطين.
- سونيا حماد -مختبر الادلة الرقمية وحده الجرائم الإلكترونية الادارة العامة للمباحث العامة الشرطة الفلسطينية .
- عبد الله السوداني، مبرمج تكنولوجيا معلومات، مقابلة شخصية ، رام الله .

- محمد مسعود، مختبر الأدلة الإلكترونية، جهاز الشرطة ، وحده الجرائم الإلكترونية، مقابلة شخصية.

#### تقارير ومؤتمرات وورشات عمل:

- ابراهيم راشد بشير، التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية -امارة ابو ظبي دراسات استراتيجية تصدر عن مركز الامارات للدراسات والبحوث الاستراتيجية العدد 131 ،الامارة العربية المتحدة، 2008.
- تقرير الاحصائيات الصادر من قيادة الشرطة المدنية عام 2018.
- خير عبد الناصر محمد محمود فرغلي د.محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلية الجنائية والطب الشرعي ، الرياض 2-14/11/1428هـ الموافق 12-14/11/2007.
- عصام عابدين ، القانون من اجل الانسان، جهود مؤسسة الحق في مواجهة قرار بقانون الجرائم الإلكترونية، مؤسسة الحق، 2018.
- ممدوح حسن مانع العدوان، حجية الدليل الإلكتروني في الاثبات الجزائي ،كلية الشريعة والقانون جامعة العلوم الإسلامية / الأردن،المجلة العالمية للتسويق الإسلامي /المجلد السادس - العدد الاول ، لندن - المملكة المتحدة
- مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين .
- مؤتمر الامن الوقائي بعنوان الفضاء الالكتروني في ظل تطور الجريمة والارهاب المؤتمر الامني الرابع المنعقد باريجا .
- المؤتمر الدولي لحقوق الانسان بطهران المنعقد في الفترة الممتدة من 22 ابريل الى 13 .
- النيابة العامة ، التقرير السنوي لعام 2018 .

• مواقع الكترونية :

- <http://www.phishingaware.com>
- <http://www.radionisaa.ps/article/6211/%D8%A7>
- <http://www.soutalomma.com/Article/>
- <https://m.annabaa.org/arabic/informatics>
- <https://www.almaany.com/ar/dict/ar>
- <https://www.mohamah.net/law/>

## فهرس المحتويات

أ.....	إقرار
ب.....	الشكر والتقدير
ج.....	الملخص:
د.....	Abstract:
ه.....	مقدمة
و.....	أهمية الدراسة:
ط.....	إشكالية الدراسة:
ي.....	خطة الدراسة:
ي.....	منهج الدراسة
ي.....	مخطط الدراسة:
1.....	الفصل الأول
1.....	الطبيعة القانونية للجريمة الإلكترونية.
3.....	المبحث الأول: ماهية الجريمة الإلكترونية
3.....	المطلب الأول: مدلول الجريمة الإلكترونية
3.....	الفرع الأول: تعريف الجريمة الإلكترونية
9.....	الفرع الثاني: خصائص الجريمة الإلكترونية والادوات المستخدمة في ارتكابها.
14.....	الفرع الثاني: الادوات المستخدمة في ارتكابها
18.....	المطلب الثاني: مفهوم المجرم الإلكتروني
18.....	الفرع الأول: تعريف المجرم الإلكتروني:
19.....	الفرع الثاني: خصائص المجرم الإلكتروني
25.....	المبحث الثاني: المواجهة التشريعية للجريمة الإلكترونية.
25.....	الفرع الاول: الجهود الدولية للحدّ من الجرائم الإلكترونية.
31.....	الفرع الثاني: الجهود التشريعية الفلسطينية لمكافحة الجريمة الإلكترونية:

المطلب الثاني:أركان الجريمة الإلكترونية والتحديات التي تواجه مكافحتها	40
الفرع الاول :أركان الجريمة الإلكترونية	40
الفرع الثاني:التحديات والصعوبات التي تواجه التصدي للجريمة الإلكترونية في التشريع الفلسطيني:	48
الفصل الثاني	53
الأحكام الاجرائية لمكافحة الجريمة الإلكترونية في التشريع الفلسطيني	53
المبحث الأول: الاجراءات التحقيقية في الجريمة الإلكترونية	54
المطلب الأول: التحقيق التمهيدي ((البحث والاستدلال))	54
الفرع الاول :البحث والاستدلال في الجرائم التقليدية	55
الفرع الثاني: مرحلة جمع الاستدلالات في الجريمة الإلكترونية	61
المطلب الثاني : التحقيق الابتدائي في الجريمة الإلكترونية	81
الفرع الأول: الجهة المختصة بالتحقيق في الجرائم الإلكترونية	81
الفرع الثاني :اثبات الجريمة الالكترونية	88
المبحث الثاني: مرحلة المحاكمة في الجرائم الإلكترونية	111
المطلب الاول : المبادئ العامة للاختصاص في الجرائم الإلكترونية	112
المطلب الثاني: الاجراءات المتبعة في مرحلة المحاكمة في الجرائم الإلكترونية	116
المطلب الثالث: الآثار المترتبة على عدم مشروعية الاجراءات	120
الفرع الأول: آثار البطلان على الإجراء المعيب ذاته	120
الفرع الثاني :آثار البطلان على الإجراءات الأخرى	121
الخاتمة	124
النتائج:	125
التوصيات:	126
قائمة المصادر والمراجع:	128
فهرس المحتويات	136