

جامعة النجاح الوطنية

كلية الدراسات العليا

وسائل البحث والتحري عن الجرائم الإلكترونية

إعداد

أدهم باسم نمر بغدادي

إشراف

د. أنور جانم

قُدمت هذه الأطروحة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام بكلية الدراسات العليا، في جامعة النجاح الوطنية، نابلس - فلسطين.

2018

وسائل البحث والتحري عن الجرائم الإلكترونية

إعداد

أدهم باسم نمر بغدادى

نوقشت هذه الأطروحة بتاريخ 2018/4/5م، وأجيزت.

أعضاء لجنة المناقشة:

1. د. أنور جانم / مشرفاً ورئيساً

2. د. رائد طه / ممتحناً خارجياً

3. د. بهاء الأحمد / ممتحناً داخلياً

التوقيع

المرحوم
رائد طه
بهاء الأحمد

الإهداء

إلى من سهرت الليالي " أمي الحبيبة "

إلى من أعطاني لأكون " لأبي الغالي "

إلى مصدر فرحي " إخوتي وأبنائهم "

ولمن كانت لي عوناً ومصدر عطائي؛ سهرًا وحباً " خطيبتني "

إلى من صادقتهم فصدقوا " أصدقائي "

إلى من أعطاني ولم يبخل علي بحرف

ولا أنسى فلسطين وشهداءها وجرحاها وأسراها

إليهم أهدي هذا العمل المتواضع ..

الشكر والتقدير

إن الحمد لله، الذي علم الإنسان ما لم يعلم، وعلمه البيان ليفرق الحق عن الباطل، والذي بعونه وتوفيقه أنجزت هذا العمل.

فإنني أتقدم بعد الشكر لله، بوافر شكري وعرفاني لكل من علمني حرفاً ويشرفني أن أتقدم بأسمى آيات الشكر والعرفان إلى أستاذي الفاضل (الدكتور أنور جانم) الذي تولى مهمة الإشراف على هذا البحث، والذي أشرف على هذه الرسالة ولم يبخل في تقديم النصح والإرشاد من أجل إنجاح هذه الدراسة، ووضعها في قالبها الصحيح، والذي كان له كبير الأثر في إخراجها إلى النور. كما أشكر الدكتور رائد طه والدكتور بهاء الأحمد على إشرافهم لرسالتني. كما لا يفوتني أن أخلص بالشكر إلى كل من ساعدني ولو بالكلمة الطيبة، كما أشكر جامعة النجاح الوطنية الصرح الكبير التي وفرت لنا طاقماً أكاديمياً رائعاً.

والشكر المتواصل إلى أبي وأمي وأفراد عائلتي وخطيبتني، وإلى من قام بإعطائي أية معلومة أثرت نفعا في هذا البحث، كما أشكر الأستاذ الفاضل رائد راعي على مراجعة الرسالة من حيث لغوية وتركيبية وإملائية.

الشكر كل الشكر والتقدير لكل الأصدقاء الذين أسهموا في إتمام هذا العمل. إلى كل هؤلاء أتمنى حسن الجزاء وخير الثواب من الله عز وجل.

الإقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل العنوان:

وسائل البحث والتحري عن الجرائم الإلكترونية

أقر بأن ما اشتملت عليه هذه الرسالة إنما هو نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه
حيثما ورد، وأن هذه الرسالة ككل، أو أي جزء منها لم يقدم من قبل لنيل أية درجة علمية أو بحث
علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

Declaration

The work provided in this thesis, unless otherwise referenced, is the
researcher's own work, and has not been submitted elsewhere for any other
degree or qualification.

Student's name :

اسم الطالب:

Signature :

التوقيع:

Date:

التاريخ:

فهرس المحتويات

الصفحة	الموضوع
ج	الإهداء
د	الشكر والتقدير
هـ	الإقرار
ح	الملخص
1	المقدمة
7	الفصل الأول: التقنية الإلكترونية ووسائل البحث والتحري عنها
7	المبحث الأول: ماهية الجريمة الإلكترونية
7	المطلب الأول: تعريف الجريمة الإلكترونية
11	المطلب الثاني: خصائص الجريمة الإلكترونية
16	المطلب الثالث: أركان الجريمة الإلكترونية
16	الركن الشرعي
21	الركن المادي
23	الركن المعنوي (القصد الجرمي)
25	المبحث الثاني: العلاقة القانونية للبحث والتحري
26	المطلب الأول: تعريف البحث والتحري
31	المطلب الثاني : المخولون بالقانون بالبحث والتحري
42	المطلب الثالث: صفات المحققين بالجريمة الإلكترونية
44	المطلب الرابع: مشروعية البحث والتحري
48	الفصل الثاني: وسائل التحقيق الجنائي في الجرائم الإلكترونية
49	المبحث الأول: إجراءات التحقيق الجنائي بالوسائل التقليدية
53	المطلب الأول: التبليغ
58	المطلب الثاني: المراقبة أو الت رصد الالكروني
62	المطلب الثالث: الشهادة
64	المطلب الرابع: التفتيش والضبط
72	المطلب الخامس: صعوبات يواجهها المحققون في الجرائم الإلكترونية
73	المبحث الثاني: إجراءات التحقيق الجنائي الحديثة
75	المطلب الأول : تعاون مزودي الخدمة مع جهات التحقيق

78	المطلب الثاني: تسجيل واعتراض المراسلات
79	المطلب الثالث: الخبراء الإلكترونيون
83	المبحث الثالث: آليات التحقيق عن الجرائم الإلكترونية في الاتفاقات الدولية
84	المطلب الأول: التعاون الدولي في مجال البحث عن الجريمة الإلكترونية
89	المطلب الثاني: إتفاقية بودابست وقواعدها الإجرائية لسلطتها في البحث والتحري
92	المطلب الثالث: إتفاقية مجلس أوروبا بشأن الإجرام السيبراني لعام 2000
94	المطلب الرابع: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات
97	الخاتمة
97	النتائج والتوصيات
101	قائمة المصادر والمراجع
b	Abstract

وسائل البحث والتحري عن الجرائم الإلكترونية

إعداد

أدهم باسم نمر بغدادي

إشراف

د. أنور جانم

الملخص

مع إنتشار استخدام الحاسوب والشبكة الإلكترونية، وما صاحب هذا الإنتشار من إرتفاع في المستوى العام لقدره الأفراد على التعامل مع هذه التقنيات الحديثة من تسخيرها لتحقيق أهدافهم، تظهر لنا الأهمية الذي يمكن ضبط الشرط على التعامل مع هذه التقنيات بالمستوى نفسه أو بمستوى أفضل وقدرتهم على البحث والتحري عن الجريمة الإلكترونية. وسأتناول في هذه الدراسة وسائل البحث والتحري عن الجريمة الإلكترونية من منظور القوانين الفلسطينية، وخاصة بعد صدور القرار القانون الصادر حديثا بخصوص الجرائم الإلكترونية رقم 16 لسنة 2017.

بما أنّ الجريمة الإلكترونية حديثة النشأة وتطرق في جنباتها أجراس الخطر، سأتناول في الفصل الأول مفهوم الجريمة الإلكترونية، و ذكر خصائصها، وسأنتطرق إلى أركان الجريمة الإلكترونية لأهميتها، وإلى مفهوم البحث و التحري للجريمة الإلكترونية، ومن هم المخولون بالبحث والتحري بالإضافة إلى صفاتهم، وسأتناول أيضا مشروعية البحث والتحري وعدم مساسه بالحرية الشخصية للشخص كون القوانين والأعراف حفظت هذا الحق الإنساني.

أمّا في الفصل الثاني، سأتناول فيه التحقيق الجنائي بإيقاع الإجراءات التقليدية في البحث والتحري عن الجرائم الإلكترونية، ومنها الإبلاغ عن وقوع جريمة الإلكترونية، والتفتيش، والمراقبة بشتى الوسائل، وسأنتطرق بالبحث عن الوسائل الحديثة للتحقيق في الجرائم الإلكترونية من خلال تعاون مزودي الخدمة مع جهات التحقيق لتمكينهم من سهولة المعاملة بأجهزة الحاسوب ولخبرتهم فيها، واعتراض المراسلات من خلال خبراء إلكترونيين في حال كان هناك تلبس بجريمة، وهذا يأتي من خلال السماح باعتراض المراسلات وتسجيلها وكشف سرّيتها في حال اقتضت ضروريات

البحث والتحري التحقيق، ومن الوسائل التي تجدي نفعاً التعاون الدولي لتحديد هوية الجاني لكون هذه الجرائم عابرة للقارات ويمكن له أن تضر باقتصاد دول و أمنها، وحديثاً قد نص قرار بقانون بشأن الجرائم الإلكترونية رقم (16) لسنة (2017) عن تسير التعاون في فلسطين مع نظيرتها في البلاد الأجنبية بقصد الإسراع في تبادل المعلومات ما بينهما ما من شأنه أن يكفل الإنذار المبكر في اكتشاف الجريمة الإلكترونية.

المقدمة

جاء استخدام وسائل التكنولوجيا في مناحي الحياة كافة؛ الى تحويل تلك المعمورة الى قرية إلكترونية صغيرة تتدفق المعلومات بين ارجائها في سهولة وسرعة، ويحصلون على آية معلومات يريدونها بسرعة فائقة وبدون أي عناء، والتي سميت بالثورة الإلكترونية أو المعلوماتية، وجاء هذا من خلال التطور الحافل السريع بالأجهزة الإلكترونية والتي أصبحت سهلة لمتناول الأفراد¹، بات من غير المنطقي أن يعيش الإنسان بعيداً عن هذا التقدم التكنولوجي الكاسح في أوجه الحياة كافة، وبات استخدام الكمبيوتر والإنترنت من أهم عناصر الحياة الحديثة. ولقد صاحب هذا التطور بروز صور مُختلفة من الجرائم الجديدة وفي فلسطين ففي عام 2015 سُجّلت 502 قضية تتعلق بالجرائم الإلكترونية أمام المحاكم الفلسطينية، أما في عام 2016 سُجل 1070 قضية²، رغم عدم وجود تشريع خاص يُجرّم هذا النوع من الجرائم، وهي الأمور التي تتطلب زيادة وعي الجهات القائمة على إنفاذ القانون و المُكافحة من أجل التصدي لهذه الصور المُستحدثة التي باتت تغزو المُجتمعات كافة، فبات من الضروري وجود جهات وأجهزة مختصة في البحث والتحري لأن هذه الجرائم عابره للدول³، وللد من أضرارها ومخاطرها على الساحة المحلية وعلى الساحة الدولية.

حيث إن تقنية الحاسوب أصبحت تستعمل كوسيلة لارتكاب الجرائم الإلكترونية، وأصبح هذا النوع المستحدث من الجرائم الإلكترونية يرتكب في وسط افتراضي غير متعارف عليه، ولا يشبه الوسط التقليدي للجرائم التقليدية، إلا أن هناك جانباً من الفقهاء قد اعتبروها امتداداً للجريمة التقليدية وذلك على منظور تطور الجريمة من حيث الزمان، والبعض الآخر من الفقهاء اعتبرها

¹ المقبل، صالح بن سعد: بناء نموذج لمهارات التحقيق الاستدلالي في جرائم الابتزاز الالكتروني.(رسالة ماجستير منشورة). جامعة نايف العربية للعلوم الأمنية. الرياض. السعودية. 2015، صفحة 2.

² ارزىقات، لوي: الناطق الإعلامي باسم الشرطة الفلسطينية، فيديو منشور على موقع الشرطة الفلسطينية، تاريخ الزيارة 2016/10/3 .

³ المالكي، محمد بن احمد: رؤية إستراتيجية لربط شبكة المعلومات الأمنية بين دول مجلس التعاون لمكافحة الجرائم الالكترونية. (رسالة ماجستير منشورة). جامعة نايف العربية للعلوم الأمنية. الرياض. السعودية، 2015، صفحة 2.

جريمة مستقلة بذاتها¹، وعلى الرغم من الخدمات التي توفرها الشبكة العنكبوتية من سرعة الاتصال والتواصل، وذلك قيام بعض المجرمين بارتكابهم الجرائم وأساءه استخدامها واستغلالها على نحو غير مشروع²، استغله مرتكبو الجرائم الإلكترونية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة بل تجاوزت حدود الدول³.

وعليه يمكن القول بأن للتطور الإلكتروني آثار سلبية رغم إيجابياته المجله⁴.

وعليه سنتناول هذه الدراسة وسائل البحث والتحري عن الجرائم الإلكترونية كونه موضوعاً حديثاً على الساحة الفلسطينية، وكذلك إن الحديث عن هذا الموضوع سيثيري نفعا من الناحية التطبيقية للمحاكم، وكذلك للأمن العام لأن هذه الجرائم تشكل نسبة هائلة من القضايا المنظورة أمام القضاء، كالسرقة، والابتزاز، والاحتيال...، فمعرفة وسائل البحث والتحري عن الجريمة أمر في غاية الأهمية لمكافحة هذه الجريمة المستحدثة والحد منها.

فإذا كانت الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين معتادة على التعامل مع الجريمة بصورتها التقليدية لما يمكن أن يخلفه مرتكبوها من آثار مادية، فإن على الجهات المكلفة في الجرائم الإلكترونية الإسراع في الكشف عن هذه الجرائم لسهولة محو آثار هذه الجريمة وصعوبة إكتشافها.

¹ صغير، يوسف: الجريمة المرتكبة عبر الانترنت. (رسالة ماجستير منشورة). جامعة مولود معمري- تيزي وزو. 2013، صفحة 5.

² المشجري، ليلي احمد سالم: الجرائم الاقتصادية عبر الشبكة العالمية للمعلومات. (رسالة ماجستير منشورة). كلية الدراسات الإسلامية العربية- دبي. 2014، صفحة 60

³ صغير، يوسف: الجريمة المرتكبة عبر الانترنت. (رسالة ماجستير منشورة). جامعة مولود معمري- تيزي وزو. 2013، صفحة 2

⁴ المقبل، صالح بن سعد: بناء نموذج لمهارات التحقيق الاستدلالي في جرائم الابتزاز الالكتروني، رسالة ماجستير منشورة). جامعة نايف العربية للعلوم الأمنية. الرياض. السعودية. 2015، صفحة 3.

أهمية الدراسة

تترتب أهمية الجرائم الإلكترونية أنها جرائم مستجدة نسبيا تفرع في جنباتها أجراس الخطر؛ لتنبه مجتمعات العصر الراهن لحجم المخاطر، وهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة: بيانات، ومعلومات، وبرامج بكافة أنواعها، فهي جريمة تقنية تنشأ في الخفاء، يمتلكون الجناة أو المخترقين أدوات المعرفة التقنية، تُوجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الكمبيوتر المخزنة، والمعلومات المنقولة، عبر نظم المعلومات وشبكاتها، وكذلك أهميتها من الناحية العملية كونها ترمي إلى البحث عن الجرائم الإلكترونية، وكذلك إيقاع العقوبة على مرتكبيها، وبعد إصدار السيد الرئيس محمود عباس القرار بقانون بشأن الجرائم الإلكترونية ويحمل رقم 16 لسنة 2017 أصبح يمكن تكيف التهمة سندا على هذا القرار بقانون وإيقاع العقوبة الرادعة على مرتكبي هذه الجرائم الإلكترونية.

وأثناء المقابلة الشخصية مع السيد بدر شواهنة رئيس نيابة قلميلية وجاءت هذه المقابلة قبل صدور قرار بقانون بشأن الجرائم الإلكترونية لعام 2017، أشار بأنه من الضروري إقرار قانون متعلق بالجرائم الإلكترونية، وفي ظل عدم وجود قانون يتعلق بالجرائم الإلكترونية يتم اللجوء - كلما أمكن - لقانون العقوبات، حيث توجد بعض النصوص التي تنطبق على بعض الوقائع وأفعال لا يوجد لها نص يسعفها، وأشار إلى أن قانون الاتصالات بحاجة إلى تعديل، إلا أنه الآن يمكن للنيابة العامة أن تستند إلى القرار بقانون بشأن الجرائم الإلكترونية وتعمل على البحث والتحري عن وقوع جريمة الإلكترونية وتدونة في محضر استدلال وكذلك تكيف التهمة المرتكبة في لائحة الاتهام.

ويرى الباحث أنه بعدما أُقرَّ هذا القرار بقانون بشأن الجرائم الإلكترونية أصبح على مأمور الضبط القضائي سهولة البحث والتحري في حال وقعت جريمة الإلكترونية، وأيضا إسناد الفعل إلى الجاني يتم من خلال القرار بقانون الصادر حديثاً، بحيث أيضاً تتم عقوبة على فعله حسب ما جاء بهذا القرار بقانون.

صعوبة الدراسة

هنالك صعوبات جمة تكمن في هذا البحث، عدم وجود قرارات قضائية في حال طُعن أمام المحاكم عن أليات البحث والتحري عن هذه الجرائم الالكترونية في حالة كانت غير مشروعة قانونياً، وأيضاً عدم توفر الخبرة الفنية العالية الى سلطات الضبط القضائي مختص بالبحث والتحري في الجرائم الالكترونية، وحديثاً تم إنشاء النيابة الخاصة بالجرائم الالكترونية، إلا انه يبقى قصور في البحث والتحري عن الجرائم الالكترونية والتحقيق فيها كون ان سلطات الضبط القضائي يتعاملون بشكل عام بالجرائم التقليدية.

إشكالية الدراسة

بما أن الجرائم الالكترونية من الجرائم المستجدة والتي تطلبت تدخل تشريعي لمواجهة مثل هذا النوع من الجرائم المسحذة خاصة في ظل عجز القوانين التقليدية لمواجهة هذا النوع من الجرائم المستجدة، ومع تزايد انتشار هذه الجريمة بمختلف أشكالها وصورها كان لا بد من تدخل المشرع الفلسطيني لافراد قانون لمواجهة مثل هذا النوع للجرائم الالكترونية، إلا أنه يثور التساؤل في ظل وجود قرار بقانون بشأن الجرائم الالكترونية فما مدى نجاعة الوسائل المتبعة في البحث والتحري للكشف عن الجرائم الالكترونية؟

وانطلاقاً من هذه الاشكالية يتفرع عنها بعض الاسئلة الفرعية وأهمها:

1- مدى صلاحية الوسائل التقليدية في البحث والتحري عن الجريمة الالكترونية في ظل خصوصية هذه الجريمة؟

2- ما هي الوسائل التي يمكن استخدامها للبحث والتحري عن الجريمة الإلكترونية، في ظل عدم وجود الخبرة والمعرفة الفنية لدى المحققين؛ وما يؤدي ذلك إلى ضياع الفرص والأضرار بعملية التحقيق بأكملها ؟

3- هل بالإمكان استخدام الوسائل التحقيق التقليدية للبحث عن الجرائم الإلكترونية؟

منهجية الدراسة

اعتمدت في هذه الدراسة على المنهج الوصفي التحليلي، من خلال و تحليل النصوص القانونية ذات الصلة بالموضوع، وتحليلها، وبيان المبدأ القانوني التي تقوم عليه، وجمع الحقائق والبيانات ووضعها في البحث.

نطاق الدراسة

اقتصرت مجال البحث في القوانين الفلسطينية المتعلقة بالجرائم الالكترونية وتحليلها بما يتوافق مع موضوع البحث القائم عليه وبالإشارة إلى جزء من مواد قانون الاجراءات الجزائية الفلسطيني النافذ لما له أساس عملي، بالإضافة إلى تحليلها ومقارنتها مع بعض قوانين الدول العربية.

بيانات الدراسة

أستخدمت هذه الدراسة مجموعة من البيانات الثانوية، وهي عبارة عن مجموعة من المصادر الرئيسية والمراجع الثانوية، فمن المصادر الرئيسية التي اعتمدتها في هذه الدراسة قانون الإجراءات الجزائية الفلسطيني، والقرار بقانون بشأن الجرائم الإلكترونية الصادر حديثاً في فلسطين رقم (16) لسنة (2017)، بالإضافة الاعتماد على المقابلات الشخصية مع أصحاب العلاقة والعلم والمعرفة، أما بخصوص المراجع الثانوية فهي مجموعة من الكتب ورسائل الماجستير والدكتوراه المتعلقة بالجرائم الإلكترونية التي عاجلت أو تطرقت إلى موضوع البحث.

الدراسات السابقة

1- عالج (العنزي، 2003، رسالة ماجستير منشورة في اكااديمية نايق العربية للعلوم الامنية) في دراسته عن وسائل التحقيق في نظم المعلومات، وأهم المعوقات التحقيق في جرائم نظام المعلومات لدى المحققين بالأجهزة الأمنية، عدم توفر كوادر بشرية لديها مهارات تمكنها من التحقيق في الجرائم الإلكترونية، وضرورة توفر خبراء للحاسب الآلي المتخصصين، وتوفر التدريب في معاهد متخصصة بالتحقيق في الجرائم الإلكترونية.

2- (السرحاني، 2004، رسالة ماجستير منشورة في اكااديمية نايق العربية للعلوم الامنية) وتناول منها الباحث المهام الواجب النظر فيها في النظام السعودي، وخلص لضرورة توفر المهارات الخاصة لدى المحققين ذات طابع خاص يجب أن يتمتع بها ضابط الشرطة ليكون قادراً على القيام بهذا النوع من التحقيق و يمكن من خلالها الإطلاع على واقع المهارات المتوفرة لدى ضباط الشرطة في مجال التحقيق في جرائم الحاسوب والإنترنت، وخطوة نحو لفت انتباه العاملين في المجال الأمني إلى ضرورة مواكبة المستجدات في مجال الجريمة.

اتفقت هذه الدراسة مع الدراسات السابقة على ضرورة تجريم هذا النوع من الجرائم بتشريع خاصة في ظل عجز النصوص التقليدية على مواجهة هذا النوع من الجرائم.

والواضح بان هذه الدراسة تتعلق بالحالة الفلسطينية في ظل بروز هذا القانون بالحالة الجديدة، في ظل ريع وتطور الجرائم الالكترونية، لذا بات من المهم على انشاء معاهد متخصصة تحتوي على عقد دورات وتوعية من اجل تدريب افراد الاجهزة الامنية على وسائل البحث والتحري على الجرائم الالكترونية والاسس الصحيحة للضبط والتفتيش عن الادلة.

الفصل الأول

التقنية الإلكترونية ووسائل البحث والتحري عنها

أصبح وجود التقنية الإلكترونية مهماً في حياتنا، فلا يمكن الاستغناء عنه، ولهذا كان لهذه التقنيات مساهمة كبيرة في ارتكاب الجريمة الإلكترونية على الشبكة المعلوماتية، فمن خلال هذا الفصل سأتناول البحث عن الجريمة الإلكترونية، كما سأسلط الضوء على الناحية الفلسطينية للأهمية ولكثرة ارتكاب الجريمة الإلكترونية، وأيضاً من خلال هذا الفصل لا بد من التطرق إلى ماهية الجرائم الإلكترونية وتعريفها، وكذلك معرفة من هم المخولون بالبحث والتحري عن الجرائم الإلكترونية حسب القوانين الفلسطينية.

المبحث الأول: ماهية الجريمة الإلكترونية

الجريمة الإلكترونية بوصفها ظاهرة إجرامية ذات طبيعة خاصة، صعبت من جهود الفقه وكذلك من رجال القانون الجنائي في التوصل إلى اتفاق حول مصطلح دقيق يعبر عن هذه الظاهرة، يجدر بنا من خلال هذا المبحث أن نبين مفهوم الجريمة بشكل عام، من خلال تجريم الفعل المرتكب بعد سن الدولة قانون خاص بالجرائم الإلكترونية يحدد العقوبات والإجراءات المتبعة، ومن ثم يتطلب الأمر منا بيان ماهية الجريمة الإلكترونية في (المبحث الأول)، بشكل خاص مع تعريفات مقارنة لها مع الدول الأخرى، والتطرق إلى خصائص هذه الجريمة، وأركانها، و يجدر بنا أولاً أن نتحدث عن الطبيعة القانونية للبحث والتحري في (المبحث الثاني)، من حيث تعريف البحث والتحري، ومن هم المخولون قانونياً للبحث والتحري، وصفاتهم، ومشروعية البحث والتحري.

المطلب الأول: تعريف الجريمة الإلكترونية

تعرف الجريمة، كل فعل أو إمتناع عن فعل ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية يقرر له القانون عقوبة أو تدبيراً

احترازا¹، ويعرف القانون الجنائي بأنه: "مجموعة من القواعد القانونية التي تسنها الدولة لتنظيم حقها في توقيع العقوبة على مرتكب الجرم"².

لم يتفق الفقه على وضع تعريف شامل للجرائم الإلكترونية³، نظراً لحدثة الجرائم على الصعيد العالمي والإقليمي، فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الآخر يطلق عليها جريمة الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية⁴.

أما جريمة الكمبيوتر أو الجرائم النظيفية، فقد وضع لها الفقهاء والدارسون عددا ليس بالقليل من التعريفات، فاختلقت بين أولئك الباحثين في الظاهرة الإجرامية الناشئة عن استخدام الكمبيوتر من الوجهة التقنية، وذلك لصعوبة اكتشاف دليل ثبوتها؛ فلا أثر لأي عنف أو دماء، وإنما مجرد أرقام وبيانات واختيار المصطلح يتعين أن يتم الدمج ما بين البعدين التقني والقانوني⁵.

وفي ظل هذا الفراغ القانوني ظهر محاولات فقهية متعددة لإيجاد تعريف للجرائم الإلكترونية وانقسمت بدورها إلى اتجاهين رئيسيين: اتجاه مضيق لمفهوم الجرائم الإلكترونية، واتجاه موسع لمفهوم الجرائم الإلكترونية.

من أهم التعريفات التي وضعها أنصار الاتجاه الضيق على أنها: "كل سلوك غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى"⁶.

¹ الشكري، عادل يوسف عبد النبي: الجريمة المعلوماتية وأزمة الشرعية الجزائية. الجريمة المعلوماتية. العدد السابع. 2008. صفحة 113. الموقع الإلكتروني: www.iasj.net/iasjfunc=fulltext&aId=29515.

² الدرة، ماهر عبد شويش: قانون العقوبات القسم الخاص، ط2. المكتبة القانونية. بغداد. لا يوجد سنة نشر، صفحة 4.

³ المؤمني، نهلا عبد القادر: الجرائم المعلوماتية، ط1. دار الثقافة للنشر والتوزيع. عمان. 2008، صفحة 46.

⁴ عرب، يونس: جرائم الكمبيوتر والانترنت - المعنى والخصائص والصور وإستراتيجية المواجهة القانونية، بحث منشور على الانترنت على الموقع الإلكتروني: www.arablalaw.org.

⁵ العريان، محمد علي: الجرائم المعلوماتية. لا يوجد طبعه. دار الجامعة الجديدة للنشر. الإسكندرية. 2004، صفحة 35، 36.

⁶ عبد الحكيم، مولاي براهيم، الجرائم الإلكترونية. مجلة الحقوق والعلوم الإنسانية - جامعة زيان عاشور بالجلفة. الجزائر. الجزائر. عدد 23 / جوان 2015. 13. صفحة 213.

ومن خلال هذا التعريف يتبين لنا بأن لا يكفي أن تتوفر معرفة بتكنولوجيات الحاسبات الآلية من أجل ارتكاب الجريمة الإلكترونية، ولكن أيضا يجب أن يتوفر لدى الشخص العلم الكافي والمعرفة من أجل ملاحقتها ومتابعتها، حيث من غير الممكن ارتكاب فعل دون أن يكون قاصداً منه تحقيق الغرض المراد، كارتكاب فعل غير مشروع مثلا الدخول الغير مشروع للأجهزة الحاسوبية.

أما الاتجاه الموسع لمفهوم الجريمة الإلكترونية فإنه نظر إليها من مفهوم واسع خشية من حصرها في مجال ضيق لتستوعب القدر الكافي من الأفعال المجرمة وهي: " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب¹. والبعض عرفها أنها: " كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دورا لإتمامه، على أن يكون هذا الدور قدراً من الأهمية"².

وفقا للنظام الانجلوسكسونية³ فقد عرف قانون الولايات المتحدة الأمريكي جرائم الحاسب الآلي الرقمي المتمثلة بعدة صور:

1- **العبث بالحاسب الآلي:** وتقوم هذه الجريمة إذا قام عن علم ودون إذن من مالك الحاسب الآلي.

2- **الإخلال بأمن الحاسب الآلي:** من خلال استعمال الحاسوب دون موافقة سارية المفعول من مالك الحاسوب على أن يكون لديه العلم بأن هناك جداراً أمنياً وقام بالإخلال به، أو تمكنه من الدخول على بيانات مخزنة أو محفوظة في الحاسوب مع علم الجاني أيضا أن هناك جدار حماية قصد به منعه من اكتساب الدخول إلى قاعدة البيانات تلك .

¹ عبد الحكيم، مولاي براهيم، *الجرائم الإلكترونية*. مجلة الحقوق والعلوم الإنسانية- جامعة زيان عاشور بالجلفة. مرجع سابق، صفحة 213.

² عبد الحكيم، مولاي براهيم، *الجرائم الإلكترونية*. مجلة الحقوق والعلوم الإنسانية- جامعة زيان عاشور بالجلفة. مرجع سابق، صفحة 213.

³ موسى، مصطفى محمد: *التحقيق الجنائي في الجرائم الإلكترونية*. ط1. القاهرة: مطابع الشرطة. 2008-2009، صفحة 120.

3- **غش الحاسب الآلي:** ترتكب هذه الجريمة إذا كان لدى العلم بالدخول أو يسبب الدخول إلى الحاسوب الآلي لوضع أو ابتكار حيلة للغش لتنفيذ مشروع في الحاسوب الآلي بطريقة مخادعة. ومن أكثر أساليب الغش استعمالاً وشيوعاً، ما يتم بغاية تحقيق مصلحة أو منفعة مادية مباشرة أو غير مباشرة سواء لمصلحة مرتكب الجريمة أو لشخص آخر، ومن الأمثلة عليها القيام بتحويلات مالية من حساب إلى آخر عن طريق استعمال بطاقات ائتمان مسروقة أو مزيفة¹.

ومن الناحية الفلسطينية ظهر تعريف للجريمة الإلكترونية من خلال ما القرار بقانون الجرائم الإلكترونية لعام 2017" هو: "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا القانون"².

و قبل اصدار القرار بقانون رقم (16) لسنة (2017) بشأن الجرائم الإلكترونية كانت المحاكم كانت المحاكم الفلسطينية تطبق المواد الواردة في قانون الاتصالات للبت في قضية، والتي لم تكن قادرة على استيعاب كافة صور الاجرام الإلكتروني، وكان تعمل المحاكم في نص المادة(91) وهذا كان قبل القرار بقانون بشأن الجرائم الإلكترونية رقم (16) لسنة 2017³، حيث أن يرى الباحث أنه بعد ما أُقر قانون خاص ينظم عمل الجرائم الإلكترونية وتم اعتماده أمام المحاكم تمكن هذا القانون من تحصين الردع لمرتكي الجريمة الإلكترونية أو فعل غير مشروع بواسطة الأجهزة الإلكترونية بواسطة الانترنت وحديثاً تم إنشاء نيابة خاصة لمتابعة الجرائم الإلكترونية، وبحاجة ماسة إلى توحيد القوانين الفلسطينية في هذا المجال في ظل بروز تعديل على

¹ فالي، علل: خصوصيات الجريمة المعلوماتية على ضوء التشريع و القضاء المغربي. مجلة القضاء التجاري. المغرب. ع2013/1. 20، صفحة 128.

² قرار بقانون الجرائم الإلكترونية رقم (16) لسنة 2017، المادة 1

³ قانون الاتصالات الفلسطيني رقم (3) لسنة 1996، الباب الرابع عشر، الجرائم والعقوبات .

- المادة 91:

أ. كل من قام بتهديد أي شخص أو أهانته أو نقل خبراً مختلفاً بأي وسيلة من وسائل الاتصالات بقصد إثارة الفرع 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 للنظام 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.

قانون المطبق في قطاع غزة والقانون المطبق في الضفة الغربية والعمل على توحيد العمل به، وتعزيز التعاون بين الأجهزة الأمنية في شطري الوطن.

المطلب الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بخصائص تميزها عن الجريمة التقليدية، ولعل من أهمها ما يأتي:

أولاً: جريمة عابرة للقارات، ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم¹؛ مما أدى إلى انعكاس على طبيعة الأعمال الإجرامية التي يعتمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محلياً بل أصبح عالمياً². فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان إلى تحديات قانونية إدارية فنية، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية، القيام بإعداد أحد البرامج في بلد ما ثم يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم.³

ثانياً: جرائم ناعمة ومغرية للمجرمين: إذا كانت الجريمة بصورتها التقليدية تحتاج في الأغلب إلى مجهود عضلي كجرائم القتل والاغتصاب، فإن الجريمة الإلكترونية على العكس لا تحتاج إلى أدنى مجهود عضلي، بل تعتمد على الدراية الذهنية والتفكير المدروس القائم على معرفة بتقنيات الحاسب الآلي⁴، فالجرائم الإلكترونية لا تحتاج، وقت ارتكاب الجريمة إلى أي درجة من القرب أو التلامس المادي بين الجاني والضحية، ويمكن أن ترتكب الجريمة ضد مجني عليه يسكن في مدينة

¹ مصطفى، يونس خالد عرب: جرائم الحاسوب دراسة مقارنة. (رسالة ماجستير منشورة). الجامعة الأردنية. عمان. الأردن. 1994. صفحة 81.

² سعيداني، نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. (رسالة ماجستير منشورة). جامعة الحاج لخضر. باتنة. الجزائر، 2012-2013، صفحة 30.

³ هروال، نبيلة هبة: الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات. ط1. الإسكندرية: دار الفكر الجامعي. 2007. صفحة 35-40.

⁴ ثنيان، ناصر آل ثنيان: إثبات الجريمة الإلكترونية. (رسالة ماجستير منشورة). جامعة نايف العربية للعلوم الأمنية، ابو ظبي، الإمارات، 2012، صفحة 23.

أخرى، لذا تتسم جرائم العالم الافتراضي بأنها أقل عنفا وخشونة من الجرائم التقليدية، كالقتل أو السرقة المقرونة بالكسر أو اقتحام، حيث لا تلتقي الضحية والمجرم في مكان واحد¹.

ثالثاً: وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات، حيث يقع تعريف عملية المعالجة وفقاً للفقهاء الفرنسيين بأنه: " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات والتي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعاً لنظام الحماية الفنية"². وعرفها المشرع الفلسطيني: بأنها " إجراء و تنفيذ عملية أو مجموعة عمليات على البيانات سواء تعلق بأفراد أو خلافه، بما في ذلك جميع تلك البيانات أو استلامها أو تخزينها أو تعديلها أو نقلها أو استرجاعها أو محوها أو نشرها أو إعادة نشر بيانات أو حجب الوصول إليها و إيقاف عمل الأجهزة أو إلغاؤه أو تعديل محتوياته"³.

وهي من الشروط المهمة لتحقيق الجريمة الإلكترونية، إذ بها لا تقع الجريمة لقيام مجموعة من العلاقات بين المدخلات والمخرجات وترابطهما معاً لتحقيق النتيجة، ونظام الحماية لهذه المعلومات وفقاً للقانون الفرنسي المعدل لسنة (1994) أن يكون لهذا النوع من الجريمة حماية ويبين الآليات القانونية لمكافحتها وكذلك حماية الأموال المتداولة عبر شبكة الانترنت⁴.

وترتكب هذه الجريمة بالإخلال بمعالجة المعلومات العائدة للغير، بحيث يغير المعلومات أو يحتبسها أو يجعلها غير قابلة الاستعمال سواء بضرب البرامج المحملة على جهاز الحاسوب أو بسرقة المعلومات أو بتنزيل برنامج لمراقبة النظام الداخلي للحاسوب، وهذا يأتي من خلال الاعتداء على البرمجيات Software، أو على المعالج وحامل المعلومات Hardware⁵.

¹ سقف الحيط، عادل: جرائم الذم والقدح والتحقيق المرتكبة عبر الوسائط الإلكترونية "دراسة قانونية مقارنة". ط1. عمان: دار الثقافة للنشر والتوزيع. 2011، صفحة 184.

² إبراهيم، خالد ممدوح: أمن الجريمة الإلكترونية. لا يوجد طبعة. الإسكندرية: الدار الجامعية. 2008، صفحة 50.

³ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 1

⁴ إبراهيم، خالد ممدوح: أمن الجريمة الإلكترونية. مرجع سابق، صفحة 51.

⁵ السالك، كامل فريد 2000. تطرق للحديث عن مفهوم الجريمة المعلوماتية وقال بأن المعلومات المعالجة ألياً لم تحظ بالحماية القانونية الجزائية، وإن خطر الجرائم الإلكتروني موجودة والفئة التي يلقي بالقبض عليهم إلا فئة قليلة والقسم الأكبر خارج نطاق التجريم ولم يلقي القبض عليهم، وإن التشريع السوري مبني في الرد على الأفعال التي تستحق التجريم مما تخلفه الحياة الحديثة المتطورة . مؤتمر للجمعيات السورية للمعلوماتية: 21-23 تشرين الأول 2000: حلب. الجمعية السورية للمعلوماتية. الصفحات 1-9.

رابعاً: تدني نسبة الإبلاغ عن تلك الجرائم من المجني عليه خاصة في شركات ومؤسسات الأعمال، لتجنب الإساءة للسمعة ورغبة في عدم زعزعت ثقة العملاء، ففي إحدى الوقائع تعرض أحد البنوك، هو بنك Mar chant bank city في بريطانيا لسرقة (8) مليون جنية إسترليني من إحدى أرصده إلى رقم في سويسرا، وتم ضبط الفاعل متلبساً بسحب المبلغ المسروق، وبدلاً من محاكمته قام البنك بدفع مليون جنية له بشرط التزام الفاعل بعدم الإعلام عن جريمته، وإعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي¹، وإذا كان المنع بغاية القصد أو أبلغ بشكل خاطئ عن وقوع جريمة يعاقب الفاعل حسب التشريع الفلسطيني².

وأيضاً يطرأ تدني نسبة الإساءة خوفاً مما يترتب من كشف أسرار العمل واليات إدارته، وكشف نظم الحماية المستخدمة لأمان نظام الحاسوب لديهم³.

خامساً: صعوبة إثبات الجريمة الإلكترونية يتفاوتت القضاة في الأخذ بالأدلة الإلكترونية لأسباب مختلفة، وتقام البيئة في الدعاوى الجزائية بموجب قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 بجميع طرق الإثبات، إلا إذا نص القانون على طريقة معينة للإثبات وإذا لم تقم البيئة على المتهم قضت المحكمة ببراءته⁴ أو حفظ الدعوى لعدم كفاية الأدلة⁵، وتخضع المحررات كغيرها من الأدلة التي تقدم أثناء نظر الدعوى إلى تقدير المحكمة حيث يسود مبدأ حرية القاضي في تكوين عقيدته، وهو ما يختلف فيه القاضي المدني حيث يتقيد هذا الأخير بطرق معينة في الإثبات، فالقاضي الجنائي له مطلق الحرية في تقدير الدليل المطروح أمامه، وله أن يأخذ به أو يطرحه ولا يجوز تقييده بأي قرائن أو افتراضات⁶، فإن كل دليل يتم الحصول عليه من خلال

¹ مصطفى، يونس خالد عرب: جرائم الحاسوب دراسة مقارنة. (رسالة ماجستير منشورة). مرجع سابق. صفحة 72.

² قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 51

³ مصطفى، يونس خالد عرب: جرائم الحاسوب دراسة مقارنة. (رسالة ماجستير منشورة). مرجع سابق. صفحة 96.

⁴ الشالدة، محمد فهاد، وربعي، عبد الفتاح أمين: الجرائم الإلكترونية في دولة فلسطين المحتلة في ضوء التشريعات الوطنية والدولية. بحث مقدم إلى المؤتمر العلمي الحادي عشر لكلية القانون في جامعة جرش حول الجرائم المعلوماتية. فلسطين: 2015/1-27، صفحة 13.

⁵ قرار محكمة صلح قلميلية جنح رقم 2016/1306، حيث يفيد هذا القرار إعلان براءة المتهم لعدم كفاية الأدلة- هذا القرار القرار الصادر ليس الأول وليس الأخير- وإنما هي في ازدياد.

⁶ سلامة، مأمون: الإجراءات الجنائية في التشريع الليبي. ط1. ج 2، منشورات المكتبة الجامعة، 2000، ص151.

تكنولوجيا المعلومات يجب أن يعرض في جلسة المحكمة وليس من خلال ملف الدعوى أو التحقيق الابتدائي ليتم مناقشته بالأدلة الإلكترونية، وهذه الأحكام تنطبق على كافة الدلائل الناتجة عن الحاسبات الآلية، وكذلك الحال بالنسبة لشهود الجرائم الإلكترونية، الذين سمعت شهادتهم في التحقيق الابتدائي فإنه يجب أن يعيدوا أقوالهم في مرة أخرى من جديد أمام المحكمة وهذا يعني أن كافة المخرجات الإلكترونية سواء كانت مطبوعة أو بيانات يجب أن تناقش أمام هيئة المحكمة¹.

ولم تشهد قوانين الإثبات العربية تعديلات في حقل حجية مستخرجات الكمبيوتر والمواد الإلكترونية في الشق الجزائي أو كونها بحاجة إلى تعديل لمعالجة جريمة الاختراق في قانون جرائم المعلوماتية لسنة (2007) السوداني في الفصل الثاني منه².

فالجرائم الإلكترونية تتصف بالخفاء، أي عدم وجود لآثار المادية، وهي صعبة الاكتشاف، أو هي صعبة تحديد مكان فعل الجريمة ويمكن أن ترجع صعوبة إثبات الجريمة الإلكترونية لعدة أمور وهي كالتالي:

1- أنها كجريمة لا تترك أي آثار مادية لها بعد ارتكابها³، ويمكن أن نصف هذا العمل بنقل المعلومات وتداولها بالنبضات الإلكترونية غير المرئية ولا يوجد فيها مستندات ورقية وتتم عن طريق برمجة ولغة تشفير بين المخترقين، وعلاوة على صعوبة الاحتفاظ الفني بآثارها إن وجد، ولا يترك المجرم المعلوماتي أو الإلكتروني في كثير من الأحيان آثار تقودنا إليه من أجل معاقبته لتعامل المجرم المعلوماتي بصيغة 010 يصعب على مأموري الضبط القضائي كشفه إلا إذا وجد

¹ البلوشي، راشد بن حمد: *الدليل في الجريمة المعلوماتية*. مجلة الحقوق للبحوث القانونية الاقتصادية. مجلد. 2008م. الصفحات 1-58، صفحة 31.

² قانون جرائم المعلوماتية السوداني لسنة 2007، نصت المادة الرابعة منه "كل من يدخل موقعا أو نظام معلومات دون أن يكون مصرحا له ويقوم :

أ- بالاطلاع عليه أو نسخه، يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معا.
ب- بإلغاء بيانات أو معلومات ملكا للغير أو حذفها أو تدميرها أو إفشائها أو إتلافها أو تغييرها أو إعادة نشرها أو تغيير تصاميم الموقع أو إغائه أو شغل عنوانه يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا"
³ مصطفى، يونس خالد عرب: جرائم الحاسوب دراسة مقارنة. (رسالة ماجستير منشورة). مرجع سابق. صفحة 93.

خبير تقني يسهل له كشفها، دون أي شعور قد تتعرض للسرقة أو تخترق المواضيع دون ترك أي دليل مادي¹.

2- تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها، حيث أنها تتطلب الإلمام الواسع بمجال الانترنت والكمبيوتر ونظامها، حتى تمكن الخبراء سهولة التعامل مع المجرمين واستجوابهم والتحقيق معهم².

سادساً: نقص الخبرة لدى الأجهزة الأمنية والقضائية، وذلك يتطلب على رجال الاستدلال والتحقيق الإلمام بأمور فنية وتقنية وكذلك إتباع أسلوب خاص في التحقيق، نظراً لعدم التعامل مع جرائم تقليدية وإنما حديثة المنشأ، الأمر الذي دفع بعض الدول غير القادرة على التعامل مع هذه الجرائم بالتعاون مع بعض المجرمين الذين يطلق عليهم الهاكرز (Hachers) : " وهو الشخص الذي لديه مهارات أو دراية بالتكتيك المستخدم في نظام الحاسب الآلي الالكتروني والقادر على استخدام هذا التكتيك لاختراق الكود السري لتغيير المعلومات أو لتنفيذ البرامج أو لتحويل من الحاسبات عن طريق استخدام الحاسوب نفسه"³، للكشف عن غموض بعض الجرائم، وبناءً على ذلك قامت بعض الدول بإنشاء مركز لتدريب جهات الاستدلال والتحقيق والقضاء والادعاء تدريباً خاصاً للتعامل مع هذه الجرائم واكتسابهم الخبرة اللازمة؛ لان الجاني لديه قدر كبير من الذكاء والخبرة بتعامله مع إخفاء آثار الجريمة والتعامل معها⁴. ولضرورة هذه البند ولأهمية قد نص قرار بقانون رقم (16) لسنة (2017) بشأن الجرائم الإلكترونية عليها في نص المادة (33) فقره (5/4) بالاستعانة بأهل الخبرة بقصد الحصول على البيانات والمعلومات وكذلك أن يكون مأمور الضبط القضائي مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية⁵.

¹ ريان، محمد عادل: جرائم الحاسب الآلي وأمن البيانات، مقال منشور على الانترنت على الموقع التالي: www.anaharonline.com

² بن بادرة، عبد الحليم: إجراءات البحث والتحري عن الجريمة المعلوماتية الخصوصية والإشكالات، مجلة الحقوق والعلوم الإنسانية. عدد23. 2015م/98/76، صفحة 83.

³ قشقوش، هدى حامد: جرائم الحاسب الإلكتروني في التشريع المقارن. القاهرة: دار النهضة العربية، 1992، صفحة 27

⁴ المشجري، ليلي احمد سالم: الجرائم الاقتصادية عبر الشبكة العالمية للمعلومات. (رسالة ماجستير منشورة). مرجع سابق، صفحة 67.

⁵ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 5/4/33.

أن ما تم إثباته من خلال المستوى الثقافي لرجال الأمن والمحققين العاملين في مجال الجرائم الإلكترونية، تم إثبات أن هنالك جرائم متعلقة بالحاسب الآلي ارتكبت على مرأى ومسمع رجال الأمن، من خلال ما قدمه رجال الأمن يد المساعدة لمرتكبي الجريمة يد العون وعن جهل ليس تقصيراً من رجال الأمن وإنما عدم العلم الكافي بالتحقيق في مجال الجرائم الإلكترونية¹. بمعنى آخر عندما يغيب عن رجل الأمن إليه البحث والتحري عن الدليل لإسناده إلى المجرم المعلوماتي وفي حالة تلبس المجرم بالجريمة وعدم تمكن سلطات الضبط القضائي ضبط الأدلة بشكل صحيح مما تؤدي لتلفها كون هذه الأدلة هي بيانات وبرامج محوسبه، وعندما لا يكون لسلطات البحث والتحري العلم الكافي بالطريق السليمه الناجحة والتسلسل الصحيح للكشف عن الجريمة الالكترونية؛ يؤدي إلى عدم القدرة على ضبط الدليل وعدم معرفة سلطات الضبط القضائي اثبات الجريمة الالكترونية وذلك بسبب ضياع إحدى الأدلة وعدم قيام سلطات الضبط القضائي بضبطه وتدوينه.

ويرى الباحث أنه في ظل ازدياد الجريمة الإلكترونية على الساحة الوطنية والعالمية يجب أن يكون هناك علم ودراية كبيرة لدى المحقق في المجال الإلكترونية، وتكثيف دورات خاصة بهذا المجال، وأن على مأموري الضبط القضائي أن يتعامل الادلة المضبوطة في مسرح الجريمة بجدية حتى لا يتسبب المحقق دون قصد أو بطريق الخطأ في إتلاف الدليل الالكتروني أو ظناً منه بتجاهل أمر غير مهم مرتبط بالجريمة الإلكترونية ولا يقوم بمصادرتها كالتابعة مثلاً.

المطلب الثالث: أركان الجريمة الإلكترونية

في ظل خصائص هذه الجريمة المستحدثة وما تتميز به من ملامح لا تتوفر في الجرائم التقليدية، فهل يتطلب القانون في هذه الجريمة ذات الأركان والعناصر المكونه للجرائم التقليدية؟

الركن الشرعي: انطلاقاً من المبادئ المُستقر عليها في القانون الفلسطيني بأنه: "لا جريمة ولا عقوبة إلا بنص قانوني"² والواقع العملي ذلك يتعدى النص ومنطقه تمشياً مع التطور العلمي

¹ البشري، محمد أمين : *التحقيق في جرائم الحاسب الآلي والانترنت* . المجلة العربية للدراسات الأمنية والتدريب، عدد 30. مجلد 15. ط1. 2000/الصفحات 317-380. الصفحة 351.

² انظر القانون الأساسي الفلسطيني المعدل لسنة 2005، المادة 15.

ومقتضيات الدفاع عن المجتمع باتباع قانون الاتصالات الفلسطيني لتطويع نص المادة (91) منه بالعقوبة و التكيف يأتي قياسا لقانون العقوبات لسنة 1960 بحيث يطبق تحت لوائها بعض الجرائم المتعلقة بالكمبيوتر كنصوص جرائم السرقة والنصب والإتلاف وغيرها¹ وهذا قبل إقرار قانون خاص بالجرائم الإلكترونية، أما بعدما صدر قانون مختص بالشأن الإلكتروني أصبح الأمر أسهل من ذي قبل من حيث إسناد التهمة بحسب الفعل المقترف من الجاني، وسهولة إيقاع العقوبة عليه كلاً بحسب جرمه.

اما بعدما أقر قرار بقانون رقم (16) لسنة 2017، أصبحت العقوبات تُطبق وفي حالة تم النقاط ما هو مرسل عن طريق الشبكة، أو سُجل أو اعترضه، أو تنصت عليه بدون وجه حق يعاقب على هذا الفعل، بالحبس، أو بالغرامة التي لا تقل عن 1000 دينار ولا تزيد عن 3000 الاف دينار اردني او بالعقوبتين معا².

بحيث إذا تم تطبيق النصوص التقليدية على هذه الأنماط المستحدثة من الجرائم يسهم بكثير في حل المشكلات القانونية، فصدرت أحكام تطبيق النصوص التقليدية عليها وتضاربت أحكام القضاء، وفي حين اعتبرته أحكام أخرى سلوكاً مباحاً لم يرد بشأنه نص يجرمه التزاماً بمبدأ لا جريمة ولا عقوبة إلا بنص³، وتعتبر جرائم الانترنت التي أفرزتها تقنية الانترنت إحدى التحديات الكبرى التي تقف أمام تطبيقات القانون الجنائي، والذي يكون في كثير من الأحيان محلاً لقصور بين في تنظيم تلك الجرائم المستحدثة وهذا ما يسهل للكثير من المجرمين ارتكابها والإفلات من العقاب⁴.

وتعد القاعدة القانونية (لا جريمة ولا عقوبة إلا بنص من القانون) ضماناً لمصلحة الأفراد فهو السور الحقيقي لحماية حقوق الأفراد من الاعتداء عليها ووضع العقوبة الرادعة على متعديها، وإن

¹ الأستاذ بدر شواهنة، رئيس نيابة العامة في قلقيلية، تاريخ المقابلة 2016/8/18.

² قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، المادة 7.

³ الشكري، عادل يوسف عبد النبي: الجريمة المعلوماتية وأزمة الشرعية الجزائية. الجريمة المعلوماتية. العدد السابع.

2008. الصفحات 111-138. صفحة 111. الموقع الإلكتروني: www.iasj.net/iasjfunc=fulltext&aId=29515.

⁴ نبيلة هبة هروال: الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات. مرجع سابق. صفحة 41-43.

إسناد مهمة تحديد الجرائم والعقوبات يعود إلى السلطة التشريعية لعدم الاعتداء على الحقوق والحريات ، فلا تستطيع السلطة القضائية ملاحقة أفعال لم يجرمها المشرع ولا تقرير عقوبات غير التي حددتها النصوص القانونية وهذا ما ذهبت إليه التشريعات الانجلوسكسونية¹ وفي مقدمتها القانون الانجليزي، فالقانون الانجليزي مصدره العرف ومع هذا لم يخرج عن مبدأ الشرعية وحاجته إلى مصادر تكميلية كاللوائح التشريعية واللوائح التفويضية²، وقد اصدر المشرع الفدرالي الأمريكي في أكتوبر عام 1984 قانون الولوج غير المصرح به إلى الحاسب الآلي الذي ينص على أنه: "يعاقب كل من ولج عمداً إلى حاسب آلي دون إذن أو من لم يكن مسموحاً له بالولوج إليه استغل الفرصة التي سنحت له عن طريق هذا الولوج لأغراض مخزنة في الحاسب، متى كان هذا الأخير يعمل باسم ولصالح الحكومة الأمريكية وطالما أثرت هذه الأفعال على أداء وظيفته...." ويطبق هذا النص على كل الجرائم الإلكترونية، وطبقاً لقانون غش الحاسب وإساءة استخدامه لسنة 1986 يعتبر مرتكباً لجناية كل من يدخل إلى أنظمة الحواسيب الفدرالية طالما أنه غير مسموح له بالولوج بهذا الحاسوب³.

¹ بتصرف من الشكري، عادل يوسف عبد النبي: الجريمة المعلوماتية وأزمة الشرعية الجزائية. الجريمة المعلوماتية. مرجع سابق. صفحة 118 وما بعد. الموقع الإلكتروني: www.iasj.net/iasjfunc=fulltext&aId=29515، ومن الأمثلة على الدول ذات النظام الانجلوسكسوني من خلال إصدارها للقوانين ذات العلاقة بالجرائم الإلكترونية.

- في البرتغال صدر قانون المعلومات الجنائي في 17 آب 1991 وتضمن في القسم الأول المادة السابعة المتعلقة بالجرائم الإلكترونية.

- في بولندا أضيف إلى قانون العقوبات مواد وجميعها تتعلق بحظر الدخول للأنظمة وإساءة البيانات والمعلومات.
- في استراليا صدر تشريع الجرائم الاتحادي عام 2001 والذي تضمن تعديل قانون العقوبات الصادر عام 1995 وذلك باستبدال الجزء المتعلق بجرائم الحاسوب من خلال المادة 475/أ حيث حظرت الدخول وتبديل المعلومات.

- في الهند صدر تشريع لتكنولوجيا المعلومات برقم 21 لسنة 2000 وتم وضعه في الباب الأول من قانون العقوبات تضمنه المادة 66 وسمي القرصنة على نظام الكمبيوتر.

- أما في جنوب إفريقيا لم يصدر تشريع خاص بالجرائم المعلوماتية واكتفي بتطبيق الباب الثاني بتطويع بنوده على الجرائم المعلوماتية

- وكذلك الحال اسبانيا لم تقم بإصدار قانون خاص بالجرائم الإلكترونية وإنما تطوعت الباب الأول من قانون العقوبات على الجرائم المعلوماتية

² الشكري، عادل يوسف عبد النبي: الجريمة المعلوماتية وأزمة الشرعية الجزائية. الجريمة المعلوماتية. مرجع سابق. صفحة 118-119. الموقع الإلكتروني: www.iasj.net/iasjfunc=fulltext&aId=29515.

³ جبر، رُهام سائد احمد: جريمة الاحتيال الإلكترونية وإجراءات الضبط والتحقيق بها دراسة مقارنة. مرجع سابق، صفحة 65-66.

من المؤكد أن الخدمات الإلكترونية في هذه الوقت وبعد انتشارها في أواسط المجتمع، كان من المنطق أن تتجه السياسة التشريعية في معظم قوانين العالم إلى حماية الأشخاص والأموال عن طريق تجريم الاعتداء على الأموال المعلوماتية مادية كانت أو معنوية، وما يمكن أن تسبب هذه الاعتداءات من مساس بالأشخاص أو بالأموال¹.

أما في قطاع غزة، لم يكن القانون الفلسطيني يعاقب على الجرائم الإلكترونية إلا بعد عام 2009، فقد استحدثت المشرع الفلسطيني المادة 262 مكرر من قانون العقوبات رقم 74 لسنة 1936 المعدل لسنة 2010 وتم نشرها في الوقائع الفلسطينية بتاريخ 2009/6/25م، وتناولت هذه المادة مجموعة من الجرائم وتضمنت العقوبات عليها وفقاً معيار عقوبة الجرح مهما كانت ذروتها لم يتطرق المشرع في غزة إلى باقي الجرائم الإلكترونية مثل نشر الفيروسات، والسرقة من بطاقات الائتمان والحسابات البنكية، والترويج للمخدرات عبر مواقع التواصل الاجتماعي²، ولا بد لنا من التنويه بأن هذا القانون قد صدر وعُدل ونشر في الوقائع الفلسطينية دون موافقة رئيس دولة فلسطين عليه، إلا أنه يبقى سارياً فقط في قطاع غزة

وحديثاً أصدر النائب العام المستشار أحمد براك تعليماته بإنشاء نيابة مكافحة الجرائم الإلكترونية فقد تم تكليف أعضاء نيابة عامة من وكلاء ومعاونين في كل نيابة جزائية بمختلف المحافظات، بالإضافة إلى تكليف رئيس ووكيل نيابة في مكتب النائب العام لمتابعة قضايا الجرائم الإلكترونية الواردة إلى النيابة العامة وتأتي هذه الخطوة الهامة تماشياً مع تطور الجريمة في فلسطين وترسيخاً لرؤية ورسالة النيابة العامة في مواكبة التطور في الجريمة كما ونوعاً³، وبين الدكتور أحمد براك أن الجرائم التي ترتكب عبر الوسائل المعلوماتية أو الإلكترونية، تتمثل في جرائم

¹ قشقوش، هدى حامد: جرائم الحاسب الإلكتروني في التشريع المقارن. مرجع سابق، صفحة 67.

² العفيفي، يوسف خليل يوسف: الجرائم الإلكترونية في التشريع الفلسطيني. (رسالة ماجستير منشورة). مرجع سابق، صفحة 75، والجرائم التي تم استحداثها في قطاع غزة عام 2009 وهي كالتالي:

- جرائم الاعتداء على الحياة الخاصة والجرائم الإباحية.

- جرائم دخول الأنظمة بوجه غير مشروع.

- جرائم أنظمة المعلومات.

³ تقرير صادر عن وكالة معا الإخبارية، تاريخ الزيارة 2017/1/2، على الموقع الإلكتروني:

<http://www.maannnews.net/Content.aspx?id=884469>

الذم والقدح والتحقير والسرقة والاحتيايل، موضحاً أن هناك العديد من الجرائم التي ترتكب عبر هذه الوسائل التي لا تقع تحت الحصر، مشيراً إلى أن هناك من الجرائم ما توجب على المشرع الفلسطيني وضع تشريع لها¹.

لقد قام المشرع الجزائري بوضع حماية في قانون العقوبات جراء ارتكابها وخطا خطوة في الاتجاه السليم².

وعملت الدول العربية إلى وضع تشريعات قانونية لمعالجة الجرائم الإلكترونية³.

¹ تقرير صادر عبر موقع المجلس القضاء الأعلى تاريخ الزيارة 2017/1/2، على الموقع الإلكتروني: <http://www.pgp.ps/ar/NC>

² عبد الحكيم، مولاي براهيم، *الجرائم الإلكترونية. مجلة الحقوق والعلوم الإنسانية- جامعة زيان عاشور بالجلفة*. مرجع سابق. صفحة 221 وهي كالتالي من قانون العقوبات الجزائري :

- الدخول للمنظومات المعلوماتية عن طريق الغش: فقد اعتبرها جريمة بسيطة قرر لها عقوبة الحبس من 3 أشهر إلى سنة وبغرامه 50.000 إلى 100.000 د.ج، وتضاعف العقوبة أن كان هنالك حذف أو تعديل وإن كان هناك تخريب لنظام اشتغال المنظومة يعاقب الفاعل من 6 شهر إلى سنتين والغرامة من 50.000 إلى 150.000 د.ج. أما أن أزال أو عدل المعطيات التي يتضمنها نظام المعالجة الآلية يعاقب الفاعل بالحبس من 6 إلى 3 سنوات وبغرامة من 500.000 إلى 2.000.000 د.ج.

- التصرف عمدا في المعطيات عن طريق الغش يعاقب الفاعل بالحبس من شهرين إلى ثلاثة سنوات وبغرامة من 1.000.000 إلى 5.000.000 د.ج.

- تضاعف العقوبة إن استهدفت الجريمة الدفاع الوطني أو المؤسسات الخاضعة للقانون العام.

- تضاعف العقوبة المقرر للشخص العادي خمس مرات إن كان الفاعل شخص معنوي

- تصدر الأجهزة والبرامج المستعملة في ماديات الجريمة مع الاحتفاظ بحقوق الغير حسن النية.

³ التشريعات العربية:

- قانون جرائم تقنية المعلومات العُماني، تاريخ الزيارة 2016-11-10
<http://www.omanlegal.net/vb/showthread.php?t=16297>

- قانون رقم (60) لسنة 2014 بشأن جرائم تقنية المعلومات الصادر عن مملكة البحرين بتاريخ 30 سبتمبر 2014م
- قانون جرائم تقنية المعلومات الكويتي الصادر بداية من يوم 2016/1/12، وذلك بعد ما تم نشره في الجريدة الرسمية بتاريخ 2015/7/7.

- جرائم أنظمة المعلومات لسنة 2010 الأردني الصادر في الجريدة الرسمية بتاريخ 2010/9/16
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية في القاهرة بتاريخ 2010/12/21 ولقد قامت فلسطين بالانضمام لهذه الاتفاقية بتاريخ 2013/5/21

- مرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات صادر عن دولة الإمارات العربية المتحدة بتاريخ 13/ أغسطس/ 2012.

- في غزة قامت الحكومة بتعديل مادة في قانون العقوبات رقم 74 لسنة 1936 المعدل لسنة 2010 وتم نشرها في الوقائع الفلسطينية بتاريخ 2009/6/25م وفي فلسطين صدر قرار بقانون الجرائم الإلكترونية رقم 16 لسنة 2017

- صدر نظام مكافحة جرائم المعلوماتية السعودي بقرار مجلس الوزراء رقم 79 وتاريخ 1428/3/7هـ، وتمت المصادقة عليه بموجب المرسوم الملكي رقم م/17 وتاريخ 1428/3/8هـ (نظام مكافحة الجرائم المعلوماتية السعودي رقم 17 لسنة 2007)

- قانون العقوبات الجزائري رقم 15 لسنة 2004 المؤرخ في 2004/11/10 المتمم والمعدل للأمر 156/66، وتم إضافة القسم السابع منه مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

لقيام الجرائم الإلكترونية يتطلب وجود ركن مادي ومعنوي ويتمثل الركن المادي بفعل الدخول الذي يطلق عليه الدخول المنطقي، وذلك بغرض فتح باب يؤدي إلى الحاسوب بمكوناته المنطقية، أما الركن المعنوي فيتمثل بالقصد الجنائي كون هذه الجريمة من الجرائم العمدية فيجب توافر العلم والإرادة للجاني عند دخوله لنظام الحاسوب¹.

الركن المادي بصورة عامة هو: " مجموعة من العناصر المادية التي تتخذ مظهراً خارجياً للحواس، ويرتب القانون لها عقوبة حين تظهر بالخروج"²، كما أنه سلوك إجرامي يرتكب الجاني فعلاً أو الامتناع عن فعل أمر به القانون وعاقب على مخالفته، فهو السلوك المادي الخارجي الذي ينص القانون عقوبة له³.

ويتمثل الركن المادي في الجريمة الالكترونية الولوج والبقاء الذي يهدف من خلاله انتهاء نظام الحماية الأمنية للمواقع والأنظمة الإلكترونية⁴.

السلوك المادي في جرائم الإنترنت يتطلب وجود بيئة رقمية واتصال بالإنترنت ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته. فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة. فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلي تهيئة صفحات تحمل في طياتها مواد تثير من جلب المستخدم لها كصفحات مخلة بالآداب العامة وتحميل هذه الفيروسات على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها⁵.

يعتبر السلوك الإجرامي بشقية الايجابي والسلبي من أهم عناصر الركن المادي، حيث إن هذا الجزء تعتبر الجريمة بأنها غير تامة، فالسلوك الإجرامي له شكلان: الايجابي والسلبي:

¹ إبراهيم، خالد ممدوح: الجرائم المعلوماتية، ط1، الإسكندرية: دار الفكر الجامعي. 2002، صفحة 242.

² البقمي، ناصر بن محمد: جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، ط1: السعودية: مطابع الحميضي. 1430 هـ - 2009 م، صفحة 221.

³ الحيارى، معن احمد: الركن المادي للجريمة، ط1. لبنان: منشورات الحلبي. 2010، صفحة 93

⁴ زين الدين، بلال أمين: جرائم نظم المعالجة الآلية للبيانات، ط1. الإسكندرية: دار الفكر الجامعي، 2008، صفحة 271

⁵ جمال، فؤاد: الجرائم المعلوماتية، بحث منشور على الانترنت . www.lawofcrime.com ، صفحة 13.

أ- السلوك الايجابي حيث أن هذا السلوك قائم على تحريك الجاني عضواً من أعضاء جسمه بشكل إداري لإحداث اثر ملموس ومحدد¹، والذي يتطلب مجهوداً بدنياً في العالم الخارجي من حركات عضوية بهدف الاعتداء على المصلحة الذي يحميها المشرع، ومن الأمثلة على ذلك: السلوك الإجرامي الايجابي لاستخدام وسائل الاتصال، كأن يقوم باختراق شبكات التواصل أو يقوم باختراق شبكات الاتصال ويحصل على بيانات الشركات الخاصة ويقوم بنشرها، أو يهدد أصحابها باستخدامها بشكل غير قانوني².

ب- السلوك السلبي وهو يفترض على الجاني بأن يقوم بنشاط معين يفرض عليه القانون واجب القيام به، وبعبارة أخرى هو إمساك إداري عن الحركة العضوية في الوقت المناسب التي كانت الحركة واجبة بقوة القانون³.

النتيجة الجرمية الضارة: فالفقه تطرق إلى هذه في مفهومين: الأول مادي وهو عبارة عن ظاهرة لها أثر مباشر ملموس للسلوك المجرم، والثاني قانوني وهو عبارة عن اعتداء على المصالح والحقوق التي تحميها النصوص، أي عند مخالفه النص القانوني تقع العقوبة على نتيجته، والجرائم الاقتصادية والجرائم الإلكترونية من ضمن الجرائم التي لا يكون لها اثر ملموس إلا إنها تشكل خطورة على المجتمع لما تتضمنه من أخطار وأضرار محتملة⁴، وهي الأثر الذي يحدثه السلوك الجرمي والذي يرتب عليه المشرع أحكاماً قانونية⁵.

¹ صالح، نائل عبد الرحمن: الجرائم الاقتصادية في التشريع الأردني، ط1: عمان - الأردن: دار الفكر للنشر والتوزيع. 1990، صفحة 96-97.

² العفيفي، يوسف خليل يوسف: الجرائم الإلكترونية في التشريع الفلسطيني. (رسالة ماجستير منشورة). الجامعة الإسلامية. غزة، 2013، صفحة 52.

³ صالح، نائل عبد الرحمن: الجرائم الاقتصادية في التشريع الأردني، مرجع سابق، صفحة 96 وما بعد.

⁴ صالح، نائل عبد الرحمن: الجرائم الاقتصادية في التشريع الأردني، مرجع سابق، صفحة 96 وما بعد.

⁵ القاضيان، أسامة احمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، والتوزيع، 2014، صفحة 55.

العلاقة السببية: وهي العلاقة التي تربط بين التصرف أو السلوك المجرم بالنتيجة الإجرامية، وان يتم إثبات بأن الفعل حصل بموجب النتيجة¹.

فالركن المادي يكون قائماً في الجرائم الإلكترونية بجريمة التهديد والابتزاز بأن تحقق لدى الجاني تحقيق محل وعيده وتهديد، كأن يقوم الجاني بالقول المباشر للمجني عليه أو بطريقة غير مباشرة، ويجب أن يكون من شأن التهديد بإفشاء هذه المعلومة بالتحديد أن يولد الرهبة لدى المجني عليه من إلحاق ضرر به².

تعد هذه الجرائم من الجرائم القصدية (العمدية): فهي لا تقوم إلا بتوافر القصد الجرمي لدى الجاني، والقصد هنا قصد عام يندرج تحت عنصر العلم والإرادة، أما العلم فهو ثبوت ما يقوم بالجاني بإتيانه من إشارات أو عبارات أو ألفاظ أو صور أو رموز، من شأنها أن تمس بكرامة المعتدى عليه وحياته وسمعته، وأما الإرادة فهي نية الفاعل وتوجيهها إلى إحداث هذه الأفعال بإرادته الحرة دون إكراه أو تشویش³.

يجب أن تتجه إرادة الجاني أو قصده الجنائي والعلم بما يرتكبه من اختراق، فإذا كان قصده تعدياً على المعلومات ومعالجة البيانات كالدخول غير المشروع لجهاز حاسوب آخر، فإننا سوف نكون أمام جريمة الإلكترونية أخرى بحيث أنه إستغل معرفته بهذه المعلومات للابتزاز أو تهديد صاحب المعلومة، وذلك من أجلها أن تمس حياة شخص أو عدة أشخاص⁴.

¹ صالح، نائل عبد الرحمن: الجرائم الاقتصادية في التشريع الأردني، مرجع سابق، صفحة 96 وما بعد.

² المضحكي، حنان ربحان مبارك: الجرائم المعلوماتية "دراسة مقارنة". ط1. بيروت: منشورات الحلبي الحقوقية. 2014، صفحة 338.

³ سقف الحيط، عادل: جرائم الذم والقدح والتحقيق المرتكبة عبر الوسائط الإلكترونية "دراسة قانونية مقارنة". مرجع سابق، صفحة 80.

⁴ المضحكي، حنان ربحان مبارك: الجرائم المعلوماتية "دراسة مقارنة". مرجع سابق، صفحة 335 وما بعد.

ومن المتفق عليه في الفقه والقضاء الفرنسي، بأن القصد الجنائي على سبيل المثال في جريمة التقليد مفترض، بمعنى إذا تحققت صور إحدى النشاط الإجرامي تعد قرينة عليه وعلى حسن النية إثبات عكس ذلك لتبرئته من التهم الموجه إليه¹.

ومن خلال القصد الجنائي يمكن معرفة طبيعة السلوك المرتكب وماهيته والهدف منه، ومن خلاله يمكن وضع التكيف المناسب للجرائم الإلكترونية، وذلك لمعرفة النص القانوني الواجب تطبيقه، والذي يتناسب مع هذه الجريمة، فإن معظم هذه الجرائم الإلكترونية تبدأ بخطوة، وهي الدخول إلى النظام والولوج إليه، ومن ثم ينفذ أو ينسخ أو يحرف .. وهذا ترجع إلى هدف المنفذ فإن لم يثبت الهدف من وراء الاختراق نكون بصدد جريمة الدخول غير المشروع².

ولكن هناك جزء من الفقهاء يؤيدون في حال عدم وجود قاعدة قانونية أو نظراً للفراغ أو النقد التشريعي في عدم وجود قانون خاص بالجرائم الإلكترونية، بأنه يمكن تطبيق النص الجنائي التقليدي على وقائع جديدة لم ترد بذهن الشارع وقت وضع هذا النص، ومع ذلك نكون في نطاق الشرعية الجنائية طالما هذه الوقائع جديدة تدخل في قصد الشارع، واتجهوا بالحديث بالعبارة بالتفسير المقرر أو الكاشف وليس بالتفسير الضيق كما يتراءى للبعض³.

ونرى من خلال ما تم التطرق إليه إلى أن أغلب الجرائم الإلكترونية تتم بشكل قصدي، في ظل إن مرتكب هذه الجرائم على علم ودراية بما يقوم بها، وأن عمل الجاني من المؤكد بأنه يسعى لتحقيق نتيجة، وأن نيته الإجرامية قائمة، فلا يمكن أن نعتبر دخوله إلى الجهاز والعبث فيه بمجرد التجربة أو إلى أي سبب آخر، وأنّ الدخول لا بد وأن يقوم بأعمال تحضيرية سابقة على تنفيذ

¹ القهوجي، علي عبد القادر: الحماية الجنائية لبرامج الحاسوب. مجلة الحقوق للبحوث القانونية الاقتصادية. مصر. ع1/1992. 97 عدد صفحات المجلة، صفحة 298.

² قانون العقوبات الفلسطيني المطبق في غزة رقم 74 لسنة 1936، المادة 2/11 " لا عبثاً للنتيجة التي كان القصد أن يؤدي إليها ارتكاب فعل أو ترك إلا إذا ورد نص صريح على نية الوصول إلى تلك النتيجة تؤلف عنصراً من عناصر الجرم التي يتكون كله أو بعضه من ذلك الفعل أو الترك".

³ الصغير، جميل عبد الباقي عبد الوهاب: الجرائم الناجمة عن الحاسب الآلي والانترنت. المؤتمر الدولي الأول لقانون الانترنت (نحو علاقات قانونية وإدارية واقتصادية وسياسية واجتماعية جديدة). المنظمة العربية للتنمية الإدارية. المنظمة العربية للتنمية الإدارية. مؤتمر 1. مصر: المنظمة العربية للتنمية الإدارية. 76/2005. صفحة 28.

الجريمة من خلال تنزيل البرامج أو التحضير المسبق لما يراه الجاني - في ظل إن الحالة النفسية للجاني مهينه لفعله.

والقاعدة العامة بأن الجهم المختصة بإثبات القصد الجنائي هي النيابة العامة، أما إذا كان ظاهر الحال إلى جانب المتهم ويشير إلى عدم اعترافه بالجريمة، تبقى مسألة توافر العلم خاضعة لسلطة القاضي التقديرية، وبهذه الحالة تبقى أكاذيب المتهم وعدم اعترافه بما صدر منه دليلاً كافياً على سوء نيته¹

المبحث الثاني: العلاقة القانونية للبحث والتحري

يهتم قانون الإجراءات الجزائية على توافر شرط التجريم بمعنى ان يكون هناك نص قانوني في القرار بقانون بشأن الجرائم الالكترونية رقم (16) لسنة 2017 يحدد العقوبة المقررة على الجريمة حتى يكمن تطبيق العقوبة، من الجوانب العملية لقانون الاجراءات الجزائية التي تقع الأهمية من خلال البحث والتحري عن الجريمة، حيث ينتقل قانون الإجراءات الجزائية من السكون إلى الحركة من خلال البحث والتحري عن وقوع الجريمة الالكترونية، ففعالية وتنظيم قانون الإجراءات الجزائية يحمي مصالح الأفراد عندما تقع العقوبة على مُرتكب الجريمة².

لكل جريمة ظروفها المادية وعدم إجراء البحث والتحقيق عن جريمة ما يؤدي الإخلال بالحصول على الأدلة الكافية، ولهذا حتى يسهل على المحقق في الكشف عن قيام جريمة سواء كانت الإلكترونية أو تقليدية عليه أن يبحث ويحقق بها لإظهار الحقيقة، ويقصد بالتحقيق بمفهومه الواسع، الإجراءات التي تجريها سلطات التحقيق المختلفة قبل المحاكمة وأثناءها، وفي ظل بحثي عن البحث والتحري عن الجرائم الإلكترونية سأبحث بالبحث والتحري من قبل أن تصل إلى سلطة المحكمة وقيامها بالبحث عن الجريمة.

¹ جبر، رُهام سائد احمد: جريمة الاحتيال الالكترونية وإجراءات الضبط والتحقيق بها دراسة مقارنة. رسالة غير منشورة. جامعة القدس. القدس. فلسطين. 2015، صفحة 42.

² سرور، احمد فتحي: الوسيط في قانون الإجراءات الجزائية. القاهرة: دار النهضة العربية. 1996. صفحة 9.

وإجراءات التحقيق نوعان¹:

1- إجراءات خاصة بجمع الأدلة.

2- إجراءات خاصة بالاحتياط ضد شخص المتهم.

وإجراءات جمع الأدلة، هي:

1- سماع الشهود كمصدر للأدلة المعنوية.

2- المعاينة والتفتيش والضبط .

3- ندب الخبراء².

ولم ترد هذه الإجراءات في قانون الإجراءات الجزائية على سبيل الحصر؛ لأن المحقق له أن يختار بأي وسيلة يراها مناسبة ومفيدة للإثبات ولا تنال من حرية الأفراد، ولا حرمة مسكنهم، ولو لم يرد لها المشرع ذكر في القانون لحماية المجتمع من أفة الجرائم، وأشترط المشرع فقط ان تكون هذه الاجراءات مشروعة وغير مخالفة للقانون³.

المطلب الأول: تعريف البحث والتحري

وتعريف البحث التحري: "هي الإجراءات المتبعة وفقا للقانون والعمل المنظم الذي تقوم به أجهزة البحث الجنائي وتكون هذه الإجراءات مشروعة، والهدف من ورائها جمع المعلومات والاستدلالات

¹ مراد، عبد الفتاح: التحقيق الجنائي التطبيقي. لا يوجد طبعة. الإسكندرية: دار الكتب والوثائق المصرية. لا يوجد سنة نشر، صفحة 30.

² قانون الإجراءات الجزائية رقم (3) لسنة 2001 م، المادة 64 "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 بذلك".

³ مراد، عبد الفتاح: التحقيق الجنائي التطبيقي. مرجع سابق، صفحة 30.

الصحيحة، وأن يكون القصد منها كشف النشاط الإجرامي ومعرفة حقيقة الأشخاص وجوانب الفعل والية ارتكابه¹.

المحقق وما يراد به هو الذي يقوم بمباشرة التحقيق بمعناه القانوني، أي أعضاء النيابة العامة أو قضاة التحقيق أو أي شخص يعهد إليه بموجب القانون بمباشرة الإجراءات المتعلقة بالتحقيق، ولا يتصرف لفظ المحقق إلى مأمور الضبط القضائي الذي يباشر سلطة الاستدلالات²

لا بد لنا وأن نتحدث عن كيفية البحث عن الجرائم الإلكترونية:

قبل البدء في التحريات الأولية يكون البدء بالتحقيق للحصول على أكبر عدد ممكن من المعلومات عن السلوك المكون للجريمة وأسلوب وظروف ارتكابها³.

وحدثاً أصدر النائب العام المستشار أحمد براك تعليماته بإنشاء نيابة متخصصة بالجرائم الإلكترونية، فقد تم تكليف أعضاء نيابة عامة من وكلاء ومعاونين في كل نيابة جزائية بمختلف المحافظات كما تم انشاء وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطينية، و تتمتع هذه الوحدة بالضابطة القضائية، وتتولى النيابة العامة الاشراف على مأمور الضبط القضائي كل في دائرة اختصاصه⁴.

وعند النظر بالوحدة الخاصة بالجرائم الإلكترونية تطرق المقدم سامر الهندي بالحديث بأنه من تعرض لأي جريمة إلكترونية يمكن له اللجوء الى النيابة العامة لتقديم إفادة عندما يتعرض لإحدى

¹ الصبحي، داوود سليمان: إجراءات التحري والمراقبة والبحث الجنائي، جامعة نايف العربية للعلوم الأمنية. الرياض. 2012. صفحة 4.

² البحر، ممدوح خليل: مبادئ أصول المحاكمات الجزائية. ط1. دار الثقافة للنشر والتوزيع. 1998 عمان، صفحة 194.

³ فضل، سليمان احمد: المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. لا يوجد رقم طبعة. القاهرة: دار النهضة العربية. 2013. صفحة 271.

⁴ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية منه المادة 1/3 على أن " تنشأ وحدة متخصصة في الجرائم الإلكترونية في الأجهزة الشرطية وقوى الأمن على أن تتمتع بصفة الضابطة القضائية وتتولى النيابة العامة الاشراف على مأموري الضبط القضائي كل في دائرة اختصاصه 2- تتولى المحاكم النظامية والنيابة العامة وفقا لاختصاصاتهما بالنظر في دعوى الجرائم الإلكترونية".

هذه الصور والجرائم مثلاً: إختراق الخصوصية والإبتزاز والتهديد الإلكتروني، وعلية نبدأ بالبحث والتحري عن المتهم، واستجوابه والتحقيق معه¹.

بعد مقابلة شخصية مع موقع جريدة القدس نتحدث الاستاذة رئيسة النيابة العامة نسرين الرشماوي، بأن الوحدة المتخصصة بالبحث والتحري عن الجرائم الالكترونية بالتنسيق مع النيابة العامة على تعمل مطاردة الجريمة الالكترونية في فلسطين وخارج فلسطين².

لذا يجب أن يأخذ المحقق عدة اعتبارات هامة عند وضع خطة التحريات الأولية³:

1- إن الدليل المستند إلى المعالجة الآلية للبيانات يمكن أن يكون متاحاً لفترة وجيزة، بمعنى على المحقق أن يبذل كل مجهوده للحفاظ على الدليل.

2- يمكن للجريمة التي يجرى البحث والتحري عليها أن تكون مستمرة بنتائجها أو بتنفيذها.

3- يمكن للجريمة التي يجرى البحث والتحري عنها أن تكون غطاءً على جريمة أخرى، لذا إذا توافر هذا الفعل أن يكون إجراء البحث والتحري أكثر دقة حول الواقعة

والحقائق المفترض إظهارها في التحريات الأولية هي⁴:

1- التثبت من وقوع الجريمة.

2- طبيعة الجريمة المرتكبة.

3- التقنيات المستخدمة في ارتكاب الجريمة.

¹ موقع الحدث، الابلاغ عن الجرائم الالكترونية، تاريخ الزيارة 2018/5/2 الموقع الالكتروني: <https://www.alhadath.ps/article/66802>.

² موقع جريدة القدس، النيابة الالكترونية. تاريخ الزيارة 2018/5/2 الموقع الالكتروني <http://www.alquds.com/articles/1484890275698412300> / الرشماوي في مقابلة خاصة مع القدس.

³ فضل، سليمان احمد: المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. لا يوجد رقم طبعة. دار النهضة العربية. القاهرة. 2013. صفحة 348.

⁴ فضل، سليمان احمد: المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. مرجع سابق. صفحة 348.

4- الجاني أو الجناة المشتبه في ارتكابهم هذه الجرائم النوعية.

5- الأسباب أو الدوافع التي جعلت من الجناة ارتكابها.

6- الاستدلال على الشهود في حال وجودهم.

7- الادلة الجنائية.

فمن من المعلوم أن مرحلة الاستدلال وجمع المعلومات تتم قبل تحريك الدعوى والأشخاص القائمين على سلطات الاستدلال هم سلطات الضبط القضائي ومن ثم يعملون على جمع الأدلة الناتجة عن مرحلة الاستدلال التي تلزم للتحقيق¹.

تختص سلطات الضبط القضائي بالبحث عن أدلة الجريمة وأن تقديم بلاغ أو شكوى لا يكفي لتحريك الدعوى الجزائية، بل يجب على سلطات الضبط القضائي أن تتحرى هذه البلاغات و تتأكد من مدى صحتها في حال وقعت جريمة أو كونها مستمرة وجمع المعلومات عن الجريمة التي تم التبليغ عنها والهدف الأساسي من سلطات الضبط القضائي في هذه المرحلة هو كشف الغموض ومعرفة الحقيقة عن هذه الشكوى واستقصاء كافة المعلومات التي تفيد عن الجريمة، و لها أيضا أن تسمع الشهود الذين كانوا في موقع الحادث لمعرفة تفاصيل ارتكاب الجريمة وغيرها من المعلومات التي تساهم في كشف الجناة²

¹ قانون الإجراءات الجزائية رقم (3) لسنة 2001 م.

- المادة 19

1- يتولى أعضاء النيابة العامة مهام الضبط القضائي والإشراف على مأموري الضبط كل في دائرة اختصاصه.
2- يتولى مأمورو الضبط القضائي البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى".

² زعنون، سالم. و الحلبي ، محمد : شرح قانون الإجراءات الجزائية الفلسطيني . لا يوجد طبعه. مكتبة دار الفكر . 2002 م.
صفحة 201-202 .

وعند البدء في التحقيق مع الأشخاص في الجرائم الإلكترونية يعمل بهذا الخطوات التالية¹:

أولاً: قبل البدء في التحقيقات مع الشهود والمشتبه فيهم أو استجواب المتهمين، يقوم خبير أجهزة الحاسوب والمحقق بتبادل فيما بينهم بالمعلومات، بحيث يمكن لهم لتوجيه الأسئلة وتوجيهها لهم.

ثانياً: يعمل المحقق على حصر النقاط التي تبادلها مع الخبير ، ومن ثم يتولى المحقق بترتيب تلك النقاط حتى يسهل عليه الشروع في استجواب المشتبه فيهم.

ثالثاً: يقوم المحقق بالحصول على المصطلحات كافة من الخبير التي يمكن استخدامها للاستفادة منها عند الضرورة.

رابعاً: يعمل المحقق على وضع خطة التحقيق على ضوء معطيات يراها كما ينبغي له حسب دوره في التحقيق بهذه الجرائم من المنظور الأمني.

خامساً: يبدأ المحقق باستجواب الشهود والمتهمين بحضور الخبير، ويمكن للخبير توجيه الأسئلة الفرعية أثناء استجوابهم، وهذه تتم في حالة حضور الخبير عندما يتم استجواب المتهم؛ للخبرة الكافية الذي يعلم بها، بحيث يمكن للخبير فرض اسئلة على المتهم للوصول الى الحقيقة، وعندما نتحدث عن هذه الحالة تكون باتفاق مسبق مع المحقق لحضور الخبير مراحل استجواب المتهم.

سادساً: يجب مراعاة القوانين الوطنية فيما يتصل في بسلطة التحقيق.

سابعاً: مراعاة التنسيق بين الخبير والمحقق في الحصول على البيانات المخزنة على الحاسوب الآلي نظراً لأن المجرم المتخصص في الحاسوب الآلي يحتفظ بمعلوماته وخطته في الحاسوب الآلي أو على أقراص مرئية، ويجب الأخذ بعين الاعتبار عدة أمور منها مثلاً: تقادي ضياع الوقت في التحقيق حول الجرائم الإلكترونية التي لا يمكن اكتشافها، ومراعاة المحققين والخبراء من خلال تعاملهم في الأدلة الإلكترونية، ومراعاة الخصوصية الفردية للمتهم أو المشتبه فيه بعدم المساس بالبريد الإلكتروني، والعناية بإصدار الأوامر القضائية الخاصة بإذن التفتيش وضبط أجهزة

¹ فضل، سليمان احمد: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. لا يوجد رقم طبعة. القاهرة: دار النهضة العربية. 2013. صفحة 348.

الحاسوب الآلي وملحقاتها، وحفظ الأدلة الجنائية المناسبة لكل حالة على حدة حتى تقدم إلى المحكمة على حالتها الراهنة.

لقد نص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 على صلاحيات الضبط القضائي:

1. البحث والتحري والاستدلال والاستقصاء لجمع المعلومات عن الجريمة.
 2. تلقي البلاغات و الشكاوي التي ترد إليهم.
 3. إجراء الكشف والمعاينة وإجراء الإيضاحات و الاستعانة بالخبراء وكل ما هو من شأنه أن يساعد في كشف معالم الجريمة.
 4. اتخاذ جميع الوسائل للحفاظ على أدلة الجريمة.
 5. إثبات جميع الإجراءات التي تقوم بها في سبيل الكشف عن الجريمة.¹
- إن إجراءات البحث والتحري يقوم بها مأموري الضبط القضائي للكشف عن الجرائم ومرتكبيها، وهي عملية تجميع القرائن والأدلة التي تثبت وقوع الجريمة ونسبتها الى فاعلها².

المطلب الثاني: المخولون بالقانون بالبحث والتحري

إن مرحلة جمع الاستدلالات التي يتولى بها رجال الضبط القضائي مهام الضبط القضائي والاشراف على مأموري الضبط كل في دائرة اختصاصه لمباشرة البحث والاستقصاء عن الجرائم التي تلزم التحقيق في الدعوى الجزائية، ومن خلال النيابة العامة تتولى عملية التحقيق بشكل واسع في عملية البحث والتحري عن الجرائم الالكترونية، ويلاحظ أيضا أن القانون الإماراتي والمصري قد أناط لمأمور الضبط القضائي، الذين يقومون بها بصفتهم سلطات ضبط قضائي تأتي بمرحلة

¹ قانون الإجراءات الجزائية رقم (3) لسنة 2001 م، المادة 19 والمادة 22.

² فضل، سليمان احمد: المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. لا يوجد رقم طبعة. القاهرة: دار النهضة العربية. 2013. صفحة 277

الاستدلال حين تقع جريمة الكترونية يترتب البحث والتحري عن الادلة الناتجة عنها، أما الإجراءات الإدارية التي تأتي للوقاية أو للاحتياطات الأمنية التي ينفذها رجال الشرطة قبل وقوع الجريمة¹، والتي يختص بإجراءات جمع الاستدلالات هم مأموري الضبط القضائي، والتي يكون النائب العام له سلطة الإشراف والمسؤول عن أعمالهم وتمتد سلطة الإشراف على أعمال الضبطية القضائية، كما يحق له مطالبة الجهات المختصة مسائلة مأموري الضبط القضائي تأديبا عن تقصيرهم أو مخالفتهم لواجبات عملهم².

وان إجراءات جمع الاستدلالات ينطوي فيها عملية البحث والتحري حول الجريمة والتمهيد والتحقيق فيها دون التوغل في عملية التحقيق فيما تختص النيابة العامة دون غيرها³، فالاصل أن مأمور الضبط القضائي لا يملك اتخاذ اجراءات ماسة بالحريات العامة، ولكن أستثنيت من ذلك في حالة التلبس التي أجاز فيها اتخاذ بعض الاجراءات⁴.

ولأهمية مرحلة الاستدلال أهمية كبيرة في كشف حقيقة وقوع الجريمة، حيث تفيد هذه المرحلة في تكوين عقيدة وقناعة للنياية العامة بالأدلة إما بالإثبات أو بالنفي مما يسهل للنياية في إجراء التحقيق الابتدائي أو التصرف فيها، من الجهة الأخرى تسمح هذه المرحلة بحفظ الدعوى والبلاغات غير الجدية، وتتميز سلطات الاستدلال بفاعلية ونشاط أكثر في البحث عن الدلائل بأكثر لما تتسم به سلطات التحقيق للكشف عن الجريمة⁵.

ويرى البعض إن مهمة الضبط القضائي تبدأ حينما تنتهي مهمة مأموري الضبط الإداري فعندما تفشل سلطات الضبط الإداري في وقاية المجتمع من الجريمة وفي الحفاظ على الأمن

¹ الحمامي، علاء حسين والحمامي، محمد علاء: مفاهيم وتطبيقات الأساليب الأمنية الحديثة في التحقيق الالكتروني. لا يوجد طبعة، العدد 31، الإمارات: مركز الإمارات للدراسات والبحوث الإستراتيجية، لا وجد سنه نشر، صفحة 47

² قانون الإجراءات الجزائية رقم (3) لسنة 2001 م، المادة 19، والمادة 20.

³ العفيفي، يوسف خليل يوسف: الجرائم الالكترونية في التشريع الفلسطيني. (رسالة ماجستير منشورة). مرجع سابق، صفحة 97.

⁴ العفيفي، يوسف خليل يوسف: الجرائم الالكترونية في التشريع الفلسطيني. (رسالة ماجستير منشورة). مرجع سابق، صفحة 115.

⁵ فضل، سليمان احمد: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. لا يوجد رقم طبعة. القاهرة: دار النهضة العربية. 2013. صفحة 279.

والنظام العام والسكينة، تتولى سلطات الضبط القضائي مهمتها في الكشف عن مرتكبي الجريمة وجمع الأدلة الكافية عنها¹.

حيث استقر القضاء الإداري الدول العربية على خروج الإجراءات التي تصدر عن أفراد هيئة الشرطة ومأموري الضبط القضائي من دائرة رقابته في ظل إنها صدرت وفق الاختصاص الجنائي لهم، وإن الأعمال التي يقومون بها من القيام بالتحريات وجمع الاستدلالات أو بالتفتيش أو القبض على المتهم في حالة تلبس تعد من الأعمال القضائية، ويلاحظ إن رجال الشرطة يقومون بمهمتين هما مهمة الضبط القضائي والضبط الإداري، فالأولى تعد أعمالهم أعمال قضائية بعد وقوع الجريمة ومتابعة أجراءاتهم وفق القانون الناظم، أما الثانية تهدف إلى حماية النظام العام².

فالاصل أن مأمور الضبط القضائي لا يملك اتخاذ اجراءات ماسة بالحريات العامة، ولكن أستثيت من ذلك في حالة التلبس التي أجاز فيها اتخاذ بعض الاجراءات التي وهي في الاصل اختصاصات النيابة العامة³.

يكون من مأموري الضبط القضائي وفقا لقانون الإجراءات الجزائية الفلسطيني هم⁴:

1- مدير الشرطة ونوابه ومساعدوه ومديرو شرطة المحافظات والإدارات العامة.

2- ضباط وضباط صف الشرطة، كل في دائرة اختصاصه.

3- رؤساء المراكب البحرية والجوية.

4- الموظفون الذين حُولُوا صلاحيات الضبط القضائي بموجب القانون.

¹ ادعيس، معن: صلاحيات جهاز الشرطة. لا يوجد طبعة. الهيئة الفلسطينية المستقلة لحقوق المواطن رام الله- فلسطين. ص 25 .

² محمد، ده شي صديق: القضاء الاداري وتنازع اختصاصاته مع القضاء العادي (دراسة تحليلية مقارنة). ط1. القاهرة: المركز القومي للإصدارات القانونية. 2016. صفحة 129.

³ العفيفي، يوسف خليل يوسف: الجرائم الالكترونية في التشريع الفلسطيني. (رسالة ماجستير منشورة). مرجع سابق، صفحة 115.

⁴ قانون الإجراءات الجزائية رقم (3) لسنة 2001 م، المادة 21.

وكما هو محدد في قانون السلطة القضائية الفلسطينية في المادة (69) منه تبعية أعضاء مأموري الضبط القضائي بنصها أن: " أعضاء مأموري الضبط القضائي يكونون فيما يتعلق بأعمال وظائفهم تابعين للنيابة العامة في البحث عن الجريمة وجمع الاستدلالات¹.

وعند الحديث عن مأمور الضبط الإداري ومأمور الضبط القضائي لا بد لنا والتفرقة بينهما وفقاً لنصوص القانون الفلسطيني:

يعرف الضبط الإداري بأنه النشاط الذي تمارسه السلطة التنفيذية ممثلة في هيئاتها الإدارية وموظفيها مستهدفة في ذلك المحافظة على النظام العام بعناصره الأربعة وهي توفير الأمن العام وتوفير السكنية العامة و صيانة الصحة العامة و الحفاظ على الآداب العامة².

لم يحدد القانون الفلسطيني ما هو المقصود بالضبط الإداري بشكل واضح وصريح وإنما اكتفى بالنص في بعض القوانين على مسؤولية وصلاحيات جهاز أو جهة أو إدارة على الحفاظ على النظام العام و توفير الأمن والسكنية والصحة العامة.

ويقصد بمأمور الضبط القضائي: جميع الموظفين الذين خولهم القانون مباشرة اجراءات الاستدلال وقد بينت المادة 19 من قانون الاجراءات الجزائية صفه مأمور الضبط القضائي، ويعهد هؤلاء الاشخاص بمباشرة اجراء الاستدلال على النحو الذي نظمة القانون ويطلق عليهم مأمور الضبط القضائي او رجال الضبطية من ناحية اخرى³.

ومن أهم المعايير التمييز بين أعمال الضبط الإداري وأعمال الضبط القضائي هو المعيار الموضوعي و الذي لا يهتم بالجهة التي تقوم بأعمال الضبط القضائي، وإنما يركز على طبيعة هذا الضبط وخلال فتره جمع الأدلة والاستدلالات الجريمة فهو يعد ضبطاً قضائياً أما إذا صدر بصورة

¹ قانون السلطة القضائية الفلسطينية رقم (1) لسنة 2002م.

² الطهرأوي، هاني علي: القانون الإداري، ط1. عمان: دار العلمية الدولية ومكتبة دار الثقافة للنشر والتوزيع. 2001، صفحة 228.

³ مرسى، علاء زكي: سلطات النيابة العامة ومأمور الضبط القضائي في قانون الاجراءات الجزائية. طبعة أولى. المركز القومي للاصدارات القانونية. القاهرة. 2014. صفحة 242.

تدابير تسعى من خلالها الإدارة إلى الحفاظ على الأمن والنظام العام فان العمل يُعتبر ضبطاً إدارياً¹.

ومعيار التمييز بين الضبط الإداري والضبط القضائي امر مهم في بالغة الأهمية، نظراً للتداخل بينهما ومن هذه المعايير تتم على النحو التالي²:

أولاً: المعيار الزمني: يقوم هذا المعيار على أساس نشاط السلطة الادارية، والذي يُعتبر مانعاً ووقائياً لوقوع الجرائم الالكترونية، فهو يسبق وقوع الإخلال بالنظام والأداب العامة، على عكس الضبط القضائي، فإنها سلطة اجرائية تقوم بجمع الاستدلالات والتحري عن مركبي الجرائم فهو لاحق على وقوع الجريمة.

ثانياً: المعيار الشكلي: يقوم هذا المعيار على أساس أن أعمال الضبط الإداري هي التي يقوم بها رجال الضبط الإداري، أما أعمال الضبط القضائي فهو التي يقوموا بها رجال الضبط القضائي والتي حُددت بموجب القانون ونص عليها القانون صراحةً، ويؤخذ في هذا المعيار بأن كثيراً من رجال الضبط الإداري هم أنفسهم رجال الضبط القضائي.

ثالثاً: معيار إنشاء القاعدة القانونية: يقوم هذا المعيار على أن أعمال الضبط الاداري تمثل خلق قاعدة قانونية لم تكن موجودة من قبل بإعتبار اجراء الضبط الإداري إجراء مبتدأ، بمعنى إنه قيام فرد بإرتكاب جريمة إلكترونية ساعدت الضبط الإداري على خلق نص قانونية، بينما عمل الضبط القضائي يقتصر على التأكد من أن احد الأفراد، قد خالف قاعدة قانونية نشأت دون ان يتعدى على خلق هذه القاعدة القانونية.

رابعاً: معيار طبيعة العمل ذاته: بحيث إذا كانت الجهة المتصرفة قد اتخذت العمل بإعتبارها مهمة مساعدة للقضاء هدفها البحث والتحري عن الجرائم ومرتكبيها تمهيداً لإقتتاح الدعوى الجزائية،

¹ صورية، العاصمي: تأثير نظام الضبط الإداري على الحقوق والحريات العامة. رسالة ماجستير منشورة. جامعة الحاج لخضر بباتنة . 2011-2012 م. ص 24 .

² الزرعوني، هشام عبد الرحمن: المسؤولية المدنية لمأموري الضبط القضائي دراسة مقارنة، طبعة أولى. حقوق الطبع محفوظة لشرطة الشارقة. الامارات العربية المتحدة. 2015. صفحة 39-40.

فالعامل يكون من أعمال الضبط القضائي، أما إذا كان العمل قد أُتخذ لحفظ النظام العام والآداب العامة دون هدف تحريك الدعوى الجزائية، فإن العمل يعتبر من أعمال الضبط الإداري.

والمسؤولية المترتبة على كل من عمل أفراد الضبط الإداري وعمل أفراد الضبط القضائي، إنّ ما ينتج من أضرار جراء نشاط الإدارة وعمالها يكون من مسؤولية الإدارة والإدارة مسؤولة بالتعويض عن أعمال الضبط الإداري والتعويض عنها في حال ارتكب رجالها أخطاء جسيمة أو فاحشة، أما أفراد الضبط القضائي فينتم بالطابع العلاجي وتتنحصر مهمته في الكشف عن الجرائم ومرتكبيها وتسليمهم للعدالة، فالسلطة الضبطية القضائية تمارس نشاطاً جزائياً يهدف إلى إثبات وقوع الجريمة وإثبات مرتكبها وجمع ادلتها، إلا أنه يمكن في بعض الحالات قد تكون المهمة مزدوجة وتحمل الصفتين معاً - صفة السلطة الإدارية الضبطية وصفة السلطة القضائية الضبطية - مثلاً عندما يقوم شرطي بتحرير بتنظيم المرور وهي وظيفة ضبط إداري فيقوم على تحرير المخالفات المرورية حال وقوع مرتكبها، ويعمل على تنظيم محضل إذا استدعى الأمر وهي وظيفة ضبطية قضائية¹.

ومن هذه الأجهزة التي أعطيت صفة الضبط الإداري:

1. **جهاز الشرطة:** حيث نص القانون الأساسي في المادة 84 على أن قوات الشرطة هي قوات مسلحة وتتنحصر وظيفتها في حماية المجتمع والأمن والنظام العام والآداب العامة والسير على الأمن.

بالإضافة إلى نص القرار بقانون الصادر حديثاً رقم (23) لسنة 2017 بشأن الشرطة الفلسطينية، نص المادة 3 منه على اختصاصات الشرطة وهي²:

1- المحافظة على النظام والأمن العام، والآداب العامة، والسكينة العامة.

2- حماية الأرواح والأعراض والأموال.

3- منع ومكافحة الجريمة، وضبط مرتكبها بموب القوانين المعمول بها.

¹ الزرعوني، هشام عبد الرحمن: المسؤولية المدنية لمأموري الضبط القضائي دراسة مقارنة، مرجع سابق، ص 39-40.

² القرار بقانون الصادر حديثاً رقم (23) لسنة 2017 بشأن الشرطة الفلسطينية، الوقائع الفلسطينية عدد ممتاز رقم 15، نص المادة 3 منه.

- 4- مكافحة أعمال الشغب وكافة مظاهر الإخلال بالأمن العام.
 - 5- حماية الحقوق والحريات المشروعة التي يكفلها القانون الأساسي والقوانين ذات الصلة، والاتفاقيات الدولية التي تكون الدولة طرفاً بها.
 - 6- حماية الممتلكات العامة والخاصة للدولة والأفراد.
 - 7- مساعدة قوى الأمن والسلطات العامة الأخرى في أداء مهامها بموجب احكام القانون.
 - 8- التعاون الشرطي العربي والإقليمي والدولي في مجال مكافحة الجريمة من خلال جمع وتوثيق وتبادل المعلومات والبيانات والأدلة عن الجرائم ومرتكبيها، وتقديم خدمات التعاون الشرطي والأمني وفقاً للتشريعات والقوانين النافذة، والاتفاقيات الدولية التي تكون الدولة طرفاً فيها.
 - 9- تنفيذ ما تفرضه عليها القوانين واللوائح والأنظمة من واجبات ومهام.
 - 10- تقديم المعلومات والإرشادات للمواطنين بالوسائل التي تساعد على مكافحة الجريمة، ووقايتهم منها، وتسهيل تنفيذ واجبات الشرطة بما يحقق ضمان مساهمة المواطنين في معاونتها ودعمها في كافة واجباتها.
 - 11- توعية المواطنين بحقوقهم وواجباتهم، لضمان المشاركة المجتمعية في حفظ النظام والأمن العام في المجتمع.
 - 12- تحقيق الأمن الداخلي للوطن والمواطنين، والمساهمة في تحقيق الأمن القومي بالتنسيق والتعاون مع الأجهزة الامنية المختصة، والمؤسسات العامة، ومؤسسات المجتمع المدني، ووسائل الإعلام، ولها تنظيم مذكرات تفاهم بهذا الخصوص.
- كما أعطى قانون الاجتماعات مدير الشرطة أن يضع الضوابط المحددة والأنظمة للاجتماعات العامة. كما ألزم الجهات القائمة على الاجتماعات بأن تبلغ مدير الشرطة قبل 48 ساعة على الأقل بموعد الاجتماع و مكانه ليتسنى له اتخاذ الإجراءات اللازمة¹.

¹ قانون الاجتماعات العامة رقم 12 لسنة 1998م، المادة 3-5.

2. **الدفاع المدني:** يتبع الدفاع المدني للأمن الداخلي، وهي من القوات التي لها مرجع قانوني واضح وصريح منذ عام 1998¹. أما اختصاصات الادارية لجهاز الدفاع المدني فقط فيما يتعلق بالكوارث والحالات الطبيعية.²

3. **المخابرات العامة:** من أهم الصلاحيات والأعمال التي تقوم بها قوى الأمن الخارجي حسب قانون المخابرات العامة:³

- اتخاذ التدابير اللازمة للوقاية من أية أعمال تعرض أمن وسلامة فلسطين للخطر واتخاذ الإجراءات اللازمة ضد مرتكبيها وفقاً لأحكام القانون.

- الكشف عن الأخطار الخارجية التي من شأنها المساس بالأمن القومي الفلسطيني في مجالات التجسس والتآمر والتخريب أو أية أعمال أخرى تهدد وحدة الوطن وأمنه واستقلاله ومقدراته.

- التعاون المشترك مع أجهزة الدول الصديقة المشابهة لمكافحة أية أعمال تهدد السلم والأمن المشترك أو أي من مجالات الأمن الخارجي، شريطة المعاملة بالمثل.

4. **قوات الأمن الوطني:** تعد قوات الأمن الوطني من القوى الثلاث التي نص عليها قانون الخدمة في قوى الأمن، وهي قوة مستقلة بحد ذاتها، ولا يوجد قوانين تنظم هذه القوى ولكن لها اختصاصات معروفة لكل قوة منها.

¹ قانون الدفاع المدني رقم 3 لسنة 1998 م.

² قانون الدفاع المدني رقم 3 لسنة 1998 م. المادة 5.

[1] جميع أعمال الدفاع المدني بما في ذلك إعداد المشروعات وخطط العمل والإشراف على تنفيذها وتدريب ما يلزم من أدوات ومهمات ودراسة أحدث وسائل الدفاع المدني وطرق نشر تعليمها بين الجمهور.

[2] اتخاذ الإجراءات الضرورية مع اللجان المعنية لمواجهة الكوارث وحالات الطوارئ في الأحوال التي يقرها رئيس السلطة الوطنية.

[3] توعية المواطنين بأعمال الدفاع المدني والتعاون مع فرقها وتوزيع النشرات والإعلانات المتعلقة بعملها في زمن السلم والحرب.

³ قانون المخابرات العامة رقم (17) لسنة 2005م، المادة 8 .

5. الأمن الوقائي: لقد نظم القرار بقانون الذي صدر بشأن الأمن الوقائي رقم 11 لسنة 2007 اختصاصات الأمن الوقائي حيث نصت المادة 6 على الاختصاصات التالية:

- 1- العمل على حماية الأمن الداخلي الفلسطيني.
 - 2- الكشف عن الجرائم التي تستهدف الإدارات الحكومية والهيئات والمؤسسات العامة والعاملين فيها.
 - 3- متابعة الجرائم التي تهدد الأمن الداخلي للسلطة الوطنية و/أو الواقعة عليه، والعمل على منع وقوعها¹.
- وعند الحديث عن سلطات الضبط القضائي ومن هم سلطات الضبط حسب القوانين الفلسطينية لا بد لنا أن نقسم عمل هذه السلطات إلى قسمين وهي كالتالي:

1. دور مأمور الضبط القضائي:

1. أعمال يباشرها رجال الضبط القضائي في الأحوال العادية مثل البحث والتحري والاستدلال وجمع المعلومات.
 2. أعمال يباشرها رجال الضبط القضائي في الأحوال غير العادية مثل ندب بعض رجال الضبط القضائي في التحقيق في الجرح أو حالة التلبس².
- 4- حسب الإجراءات في جمع الاستدلالات:

1. إجراءات جمع الاستدلالات: مثل التفتيش والتلبس.
2. إجراءات بعد جمع الاستدلالات: مثل التحقيق وسماع الشهود³.

¹ قرار بقانون بشأن الأمن الوقائي رقم 11 لسنة 2007 م، المادة 6.

² نبيه، نسرين عبد الحميد: حقوق المتهم أمام سلطات الضبط القضائي. ط1. الإسكندرية: مكتبة الوفاء القانونية. 2010م. صفحة 93.

³ قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 53.

ولكن لحماية الحق العام والحفاظ على الإجراءات والأدلة التي تقوم بها النيابة العامة في التحقيق الابتدائي ولتسريع انجاز الهدف الذي انشأ من أجله القضاء وسلطات الضبط القضائي بصفة عامة أعطى بعض الأجهزة الأمنية صفة الضبط القضائي لتخولها القيام بإجراء من إجراءات التحقيق حسب اختصاصها النوعي تحت إدارة النيابة العامة وإشرافها ومن هذه الأجهزة التي أعطيت صفة الضبط القضائي:

1. **الشرطة المدنية:** القانون أعطى صفة الضابطة القضائية للشرطة الفلسطينية لأفراد معينين ومحددin وليس إلى أعضاء الجهاز كافة بل يقتصر على مدير الشرطة ونوابه ومساعديه ومديري شرطة المحافظات والإدارات العامة بالإضافة إلى ضباط وضباط صف الشرطة كل منهم في دائرة اختصاصه¹، وأعطى القرار بقانون صفة الضابطة القضائية الى الشرطة الصادر حديثا ويحمل رقم (23) لسنة 2017 بشأن الشرطة الفلسطينية، حيث نصت المادة (6) بأنه: " يتمتع الضابط وضباط صف الشرطة بصفة الضبطية القضائية أثناء تأدية واجباتهم، كل في حدود اختصاصه، وفقاً لأحكام قانون الاجراءات الجزائية النافذ، ويباشرون أعمالهم بصفتهم ضابطة قضائية تحت إشراف النائب العام بصفته رئيس الضابطة القضائية"².

6. **الدفاع المدني:** حيث نص قانون الدفاع المدني رقم (3) لسنة 1998 على اختصاص بعض الأفراد بصفة الضابطة القضائية "يكون للموظفين الذين ينتدبهم الوزير من موظفي وزارة الداخلية وغيرها صفة الضبط القضائي في تنفيذ أحكام هذا القانون والقرارات المنفذة له، ويكون لهم حق الدخول إلى أي مكان للتأكد من تنفيذ التدابير المنصوص عليها في هذا القانون أو القرارات الصادرة بموجبه"³.

¹ الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 21:

1- مدير الشرطة ونوابه ومساعدوه ومديرو شرطة المحافظات والإدارات العامة.

2- ضباط وضباط صف الشرطة، كل في دائرة اختصاصه.

3- رؤساء المراكب البحرية والجوية.

4- الموظفون الذين خولوا صلاحيات الضبط القضائي بموجب القانون.

² القرار بقانون الصادر حديثا رقم (23) لسنة 2017 بشأن الشرطة الفلسطينية، الوقائع الفلسطينية عدد ممتاز رقم 15، نص المادة 3 منه

³ قانون الدفاع المدني رقم 3 لسنة 1998 م. المادة 23.

2. **موظفو وزارة الاتصالات الفلسطينية:** حديثاً بعد إصدار قرار بقانون رقم () بشأن المعاملات الإلكترونية تم استحداث جزء من موظفين وزارة الاتصالات وتكنولوجيا المعلومات؛ لتكون وظيفتهم سلطة ضبط قضائي، وكذلك على الجهات المختصة والأجهزة الأمنية مساعدتها في حال قيامهم بالمهام المناطة لهم¹، وحديثاً بعد صدور القرار بقانون رقم (16) لسنة 2018 بشأن الجرائم الإلكترونية من توقيعه من السيد الرئيس محمود عباس، نصت المادة (58) من على التالي " تتولى الوزارة وفقاً لاختصاصها تقديم الدعم والمساعدة الفنية لجهات انفاذ القانون، ويعتبر موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ احكام هذا القرار بقانون"². وعليه يعتبر موظفو وزارة الاتصالات الفلسطينية مأموري ضبط قضائي.

3. **الأمن الوقائي:** حيث صدر قرار بقانون رقم (11) لسنة 2007 ينظم عمل جهاز الأمن الوقائي ونصت المادة (7) على منح صفة الضابطة لضباط و ضباط صف الإدارة العامة في الأمن الوطني . ومن أهم المهام التي تقع على عاتق الأمن الوقائي الكشف عن الجرائم التي تستهدف الإدارات الحكومية و الهيئات و المؤسسات العامة.

4. **المخابرات العامة:** نص قانون المخابرات العامة على امتلاك أفراد المخابرات العامة لصفة الضابطة القضائية و كان ذلك في نص المادة 12 من قانون المخابرات العامة رقم 17 لسنة 2005 " يكون للمخابرات في سبيل مباشرة اختصاصاتها المقررة بموجب هذا القانون صفة الضبطية القضائية." وهنا يلاحظ أن اختصاص صفة الضابطة القضائية لكل أفراد جهاز المخابرات على العكس مما هو في جهاز الأمن الوقائي و الشرطة و الدفاع المدني الذي أناط صفة اختصاص الضابطة القضائية لأفراد معينين.

¹ قرار بقانون بشأن المعاملات التجارية رقم () لسنة 2017. المادة 47 " تمنح الوزارة عدد من موظفيها صفة الضبط القضائية، وعلى كافة الجهات المختصة والأجهزة الامنية تقديم المساعدة لهم للقيام بمهامهم".

- البيانات الإلكترونية: بيانات ممثلة أو مرمزة الكترونياً سواء على شكل نص أو رمز أو صوت أو صور أو غيرها .
- السجل الإلكتروني: مجموعة المعلومات التي يتم إنشاؤها أو إرسالها أو تسليمها أو تخزينها بوسائل إلكترونية، والتي تشكل مجملها وصفا لحالة شخص أو شي ما.

² قرار بقانون بشأن الجرائم الإلكترونية رقم (16) لسنة 2017. المادة 58

5. الضابطة الجمركية: في عام 2016 صدر قرار بقانون وجاء في القرار: " يكون لمنتسبي الضابطة الجمركية من ضباط وضباط صف في سبيل تسهيل مهمتهم وفقاً للقانون. صفة الضبط القضائي فيما يختص بعملهم¹."

وأن طبيعة عمل جهاز الضابطة الجمركية يتيح له ان يكون له صلاحيات الضبط القضائي وأن تمارس المهام والصلاحيات الموكلة إليها مثل التفتيش .

حيث أجازت أحكام قانون الجمارك للموظف أو الشرطي أن يوقف أية وسيلة من وسائل النقل ويفتشها للتأكد مما إذا كان فيها بضائع مهربة إذا كان لديه سبب معقول².

المطلب الثالث: صفات المحققين بالجريمة الإلكترونية

هناك صفات يجب توافرها في رجال البحث الجنائي تساعده على أداء عمله بالوجه المرجوة منه والتوصل إلى مرتكبيه وتقديمهم إلى العدالة بالحنكة والأداء العالي بعد التحلي بهذه الصفات:

أولاً- التركيز وقوة الملاحظة: من المفاتيح الهامة لرجال البحث الجنائي التركيز وقوة الملاحظة، ويجب على رجال البحث عند معاينة مسرح الجريمة أو مناقشة أو تتبع المتهمين أو الشهود أن يكون قوي الملاحظة لكل ما تقع عليه عينه أو تسمعه أذنه، وملاحظة لغة جسدهم من خلال الانفعالات الداخلية التي تبرز للخارج جراء التوتر الزائد³.

ثانياً- السرعة في إنجاز العمل المكلف فيه: يجب على المحقق الانتقال فور ورود البلاغ مباشرة ويجب على المحقق أن يقوم بحصر الشهود وسؤالهم قبل التأثير عليهم أو نسيان لبعض الوقائع، ولا يقصد هنا السرعة العجلة لا التعجل تؤدي ذلك إلى عواقب وخيمة، وعلى المحقق سرعة إخطار الخبراء الفنيين في الحاسبات وبرامجها ونظمها والتصوير الجنائي حرصاً على أدلة الجريمة⁴.

¹ تقرير صادر إلى قائد جهاز الضابطة الجمركية العميد إياد بركات ، تاريخ الزيارة 2016/9/25 على الموقع الإلكتروني: <http://www.palsafar.ps/%D8%A7%D9%84%D8%B3%D9%8A%D8%AF> .

² قانون الجمارك والمكوس قانون رقم 1 لسنة 1962. المادة 143

³ أبو الروس، احمد: منهج البحث الجنائي. لا يوجد طبعة. الإسكندرية: المكتب الجامعي الحديث. 2009، صفحة 29.

⁴ موسى، مصطفى محمد: التحقيق الجنائي في الجرائم الإلكترونية. مرجع سابق، صفحة 269.

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 الجريمة¹. ومنع من كان حاضراً حين وقوع الجريمة حتى يحرر محضراً بإفادات الموجودين².

ثالثاً- كتمان السر: يجب على المحقق أن يكون كتماً لمجريات التحقيق ضماناً لسر صحة مجريات التحقيق، ولا يجوز له إفشاء ما توصل إليه من معلومات إلى وسائل الإعلام ووكالات الأنباء ولا يجوز للمحقق إذاعة القضايا والتحقيقات، ولا أن يطلع عليها أحداً من غير الأشخاص الذين لهم صلاحية النظر فيها بموجب القوانين والأنظمة³.

رابعاً- الترتيب والدقة والتأني وبذل العناية: يجب على المحقق أن يتميز بالترتيب والدقة بالانتقال في الوقت المناسب إلى مكان الحادث ويعاينه بحضور المتهم والشهود ويفحصه فحصاً دقيقاً، وعليه التأني فيما قد يكون الجاني قد تركه من آثار تقيد في كشف الحقيقة وضبط الأدلة، وبذل عناية الرجل المعتاد في الحصول على الأدلة بالدقة اللازمة⁴.

خامساً- يشترط ان يكون مأمور الضبط القضائي مؤهلاً للتعامل بالجرائم الالكترونية⁵.

¹ قانون الإجراءات الجزائية رقم (3) لسنة 2001 م، المادة 27 "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 قانون الإجراءات الجزائية رقم (3) لسنة 2001 م، المادة 1/28 "لمأمور الضبط القضائي عند انتقاله في حالة التلبس بالجرائم أن يمنع الحاضرين من مباحرة مكان الجريمة أو الابتعاد عنها حتى يتم تحرير المحضر، وله أن يحضر في الحال من يمكن الحصول منه على إيضاحات في شأن الواقعة".

³ موسى، مصطفى محمد: التحقيق الجنائي في الجرائم الالكترونية. مرجع سابق، صفحة 269-270.

⁴ موسى، مصطفى محمد: التحقيق الجنائي في الجرائم الالكترونية. مرجع سابق، صفحة 269.

⁵ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 5/33

المطلب الرابع: مشروعية البحث والتحري

القاعدة العامة هي أن كل ما يجرمه المشرع من الإجراءات يعتبر غير مشروع ولا يمكن الاستمرار به لمخالفته القانون، ويترتب عليه البطلان ويترتب عليه المسألة المدنية والتأديبية، ومن أبرز هذه الإجراءات غير المشروعة التعذيب بالضرب والإيذاء والوضع لفترات طويلة في الحديد¹.

ومبدأ المشروعية يقصد به من النطاق الواسع: هو سيادة القانون أي خضوع أفراد المجتمع بما فيها السلطة العامة بكل أجهزتها للقواعد القانونية السارية المفعول؛ حيث توافق كل التصرفات التي تصدر من المواطنين وسلطات الدولة مع القواعد القانونية المختلفة المصدر المتعارف عليه من قبل الدولة، أما مبدأ المشروعية من الناحية الإدارية: خضوع الإدارة للقانون معناه أن كل أعمال الإدارة يجب أن تكون أعمالاً مشروعة لا تخالف القانون².

والمشروعية وهي التوافق والتقيد بأحكام القانون في إطاره ومضمونه بحيث تهدف إلى ضمانات أساسية وحدة الأفراد لحماية حرياتهم وحقوقهم الشخصية ضد استغلال أو تعسف السلطة في الحالات التي أعطاها القانون لها، وبنفس الوقت حماية المجتمع من خطر الجريمة بالقدر نفسه حماية الفرد من أخطار الجريمة، لذا إن صحة الإجراءات يستلزمها أن تقوم جهة التحقيق بمبدأ المشروعية من أجل أن تثمر على دليل صحيح وسليم يعول عليه القضاء لبناء حكمه بسلامه ولا يطعن بها لذلك فإن إجراءات مبدأ شرعية الجرائم والعقوبات متلاصقة إلى مبدأ مشروعية سلامة إجراءات التحقيق والبحث عن الجريمة، فإذا انتهكت سلامة الفرد تستلزم عدم قبول أي دليل³.

ومن حيث نطاق تطبيق مبدأ المشروعية يكون من خلال خضوع الجميع لأحكام القانون بمعناه الواسع إلى كفالة حقوق وحريات الأفراد، ويتحقق بموجبه التزام كل الأفراد بمبدأ المشروعية.

¹ علوني، هليل فرج: التحقيق الجنائي والتصرف فيه. لا يوجد طبعة. الإسكندرية: دار المطبوعات الجامعية. 2006، صفحته 473.

² الشامل للأبحاث الإلكترونية، مبدأ المشروعية، بحث منشور على الانترنت <http://droit.moontada.com/t70-topic>

³ سعيداني، نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مرجع سابق، صفحة 207-208.

ويترتب من خلاله منع الاستبداد ويمكن للأفراد وللإدارة ممارسة وظائفهم طبقاً لقواعد معلومة للجميع¹.

عند الحديث عن مشروعية البحث والتحري لدى سلطات الضبط القضائي في سبيل جمع الاستدلالات ، ظهر عن الفقهاء نظريتان بمدى مشروعية البحث والتحري، والنظرية الأولى تتمحور إذا كان محل الجهاز مستقلاً عن الشبكة العنكبوتية وبدأت الأجهزة الأمنية بالبحث والتحري لا يترتب عليه انتهاكاً لحرمة الحياة الخاصة لأي شخص حيث يقصر البحث فقط عن محل الجريمة. والنظرية الثانية إذا كان الجهاز المرتكب فيه الجريمة الإلكترونية مرتبطاً بشبكة الانترنت هنا اعتبره خروج عن حدود المشروعية ويترتب عليه بطلان تلك الإجراءات لانتهاكه لحرمة الحياة الخاصة².

ومن المقرر أن الأدانة في أي جريمة لا بد و أن تكون مبنية على أدلة مشروعة تم الحصول عليها وفقاً للقواعد القانونية وبإحترام القانون من طرف الجهة المختصة بجمع الأدلة وما يتضمنه من أدلة مستخرجة من الشبكة العنكبوتية، ولا يكون هذا الدليل مشروعاً إذا كانت عملية تقديمه إلى القضاء بغير الطرق التي رسمها القانون، فمتى تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد بقيمته مهما كانت دلالاته الحقيقية وذلك لعدم مشروعيته، وعليه إذا كان الادلة الالكترونية المتحصلة عبر الشبكة العنكبوتية خالفت القواعد الإجرائية فإنها تكون باطلة، وبالتالي بطلان الدليل المستمد منها ولا تصلح لأن تكون ادلة تبنى عليها الأحكام القضائية، مثلاً في حالة: تفتيش جهاز الشرطة بمراقبة الاتصالات دون ان يكون محلاً لأذن من السلطة المختصة او إتخاذ ترتيبات تقنية كأختراق جهاز المتهم ووضع برامج عليه من أجل تفتيش جهاز الحاسوب دون

¹ نعيم جميل علاونة، فادي: مبدأ المشروعية في القانون الإداري وضمانات تحقيقه. رسالة ماجستير منشورة. جامعة النجاح الوطنية. نابلس، فلسطين. 2011. صفحة 50.

² العبودي، محسن. <http://www.eastlaws.com>. شبكة قوانين الشرق: 2016/9/5. متاح من:

<http://www.eastlaws.com>.

الحصول على مذكرة من جهات الاختصاص فتؤدي الى المساس بالحياة الخاصة للغير لمخالفته نصوص القانون¹.

اما في فلسطين بخصوص ضبط ومصادرة الاجهزة قد نص قرار بقانون رقم (16) لسنة 2017 في نص المادة 54 منه على التالي حفاظا لحقوق الغير وحسن النية، تصدر المحكمة قرار بمصادرة الاجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة المنصوص عليها في هذا القرار بقانون؛ بمعنى أنه احترام الحياة الفردية للأشخاص ولحقوق الغير ولحسن النية، وأنه لم يتأخذ مبدأ بشأن الضبط في حال كان الجهاز متصل في الانترنت أم لا.

ولحساسية عمل الوحدة تتطلب اجراءات محددة في بعض الحالات حيث يتم التنسيق بالبداية من قبل النيابة الجزائية بناء على الاحتياج مع رئيس النيابة المختصة ويتم مخاطبة النائب العام، وهو الجهة الاصلية المخولة بمخاطبة وزارة الاتصالات وشركة الاتصالات ومزودي خدمة الانترنت بموجب قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 المادة 51 تقاديا لانتهاك الخصوصية في بعض القضايا.²

ويرى الباحث بالنظر والتدقيق في النظريتين بأن الأفضل والأنسب الجمع بين هاتين النظريتين وخروج بمبدأ يعمل على ضبط الجريمة والحصول على الادلة سواء كان المضبوط موصول في الانترنت أو غير موصول بالانترنت فالحقيقة اسمى للكشف عن الجاني وردعه بالعقوبة المقرره حسب القانون، وعلى ان تكون عملية الضبط متوافقه مع القانون والاصول المتبعة. في ظل ارتكاب الجريمة الإلكترونية إلا باتصال دائم في الانترنت، حيث يمكن لمرتكبي الجرائم الإلكترونية

¹ سعيداني، نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مرجع سابق، صفحة 210.

² موقع جريدة القدس، النيابة الالكترونية. تاريخ الزيارة 2018/5/2 الموقع الالكتروني <http://www.alquds.com/articles/1484890275698412300>، نسرین الرشماوي في مقابلة خاصة مع القدس.

إخفاء رقم (IP) واعتبارهم غير متصلون بالشبكة العنكبوتية وتحقيق كافة أركان الجريمة الإلكترونية.

وقد قضى القضاء الفرنسي من خلال عدد من القرارات بحيث اعتبر إذا فحص عنوان IP الخاص بجهاز الحاسوب لا يعتبر مساساً بالخصوصية ولا بالمعطيات الشخصية¹

والمشروعية من المخرجات في الحاسوب الآلي يجب أن يتفق الإجراء مع القواعد القانونية، أي أن مشروعية الدليل الجنائي لا تقتصر على مطابقة الدليل بالقاعدة القانونية بل تمتد إلى إعلانات حقوق الإنسان والمواثيق الدولية².

تمد المسؤولية مدنياً وجزائية في فلسطين على أفراد الشرطة عند ارتكاب فعل، ويعاقب عناصر الشرطة تأديباً عند قيامهم بمخالفة القرار بقانون، والتعليمات الصادرة من الوزير أو المدير العام، الخروج عن مقضيات الضبط الربط للوظيفة الشرطية، والقيام بسلوم من شأنه الإخلال بكرامة الوظيفة³.

وتتحمل الدولة دفع أي تعويضات قانونية مترتبة عن عناصر الشرطة، عن الأضرار التي تحدث للغير أثناء تأديتهم للعمل الرسمي ضمن القانون، ولا يعفى أي من عناصر الشرطة من العقوبة في حال تنبيه فرد الشرطة من المخالفة، ولا يُسأل أيّاً من عناصر الشرطة مدنياً إلا عن خطأهم الشخصي⁴.

¹ مختاري، إكرام: *الدليل في الجريمة الإلكترونية*. مجلة المنارة للدراسات القانونية والإدارية - المغرب. عدد خاص. 2015/9-33. صفحة 32.

² احمد، هلاي عبد الله: *حجية المخرجات الكمبيوترية في المواد الجنائية دراسة مقارنة*. لا يوجد طبعة: لا يوجد دار نشر. 2000. صفحة 121 وما بعد.

³ *القرار بقانون الصادر حديثاً رقم (23) لسنة 2017 بشأن الشرطة الفلسطينية، الوقائع الفلسطينية عدد ممتاز رقم 15، نص المادة 24 منه.*

⁴ *القرار بقانون الصادر حديثاً رقم (23) لسنة 2017 بشأن الشرطة الفلسطينية، الوقائع الفلسطينية عدد ممتاز رقم 15، نص المادة 25 منه.*

الفصل الثاني

وسائل التحقيق الجنائي في الجرائم الإلكترونية

الإجراءات التحقيق المتبعة في كافة الجرائم تأخذ بجميع عناصر التحقيق الجنائي المتكامل وتتم بذات المراحل الفنية والشكلية، وتعد هذه الإجراءات في أي جريمة تماماً كما هو الحال في الجرائم الأخرى أو كانت جريمة إلكترونية فالمحصل النهائي في التحقيق هو العثور على أدلة واضحة يمكن أن تستدل المحكمة فيها وتصدر العقوبة عليها¹.

يبدو جلياً بأن عمل الأجهزة الشرطية والمخولين بذلك في البحث والتحقيق عن الجريمة، ما هو إلا التوفيق بين مقتضيات كشف الحقيقة عند وقوع الجريمة وبين حرية المتهم التي تصونها النظم القانونية باعتباره بريئاً إلى أن تثبت إدانته، وضرورة التحرك لجمع الأدلة والإسراع بها دون تأخير².

ويعرف التحقيق: مجموعة من الإجراءات التي تتبعها السلطات لاستظهار الحقيقة لجريمة معينة والتثبت من كافة أركانها وكشف جوانبها تمهيداً للمسؤولية وإيقاع العقوبة على المتسبب. وتعرف كذلك علم متمم لقانون الجزاء وأصول المحاكمات الجزائية يرشد المحقق إلى السير في التحقيق من البداية إلى النهاية ويجمع الأدلة المثبتة لوقوعها، وكيفية ارتكابها والقبض على المتهم ومحاكمته³.

ومن المسلم به أن الإجراءات السابقة لنشوء المحكمة للنظر في التحقيقات تنحصر في ثلاث إجراءات هي الاستدلال والاثام والتحقيق الابتدائي، وإن مسألة البحث والتحقيق في جرائم الانترنت مسألة في غاية الأهمية، ولخصوصيتها فقد نصت بعض القوانين مثل مصر والإمارات على إعطاء الحق لوزير العدل بالاتفاق مع الوزير المختص أو السلطة المختصة بتحويل بعض

¹ البشري، محمد أمين : *التحقيق في جرائم الحاسب الآلي والانترنت*. مرجع سابق. الصفحة 349.

² عبد الحميد عبد المطلب، ممدوح: *البحث والتحقيق الجنائي في جرائم الكمبيوتر والانترنت*. لا يوجد طبعة. مصر: دار الكتب القانونية. 2006. صفحته 64-66.

³ الأكاديمية العربية للعلوم المالية والمصرفية. *مسرح الجريمة والتحقيق فيها*، عمان. 2016/8/31. الموقع الالكتروني:

<http://www.aabfs.org/ar> . صفحة 37.

الموظفين إلى صفه مأموري الضبط القضائي بالنسبة إلى الجرائم التي تقع في دائرة اختصاصهم¹.
وشبيه وهذا في فلسطين كما تحدثنا في الفصل الأول بإعطاء صفه مأمور الضبط القضائي إلى
مجل الأجهزة الأمنية الفلسطينية كل حسب اختصاصه

وفي مجال التحقيق في الجرائم الإلكترونية تكمن صعوبة اكتشاف هذه الجرائم ومقاضاة المتهم
في عدم وجود الخبرة الكافية والمعرفة الفنية لدى المحققين في استنتاج الأدلة التي تم استخدامها في
ارتكاب الجريمة، والذي يحتاجون إلى المزيد من الخبرة العالية والكفاءة، وعدم وجود الخبرة الكافية
والمعرفة الفنية في مجال الانترنت أدى ذلك إلى فشل كثير من أجهزة الشرطة في ضبط مرتكبي
هذا النوع من الجرائم وضبط أدلتها²، وهذا ما ارتأى إليه المشرع الفلسطيني حديثاً في قرار بقانون
الجرائم الإلكترونية " لوكيل النيابة العامة إن يأذن بالنفاذ المباشر لمأمور الضبط القضائي أو من
يستعينون بهم من أهل الخبرة إلى أية وسيلة من وسائل تكنولوجيا المعلومات وإجراء التفتيش فيها
بقصد الحصول على البيانات أو المعلومات"³.

المبحث الأول: إجراءات التحقيق الجنائي بالوسائل التقليدية

بوقوع جريمة ينشأ حق الدولة والمجتمع في معاقبة مرتكبيها، وهذا لا يتم إلا من خلال
إجراءات التحقيق في الجريمة كافة الوسائل والطرق المتاحة حتى التوصل إلى نتيجة يمكن إدانة
مرتكبها، وبموجب ذلك، فإن النيابة العامة هي المختص الوحيد بتحريك الدعوى العمومية، وذلك
بإجراء التحقيق فيها بنفسها أو من تفوضه من مأموري الضبط القضائي وفقاً لأحكام القانون، ومن
ثم بعد انتهاء التحقيق في الجريمة، تحال إلى المحكمة المختصة للنظر بها وإصدار حكم قطعي،
وذلك بصريح نص المادة (1\1) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001⁴ "
تختص النيابة العامة دون غيرها بإقامة الدعوى الجزائية ومباشرتها ولا تقام من غيرها إلا في

¹ عبد الحميد عبد المطلب، ممدوح: البحث والتحقيق الجنائي في جرائم الكمبيوتر والانترنت. مرجع سابق. صفحه 64-66.

² رستم، هشام محمد فريد: الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة. طبعة 4: مصر - أسبوط: مكتبة الآلات الحديثة. 1994، صفحة 13.

³ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 4/33.

⁴ قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 1.

الأحوال المبينة في القانون." كما تنص المادة (67) من قانون السلطة القضائية الفلسطيني على أنه¹: "تمارس النيابة العامة الاختصاصات المخولة لها قانوناً، ولها دون غيرها الحق في رفع الدعوى الجنائية (دعوى الحق العام) ومباشرتها ما لم ينص القانون على خلاف ذلك."

ونص قرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية منه المادة 1/3 على أن "تتشأ وحدة متخصصة في الجرائم الإلكترونية في الأجهزة الشرطية وقوى الأمن على أن تتمتع بصفة الضابطة القضائية وتتولى النيابة العامة الإشراف على مأموري الضبط القضائي كل في دائرة اختصاصه".²

والإجراءات التي تمر في النيابة العامة في الدعوى العمومية من خلال التحقيق في الجرائم، لذا في هذا البحث سوف يتطرق الباحث إلى دورين لعمل النيابة العامة في مجال البحث والتحقيق عن الجريمة المرتكبة:

أ- دور النيابة العامة خلال جمع الاستدلالات وهي مرحلة جمع الأدلة ومرحلة البحث والتحري عن الجريمة والاستقصاء عن الجرائم والتي تلزم في الدعوى بعد التحقيق فيها ومن قام بارتكابها³.

حيث يستلزم في هذه المرحلة عمل النيابة العامة مع سلطات الضبط القضائي وهذا من أجل الحصول على أكبر قدر من الأدلة التي تثبت وقوع الجريمة⁴، وهذا من خلال معاينة مسرح الجريمة من خلال معاون النيابة العامة، وبعد الانتهاء من مرحلة جمع الاستدلالات، تقوم النيابة بتقييم محضر جمع الاستدلالات ومدى إمكانية إقامة دعوى بناء على هذا المحضر أو لا⁵، حيث نصت عليها المادة (53) من قانون الإجراءات الجزائية الفلسطيني على أنه: "إذا رأت النيابة

¹ قانون السلطة القضائية الفلسطينية رقم (1) لسنة 2002م المادة 67.

² قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 3.

³ قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 70.

⁴ قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 2/19.

⁵ عمران، آية: النيابة العامة الفلسطينية وفقاً لقانون الإجراءات الجزائية رقم 3 لسنة 2001 وقانون السلطة القضائية رقم 1 لسنة 2002، الهيئة المستقلة لحقوق الإنسان (ديوان المظالم). سلسلة تقارير قانونية رقم 71. تشرين الأول. 2009، صفحة 47.

العامّة في مواد المخالفات والجنح أن الدّعى صالحة لإقامتها بناءً على محضر جمع الاستدلالات تكلف المتهم بالحضور مباشرة أمام المحكمة المختصة".¹

ب- دور النيابة العامّة خلال مرحلة التحقيق الابتدائي وهذا بعد الرجوع إلى قانون الإجراءات الجزائية نص المادة (1/55) حيث نصت صراحةً " تختص النيابة العامّة دون غيرها بالتحقيق في الجرائم والتصرف فيها".² والقانون شرع إلى النيابة تفويض أحد رجال الضبط القضائي للقيام بأعمال التحقيق فقط في الجنح " للنائب العام أو وكيل النيابة العامّة المختص تفويض أحد أعضاء الضبط القضائي المختص بالقيام بأي من أعمال التحقيق في دّعى محدّدة، وذلك عدا استجواب المتهم في مواد الجنائيات".³

حيث أنه يمكن أيضاً توقيف المتهم ويقوم عضو النيابة العامّة باستجواب المتهم ومناقشته بصورة تفصيلية عن الأفعال المنسوبة إليه والشبهات عن التهمة المسندة إليه، ومن ثم إحالة ما تم التوصل إليه من تحقيقات ومن مضبوطات عثر عليها أثناء التحري والبحث من قبل رجال الضابطة القضائية إلى النيابة العامّة⁴، " يتم ضبط جميع الأشياء التي يعثر عليها أثناء إجراء التفتيش والمتعلقة بالجريمة وتحرز وتحفظ وتثبت في محضر التفتيش وتحال إلى الجهات المختصة".⁵

¹ قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 53.

² قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 1/55.

³ قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 2/55. حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدّعى الجزائية رقم 188 لسنة 2012 " إذا كانت التهمة التي تم إسنادها للمتهم سواء في لائحة الاتهام المقدّمة من النيابة أو في استدعاء الشكوى المقدّمة من المشتكي لا تخرج كونها من الجنح فإنه على ضوء ما نصت عليه المادة 95 من قانون الإجراءات الجزائية يكون أمر استجواب المتهم متروكاً للنيابة العامّة ما ترتبته بخصوص إجراء الاستجواب من عدمه"

⁴ عمران، آية: النيابة العامّة الفلسطينية وفقاً لقانون الإجراءات الجزائية رقم 3 لسنة 2001 وقانون السلطة القضائية رقم 1 لسنة 2002، مرجع سابق، صفحة 49.

⁵ قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 2/50.

حيث أن الأدلة المادية واستخراجها وحفظها هي الجزء الأساسي من العمل، وهي تستهدف العثور على أكبر قدر الأدلة التي يحتمل أن تكون في غاية الأهمية، وتحديد ماهيتها، واختيار أساليب لاستخراجها، وتغليفها للحفاظ على سلامتها¹.

ومن ثم تتصرف النيابة العامة في المضبوطات في حرز مغلق وتكتب البيانات كافةً عليها وتحفظ أما في مخزن النيابة أو أي مكان تقرره ذلك، من أجل المحافظة على الدليل، وإذا ارتأت النيابة العامة بأن الشئ المضبوط قابلٌ للتلف يمكن لها أن تبيعه في مزاد علني إذا سمحت بذلك مقتضيات التحقيق، حيث أنه يستطيع عضو النيابة الاستعانة بالخبراء وذلك لإثبات الجريمة المرتكبة، وسماع شهادة الشهود لمساعدتهم على كشف الحقيقة، وتستطيع النيابة العامة إصدار مذكرات بحق المتهم للتحقيق معه وإذا ارتأت النيابة العامة بان التحقيق لم يكتفِ مع المتهم يمكن لها أن تقوم بتوقيف المتهم².

ويرى محمد السرحاني سهولة الكشف عن الجريمة الإلكترونية في ثلاث طرق³:

1. ضبط المجرم في حالة تلبس.
 2. اكتشاف الجريمة من قبل المجني عليه من خلال ملاحظة تلف أو تعديل البيانات .
 3. اعتراف الجاني بارتكاب الجريمة دون أن يكون هنالك علم من قبل المجني عليه.
- وبعد الانتهاء من التحقيق تعمل النيابة العامة أما على حفظ الدعوى أو إحالته ملف التحقيق إلى القضاء للنظر فيها⁴.

¹ الأكاديمية العربية للعلوم المالية والمصرفية. مسرح الجريمة والتحقيق فيها، مرجع سابق. صفحة 19-21.

² عمران، آية: النيابة العامة الفلسطينية وفقا لقانون الإجراءات الجزائية رقم 3 لسنة 2001 وقانون السلطة القضائية رقم 1 لسنة 2002"، مرجع سابق، صفحة 49-51.

³ السرحاني: محمد: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت. رسالة ماجستير منشورة. جامعة نايف العربية للعلوم الأمنية. السعودية. الرياض. 2004. صفحة 62 وما بعد.

⁴ عمران، آية: النيابة العامة الفلسطينية وفقا لقانون الإجراءات الجزائية رقم 3 لسنة 2001 وقانون السلطة القضائية رقم 1 لسنة 2002"، مرجع سابق، صفحة 51.

عند شروع سلطات الضبط القضائي عند التحقيق في القضية المعروضة أمامهم والدليل المستخرج منها أن يراعوا الأمور الجوهرية؛ يجب أن يصل في النهاية إلى مختبر التحليل الجنائي وقد حفظت سلامته وهويته، والحفاظ على الدليل من التلف أثناء النقل والتخزين، وعدم الاكتفاء باستخراج الدليل الأكثر وضوحاً وظهوراً قد يؤدي إلى ترك الأدلة الأكثر أهمية وإن الاستخراج العشوائي للأدلة قد يحمل المختبر عبئاً شديداً يعتقد بأنها مهمة وتؤدي في هذا الحالة إلى عرقلة البحث والتحري وعدم الاستفادة منها وضياع الوقت في أدلة غير منتجة¹.

المطلب الأول: التبليغ

ويقصد بالتبليغ عن الجريمة مجرد الإخبار عنها، ويمكن أن يكون التبليغ من مصدر معلوم أو جهة غير معلومة، ويعقب تلقي التبليغات جمع الاستدلالات مباشرة، والواقع أن التبليغ يصدر به إخبار الجهات المختصة بالتحقيق عن جريمة معينة وقعت أو على وشك الوقوع قيد التحضير أو وجود اتفاق أو عزم على ارتكابها².

من الجدير بالذكر حين يتلقى مأمور الضبط القضائي بلاغاً عن حادث أو جريمة ما، وجب عليه أن يمحّصه وأن يتأكد من صحته، فقد يكون من ورائه إزعاج السلطات وأحداث البلبلة، ويمكن لمقدم البلاغ أن يصور الحادث الذي وقع تصويراً على خلاف الحقيقة ومغايرة للتي حدثت قاصداً بذلك هدفاً أو مصلحة معينة فيجب على المحقق أن يفطن إلى ذلك³.

والقيمة القانونية للبلاغات عبر الشبكة الانترنت وإن كانت ما بين الجريمة وقعت أو قيد الوقوع فيترتب على مأموري الضبط القضائي بتتبع البلاغات وإجراءات التحريات اللازمة، فإن البلاغ ليس له القيمة القانونية الكافية يلزم به محكمة الموضوع عند النظر بمضمونه، بحيث العبرة فيما نتوصل

¹ الأكاديمية العربية للعلوم المالية والمصرفية. مسرح الجريمة والتحقيق فيها، مرجع سابق. صفحة 19-21.

² فضل، سليمان احمد: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. لا يوجد رقم طبعة. القاهرة: دار النهضة العربية. 2013. صفحة 276.

³ مراد، عبد الفتاح: التحقيق الجنائي التطبيقي. مرجع سابق، صفحة 200-201.

إليه محكمة الموضوع عن فهم للواقعة ولا عبء للبلاغ في محضر الاستدلالات ولا قيمة قانونية له.¹

وليس بالضرورة أن يكون التبليغ عن جريمة قد تمت وإنما يجوز أن يكون الإبلاغ عن أعمال تحضيره أو عن جريمة في سبيلها أو في طريقها للوقوع، وفي هذه الحالة فإن الإجراءات التي تتخذها سلطات الضبط الإداري هي وقائية منعا لوقوع الجريمة فهي بحد ذاتها أعمال إدارية لا تندرج في إطار مرحلة الاستدلالات.²

يتمثل دور مأمور الضبط القضائي باتخاذ الإجراءات اللازمة بجمع الاستدلالات التي يستلزمها التحقيق حيث يبدأ حيث انتهى عمل الضبط الإداري الذي يهدف لمنع وقوع الجريمة، فإذا وقعت الجريمة الإلكترونية بدأت إجراءات البحث والتحري عن الجريمة، حيث يتمثل سلطات الضبط القضائي في الشرطة المتخصصة في الضبط القضائي للجريمة الإلكترونية في تلاقي البلاغات، في حين أن الأصل يجب على مأمور الضبط الإداري والقضائي قبول البلاغات أو الشكاوى سواء كانت كتابية أو شفهية وتقييد في دفتر خاص.³

وتعد من الأهداف مرحلة الاستدلالات تحقيق صحة البلاغات والشكاوى التي ترد إلى سلطات الضبط القضائي عبر شبكة الانترنت، لذا يتعين على مأمور الضبط القضائي أن ينقب على كل ما من شأنه أن يعين سلطة التحقيق على كشف الحقيقة، لذا عليه أن يعالج أيضا البلاغات والشكاوى والقضايا التي تصله، فلا يتأثر بحرفية البلاغ ولا يتماشى مع أقوال المجني عليه التي تأتي بصورة مضطربة.⁴ وأشار القرار بقانون (16) لسنة 2017 الصادر حديثاً على أنه يعفي من أية عقوبة قد قرر لها هذا القرار بقانون كل من بادر من الجناة بتبليغ السلطات المختصة عن وقوع جريمة

¹ فضل، سليمان احمد: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. لا يوجد رقم طبعة. القاهرة: دار النهضة العربية. 2013. صفحة 277.

² إبراهيم، راشد بشير: التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على اماره ابو ظبي. عدد 131. لا يوجد طبعة. الإمارات: تصدر عن مركز الإمارات للدراسات والبحوث الإستراتيجية. لا يوجد سنة نشر. صفحة 50

³ موسى، مصطفى محمد: التحقيق الجنائي في الجرائم الالكترونية. مرجع سابق، صفحة 170.

⁴ فضل، سليمان احمد: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. لا يوجد رقم طبعة. القاهرة: دار النهضة العربية. 2013. صفحة 277.

الإلكترونية أو قيد التخطيط لها وأيضا تبليغ الجهات المختصة عن الأشخاص المشتركين فيها، وهذا قبل وقوع الضرر وقبل علم السلطات المختصة فيها، لكن إذا تم التبليغ بعد وقوع الجريمة للمحكمة أن توقف العقوبة المقرر بحق من بادر بالتبليغ وأدى ذلك الى ضبط باقي الجناة¹.

وفي حال قام أحد الجناة بالمبادرة في التبليغ عن وقوع جريمة الإلكترونيّة تعفي المحكمة المختصة الجناة قبل وقوع الضرر وإذا كان بعد العلم بالجريمة تعين إعفاء يكون في حال ضبط باقي الجناة في حال تعددهم أو الأدوات المستخدمة². وهذا ما أكد عليه المشرع الإماراتي أيضا³.

ويقوم المحقق بفحص البلاغ أو الشكوى ومن ثم يقوم بالإجراءات التالية:

أولاً: المعاينة

يرعى سرعة إجراء معاينة مكان الحادث والتحفّظ على الأدلة والآثار ووصف مكان الجريمة ومكان العثور على الأدلة، وتثبت هذه المعاينة في المحضر ويرفق رسماً تخطيطياً بمكان الحادث⁴.

والمعاينة بصورة مختصرة بالمفهوم التالي هي إثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة⁵.

" والمقصود بمعاينة مسرح الجريمة الإلكترونيّة هو مناظرة فحص ووصفه المكان أو الشيء، أو الشخص الذي له علاقة بالجريمة وإثبات حالته. وفي هذا الصدد تنص المادة (95) من قانون الإجراءات الجنائية المصري على أن ينتقل قاضي التحقيق إلى أي مكان كلما رأى ذلك ليثبت حالة

¹ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 57.

² نظام مكافحة جرائم المعلوماتية بقرار مجلس الوزراء رقم 79 وتاريخ 1428/3/7هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم م/17 وتاريخ 1428/3/8هـ، المادة 11

³ مرسوم قانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة تفتية المعلومات. المادة 45 ونصت على التالي " تقضي المحكمة بناء على طلب من النائب العام بتخفيف العقوبة أو بالإعفاء منها عن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقاً لأحكام هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبها أو إثباتها عليهم أو القبض على احدهم".

⁴ موسى، مصطفى محمد: التحقيق الجنائي في الجرائم الإلكترونيّة. مرجع سابق، صفحة 171.

⁵ أبو عامر، محمد زكي: الإجراءات الجزائية. ط2. الإسكندرية: منشأة المعارف للنشر والتوزيع. 1997. صفحة 233.

الأمكنة والأشياء والأشخاص ووجود الجريمة ماديا وكل ما يلزم إثبات حالته، والمقصود بهذا النص تيسير مهمة المحقق وتمكينه من انجاز التحقيق بالسرعة اللازمة قبل أن تندثر معالم الجريمة أو تطمس أدلتها فيتعذر الوصول إلى الحقيقة بعد ذلك"¹.

"ويقع دور على الشرطة في معاينة الجريمة وكل ما يفيد حتى تفي بأغراضها المنشودة، قررت بعض التشريعات الجزائية على أن من يقوم بتعديل أو بتغيير في مكان وقوع الجريمة قبل سلطة التحقيق بإجراءات المعاينة"². - بمعنى إذا قام أي شخص له صفحة بتعديل أو تغيير معالم وقوع الجريمة تقع عليه عقوبة- لكن القضاء الفرنسي استثنى العقوبة إذا حدث التغيير من قبل المتهم بعد المعاينة الأولى لسلطات التحقيق³.

والجدير بالذكر في تساؤل أهمية الجريمة الإلكترونية، أن الجريمة التقليدية غالبا يتوفر في مسرح الجريمة آثار مادية تترتب عليها الأدلة، وهذا يعطي من سلطات الضبط القضائي سهولة الكشف والتحري عن وقوع الجريمة وذلك عن طريق المعاينة والتحفظ على الآثار المادية، لكن يتضاءل دور الأدلة في مسرح الجريمة في الجريمة الإلكترونية وذلك لسببين: أولا: نادرا ما يتوفر أدلة و آثار مادية للجرائم الإلكترونية بعكس الجرائم التقليدية تحتوي غالبا على آثار.

ثانيا: حيث يمكن لمرتكب الجريمة أو الأشخاص العيب بالدليل الإلكتروني وإخفائه وهذا من خلال الفترة الزمنية لوقوع الجريمة وحتى اكتشافها والتحقيق فيها⁴، ومن الملاحظ أنه في كثير من الأحيان

¹ موسى، مصطفى محمد: التحقيق الجنائي في الجرائم الإلكترونية. مرجع سابق، صفحة 171.

² عفيفي، كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "دراسة مقارنة". لا يوجد طبعة. الإسكندرية: منشأة وتوزيع المعارف بالإسكندرية. لا يوجد رقم سنة إصدار. صفحة 476.

³ قانون العقوبات الفرنسي نص المادة 55 منه نصت على " عاقبت على هذه الجريمة بالغرامة التي لا تتجاوز 2500 فرنك وان تصل إلى الحبس إذا كان الغرض من التعديل إعاقه العدالة". نقلا عن عفيفي، كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "دراسة مقارنة". مرجع سابق. صفحة 334

⁴ حجازي، عبد الفتاح بيومي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت. ط1. الإسكندرية: دار الفكر الجامعي. 2006. صفحة 105.

يعمد الجاني أو شركاؤه إلى تضليل أجهزة البحث الجنائي من خلال تغيير محتويات مسرح الجريمة، حيث يمكن لهذا الحالة أن تفلح حيلة الجناة¹.

ثالثاً: الأعداد الكبيرة من الأشخاص الذين يرتادون مسارح الجريمة ما بين ارتكابها واكتشافها².

ومن المعلوم بأنه لا يوجد تشابه أو توحيد بين مسارح الجريمة المرتكبة، فهذا يختلف حسب نوع الجريمة المرتكبة وحسب ظروف الموقع المرتكب به، وكذلك يختلف الأمر حسب الأداة المرتكب فيها وعما إذا كان المكان مفتوحاً أو كان مغلق وكذلك يختلف الأمر حين ارتكابه للجريمة بالأسلوب المستخدم في ارتكابه للجريمة. وبات من الضروري تجنيد عدد كبير من المتخصصين والأفراد وتدريبهم وفقاً لعقد محاضرات لمسارح الجريمة المتخلفة أو محاكاة واقعة بميادين التدريب، لذلك عند عقد محاكاة حاسوبية لمواقع افتراضية للجرائم الإلكترونية سيسهم في التعامل السليم والصحيح من قبل الباحث الجنائي لمسرح الجريمة وسيؤدي إلى اكتسابهم المهارة والقدرات وتلافي الخطأ في مسرح الجريمة واتخاذ الإجراءات اللازمة للتحقيق³.

وقد تتم المعاينة في مكان عام أو في مكان خاص، حيث لا تتطلب الأولى إلى وجود إذن أو نذب طالما لمأمور الضبط أحقيه دخولها أو التواجد فيها، أما إذا كان خاصاً فلا بد لصحتها ربا حائز المكان أو وجود إذن مسبق من سلطات التحقيق حسب الأصول والقانون⁴.

5- ومن المهم إتباع القواعد والإرشادات الفنية عند إجراءات المعاينة وهي كالتالي⁵:

¹ عبد الحميد عبد المطلب، ممدوح: البحث والتحقيق الجنائي في جرائم الكمبيوتر والانترنت. مرجع سابق. صفحته 181.

² عفيفي، كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "دراسة مقارنة". مرجع سابق. صفحته 476.

³ عبد الحميد عبد المطلب، ممدوح: البحث والتحقيق الجنائي في جرائم الكمبيوتر والانترنت. مرجع سابق. صفحته 177-178.

⁴ عفيفي، كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "دراسة مقارنة". مرجع سابق. صفحته 476.

⁵ عفيفي، كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "دراسة مقارنة". مرجع سابق. صفحته 337.

أولاً: القيام بتصوير كل ما يتعلق بمحتويات الحاسب الآلي وما قد يتصل به من أجهزة طرفية ومحتوياته بصفه عامل مع بذل العناية، وتصوير الأجزاء الخلفية وملحقاته الأخرى على أن يراعي ضبط توقيت الصورة ومكانها.

ثانياً: ملاحظة طريقة إعداد النظام الخاص بالحاسب الآلي بعناية فائقة.

ثالثاً: يجب أن يُلاحظ توصيلات ووضع كابلات الحاسب الآلي والتي تكون متصلة بمكونات النظام؛ وذلك حتى يسهل عملية مقارنتها على المحكمة حين النظر في الدعوى.

رابعاً: ضرورة عدم التسرع في نقل أية معلومة من مكان وقوع الجريمة حتى لا يحدث أي تلف للبيانات المخزنة في نظام الحاسوب.

خامساً: حفظ ما تحتويه سلة المهملات من الأوراق الممزقة أو الملقاة أرضاً والشرائط والأقراص المدمجة وأي دليل يحتويه المكان بحيث يمكن أن تكون هذه الأدلة لها صلة بالجريمة المرتكبة.

سادساً: حفظ المستندات الخاصة بالإدخال والإخراج ذات العلاقة بالجريمة من أجل رفع ومضاهاة البصمات التي قد تكون موجودة عليها.

سابعاً: يجب أن تقتصر عملية المعاينة والبحث في الأدلة على مأموري الضبط القضائي من له الكفاءة العالية والخبرة الفنية ممن تلقوا التدريب الكافي لمكافحة و/أو ضبط نوعية هذه الجرائم.

المطلب الثاني: المراقبة أو التردد الإلكتروني

المقصود من المراقبة هو أن يتم وضع شخص أو مكان ما تحت الملاحظة لتسجيل كل ما يحدث من التصرف في جو من السرية، أو تقديم بلاغ عن شخص يشتبه بأنه هو الجاني، حيث يسهل على سلطات الضبط القضائي القبض عليه متلبساً بالجريمة وبالأخص الجرائم الإلكترونية¹.

¹ أبو الروس، احمد: منهج البحث الجنائي. مرجع سابق، صفحة 391.

ويرى الاستاذ سمير الامين ان الترصد الالكتروني هة تسجيل المحادثات باجهزة التسجيل ويمكن الاكتفاء باحدى الوسائل التالية لعملية المراقبة فقد تتم بمجرد التنصت وقد يكتفي بالتسجيل الذي يسمع بعد ذلك، وثم يُفرغ مضمونة في المحضر المعد لذلك¹، والاطار العام لمراقبة المراسلات السلكية واللاسلكية لارتباك المشتبه فيهم في اطار البحث والتحري عن الجريمة الالكترونية وجمع الادلة والمعلومات حول هؤلاء الاشخاص ومشاركتهم في ارتكاب الجريمة².

حيث يرى الباحث بأن مراقبة الحاسوب الالى (المشتبه فيه) أمرٌ مهم لغاية القبض عليه متلبسا بالجريمة الالكترونية، ويمكن ذلك أن يحدث من خلال مراقبة جهاز الحاسوب (I.P) من خلال الخبراء؛ حيث يحمل كل جهاز رقم خاص وهذا لا يأتي إلا من جانب الخبرة العالية في هذا المجال ومتابعة الأعمال التي يقومون بها.

وتظهر أهمية جواز الأجهزة الأمنية في رصد حركة مرتكبي الجرائم الإلكترونية واكتشاف الجرائم عن طريق رصد المشبوهين داخل المؤسسات وما حولها والرصد الميداني لحركة المعاملات؛ فالجريمة الإلكترونية لا يمكن لها أن تتم بمعزل عن تخطيط داخل المؤسسة ذاتها وخارجها حيث أن يكون من مرتكبو الجريمة على علاقة مع أفراد المؤسسات³، بمعنى أنه يمكن للأجهزة الأمنية أن تعمل على مراقبة العاملين في المؤسسة، بحيث يمكن أن يقوموا بتقديم يد العون الى الجناة مثلا: توفير بيئة خصبة لارتكاب الجريمة كالتلاعب في الكمبيوترات، او اعطاء الجنائي كافة المعلومات عن البرامج حتى يسهل عليه اختراق.

فالمراقبة بجميع أنواعها العادية أو التقنية هي الأسلوب الأمثل للوصول إلى الصورة الحية والمرئية التي تمثل الواقع العملي ومن خلالها يمكن لرجل التحري الكشف عن حقيقة النشاط الذي قام به الجاني، والمراقبة هي من أسرع الوسائل لكشف الجرائم وهي مفتاح نجاح رجال الضبط

¹ لامين، سمير: مراقبة التليفون والتسجيلات الصوتية والمرئية، ط3، دار الكتاب الذهبي. مصر. 2000. صفحة 8

² خلفي، عبد الرحمن: الاجراءات الجزائية في التشريع الجزائري المقرن، ط2، دار بلقيس للنشر والتوزيع، الجزائر، 2016، صفحة 102.

³ البشري، محمد أمين : التحقيق في جرائم الحاسب الآلي والانترنت. مرجع سابق. الصفحة 250.

القضائي أو الإداري إذا توافر فيه صفات خاصة بالمراقبة الفنية والإنسانية والفكرية¹، بمعنى إذا تمت مراقبة الجاني بأسس علمية صحيحة يمكن إلقاء القبض على الجاني من قبل سلطات الضبط القضائي متلبسا حين الشروع في قيامه للجريمة الالكترونية.

ذهب المشرع الإماراتي في القانون الخاص بالجرائم الإلكترونية بإعطاء السلطة الجوازية للمحكمة بأن تأمر الجاني تحت الإشراف أو الرقابة أو حرمانه من استخدام أي شبكة معلوماتية أو أي وسيلة تقنية أو وضعه في مركز علاجي التي تراها المحكمة مناسبة له وفقا لظروفه²، هذا بعد التحقيق لجئ له المشرع الاماراتي بمنع الجاني من استخدام الشبكة العنكبوتية لردعه وأيضا لعدم قيام الجاني في حال إلقاء القبض عليه متلبسا في جريمة اخفاء معالم الجريمة الالكترونية.

والأسباب التي يراها ذوو الاختصاص صالحة لوضع شخص معين في دائرة المراقبة³:

1. جمع معلومات عن الأنشطة لأحد الأشخاص المشتبه فيهم.
2. جمع الأدلة التي من شأنها تحدد مصير المشتبه به، ما بالنفي أو بالتأكيد على استكمال البحث والتحري.
3. جمع أدلة جديدة من شأنها ان تحدد استصدار إذن بالبحث أو بالتفتيش.
4. القبض على شخص عن طريق الأماكن التي يتردد عليها.
5. استحداث أو تطوير معلومات قديمة.
6. منع ارتكاب جريمة، أو إلقاء القبض على المشتبه فيه متلبسا.

¹ موسى، مصطفى محمد: المراقبة الالكترونية عبر شبكة الانترنت. ط1. القاهرة: دار الكتب والوثائق المصرية. 2003. صفحة 3.

² مرسوم قانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة تقنية المعلومات. المادة 43

³ أبو الروس، احمد: منهج البحث الجنائي. مرجع سابق. صفحة 391.

ومن خلال النظر في قانون الإجراءات الجزائية الفلسطيني وفقاً لنص المادة (51)، تطرق إلى موضوع المراقبة التي من خلالها تساعد للكشف عن الجريمة من خلال التعاون مع الجهات المختصة بتزويد الشبكة العنكبوتية بناءً على إذن من قاضي الصلح متى كان هذا في فائدة لإظهار الحقيقة¹. وجاء حكم محكمة النقض المنعقدة في رام الله كتالي لقانون الإجراءات الجزائية لنص المادة (2/51) "ان مجال تطبيق نص المادة (2/51) على مراقبة الخطوط الهاتفية وإجراء تسجيلات لأحاديث يكون قبل وقوع الجريمة وليس بعدها هذا أولاً، ثانياً لا مجال لتطبيق نص المادة (2/51) إلا في الجنايات والجناح المعاقب عليها بالحبس لمدة لا تقل على سنة"². نص المادة (1/37) من قرار بقانون رقم (16) لسنة 2017 على التالي " يمكن للمحكمة 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 والافعال الموجبه له ومدته"³.

وفي الدول الغربية مثل اليابان المشرع لم يُجز استخدام التصنت وإنما أعطت المحاكم شرعية التصنت وهولندا أجاز القانون لقاضي التحقيق شرعية التصنت على شبكة الحاسب الآلي للبحث عن الأدلة وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات⁴.

تكون إجراءات التحري والتحقيق سرية، فنظراً لخطورة هذه العمليات على حرمة الحياة الخاصة للأفراد، فالسرية تعني القيام قر الاماكن ممن هو قائم بالتحري، أو مكلف باجراءات من إجراءاته أو ساهم فيه بالمحافظة على السر المهني وبالتالي صارت السرية ليس كما كان عليه هو قمع للمتهم

¹ قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 3/2/51.

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

² حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم 118 لسنة 2011.

³ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 1/37

⁴ العبيدي: أسامة بن غانم: *التفتيش عن الدليل في الجرائم المعلوماتية*. المجلة العربية الأمنية والتدريب. عدد 58. مجلد 29، 2013. الصفحة 95.

وانما صارت وسيلة لضمان الحرية الشخصية، من خلال إذا وقعت جريمة الالكترونية يبقى في ذهن المجني عليه بأن هناك من سوف يعمل على البحث عن هذه الجريمة ومن ثم ايقاع العقوبة عليه.¹

المطلب الثالث: الشهادة

كان ولا يزال سماع الشهود مصدراً أساسياً وغالباً من مصادر الأدلة الجنائية حيث أنه في مجمل القضايا تندر أن تكون هناك قضية دون شهود، فالشاهد حين يدلي بمعلوماته لا يكون له ارتباط بالدعوى بأي ارتباط إذ هو ليس من أطرافها الأصليين أو المنضمين وإنما يقدم معونة ضرورية لتحقيق الحقيقة، والشاهد ملتزم بتقديم الشهادة بصفته في المجتمع كفرد في جماعة، والالتزام المفروض عليه يعرضه للمسألة القانونية وفرض غرامة مالية وأيضا إحضارة للمحكمة إذا نكل عن الشهادة أو زور مضمونها، ولا تقتصر الشهادة على التحقيق الابتدائي بل لازمة أيضا في التحقيق النهائي، ولا تكون فقط في التحقيق القضائي، فرجال البحث والتحري يمكنهم أن يقوموا بتحقيق أولي يستمعون فيه إلى الأقوال.²

في معظم القضايا خاصة التي تحيطها ظروف غامضة، فإن الشهود يتوفرون سواء أشار إليهم المشتكي في بلاغة أو قام بتوثيقهم المتحري من خلال إفادة المشتكي أو أتوا طائعين مختارين للإدلاء بشهادتهم، لذا يجب أن يتوافر في الشهود شروط مهمة؛ أن يكون ذا أهلية، وعاقلا، ويتمتع بالحاسة التي تمكنه من إدراك المعلومة التي سوف يشهد عليها كافة تفاصيلها.³

¹ بن عبد العزيز، زينب: الت رصد الالكتروني وحماية الحرية الشخصية في قانون الفساد، رسالة ماجستير منشورة. جامعة قاصدي مرباح. الجزائر. 2017/5/21. صفحة 36

² عصفور: مي خميس: المواعيد والمدد في قانون الإجراءات الجزائية الفلسطينية (دراسة مقارنة). رسالة ماجستير منشورة. جامعة الأزهر. غزة. 2010. صفحة 65-66.

³ قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. الفصل الرابع. المادة 77 وما بعد
كما يجوز له مراقبة المحادثات السلكية واللاسلكية، وإجراء تسجيلات لأحاديث في مكان خاص بناءً على إذن من قاضي الصلح متى كان لذلك فائدة في إظهار الحقيقة في جناية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سنة. الفقرة 3 من نص المادة 51 يجب أن يكون أمر الضبط أو إذن المراقبة أو التسجيل مسبباً، ولمدة لا تتجاوز خمسة عشر يوماً قابلة للتجديد لمرة واحدة.

وهناك عوامل تؤثر في الشهادة قد يرغب الشاهد قول الحقيقة لكنه لا يستطيع ذلك لسبب أو لآخر قد يكون ضعيف الإدراك، أو صغر وكبر سنه، أو لضعف بصره..الخ، أو قلة الخبرة التي يتمتع بها الشاهد، ولوجود الاختلافات بين الناس في درجة استيعابهم وإدراك تفاصيل الحادث التي تجري أمامهم، حتى الأحداث اليومية التي تحدث معهم ناهيك عن الأحداث المثيرة¹.

والشهادة في الجريمة الالكترونية هو ذلك الشخص الفني صاحب الخبرة العالية في علوم الحاسب الالي وصاحب التخصص الذي لديه العلم والدراية عن ماذا سوف يدلي بوقائع شهادته، والذي يكون لديه معلومات جوهرية هامة او لازمه للدخول الى نظام المعالجة الالية للبيانات اذا كانت مصلحة التحقيق تقتضي ذلك للتقريب عن ادلة الجريمة الالكترونية ويمكن ان يكون الشاهد احدى الطوائف التالية²:

- 1- مشغلو الحاسب الالي: وهم الخبراء الذي لديهم الدراية العالية بتشغيل الحاسوب الالي ومعرفة التطبيقات وقواعد البيانات والاجهزة والملحقات الوصلة بالحاسوب.
- 2- المحللون: هو المحلل الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين وتحليلها الى وحدات منفصلة واستنتاج العلاقات الوظيفية منها، كما يعمل على تتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات.
- 3- المبرمجون: وهم الاشخاص المختصين في كتابة اوامر البرامج كصناعة مثلا برنامج الفيس بوك او فايرس لنشره على الشبكة العنكبوتية.
- 4- مهندسو الصيانة والاتصالات: هم الاشخاص المختصين في صيانة الشبكة العنكبوتية وتقنيات الحاسوب بكافة مكوناتها .
- 5- مديرو النظام: وهم الذي يوكل لهم اعمال الادارة في النظم المعلوماتية.

¹ سالم، عبد الله حسن: أقوال الشهود في مرحلة التحري والتحقيق، مجلة الفكر الشرطي - مركز بحوث الشرطة القيادة العامة لشرطة الشارقة. عدد 3. مجلد 1. 1992 / 142-163. صفحة 145 وما بعد.

² فرغلي، عبد الناصر محمد محمود، و المسماري، محمد عبيد سيف سعيد: الاثبات الجنائي بالادلة الرقمية من الناحية القانونية والفنية دراسة تطبيقية مقارنة، (رسالة ماجستير منشورة) جامعة نايف العربية للعلوم الامنية. الرياض. السعودية. 2007 . صفحة 21.

وعلى صاحب الصلاحية من الشرطة أو النيابة العامة أو القاضي عند أخذ إفادة الشهود أن ينصب عينية على أمرين هامين¹:

1- أن تغطي الشهادة جميع الوقائع أو تغطي الجزء المهم في محور القضية الذي يدلي الشاهد بأقواله عنه.

2- أن يتأكد بأن الشاهد لا يكذب ويقول الحقيقة، وهذه تأتي من خلال شهادته على محضر الإفادة أو التحقيق بأن لا يأتي بأقوال غير منطقية أو بعيدة كل البعد عن مسرح الجريمة.

المطلب الرابع: التفتيش والضبط

المقصود بالتفتيش في مدلوله القانونية لا يختلف سواء كان بالجرائم الإلكترونية أو في فقه الإجراءات الجزائية، فيقصد به بحث بوليسي أو قضائي لغاية ضبط ما يفيد في كشف الحقيقة، فالهدف من التفتيش في الجرائم الإلكترونية هو ما يحتويه الحاسب الآلي من أشياء مادية ومعنوية تساعد في كشف الحقيقة ويمكن للقضاء نسبتها للمتهم، ويمكن أن يكون المحل الحاسب الآلي أو أنظمتها أو شبكة الانترنت².

وفي حالة التفتيش، إذا كانت المكونات المادية في المنزل فإنها تخضع للتفتيش وفقا للقواعد العامة وفي حالة كانت هذه المكونات معزولة وموجودة في غير المكان المراد تفتيشه يرى الفقه أن إذن التفتيش الأصلي يسري على هذه الأماكن إذا توافر عاملان أساسيان وهما :

أولاً: إذا توافر للأجهزة الأمنية بان هنالك معلومات يخشى على ضياعها.

¹ سالم، عبد الله حسن: أقوال الشهود في مرحلة التحري والتحقيق. مرجع سابق. صفحة 147.

² مصطفى: محمود محمد: الإثبات في المواد الجنائية في القانون المقارن. ط1. القاهرة: مطبعة جامعة القاهرة. 1987.

ثانياً: إذا كان الموقع المراد تفتيش مكوناته المادية يساعد في كشف الحقيقة وهي تتكون من الأجهزة المادية من البرمجيات ومهارات الحاسوب¹، فالمكونات المادية للحاسوب تتكون من التالي²:

1- وحدة المعالجة المركزية (SPU) وتقوم هذه الوحدة على تنظيم واستلام البيانات ومعالجتها من خلال اجراء العمليات الحسابية والمنطقية.

2- وحدة الادخال (Input devices) التي تستقبل المعلومات وتحولها من اوامر الى شيفره، مثلاً: لوحة المفاتيح، الفارة، وشاشة الحاسوب.

3- وحدة اخراج المعلومات (output devices) تقوم بتحويل البيانات الالكترونية المنتجة بواسطة الحاسوب وعرضها بحيث يستطيع الفرد استخدامها بما يريد مثلاً كشاشات العرض.

لذا يجب أن يكون أمر التفتيش مسبباً ومحددًا، وفي حال كان مبررات إجراءاته مستمرة يجب أن يجدد، وإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة على مأمور الضبط القضائي ان يقوم بضبطها بعد ما يتم تنظيم محضر فيها وعرضها على النيابة العامة لاتخاذ الإجراءات القانونية حسب الصول والقانون³.

يعد التفتيش من أهم المراحل للعثور على الدليل، وهي من الأعمال التي يقوم بها رجال البحث والتحري الجنائي؛ لكونه هو الحاسم في نجاح جهود البحث في العثور على دليل يفيد في إثبات وقوع جريمة أو عدم وجود أدلة، وهنا يمكن لرجال البحث العثور على الدليل الجنائي إلا أنه بسبب عدم إتباع سلطات البحث بالقواعد والإجراءات الصحيحة عند القيام بالتفتيش سوف يفلت الجاني من قبضة العدالة؛ وهذا يرجع لعدم تقيد سلطات البحث الجنائي بالإجراءات الصحيحة للتفتيش الأمر الذي أدى إلى بطلان هذه الإجراءات وعدم إثبات التهمة حيال مرتكبها بالرغم من

¹ احمد، هلاي عبد الله: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي. ط1. القاهرة: دار النهضة العربية. 1997. صفحة 84

² الحسان، عطاء الله احمد: نظم المعلومات المحاسبية. الطبعة الاولى دار اليازوري للنشر. عمان. الاردن، 2013. صفحة 12-13.

³ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 33.

العثور على الدليل الجنائي، والصعوبة في ذلك يرجع بأن التفتيش يعد من الإجراءات الماسة بحرية الإنسان وحرمة مسكنه في ظل المساس بمستودع السر الخاص بالشخص الذي يحفظ أسرارهِ بداخلها¹.

ولأن التفتيش هي إجراءات تحقيقه فلا يجوز مباشرة التحقيق دون مذكرة من قبل النيابة العامة أو في حضورها، وذلك ضمن شرائط معينة بناءً على وجود اتهام موجه إلى شخص يقيم في المنازل أو وجود قرائن قوية على أشياء تتعلق بالجريمة، ولقد حرص المشرع الفلسطيني في قانون الإجراءات الجزائية بوضع نص مادة خاصة بالتفتيش، حيث إن المساكن لها حرمتها الخاصة فلا يجوز دخولها بغير إذن أهلها إلا وفقاً لأحكام القانون وهي محددة². فطبيعة التفتيش كونها عملاً من أعمال التحقيق لا يتم التفتيش إلا بعد وقوع الجريمة فعلاً، فلا يمكن أن يتم التفتيش عن جريمة محتملة الوقوع وإلا سيترتب على آثارها البطلان³.

يتطلب من سلطات البحث والتحري ببعض الإجراءات تتمثل في سرعة الانتقال إلى الموقع المراد تفتيشه لمنع الجاني من إخفاء الأدلة، ويترتب على سلطات البحث الدقة وعدم التسرع في التفتيش، ويجب أن يكون قوي الملاحظة وسريع البديهة⁴. وعلى رجل التحريات أن يستشعر بأن كتابة المحضر ليس أليه، بل عليه أن يستعمل المواهب والقدرات الثقافية، فالمحضر هي صورة حية لشخصية معدة، وكذلك تحديث واقعي لمكان إلقاء القبض على الشخص الجاني⁵.

¹ عبد الحميد عبد المطلب، ممدوح: البحث والتحقيق الجنائي في جرائم الكمبيوتر والانترنت. مرجع سابق. صفحة 183-184

² قانون الإجراءات الجزائية رقم 3 لسنة 2001 م. المادة 39:

1- دخول المنازل تفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها، بناءً على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو لوجود قرائن قوية على أنه يحوز أشياء تتعلق بالجريمة.

2- يجب أن تكون مذكرة التفتيش مسببة.

3- تحرر المذكرة باسم واحد أو أكثر من مأموري الضبط القضائي

³ المعهد القضائي الفلسطيني. التفتيش في قانون الإجراءات الجزائية الفلسطيني. بحث منشور على موقع الدكتور احمد براك. رام الله. 2012. صفحة 6.

⁴ عبد الحميد عبد المطلب، ممدوح: البحث والتحقيق الجنائي في جرائم الكمبيوتر والانترنت. مرجع سابق. صفحة 184.

⁵ سلامة، سعد احمد محمود: التبليغ عن الجرائم رسالة مقارنة. أكاديمية الشرطة . القاهرة. مصر. 2003. صفحة 303.

وهناك قواعد عامة للتفتيش؛ لا يجوز التعسف في استعمال حق التفتيش كان يقوم رجل الشرطة بعبثة محتويات المنزل، أو الملابس ولا يجوز تجاوز الغرض من التفتيش الذي من أجله صدر الإذن بالتفتيش وإلا يقع باطلا، يجب أن يكون التفتيش مفاجئاً وبصورة غير متوقعة¹.

والسؤال الذي يدور حالياً بأنه، هل يمكن تفتيش الحاسب الآلي، من المعروف ان الحاسب الآلي هو مكون من Hard Ware ومن Soft Ware²

وفي حالة التفتيش بأنه إذا كانت الغاية من وراء التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الأدلة، فان هذا المفهوم يشمل البيانات الإلكترونية؛ بمعنى آخر وفقاً لهذا الرأي بأنه إذا تم التفتيش وكانت الغاية من وراءه ضبط الأدلة المادية والمقصود فيها الأدوات التي تمت فيها الجريمة مثل جهاز الحاسوب وموزع الانترنت وكل ما يتعلق بهذه الأدوات، حيث يستطيع تمحيص البيانات الإلكترونية مثل فحص المواقع الإلكترونية التي أدى من خلالها الى ارتكاب الجريمة³، أو وجود هذه الأدلة في الأقراص الصلبة والخارجية والطابعات والكاميرات والبرمجيات وكلمات السر الذي قد تكون مكتوبة على أوراق بالحاسوب، ويمكن أن تكون هذه الأدلة موجودة في سلة المهملات عن أوراق مطبوعة ذات علاقة بالحاسوب، ومن خلال البرمجيات للنسخ الاحتياطية، والبيانات المحذوفة، وبرمجيات تتبع الاتصال الشبكي⁴.

وهذا ما تم الأخذ فيه في قانون الإجراءات اليوناني بنص المادة 251 "تخول سلطات التحقيق إمكانية القيام بأي شئ ضروري لجمع وحماية الدليل الجنائي"، وكذلك القانون الكندي "حسب نص المادة 487 تمنح سلطة إصدار إذن الضبط -لأي شئ- طالما توافرت أسس معقولة للاعتقاد بأن

¹ موقع الشرطة الفلسطيني، التفتيش، تاريخ الزيارة 2017/6/15، الموقع الالكتروني: <http://www.police.ps/ar/articles-action-show-id-105.htm>

² عبد الهادي، محمد فتحي: مقدمة في علم المعلومات. ط1. القاهرة: مكتبة غريب. 1984. صفحة 217

³ حجازي، عبد الفتاح بيومي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت. مرجع سابق . صفحة 378.

⁴ جرادة: عبد القادر صابر: دستور الاستدلال والتحقيق الجنائي في التشريع الفلسطيني. ط1. فلسطين. غزة: مكتبة افاق. 2012. صفحة 363.

الجريمة التي وقعت أو يشتبه في وقوعها أو أن هناك نية في ارتكاب الجريمة بواسطته أو سوف ينتج على وقوع الجريمة"¹

أما "دستور الولايات المتحدة الأمريكية لا يمكن إصدار إذن ضبط أو تفتيش إلا على أساس معقول ومدعوم بقسم وإفادة دقيقة للمكان والأشخاص المراد ضبطها وتفتيشها"². ووفقا لما قرره المحكمة العليا الأمريكية بأن التفتيش لا ينتهك دستور أمريكا إذا تحقق واحد من هذين الشرطين.

- حالة إذا كان سلوك السلطات لا ينتهك معيار الخصوصية لدى الأفراد، حيث انه لا يتطلب إذنًا ولا يشكل ذلك تفتيشا رسميا وفقا للدستور الأمريكي.

- حالة التفتيش دون إذن حتى لو انتهك معيار الخصوصية لدى الأفراد طالما اندرج تحت استثناء يعد ذلك دستوريا³.

وعند النظر في هذه الحال تفسر -أية حالة- بأنها تمتد إلى أن تشمل البيانات المخزنة أو تلك التي تمت معالجتها إلكترونيا أي تم صياغتها من جديد وإعطائها أوامر لغاية تنفيذ المهمة الموكلة له، لذلك ضبط فيما يتعلق بالجريمة من بيانات لا يوجد فيها مشكلة حسب القانون اليوناني⁴.

¹ إبراهيم، راشد بشير: التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة أبو ظبي. عدد 131. لا يوجد طبعة. الإمارات: تصدر عن مركز الإمارات للدراسات والبحوث الإستراتيجية. لا يوجد سنة نشر. صفحة 56.

² خليفة، خالد احمد إبراهيم: قبول وإجازة الأدلة الإلكترونية لجرائم الحاسوب في الدعاوى الجنائية. المجلة العلمية جامعة الزعيم الأزهري - السودان. عدد 6. مجلد 1. 2009. الصفحات 60/73. صفحة 64.

³ عطية، طارق إبراهيم الدسوقي: إجراءات البحث الجنائي في ضبط الجريمة الإلكترونية في ضوء اتفاقية بودابست الموقعة في 23 نوفمبر سنة 2001 والمتعلقة بالإجرام الكوني. مجلة الأمن والقانون أكاديمية شرطة دبي. عدد 2. مجلد 2015. 339-23. 440. الصفحة 396.

⁴ حجازي، عبد الفتاح بيومي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت. مرجع سابق. صفحة 378.

قامت وزارة العدل الاحتلال الإسرائيلية بإعداد مشروع قانون الحاسب وذلك لمواجهة قصور قواعد التفتيش والضبط في مواجهة الجرائم الإلكترونية بإضافة عبارة "أو مادة معالجة الحاسب الالى" أوضح المشرع نفسه بأنه قاصد بها برامج الحاسب أو بيانات.¹

وكذلك الحال ظهر لنا رأي آخر مخالف، من خلاله إذا كانت الغاية من وراء التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، حينها لا فائدة في أهمية في تفتيش بيانات الحاسب الالى غير المحسوسة أو المحسوسة.²

لقد عالج تشريع جمهورية موريشيوس في نص المادة (14) من كتالي: "إذا كانت سلطة التحقيق تملك أسباباً معقولة للاعتقاد بوجود بيانات مخزنة يمكن أن تكون ذات صلة بأغراض التحقيق فانه يحق لها أن تطلب من القاضي إصدار مذكرة لدخول أي موقع والوصول والتفتيش وضبط هذه البيانات. وتتضمن صلاحية سلطة التحقيق كلاً من: ضبط نظام الحاسوب، أو أية معلومات، أو وسيط تقنيات اتصالية؛ وإنشاء نسخة عن تلك البيانات أو المعلومات والاحتفاظ بها والمحافظة على مصداقية تلك البيانات أو المعلومات المخزنة وحجب البيانات والمعلومات أو إزالتها من نظام الحاسوب، أو أي معلومات أو أي وسيط لتكنولوجيا الاتصالات."³

وبرز اتجاه آخر يرى فيه أن البيانات الإلكترونية ما هي إلا ذبذبات الكترونية أو موجات كهرومغناطيسية تقبل التخزين أو الحفظ والتسجيل على وسائط مادية، وبالتالي فان يمكن إعادة إنتاجها أو نقلها- طباعتها على أوراق أو تخزينها في أقراص قابلة لحفظ الأدلة-، فان وجودها المادي لا يمكن تجاهله أو إنكاره.⁴

¹ رستم، هشام محمد فريد: الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة. مرجع سابق، صفحة 67.

² حجازي، عبد الفتاح بيومي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت. مرجع سابق . صفحة 389.

³ عمري، محمد محمود: الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية دراسة مقارنة. مجلة العلوم القانونية والسياسة. عدد 2. مجلد 2016/12-291-334، صفحة 304.

⁴ العبيدي: أسامة بن غانم: التفتيش عن الدليل في الجرائم المعلوماتية. المجلة العربية الأمنية والتدريب. عدد 58. مجلد 29. 2013. الصفحات 85-132. الصفحة 109.

وجاء في قرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية الفلسطيني بخصوص ضبط الأجهزة والأدوات أو الوسائل أو بيانات المرور والبيانات المتعلقة بحركة الاتصالات ويمكن للنيابة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه¹، والتي من خلالها يمكن لنا أن نستنتج دور سلطات الضبط القضائي الذي يمكن له تفتيش الأدلة المادية ويمكن له الامتداد للبرامج والتي تعرف " بالسوفت وير"، وإنما يمكن أن يفتش "الهارد وير"، وما ينتج عن الجريمة الإلكترونية يضبط ويسجل وجاء المشرع الفلسطيني حاسم بهذه المسألة عند النظر فيها حيث نص على أنه لو كان الفاعل حسن النية يتم ضبطتها ومصادرتها، وتحدثت رئيسة النيابة العامة مسؤولة وحدة الجرائم الإلكترونية نسرين الرشماوي بأن الشركات مجبرة على تزويدنا بالبيانات اللازمة وأن كل شخص ملزم بتسجيل بيانات كاملة وبذلك تكون حماية الحقوق لجميع الاطراف محمية². وهذا ما أكد عليه المشرع السعودي في نظامه من حيث حسن النية في ضبط ومصادرة الأجهزة أو البرامج أو الأدوات المستخدمة في ارتكاب الجرائم المنصوص عليها في النظام.³

وكذلك جاء في نص المادة (13) من نظام مكافحة الجرائم المعلوماتية السعودي، "مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها، كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مَصْدرًا لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكة"⁴. وهذا ما أكد عليه قانون

¹ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 54.
1- دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون وحقوق غير حسن النية تصدر المحكمة قراراً بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون أو الأموال المتحصلة منها على أن تكون إزالة المخالفة على نفقة الفاعل.
2- تصدر المحكمة قراراً بمدة إغلاق المحل وحجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطة تلك الجرائم بحسب الأحوال.

² موقع جريدة القدس، النيابة الإلكترونية. تاريخ الزيارة 2018/5/2 الموقع الإلكتروني <http://www.alquds.com/articles/1484890275698412300> /نسرين الرشماوي في مقابلة خاصة مع القدس.

³ نظام مكافحة الجرائم المعلوماتية السعودي رقم 17 لسنة 2007، المادة 12.

⁴ نظام مكافحة الجرائم المعلوماتية السعودي رقم 17 لسنة 2007.

الإمارات العربية المتحدة بشأن مكافحة جرائم تقنية المعلومات في نص المادة (41)¹، وكذلك نص
المشرع الكويتي بنص مشابه للقانونين السابقين السعودي والإماراتي ولكنه أيضا أضاف المطالبة
بالتعويضات المناسبة²

إلا أنه وفقا لقرار بقانون بشأن المعاملات التجارية عرف المشرع البيانات الإلكترونية والسجل
الإلكترونية إذ من خلالها يمكن لمأمور الضبط القضائي ان يقوم بتفتيش هذه البيانات ومن خلالها
يستطيع أن يستخلص الجريمة قيام الجاني بجريمتة³، وايضاً بخصوص الضبط والتحفيز لتفتيشها
تطرق القرار بقانون بشأن الجرائم الإلكترونية رقم (16) لسنة 2017 من خلال نص المادة (34)
منه على ان للنيابة العامة الاذن بالضبط والتحفيز على كامل نظام المعلومات من شأنها تساعد في
كشف الحقيقة او أي جزء من مكونات المادية وغير المادية⁴.

وفي قانون الإجراءات الجزائية الاتحادي الإماراتي رقم 1992/87 ترك الباب مفتوحا لإمكانية
تفتيش الكيانات المعنوية حيث أنها لا تختلف عن الكيانات المادية⁵، ونصت المادة 25/أ من

¹ مرسوم قانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة تقنية المعلومات. المادة 41 نصت كالتالي "مع عدم الإخلال
بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من
الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو يمحى المعلومات أو البيانات أو إعدامها كما
يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم وذلك إما إغلاقا كلياً أو للمدة التي تقدرها المحكمة".

² القانون الكويتي رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، المادة 13 نصت كالتالي "يجوز الحكم
بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال
المتحصلة منها. ويجوز الحكم بإغلاق المحل أو الموقع الذي ارتكب فيه أي من هذه الجرائم إذا كان ارتكابها قد تم بعلم
مالكها لمدة لا.

تزيد على سنة بحسب الأحوال، مع عدم الإخلال بحقوق الغير حسن النية أو بحق الضرر في التعويض المناسب. ويكون
الحكم بإغلاق المحل أو الموقع وجوباً إذا تكرر ارتكاب أي من هذه الجرائم بعلم مالكها".

³ قرار بقانون بشأن المعاملات التجارية رقم (1) لسنة 2017. المادة 1.

- البيانات الإلكترونية: بيانات ممثلة أو مرمزة الكترونياً سواء على شكل نص أو رمز أو صوت أو صور أو غيرها .
- السجل الإلكتروني: مجموعة المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية، والتي تشكل
بمجمليها وصفا لحالة شخص أو شي ما.

⁴ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 34 \ 2 " للنيابة
العامة الاذن بالضبط والتحفيز على كامل نظام المعلومات، او جزء منه، او اية وسيلة من وسائل تكنولوجيا المعلومات التي
من شأنها تساعد على كشف الحقيقة".

⁵ إبراهيم، راشد بشير: التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة أبو ظبي. مرجع سابق.
صفحة 57.

قانون الحاسوب الهولندي على أنه "يمكن الحصول على الأدلة حتى لو كانت في إقليم دولة أخرى بواسطة الاتفاقيات الدولية الخاصة بالتعاون الأمني والقضائي والخاصة بالتفتيش وضبط الأدلة"¹.

وبعد الانتقال إلى مسرح الجريمة يعمل المحقق على السيطرة ويضع خطة دقيقة لجمع الأدلة، حيث على المحقق أن يتعامل بحذر شديد مع الأدلة الرقمية وأن تكون من خلال أيد خبيرة ومتخصصة في رفعها وتحريزها²، ومن ثم يقوم خبراء التصوير بتصوير المكان بالكامب فوتوغرافيا- تصويراً ثلاثياً الأبعاد- وذلك قبل البد بالتفتيش مع التأكيد على وجود ضرورة أخذ صور فوتوغرافية لما كانت عليه الشاشات وقت حضور مأمور الضبط القضائي إلى مسرح الجريمة، ومع وجود سلطات التحقيق عليهم أن يأخذوا البصمات مع الأخذ بعين الاعتبار الموجودة على لوحة المفاتيح والفأرة³.

المطلب الخامس: صعوبات يواجهها المحققون في الجرائم الإلكترونية

عملية البحث والتحري عن الجريمة الإلكترونية هي من الاجراءات المهمة، ومن خلالها يمكن الكشف عن الجريمة إذا قام المحقق بإتمام العمل وفقاً للإجراءات القانونية السليمة، إلا أنه يمكن أن يواجه المحقق وخلال إجراءات البحث والتحري صعوبات وتحديات وتقود هذه الصعوبات لمشاكل يواجهها المحقق نفسه، أو بفعل الجاني، أو لأسباب وعوامل أخرى، وهذا ما يمكن إيجازه وفقاً للتالي:⁴

أولاً: تكتم المجني عليهم وإحجامهم عن الإبلاغ عن الجرائم الإلكترونية: ويعود هذا إلى عدة أسباب، خوف الجهات المتضررة من الإبلاغ عن الجريمة؛ خشية من عمليات التفتيش التي تقوم بها جهات التحقيق وكشف لأسرارهم أو الاطلاع على معلومات وبيانات يتكتمون عن الإفصاح عنها أو إذا قاموا بالإبلاغ عنها ستؤدي إلى ضرب المؤسسة خشية من تضرر سمعتها لنقص

¹ مختاري، إكرام: *الدليل في الجريمة الإلكترونية*. مرجع سابق. صفحة 109.

² البشري، محمد أمين: *التحقيق في جرائم الحاسب الآلي والانترنت*. مرجع سابق. الصفحة 360.

³ جرادة: عبد القادر صابر: *دستور الاستدلال والتحقيق الجنائي في التشريع الفلسطيني*. مرجع سابق. صفحة 361.

⁴ بن بادرة، عبد الحليم: *إجراءات البحث والتحري عن الجريمة المعلوماتية الخصوصية والإشكالات*. مرجع سابق. صفحة

تقتهم في نظام الحماية الخاص بتلك المؤسسات، وأيضاً جهل المجني عليهم بأن هذه الهجمات هي هجمات إجرامية إلكترونية تؤدي إلى تلف أو دمار بنظام المؤسسة.

ثانياً: اهتمام الشركات والمؤسسات بالجانب الترويجي والتسويقي لمنتجاتها وتحقيق الأرباح وإهمالها للجانب الأمني للحصول على كم هائل من الأرباح؛ من خلال تبسيط الإجراءات للبرامج وملحقاتها وهذا بدوره يمنع هذه المؤسسات من الإبلاغ خوفاً على سمعتها.

ثالثاً: عدم إدراك خطورة الجرائم الإلكترونية من قبل المجني عليه كما أسلفنا سابقاً، إما لعدم علمه الكافي بأن حاسوبه الآلي يتعرض للهجمات الإلكترونية، أو يعلم بذلك لكن لا ينظر إلى ما يتعرض له بنوعٍ من الجدية.

رابعاً: نقص الخبرة من جهات البحث والتحري والتحقيق في الجرائم الإلكترونية: حيث أن عمل جهات البحث والتحري من أهم الأعمال التي من خلالها تؤدي إلى كشف الحقيقة ولنقص الخبرة في هذا المجال تؤدي للعزوف بالمقدرة عن البحث والتحري، ويشترط على من يتعامل بهذه الطبيعة الخاصة للجرائم أن يكون مؤهلاً عالي للتعامل بها¹.

المبحث الثاني: إجراءات التحقيق الجنائي الحديثة

التحقيق في الجرائم الإلكترونية، هي بحد ذاتها إجراءات متوافقة مع بعضها البعض كما ذكر في المبحث الأول، إلا أنه هناك إجراءات خصوصية يمكن أن يعمل بها لتكملة إجراءات التحقيق ومباشرتها والحصول على الأدلة، ولسبيل تحقيق هذه الإجراءات لا بدّ وأن تكون غايتها سليمة.

وقد وجدت أجهزة الشرطة بأن التحقيق يتخلله صعوبات جمة منذ بداية ظهور هذا النوع المستحدث من الجرائم، على نحو استدعى إعداد برامج تدريب وتأهيل لهذه الكوادر من الناحية الفنية على نحو يمكنها من تحقيق المهمة المطلوبة منها وبالكفاءة المطلوبة ففي الفترة الأولى لظهور هذا النوع من الجرائم، وجراء عدم الخبرة هذه وقعت الشرطة في أخطاء جسيمة أدت إلى الإضرار بالأجهزة أو الملفات، أو الأدلة الخاصة بإثبات الجريمة. ولتخطي هذه الأخطاء يجب

¹ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 5/33.

تأهيل المحققين بهذه الجرائم بالشكل الصحيح¹ من خلال تدريبهم أعدادهم بشكل يمكنهم التعامل مع هذا الجرائم المستحدثة.

يمكن تعريف التحقيق الجنائي في الجرائم الإلكترونية: بأنها عمل قانوني يقوم به مأمور الضبط القضائي المختص بضبط الجرائم الإلكترونية الرقمية من فاعل ودليل الكتروني رقمي؛ وذلك من أجل تقديمهم إلى سلطات التحقيق التي يجب أن تكون متخصصة في هذه النوعية من الجرائم الإلكترونية².

ولخصوصية الجرائم الإلكترونية يجب تطوير أساليب التحقيق وإجراءاته بصورة تتلاءم مع خصوصيته، وتمكن رجال التحقيق من الغرض المكلف به، ولتحقيق ذلك يجب تدريب الكوادر التي تباشر التحريات والتحقيقات مع الاستعانة بذوي الخبرة الفنية³.

وفي مرحلة التحريات يجب على مأموري الضبط القضائي أن يأخذوا اعتباراتهم من مجموعة الخطوات من أجل ضبط مرتكبي الجرائم الإلكترونية والتي يمكن ذكر أهمها⁴:

- تحديد وضع نظام المعالجة الآلية للكمبيوتر بمعنى كمبيوتر موصول أو متصل بالانترنت.
- وضع خطة إجمالية للمنشأة وإعداد كشف بأسماء المسؤولين عنها
- فصل التيار الكهربائي من مكان خارج الموقع قبل الشروع بالدخول إليه، فمن خلال هذا الإجراء يمكن أن يمنع المستخدم من التلاعب في المعلومات أو محوها
- فصل خطوط التلفون لعدم تمكن الجاني من استخدام مودم في جهاز معالجة المعلومات

¹ عقيدة، محمد أبو العلا: التحقيق وجمع الأدلة في الجرائم الإلكترونية. الموقع الالكتروني:

www.kambota.forumarabia.net. صفحة 6.

² موسى، مصطفى محمد: التحقيق الجنائي في الجرائم الإلكترونية. مرجع سابق ، صفحة 166.

³ عقيدة، محمد أبو العلا: التحقيق وجمع الأدلة في الجرائم الإلكترونية. الموقع الالكتروني:

www.kambota.forumarabia.net. مرجع سابق. صفحة 7.

⁴ الصغير، جميل عبد الباقي عبد الوهاب: أدلة الإثبات الجنائي والتكنولوجيا الحديثة، الحاسبات الآلية دراسة مقارنة. مجلة العلوم القانونية والاقتصادية كلية الحقوق جامعة عين شمس - مصر. عدد 1 مجلد 50. 2008/1-60. صفحة 35-36.

- تصوير الأجهزة المستهدفة من الأمام والخلف لإثبات إنها كانت قيد العمل.

ولقد أوضحت توصيات المؤتمر الدولي الثاني للاتجاهات الحديثة في الإثبات والتحقيق الجنائي المنعقد في أمستردام في عام 1999 والذي شارك فيه (170) من العلماء ورجال القانون والخبراء وأكدت هذه التوصيات على ضرورة مواكبة مشكلات الإجرام وخصوصاً الجرائم الإلكترونية، وتأهيل رجال الأمن والأجهزة الشرطية وتخطيط عمل دؤوب لوضع برنامج تدريبي ووضع أساليب حديثة لتعليمهم¹.

أوضحت الدراسات معوقات استخدام وسائل التحقيق في الجرائم الإلكترونية، وأفادت هذه أن نسبة المعوقات تتراوح بنسب متفاوتة ما بين 3.5% إلى 93% وتقوم هذه الى عدم معرفة المحققين

بمكونات عناصر الجريمة المعلوماتية، وعدم التدريب على استخدام التقنية المساعدة في كشف المجرمين، وعدم قناعة العاملين في مجال المعلومات في تدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية، وعدم استخدام أدوات وبرامج التحقيق وقلة التنسيق بين الأجهزة الأمنية والمؤسسات المستخدمة لنظم المعلومات، وعدم توافر المتخصصين والخبراء في البحث والتحري عن الجرائم الإلكترونية².

المطلب الأول: تعاون مزودي الخدمة مع جهات التحقيق

لما كان الدليل الرقمي قابع في البيئة الإلكترونية، ويمكن للجاني أن يقوم بفعله بواسطة الحاسوب الألي وقادر أيضاً على إخفاءه، وفي حال ارتكب الجاني جريمة إلكترونية ولم يضبط أي دليل لا يكون هناك عقوبة جزائية على فعله، بحيث وضع القانون إلزام على مزود الخدمات بتزويد الجهات المختصة بجميع البيانات والمعلومات التي تساعد في الكشف عن الحقيقة وهذا من خلال طلب النيابة العامة أو المحكمة المختصة³.

¹ العنزي، سليمان مهجع: وسائل التحقيق في جرائم نظم المعلومات. رسالة ماجستير منشورة. أكاديمية نايف العربية للعلوم الأمنية. الرياض. السعودية. 2003. صفحة 6.

² العنزي، سليمان مهجع: وسائل التحقيق في جرائم نظم المعلومات. رسالة مرجع سابق. صفحة 243-244.

³ سعيداني، نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مرجع سابق، صفحة 138.

يتسم الدليل الإلكتروني بخصائص رقمية ويبني على أساس الطبيعة المرنة التي يقوم عليها العالم الافتراضي، فإن الفاعل قادر على إزالة الدليل من على بعد باستخدام التقنية نفسها، ومن أجل ذلك إستلزم الأمر وضع إطار قانوني لحماية هذا الدليل والزام مزودي الخدمة بحفظ المعطيات¹، ويمكن القول بأن تعاون مزودي الخدمة مع سلطات الضبط القضائي من خلال عملية البحث والتحري عن الجرائم الإلكترونية لمحاربة الجريمة الإلكترونية بالقدر التي تبدو أهميتها في ظل أنها أصبحت تهدد مجموعة الخصوصيات المرتبطة بالحياة الخاصة للأفراد².

ومزود الخدمات وفقا للقرار بقانون الفلسطيني بشأن الجرائم الإلكترونية (16) لسنة 2017 بانه: " أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات أو أي شخص آخر يقوم بمعالجة أو تخزين أو إستضافة بيانات الحاسوب نيابة عن أية خدمة الكترونية أو مستخدم هذه الخدمة"³.

متعهد الخدمات هو بحد ذاته مزود خدمة الانترنت؛ وهو صاحب السلطة الحقيقية في مراقبة المعلومات التي يتم بثها، وحسب ما ورد في قانون الفرنسي لعام 1986 بأنه ملزم إخطار النائب العام، وهو ملزم بمراقبة محتوى الرسالة التي تصل إليه، وهذه السلطة هي سلطة مراقبة، لذا يمكن أن نقول أن متعهد الخدمات المذكور يقوم بأدوار عديدة فهو ممول للمعلومات، ومتعهد للخدمات، فضلا عن قيامه ببث المعلومات⁴.

لمزودي خدمة الإنترنت دور رئيس في تزويد الجهات الأمنية بجميع التفاصيل الفنية المطلوبة، كرقم هاتف الفاعل في حال تم ربطه على حساب لموقع تواصل اجتماعي، ومعلومات الشرائح المستخدمة وسجلات الصادر والوارد⁵، وتتولى هيئة الاتصالات وتقنية المعلومات تقديم يد

¹ سعيداني، نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مرجع سابق، صفحة 138.

² مختاري، إكرام: *الدليل في الجريمة الإلكترونية*. مجلة المنارة للدراسات القانونية والإدارية - المغرب. عدد خاص. 2015/9-33. صفحة 31.

³ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية. المادة 1.

⁴ حجازي: عبد الفتاح بيومي: نحو صياغة نظرية عامة في علم الجريمة والمجرم الإلكتروني. الطبعة الأولى: حقوق الطبع محفوظة للمؤلف. 2009. صفحة 322.

⁵ جبريل، دانه: الجرائم الإلكترونية. الموقع الإلكتروني: <http://7iber.com/society/facebook-cyber-crimes>. صفحة 2.

المساعدة الفنية للجهات المختصة في مراحل ضبط هذه الجرائم والتحقيق فيها إنشاء المحاكمة¹. وقد رتب المشرع الجزائري مسؤولية إدارية وأخرى جزائية على تقاعس مزودي الخدمات على حفظ البيانات والمعلومات؛ حيث أن التقاعس يؤدي بهذه المعلومات إلى عرقلة التحريات القضائية².

وعرفت الاتفاقية العربية مزود الخدمة كالتالي: " هو أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمات الاتصالات أو مستخدميها"³.

ولأهمية دور مزود الخدمة، يوجد التزام على مزود الخدمات بتزويد الجهات المتخصصة بجميع البيانات والمعلومات التي تساعد سلطات مأمور القضاء والأجهزة الأمنية بالكشف عن الحقيقة وهذا من خلال طلب النيابة العامة أو المحكمة المختصة، ويمكن لمزود الخدمة حجب رابط أو موقع أو محتوى على الشبكة العنكبوتية بناءً على أوامر من الجهات القضائية، وحفظ المعلومات عن المشترك لمدة لا تقل عن ثلاث سنوات، والتعاون ومساعدة الجهات المختصة، بناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل البيانات والمعلومات الإلكترونية والحفظ المؤقت⁴، حيث إن الاتصالات في فلسطين مصونة ولا يجوز لأحد المساس بها وللسلطة العامة وحدها في حدود القانون⁵.

¹ نظام مكافحة الجرائم المعلوماتية السعودي رقم 17 لسنة 2007، المادة 14.

² سعيداني، نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مرجع سابق، صفحة 141.

³ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموافق 2010/12/21 المنعقد في مقر الامانة العامة لجامعة الدول العربية بالقاهرة، وفلسطين من الأعضاء التي وقعت عليها بتاريخ 2013/5/21. المادة 1.

⁴ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 3/32 " الاحتفاظ بالمعلومات عن المشترك لمدة لا تقل عن 3 سنوات".

⁵ قانون الاتصالات الفلسطيني رقم (3) لسنة 1996، المادة 4 "بمقتضى هذا القانون تكون ملكية قطاع الاتصالات السلكية السلكية واللاسلكية للسلطة الوطنية الفلسطينية وتخضع للأحكام المنصوص عليها فيه".

وذهبت المحكمة الابتدائية في باريس بإصدار حكم بتاريخ 30 يناير 2013 بشأن مزودي الخدمات بأنهم ملزمون بحكم القانون بتمكين الجهات القضائية بالبيانات والمعطيات التي تدخل في حوزتهم سواء كان هذه لأغراض مدنية أو جنائية.¹

المطلب الثاني: تسجيل واعتراض المراسلات

تتضمن المراسلات بالخصوصية التي حماها المشرع من خلال تشريعات يضمن حمايتها، وأن هذا الأمر ليس مطلقاً، بحيث سمح للمشرع بإعتراض المراسلات وتسجيلها وكشف سريتها إذا إقتضت ضروريات التحري والبحث عن الجريمة المتلبس بها أو التحقيق الابتدائي فيها، ومنهم من نظر إليها على أنها اعتداء صارخ على حرمة الحياة الخاصة وسرية المراسلات ولكن ظهر استثناء في حالة إذا كان من وراء تسجيل المراسلات إظهار الحقيقة وكشف غموض ملابسات الجريمة وضبط الجناة.²

كما ألزمت هولندا في هذا المجال، بمحو بيانات مسجلة في ملفات الشرطة في حالت كانت غير قانونية، أي عدم وجود إذن لها بمراقبة الاتصالات من السلطات القضائية المختصة، أو اتخاذ ترتيبات تقنيه من أجل التفتيش تؤدي الى المساس بالحياة الخاصة للغير أو ممارسة الإكراه المادة أو المعنوي في مواجهة المشتبه فيه، أو استعمال الطرق غير المشروعة مثل استعمال الغش والتدليس للحصول على الأدلة الرقمية.³

وبالرجوع إلى القرار بقانون بشأن الجرائم الإلكترونية رقم (16) لسنة 2017 نجد أن المشرع الفلسطيني بناءً على طلب النائب العام أو أحد مساعدية ان تأذن بالأعتراض الفوري لمحتوى

¹ مختاري، إكرام: *الدليل في الجريمة الإلكترونية*. مجلة المنارة للدراسات القانونية والإدارية - المغرب. عدد خاص. 2015/9-33. صفحة 31.

² بن باردة، عبد الحليم: *إجراءات البحث والتحري عن الجريمة المعلوماتية*. مجلة الحقوق والعلوم الإنسانية. عدد 23. 2015/98-76. صفحة 85.

³ بن باردة، عبد الحليم: *إجراءات البحث والتحري عن الجريمة المعلوماتية*. مجلة الحقوق والعلوم الإنسانية. مرجع سابق. صفحة 87.

الاتصالات وتسجيلها ونسخها، وتأكيداً على حرية الاتصالات، نص على وجوب الحصول على قرار من المحكمة المختصة¹.

المطلب الثالث: الخبراء الإلكترونيين

في ظل تعقيد وتشعيب مجالات الحاسوب والإنترنت، كان لا بُد من الاستعانة بخبراء في هذا المجال بحسب ما تفرضه ظروف كل قضية وملابساتها، ومسألة استعانة المحقق الجنائي بالخبراء عادة ما تكون بتحقيق الجرائم التقليدية منذ زمن بعيد، فالمحقق يستعين في عمله بمجموعة كبيرة من الخبراء مثل الأطباء الشرعيين وخبراء الأدلة الجنائية وخبراء التصوير... وغيرهم الذين تعتمد الشرطة على خبرتهم، ولأن التحقيق في الجرائم الحاسوب والإنترنت يتطلب مهارات فنية لا توفر لدى مأمور الضبط القضائي، بات من الضروري تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم، لأهمية جرائم الحاسوب والإنترنت ولما تطلبه الإلمام بالخبرات المتنوعة والمتعددة²، لذلك نجد أن معظم القوانين نصت على ضرورة الاستعانة بالخبراء في الجرائم الإلكترونية، وعملت هذه القوانين على تنظيم بقوانين خاصة³.

والاستعانة برأي الخبير بأمر من المحقق للتعرف على مسألة معينة أو الحادثة الذي وقعت، بتحديد منطقي لما هو مطلوب مبينا فيها ذلك الأمر، حتى يستطيع الخبير أن يكون في ذهنه صورة تقريبيه عن الحادث، ويجب أن يراعى في المذكرة المشار إليها، ولا ينبغي أن يشار إلى اتجاه التحقيق نحو وجهة معينة؛ حتى لا يتأثر الخبير ولو بحسن نية باتجاه سير التحقيق، ومن المفترض أن ترسل هذه المذكرة إلى الخبير بلغة مبسطة وموجزة⁴.

¹ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 37.

² السرحاني، محمد: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت. مرجع سابق. صفحة 74.

³ حجازي، مصطفى احمد: المسؤولية المدنية للخبير القضائي. لا يوجد طبعة. مصر: دار الجامعة الجديدة للنشر. 2004.

صفحة 5

⁴ مراد، عبد الفتاح: التحقيق الجنائي التطبيقي. مرجع سابق، صفحة 304-305.

وبالرغم من الاستعانة بالخبراء تتم في مرحلة التحقيق الابتدائي إلا أن معظم التشريعات الإجرائية تجيز لمأمور الضبط القضائي في مرحلة جمع الاستدلالات الاستعانة بالخبراء ولذلك خشية من ضياع الأدلة وضياع آثار الجريمة.

وبالطبع فإن البحث عن المعلومات داخل الحاسوب ذاته يُعد أمراً بالغ التعقيد ويحتاج إلى وجود خبير، وأن يكون الخبير موثقاً فيه حتى يتمكن من الإلمام بمحتويات الأشرطة أو الاسطوانات دون إحداث تغير¹.

ومن أهل الخبرة التي يمكن الاستعانة بهم، خبراء البرمجة أو مخطو البرامج وهم الأشخاص المتخصصون في مجال الانترنت وكتابة أوامر البرامج، وكذلك المحللون وهو الشخص الذي يحلل الخطوات ويقوم بتجميع البيانات الخاصة بنظام معين، ودراسة وتحليل البيانات والنظام وتقسيمه وتتبع البيانات عن طريق نظام يسمى مخطط تدقيق البيانات، والاستعانة بمهندسي الصيانة والاتصالات وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسوب وبمكوناته هم أهل علم وخبرة؛ لتمكنهم من شبكات الاتصال المتعلق بالشبكة العنكبوتية².

وتعد الجرائم الإلكترونية من الجرائم التي تتطلب توافر خبراء متخصصين في مجال الحاسوب والانترنت، كون هذه الجرائم ترتكب في بيئة رقمية تختلف عن الجرائم التقليدية، فقلة الخبرة لدى المحققين وأعضاء النيابة تؤدي إلى ضياع الأدلة المتوافرة في هذه الجرائم، ووجود الخبراء بهذا المجال يساعد على حفظ الأدلة وسرعة الكشف عنها؛ لتعقيدها، ففي أغلب الأحيان ينقص أفراد الشرطة وأعضاء النيابة العامة الفهم المطلوب أو الخبرة اللازمة عن ملابسات الجرائم الإلكترونية³، ولعدم ضياع الأدلة ولتحقيق البحث والتحري بأسلوب يتطلب العلم والخبرة يمكن إتباع الخطوات التالية:

¹ الديري، عبد العال و إسماعيل، محمد صادر. الجرائم الإلكترونية دراسة قانونية قضائية مقارنة. القاهرة: المركز القومي للإصدارات القانونية. 2012. ط1. صفحة 319.

² حجازي، عبد الفتاح بيومي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت. مرجع سابق . صفحة 340.

³ جرادة: عبد القادر صابر: دستور الاستدلال والتحقيق الجنائي في التشريع الفلسطيني. مرجع سابق. صفحة 18-19.

1- تبادل المعلومات بين المحقق وخبير الحاسوب، قبل البدء في التحقيق أو بعد البدء أثناء استجواب المتهم أو الشهود للدلاء بالمعلومات؛ لتفادي نقص الموجد لكل من الطرفين وتكتمل له المهمة لكل من الآخر.

2- أخذ أقوال كل من الشهود والمتهمين من قبل المحقق وبحضور الخبير، بحيث يمكن له توجيه الأسئلة التقنية التي لا يعلم بها المحقق ويمكن أن تكتشف الإجابة عن خيوط الجريمة.

3- التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة على الحاسوب الآلي؛ مما يساعد كلاً من الطرفين بتقريب وجهات النظر وسرعة كشف الحقيقة.

4- الاستعانة بالتقنيات المتطورة في المجال الإلكتروني والمعلوماتي في مواجهة الجرائم الإلكترونية؛ وإن هذه التقنيات أثبتت جدارتها في جمع الأدلة¹.

ويتم الكشف عن الجريمة الإلكترونية باللجوء إلى ذاكرة الخادم الذي يتولى ربط الجهاز الإلكتروني بالعالم الافتراضي، وتتم عملية الكشف من خلال برمجيات مساعدة، للتوصل إلى الدليل الرقمي وحفظ الدليل ووجود الخبير الإلكتروني له أهمية كبيرة لتطلبها خبرة فنية خاصة، وإذا لم يكن هناك خبير يكون حكم القاضي مجافياً للمنطق العلمي ومعيباً، لعدم استناده إلى الخبرة الفنية ولعدم دراية القاضي بالجرائم الإلكترونية وكيفية ارتكابها، ولتمكن الخبير بسهولة الكشف عنها ويمكن أن تحتوي القضية على أكثر من خبير في الدعوى المنظورة².

ونص القانون البلجيكي على أنه: "يجوز لقاضي التحقيق والشرطة القضائية أن يستعين بخبير أثناء التحقيق في الجريمة لمعرفة ولدرايه الخبير عن كيفية تشغيل جهاز الحاسوب، وكيفية الدخول إليه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تستعين من الخبير تشغيل الحاسوب، أو البحث فيه أو عمل نسخة من البيانات

¹ بن باردة، عبد الحليم: إجراءات البحث والتحري عن الجريمة المعلوماتية. مجلة الحقوق والعلوم الإنسانية. عدد 23. 2015/98-76. صفحة 93.

² سقف الحيط، عادل: جرائم النذم والقدح والتحقيق المرتكبة عبر الوسائط الإلكترونية "دراسة قانونية مقارنة". مرجع سابق، صفحة 273.

المطلوبة للتحقيق أو سحب البيانات المخزونة أو المحمولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق"¹.

ولهذا يجب تدريب مأموري الضبط القضائي بجرائم تقنية المعلومات فيما يتعلق بالأساليب الفنية المستخدمة في ارتكاب الجريمة، وكذلك فيما يتعلق بطرق الكشف عنها، وكيفية فحصها فنياً، والتحفظ عليها، وهذا يتطلب تنمية استعدادهم الخاص وتكوين مهارات فنية تكون على درجة من المعرفة الفنية تتناسب بحجم المتغيرات والتطورات المتلاحقة في مجال الجرائم الإلكترونية، مع تطوير أساليب البحث عن الأدلة².

ولأهمية الخبير قد نص قرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية الفلسطيني عليها بنص المادة 33 فقره 5/4 على ضرورة الاستعانة بأهل الخبرة بقصد الحصول على البيانات والمعلومات من أجل مساعدة سلطات الضبط القضائي والسلوك القضائي لتوفر الحجم الهائل من المعلومات من قبل الخبير بسرعه في الكشف عن الجرائم وسهولة التعامل معها، وكذلك أن يكون مأمور الضبط القضائي مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية³.

ويرى الباحث في هذا المجال ضرورة توافر خبراء معتمدين من وزارة العدل، إذ دون خبراء ستضيع الأدلة المطلوبة، فالمحققون الجنائيون أو النيابة العامة خبرتها العملية والعلمية بهذا المجال ضئيلة، والخبير متفرغ لهذا المجال ويكون مُلمّاً بالتحقيق والتحري بهذه الجرائم⁴، وهذا ما أستاذ

¹ القاضي: رامي متولي: مكافحة الجرائم المعلوماتية. طبعة 1. القاهرة: دار النهضة العربية. 2011. صفحة 109، مشار لقانون تحقيق الجنايات البلجيكي لسنة 2000 المادة 88.

² حسن: سعيد عبد اللطيف: إثبات جرائم الكمبيوتر والجرائم المرتكب عبر الانترنت. لا يوجد طبعة. القاهرة: دار النهضة العربية. 1999. صفحة 129.

³ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 5/4/33

⁴ وتأكيداً على الاستعانة بالخبراء لنص المادة 64 من قانون الإجراءات الجزائية رقم (3) لسنة 2001 م، المادة 64 "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 بذلك". حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم 143 لسنة 2011 "ان الاستفادة من النص السابق ان المشرع أعطى الصلاحية لوكيل النيابة العامة ممارسة لإجراءات التحقيق الاستعانة بالطبيب المختص وغيره من الخبراء لإثبات الجريمة المرتكبة وان الاستعانة في سبيل مباشرة التحقيق حالة الجريمة ليست مقصورة على جهة معينة بالذات فله أن يلجأ إلى الطبيب المختص أو إلى غيره من ذوي الخبرة طبقاً لسلطته التقديرية". وأيضاً حكم محكمة النقض رقم 2014/1.

عليه تأكيداً لرأيه المشرع السعودي في نص المادة 76 " للمحقق أن يستعين بخير مختص لإبداء الرأي في أي مسألة متعلقة بالتحقيق الذي يجريه".¹

والحجية لرأي الخبير تكمن فيما إذا أخذ القاضي به في نهاية الأمر أو لم يأخذ فيه، وغالباً ما يأخذ القاضي برأي الخبير، لأن الخبير ينتدب إلى موضوع فني ولديه من العلم والدراية والخبرة أكثر من القاضي التي تتيح له الفصل في هذه المسائل، بالإضافة إلى أن الخبير ينتدب ويراقب أثناء عمله بمعرفة جهات التحقيق، وإلا إن أغلبية الفقهاء يرون أن حرية القاضي في تكوين قناعته برأي الخبير على جميع الأدلة المستخلصة.²

المبحث الثالث: آليات التحقيق عن الجرائم الإلكترونية في الاتفاقات الدولية

استناداً لكثرة استعمال الشبكة العنكبوتية، وسرعة وصولها واتصالها من دولة إلى أخرى ظهرت لنا هذه التقنيات بعدة مشاكل ومن أهمها الاختراقات التي تتم بواسطة الحاسوب الآلي ويمكن لهذه الجرائم أن تتعدى حدود الدولة الوطنية لتشمل الحدود الدولية، ومن هنا جاء الاهتمام الدولي بشأن هذه الجرائم؛ كون المجتمع أصبح يعاني من هذه الجرائم، وأصبح الأمر في غاية الأهمية لعقد اتفاقيات دولية بين الدول للتعاون بهذا الشأن للحد من هذه الجرائم ومكافحتها ومن هذه الاتفاقيات الذي سوف نعمل الحديث عنها. من وسائل الحد من الجرائم الإلكترونية إبرام اتفاقيات دولية في مجال حماية شبكات الانترنت خاصة، بعدما سهلت شبكات الانترنت الحصول على المعلومات خلال ثوان وضرورة التنويه إلى عقد اتفاقات دولية وإطلاع الجهات التي تضررت جراء المخاطر الواقعة على المعلومات.³

¹ الزين، إبراهيم بن سليمان بن محمد: دور تقارير الخبراء في إثبات جرائم القتل. رسالة ماجستير منشورة. جامعة نايف العربية للعلوم الأمنية. السعودية. هـ 1430. صفحة 2.

² راسخ، إبراهيم: التحقيق الجنائي العلمي. الطبعة الأولى. مطبعة الفجيرة الوطنية: دبي. الإمارات. 1991. ص 273-274.

³ بن يونس، عمر محمد أبو بكر: الجرائم الناشئة عن استخدام الانترنت. بدون طبعة. مصر: جامعة المنصور كلية الحقوق. رقم الطبعة 2004. صفحة 809.

المطلب الاول: التعاون الدولي في مجال البحث عن الجريمة الإلكترونية

والتعاون الدولي مهم عند التعامل مع الجرائم الإلكترونية، لما سيلحقه تطور في أساليب متشابهة لتحقيق قانون جنائي وإجرائي لحماية شبكات المعلومات الدولية؛ لأن هذه الجرائم هي عابرة للقارات ولا حدود لها، وعدم التعاون فيما بين الدول سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما يعطي المجرمين الآفلات من العقوبة ومضاعفة أنشطتهم الإجرامية¹.

ولأهمية التعاون بين الدول، يعتبر التفتيش العابر للحدود والذي يجب أن يتم وفقا لاتفاقيات دولية مبرمة ما بين الدول من أجل السماح بالتفتيش ولا يجوز القيام بالتفتيش العابر للحدود في غياب تلك الاتفاقيات أو على الأقل يجب أن نحصل على إذن من الدول الأخرى للقيام بالإجراءات القانونية وفقا للمعايير الوطنية².

وقد تضمنت اتفاقية بودابست مجموعة من الاجراءات الخاصة بالبحث والتحري أيضا جاءت مضامين الاتفاقية العربية مطابقة لأحكام اتفاقية بودابست خاصة على القواعد الاجرائية من خلال نص المواد (16) إلى (21) ويمكن إجمالها فيما يلي³:

- 1- سرعة التحفظ على بيانات الكمبيوتر المخزنة
- 2- اجبار مقدمي الخدمات على التزويد بالمعلومات المطلوبة
- 3- تفتيش وحجز بيانات الكمبيوتر المخزنة
- 4- التجميع الفوري لبيانات الكمبيوتر وامكانية اعتراض هذه البيانات.

إن المشرع الفلسطيني حديثا وبعد صدور قرار بقانون الجرائم الإلكترونية تحدث عن تعاون الدول بموجب الاتفاقيات عن تيسير التعاون مع نظيراتها في البلاد الأجنبية بقصد الإسراع في تبادل المعلومات فيما من شأنه أن يكفل الإنذار المبكر في حال اكتشاف الجريمة في إحدى الدول

¹ الشنفي، عبد الرحمن عبد العزيز: امن المعلومات وجرائم الحاسب الالى. الطبعة الأولى: بدون دار نشر. الرياض. السعودية 1414 هجريا. صفحة113.

² توبة: عبد الحكيم رشيد: جرائم تكنولوجيا المعلومات. عمان: دار المستقبل للنشر والتوزيع. 2008. صفحة 235

³ قجاج، يوسف: الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والقانون. مرجع سابق. صفحة 186

المُساعدة في التحقيق في الجريمة الإلكترونية المرتكبة، وبالإضافة إلى تتبع المجرمين ومرتكبيها ويتوقف التعاون بقيام الدولة الأجنبية بالالتزام بالحفاظ على سرية المعلومات وعدم نقلها أو تناقلها إلى جهات أخرى أو إستغلالها لأغراض غير الغرض المخصص له في هذا القرار بقانون¹.

وقد نص قرار بقانون بشأن الجرائم الإلكترونية رقم (16) لسنة 2017 على أنه: "يتعين على الجهات المختصة أن تقدم العون للجهات النظيرة في الدول الأخرى، لأغراض تقديم المساعدة القانونية المتبادلة وتسليم المجرمين في التحقيقات والإجراءات الجنائية المترابطة بالجرائم المنصوص عليها في هذا القرار بقانون، وفقا للقواعد التي يقرها قانون الإجراءات الجزائية والاتفاقيات الثنائية، أو متعددة الأطراف التي تكون الدولة طرفا فيها، أو بمبدأ المعاملة بالمثل وذلك بما لا يتعارض مع أحكام هذا القرار بقانون أو أي قانون آخر، ولا ينفذ طلب المساعدة القانونية، أو طلب تسليم المجرمين استنادا إلى أحكام هذه القرار بقانون، إلا إذا كانت قوانين الدولة الطالبة وقوانين الدولة تعاقب على الجريمة موضوع الطلب أو على جريمة مماثلة وتعتبر ازدواجية التجريم

¹ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 43 فقره/2/1.

- نص المادة كالتالي:

- 1- تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية أو الإقليمية و الثنائية المصادق عليها أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات بما في شأنه ان يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال وتقادي ارتكابها والمساعدة على تحقيق فيها وتتبع مرتكبيها.
- 2- يتوقف التعاون المشار إليه بالفقرة 1 من هذه المادة على الالتزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعد إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعنية بهذا القرار بقانون.

- نص المادة 2

- 1- تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه إذا ارتكبت كليا أو جزئيا داخل فلسطين أو خارجها أو امتد أثرها داخل فلسطين سواء أكان الفاعل أصليا أم شريكا أم محرضا أم مت دخلا على ان 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 بهذا القرار بقانون في إحدى الحالات التالية:
أ- إذا ارتكب من مواطن فلسطيني.
ب- إذا ارتكبت ضد أطراف أو مصالح فلسطينية.
ت- إذا ارتكبت ضد أطراف أو مصالح من قبل أجنبي أو شخص عديم الجنسية يوجد محل إقامته داخل فلسطين أو من قبل أجنبي أو شخص عديم الجنسية وجد في الأراضي الفلسطينية ولم تتوفر في شأنه شروط التسليم القانونية.

مستوفاة، بغض النظر عما إذا كانت قوانين الدولة الطالبة تتدرج الجريمة في فئة الجرائم ذاتها، أو تستخدم في تسمية الجريمة المصطلح ذاته المستخدم في الدولة بشرط ان يكون الفعل موضوع الطلب مجرماً بمقتضى قوانين الدولة الطالبة¹.

وتحدثت الاستاذة نسرین رشمای بالتطبيق العملي في فلسطين يتم التعاون الدولي مع الدول الأخرى في مكافحة الجريمة الإلكترونية بالاستثناء من اتفاقية بودابست أو الاتفاقية العربية لمكافحة تقنية المعلومات، وذلك من خلال الطرق الدبلوماسية من خلال وزارة العدل والخارجية بملاحقة هذه العصابات، وأيضاً يوجد تعاون دولي معنا عند وقوع جريمة الإلكترونية².

"التعاون القضائي هو تعاون السلطات القضائية الدولية لمكافحة الجريمة الإلكترونية، وبهدف التعاون إلى تقريب من الإجراءات الجنائية الدولية من حيث إجراءات البحث والتحري عن وقوع جريمة إلكترونية ويتم التنسيق ما بين السلطات القضائية الدولية للاتفاق على معايير موحدة"³. وفقاً للاتية:

1. التمسك بمبدأ التجريم المزدوج كشرط لتسليم المجرمين.
2. استخدام التكنولوجيا الحديثة مثل الدوائر التليفزيونية وأن يتاح للقاضي الانتقال من دولة إلى أخرى لسبيل التحقيق في الجريمة ولاكتشاف محتوياتها.
3. أن يراعى تنفيذ الأحكام الأجنبية وفقاً لضوابط تتفق عليها الدول فيما بينها.
4. ويراعى تطبيق برامج آمنة لحماية الشهود، لأن هذه الجرائم تحتوي على مجموعات كبيرة ومخطط لها مسبقاً بحيث من يقوم بارتكاب هذه الجريمة شخص له علاقات كبيرة داخل وخارج الدولة.

¹ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 44 فقره/2/1

² موقع جريدة القدس، النيابة الإلكترونية. تاريخ الزيارة 2018/5/2 الموقع الإلكترونية <http://www.alquds.com/articles/1484890275698412300> / الرشمای في مقابلة خاصة مع القدس.

³ قشوقش، هدى حامد: الجريمة المنظمة. لا يوجد طبعة. القاهرة: دار النهضة العربية. 2000. صفحة 85.

ولأهمية التعاون ما بين الدول قامت جامعة الدول العربية بعقد اجتماع لصياغة ميثاق لقانون مكافحة جرائم تقنية المعلومات بمقر الأمانة العامة بالقاهرة الموافق 2010/2/21، وتحدثت عن التعاون الدولي والقضائي في الفصل الرابع منه، وفي المادة (30) تحدثت عن الاختصاص للدول بأن كل دولة تلتزم بتبني الإجراءات في حال تحققت الجريمة في إقليم الطرف وعلى متن سفينة تحمل علم الدولة الطرف ...، وتطرق إلى موضوع تسليم المجرمين ...، وتهدف الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، وذلك من أجل الحفاظ على أمن الدول العربية ومصالحها وسلامة الأفراد فيها، وتقتضي هذه الاتفاقية بتطبيق بنودها بهدف منع الجرائم الإلكترونية والتحقيق فيها، مثل الاعتداء على سلامة البيانات، ونشر أفكار جماعات إرهابية والدعوة لها، وجرائم إساءة استخدام تقنية المعلومات، والتزوير والاحتيال..¹

بينما ظهرت اتفاقية بودابست تهدف إلى توحيد السياسة التشريعية من أجل مكافحة الجرائم الإلكترونية المترتبة في الفضاء الافتراضي وإلى تنسيق التعاون بين التشريعات الوطنية لتسهيل مكافحة الإجرام المعلوماتي، وتطبيق إجراءات تتلاءم لتحقيق وملاحقة الفضاء الافتراضي ووضع نظام تعاون دولي يتميز بالسرعة والفعالية في التنفيذ..²

وحتى يمكن تطبيق قواعد تعاون الدولي بإجراءات سليمة وصحيحة ويمكن تطبيقها كآلي:³

1- التمسك بمبدأ التجريم المزدوج كشرط لتسليم المجرمين وينص عليه المشرع صراحةً في قانون دول الاطراف الذي وقع الفعل عليها، ولكن يمكن التخلي عن تسليم الجاني في حال كان هناك إجراءات تمس بحقوق الإنسان والحريات العامة، كما نصت الاتفاقية على عدم استبعاد الاختصاص الجنائي الذي ينص عليه أحد الاطراف وفقاً لقانونه الوطني ومطالبة الدول الاطراف

¹ المالكي، محمد بن احمد خضران: رؤية إستراتيجية لربط المعلومات الأمنية بين دول مجلس التعاون لمكافحة الجرائم الإلكترونية. رسالة ماجستير منشورة. جامعة نايف العربية للعلوم الأمنية. الرياض. السعودية. 2015. صفحة 92-93.

² قجاج، يوسف: الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والقانون. عدد 28. 2015/196-182. صفحة 186.

³ قشقوش، هدى حامد: الجريمة المنظمة. مرجع سابق. صفحة 85-86.

في الاتفاقية بالتشاور حول الاختصاص القضائي الاكثر ملائمة لمحاكمة مرتكبي الجرائم الالكترونية في حالة تعدد المطالبة من طرف الاطراف باختصاصه القضائي حول واقعة معينة.

2- أن يتوفر بين الدول نظام للمساعدة القضائية في المواد الجنائية مثلاً إقتضت العدالة في التحقيق أن ينتقل القاضي الى الدولة الذي أرتكب فيه الفعل ان يكون متوفر في الدولة المساعدة للقاضي بحرية الانتقال والتحقيق أو اعطاء إنابة قضائية الى قاضي لمتابعة سير التحقيقات ويجب أن تنفذ وفقاً للمعايير الدولية، وبجميع الأحوال أن يكون هناك توافقاً في الإجراءات في كل من الدولتين وما تسمى توأمة التشريع.

ويلاحظ غالباً أن ما يتم استبعاد الإنابة في الشق السياسي والعسكري والضريبي، لأنها من شأنها المساس بالسيادة والنظام العام والمصالح الأساسية للدول، حيث يبقى النظام معيماً لارتباطه بالطرق الدبلوماسية والتي تتسم بالبطء وكثرة البروتوكولات وما يتعارض من الإجراءات السريعة لهذه الجرائم من شأن الإجراءات المعقدة أن تؤدي إلى ضياع الأدلة والبيانات واختفائها¹.

3- استخدام التكنولوجيا الحديثة مثل الدوائر التلفزيونية وأن يكون للقاضي حرية الانتقال من دولة إلى أخرى للتحقيق في القضية المعروضة عليه وهذا ليس مقتصرًا على مرحلة التحقيق الابتدائي ولكن في مرحلة الحكم أيضاً.

4- كما يجب تطبيق برامج آمنة لحماية الشهود على المستوى الدولي.

5- مراعاة في تطبيق الأحكام الأجنبية وفقاً لضوابط تتفق عليها الدول فيما بينها، والاتفاق على كيفية مصادرة الأموال محل الجريمة عبر الحدود أو إرسال المسجونين. تبادل المعلومات: وهي تشمل تقديم كل البيانات والوثائق التي تطلبها سلطة قضائية اجنبية بصدد متابعة جريمة ما والرد على الاتهامات التي وجهت الى رعاياه في الخارج وتبليغ الاجراءات التي اتخذت بحقهم².

¹ لموسخ، محمد: تنازع الاختصاص في الجرائم الالكترونية، دفاثر السياسة والقانون. عدد2/143-157. لا يوجد سنه نشر، صفحة155.

² لموسخ، محمد: تنازع الاختصاص في الجرائم الالكترونية، دفاثر السياسة والقانون. عدد2/143-157. لا يوجد سنه نشر، صفحة155.

6- نقل الاجراءات: يقصد بها قيام دولة بناء على اتفاقية باتخاذ اجراءات جنائية بصدد جريمة ارتكبت في اقليم دولة اخرى ولمصلحة هذه الدولة وهذا اذا ما توافر عدة شروط وهي¹:

- ان يكون الفعل المنسوب الى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب منها.
- ان يكون الاجراء المطلوب اتخاذه مقرر في قانون الدولة المطلوب اليها عن الجريمة ذاتها.
- ان يكون الاجراء المطلوب اتخاذاها يؤدي الى كشف الحقيقة كأن تكون الادلة موجودة بالدولة المطلوب اليها.

لتزايد الجرائم الإلكترونية وما تثيره هذه الجرائم من إشكاليات عملت منظمة الأمم المتحدة إلى عقد اتفاقيات خاصة بمكافحة استعمال التكنولوجيا لسنة 2000، بمعنى أنها أكدت على الحاجة إلى تعزيز التعاون والتنسيق بين الدول في مكافحة استعمال تكنولوجيا المعلومات، بالإضافة إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المنعقدة في فيينا في أكتوبر 2000، حيث بين المؤتمر فهرس الأمثلة المتعلقة بتسليم المجرمين وتحقيق سبل التعاون وتبادل المساعدة القانونية².

وعمل المشرع المغربي بموائمة التشريع الجنائي المغربي مع الاتفاقيات الدولية والإقليمية، وجاءت هذه الموائمة لسد الفراغ القانوني وتجاوز القصور الذي كانت تعرفه النصوص القديمة وكذلك لخلق قانوني صريح وواضح يمكن القضاء من متابعة مرتكبي الجرائم الإلكترونية³.

المطلب الثاني: اتفاقية بودابست وقواعدها الإجرائية لسلطتها في البحث والتحري

جاءت اتفاقية بودابست بضرورة إتباع سياسة جنائية هدفت من خلالها حماية المجتمع ضد الجريمة الإلكترونية، وإلى توحيد السياسة الواجب إتباعها في مكافحة الجرائم الإلكترونية المرتكبة في الفضاء الافتراضي، ومن خلال العمل المشترك ما بين الدول والتعاون لتسهيل مكافحة الجرائم

¹ لموسخ، محمد: تنازع الاختصاص في الجرائم الإلكترونية، مرجع سابق، صفحة 155.

² مزغيش، سمية: جرائم المساس بالأنظمة المعلوماتية. بحث منشور. جامعة محمد خضير بسكرة. الجزائر. 2014. صفحة 54-55.

³ فالي، علل: خصوصيات الجريمة المعلوماتية على ضوء التشريع و القضاء المغربي. مجلة القضاء التجاري. مرجع سابق، صفحة 125.

الإلكترونية، وتطبيق إجراءات والتحقيق وملاحقة المجرمين ووضع نظام تعاون دولي يتميز بالسرعة والفعالية في التنفيذ¹.

كما تضمن اتفاقية بودابست الإجراءات المتعلقة بالاختصاص القضائي للجريمة الإلكترونية وفقا لنص المادة 22، مؤكدة على ضرورة اعتماد الدول الأطراف على ما يلزم من تدابير تشريعية وأخرى تدابير أخرى؛ حتى تتمكن المحاكم في الدول الوطنية ممارسة حقها بالاختصاص القضائي ضمن صلاحياتها المتعلقة بالجرائم الواردة في الاتفاقية، بمعنى عندما ترتكب جريمة في إقليم دولة أو على متن سفينة التي ترفع علمها أو على متن إحدى الطائرات المسجلة بموجب قوانينها الخاصة أو على أحد رعاياها بحيث إذا كان القانون يعاقب عليها بموجب القانون الجنائي بمكان ارتكابها، وكذلك نصت الاتفاقية على عدم استبعاد الاختصاص الجنائي الذي ينص عليه أحد الأطراف وفقا لقانونه الوطني ومطالبة الأطراف في الاتفاقية بالتشاور حول الاختصاص بالأكثر ملائمة لتطبيقه على مرتكبي هذه الجرائم الإلكترونية².

ونشير إلى أن اتفاقية بودابست نصت على وجوب التعاون بين أطراف الاتفاقية مع بعضها البعض في تطبيق الأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية، والاتفاقيات الدولية المعتمدة على التشريعات المتماثلة والقوانين المحلية، لأغراض البحث والتحري أو الإجراءات المترابطة بالجرائم بنظم وبيانات المعلوماتية أو لجمع أدلة ذات شكل الكتروني للجريمة الجنائية³.

تضمنت هذه الاتفاقية مجموعة من القواعد الإجرائية الخاصة بالبحث والتحري ومن أهمها ما يلي⁴:

1- سرعة التحفظ على بيانات الكمبيوتر المخزنة

2- إجبار مقدمي الخدمات على التزويد بالمعلومات المطلوبة

¹ قجاج، يوسف: الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والقانون. مرجع سابق. صفحة 186-188.

² قجاج، يوسف: الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والقانون. مرجع سابق. صفحة 187.

³ بن باردة، عبد الحليم: إجراءات البحث والتحري عن الجريمة المعلوماتية. مرجع سابق. صفحة 94.

⁴ اتفاقية بودابست لمكافحة الجرائم المعلوماتية 23 \ 11 \ 2001، من مواد 16-20.

3- تفتيش وحجزها بيانات الكمبيوتر المخزنة

4- التجميع الفوري لبيانات الكمبيوتر

وتناولت اتفاقية بودابست موضوع التفتيش، حيث نصت على ضرورة تسهيل الإجراءات فيما يتعلق بالتحقيق لكل من الدول الأعضاء الموقعة على الاتفاقية من حيث تفتيش الأنظمة الإلكترونية، وتخويل سلطات التحقيق الولوج لأنظمة المعلومات المراد تفتيشها والذي لها علاقة بالجريمة الإلكترونية¹.

"وقد صادق مجلس الحكومة المغربية بتاريخ 20/11/2012 على مشروع قانون رقم 12/لسنة 136 الذي وافق بموجبة على اتفاقية بودابست المتعلقة بالجرائم الإلكترونية وكذلك على بروتوكولها الإضافية الموقع بستراسبورغ في 28 يناير 2003 بشأن تجريم الأفعال ذات الطبيعة وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر"².

ووفقا للقوانين المطبقة في فلسطين ذَهَبَ المشرع بإيجاد نصوص خاصة بالأختصاص القضائي عند النظر بالجرائم المرتكبة عبر الانترنت سواء كان الفعل كاملاً أو جزءاً منه، أو كان محرصاً أو فاعلاً أصلياً³.

¹ اتفاقية بودابست لمكافحة الجرائم المعلوماتية 2001\11\23، نص المادة 1/19 على انه "يعتمد كل طرف قد يلزم من تدابير تشريعية وتدابير أخرى، وذلك لمنح سلطات ذلك الطرف صلاحية التفتي أو الدخول على: أ- أي نظام حاسوب أو جزء منه والبيانات المخزنة فيه، ب- أي وسيط تخزين، يجوز أن تكون البيانات مخزنة فيه في إقليم ذلك الطرف"

² فالي، علل: خصوصيات الجريمة المعلوماتية على ضوء التشريع و القضاء المغربي. مجلة القضاء التجاري. مرجع سابق، صفحة 125.

³ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية.

- نص المادة 2:

1- تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها أو امتد أثرها داخل فلسطين سواء أكان الفاعل أصلياً أم شريكاً أم محرصاً أم مت دخلاً 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 بهذا القرار بقانون في إحدى الحالات التالية:

أ- إذا ارتكب من مواطن فلسطيني.

ب- إذا ارتكبت ضد إطفار أو مصالح فلسطينية.

ت- إذا ارتكبت ضد أطراف أو مصالح من قبل أجنبي أو شخص عديم الجنسية يوجد محل إقامته داخل فلسطين أو من قبل أجنبي أو شخص عديم الجنسية وجد في الأراضي الفلسطينية ولم تتوافر في شأنه شروط التسليم القانونية.

كما أن اختلاف وتباين المعايير الوطنية فيما يتعلق بتحديد الاختصاص، يصعب عملية البحث والتحري ويفضي إلى حدوث تنازع في الاختصاص بشأن هذه الطائفة من الجرائم وإعمالاً بمبدأ إقليمية النص الجنائي لوقوع جريمة الإلكترونية عابرة للحدود تخضع لاختصاص أكثر من دولة، وإذا وقع السلوك في نطاق بلد آخر فإن كلا البلدين يجب عليهما إعمال قانونهما على الواقعة، فيكتفي عند تطبيق قانون البلد على هذه الجريمة بأن الفعل غير معاقب عليه في بلد المنشأ¹.

المطلب الثالث: إتفاقية مجلس أوروبا بشأن الإجرام السيبري لعام 2000م

هي الاتفاقية الوحيدة المتعددة الأطراف بمكافحة الجرائم التي تتم باستخدام أو ضد الكمبيوتر أو شبكة الانترنت، ودخلت حيز النفاذ عام 2004 على مستوى مجلس الاتحاد الأوروبي، كما وقعت على هذه الاتفاقية غير دول مجلس الاتحاد الأوروبي مثل كندا واليابان وجنوب إفريقيا، كما صادقت عليها الولايات المتحدة الأمريكية. كما أكدت هذه الاتفاقية على ضرورة احترام حقوق الإنسان والحريات العامة التي تضمنتها الاتفاقيات الدولية والتشريعات الوطنية، واتخذت هذه الاتفاقية طابعاً توجيهياً للخطوات التي تستلزم الإجراءات الجنائية لاسيما في مرحلة التحقيق والملاحظة القضائية مثل التحفظ على الأدلة والضبط وغير ذلك.²

وقد تضمنت هذه الاتفاقية لأهميتها أقسام عدة تأتي وفقاً كالتالي³:

القسم الأول: مصطلحات تفسيرية

القسم الثاني: الخطوات الواجب اتخاذها في إطار التشريع الوطني

القسم الثالث: التعاون الدولي.

القسم الرابع: الشروط النهائية حول الانضمام إلى الاتفاقية

¹ بن باردة، عبد الحليم: *إجراءات البحث والتحري عن الجريمة المعلوماتية* مرجع سابق. صفحة 95.

² السموني: خالد الشرقاوي: *مكافحة الجرائم الإلكترونية على ضوء التشريعين الوطني والدولي*. المجلة المغربية للإدارة المحلية والتنمية. عدد 102/127-137. صفحة 133-134.

³ السموني: خالد الشرقاوي: *مكافحة الجرائم الإلكترونية على ضوء التشريعين الوطني والدولي*. مرجع سابق. صفحة

والقواعد المنظمة لاتفاقية مجلس أوروبا:¹

- 1- وجوب مراعاة صحة ودقة البيانات التي يجري جمعها ومستمدة بطرق مشروعة.
 - 2- تحديد فترة زمنية لحفظ البيانات والأغراض المعالجة من أجلها.
 - 3- عدم استعمال البيانات أو إفشاؤها في غير الأغراض المخصصة لها.
 - 4- توفير الحماية من الناحية الإدارية والتقنية لعدم الدخول غير المشروع للوصول لمعالجة البيانات.
 - 5- تحديد من هم الأشخاص المخولون والجهات المرخصة للوصول للمعلومات- مثل النيابة العامة- لتمكنهم من الحفاظ على السر المهني.
 - 6- وفي حالة كان هناك تجاوز لمن تم إعطاؤهم رخص للوصول والاطلاع على البيانات يستلزم عليهم مساءلة.
- أن إجراءات التحقيق في بيئة تكنولوجيا المعلومات وفقا لما جاءت في توصية المجلس الأوروبي رقم 95/13 تقتضي التدخل السريع لمد الإجراءات إلى أنظمة الكمبيوتر، بمعنى أن تسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع الأدلة، وهذا لا يمثل اعتداء على سيادة الدولة أو على إحكام القانون الدولي ويجب وضع قاعدة قانونية صريحة تسمح بهذا الإجراء.²
- "وللأهمية التي تقع على الدولة الموقع على هذا الميثاق أن تعمل على توأمة تشريعها الوطني بما يناسب الاتفاقية وتحددت هذه الاتفاقية التي يجب أن يتضمن في تشريعها الوطني على النحو التالي:

¹ مصطفى، يونس خالد عرب: جرائم الحاسوب دراسة مقارنة. مرجع سابق. صفحة 127.

² شرايشة، لينده: السياسة الدولية والإقليمية في مجال الجريمة الالكترونية (الاتجاهات الدولية في مكافحة الجريمة الالكترونية)، بحث منشور على الانترنت/ المركز الجامعي سوق أهراس. صفحة 251.

- 1- الجرائم المتعلقة بأمن الشبكات والمراقبة غير المشروعة والعدوان على الثقة في البيانات أو على النظام أو الإساءة إليه.
- 2- الجرائم المعلوماتية كما هو الشأن في الاختلاق والانتحال والنصب والاحتيال المعلوماتي.
- 3- جرائم الأخلاق مثل إنتاج أو بث أو حيازة ما يتعلق بدعارة الأطفال.
- 4- جرائم العدوان على حقوق الملكية الأدبية والفكرية كاستتساخ المصنفات المشمولة بالحماية.
- 5- المسؤولية الجنائية للأشخاص المعنوية".¹

وجاء في توصيات المجلس الأوروبي الصادر بين سنة 1985 وسنة 1995 بما يفيد في استحداث دوائر جديدة تضلع بموجهة مكافحة جرائم الانترنت وتزويد أهل الخبرة الأكفاء بالعلم بهذه التقنيات وبالإضافة توفير الأجهزة والمعدات التقنية اللازمة لذلك.²

المطلب الرابع: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

لضرورة الحاجة إلى وجود تعاون مشترك ظهرت الحاجة لدى الدول العربية رغبةً منها بحماية المجتمع، ومكافحة جرائم تقنية المعلومات التي تهدد امن الدول العربية ومصالحهم جميعاً، وهذا جله تم صياغته في ديباجة الاتفاقية العربية لمكافحة جرائم المعلومات الصادرة بتاريخ 2010/12/21 في جمهورية مصر العربية، وفلسطين أصبحت عضو في هذه الاتفاقية بتاريخ 2013/5/21.³

وهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات حفاظاً على أمن الدول العربية ومصالحها.⁴

ويرى الباحث أن هذه الاتفاقية مهمة من حيث وجودها والأهم من أن يتم تطبيق هذه الاتفاقية لحماية امن الدول العربية من جرائم تقنية المعلومات لانتشار هذه الجرائم، ووجود التعاون ما بين

¹ السمووني: خالد الشرقاوي: *مكافحة الجرائم الالكترونية على ضوء التشريعين الوطني والدولي*. مرجع سابق. صفحة 134

² العدوانى، محمد نافع فالح رشدان: *حجة الدليل الالكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية: دراسة مقارنة بين القانونين الكويتي والأردني*. رسالة ماجستير منشورة. جامعة الشرق الأوسط. الأردن. 2015. صفحة 94.

³ الاتفاقية العربية لمكافحة جرائم المعلومات الصادرة بتاريخ 2010/12/21 في جمهورية مصر العربية

⁴ الاتفاقية العربية لمكافحة جرائم المعلومات الصادرة بتاريخ 2010/12/21 في جمهورية مصر العربية، المادة الأولى.

الدول العربية يساهم بالحد من هذه الجرائم، وكذلك من المهم وجود اتفاقيات ما بين الدول لتسليم المجرمين أو عمل موائمة ما بين التشريع الوطني والاتفاقية العربية حتى لا يحصل تعارض في تطبيق العقوبة بين التشريع والاتفاقية.

والمادة الثالثة من الاتفاقية نصت على بعض الحالات إذا ارتكبت تنطبق هذه الاتفاقية عليها إلا أنه يوجد إستثناءات وهي كالتالي¹:

- 1- في حالة " إذا ارتكبت في أكثر من دولة.
- 2- في حالة ارتكبت في دولة أخرى وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى،
- 3- في حالة ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة،
- 4- في حالة ارتكبت في دولة وكانت لها أثار شديدة في دولة أو دول أخرى."

كما ان الاتفاقية العربية لمكافحة الجرائم الإلكترونية كان لها الأصل في وضع الجرائم في الفصل الثاني منه، ونذكر على سبيل المثال منه في حالة الاعتداء على سلامة البيانات، و جريمة التزوير، وارتكاب جريمة الاحتيال، والشروع والاشتراك في ارتكاب الجرائم ...² أما من الناحية الإجرائية فقد تضمنت هذه الاتفاقية جملة من القواعد الإجرائية في بيئة الجرائم المعلوماتية، كما اعتبرت هذه الاتفاقية بأن كل دولة تتبنى في قانونها الداخلي والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث الذي يحتوي على الأحكام الإجرائية - توأمة التشريعات-.

ظهر حديثا في التشريع الأخير الفلسطيني الصادر مؤخرا تحت رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على توأمة تشريعه بما يتناسب فعليا، لتحقيق التعاون مع البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية تحت طائلة المعاملة بالمثل بهدف الحصول على الإنذار المبكر

¹ الاتفاقية العربية لمكافحة جرائم المعلومات الصادرة بتاريخ 2010/12/21 في جمهورية مصر العربية، المادة الأولى.

² الاتفاقية العربية لمكافحة جرائم المعلومات الصادرة بتاريخ 2010/12/21 في جمهورية مصر العربية، من المادة الخامسة الى الحادي والعشرين من الاتفاقية.

بالجرائم الإلكترونية والإسراع في تبادل المعلومات والمساعدة في تحقيقها، والعمل على حفظ المعلومات وعدم استغلالها من قبل الدول الأجنبية¹.

حيث تعمل كل دولة وفقا للإجراءات المتبعة بتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر في بث الاتصالات من مزودي خدمة الانترنت وخصوصا عندما يتم الحفاظ على المعلومات إذا كانت هذه المعلومات عرضة للتلف أو للفقان أو للتعديل، وتعطي أوامر وفقا للإجراءات كل في دولته لإصدار أوامر تسليم المعلومات، وتفتيش أو الوصول إلى المعلومات المخزنة أو المخزن عليها، ويمكن هنا توسيع نطاق التفتيش للحصول على المعلومات وضبطتها وعمل نسخة عن هذه المعلومات والحفاظ على سلامتها وإزالة أو منع الوصول إلى المعلومات وأيضا نصت هذه الاتفاقية على ضرورة تبني الدول في قانونها جمع أو تسجيل لمعلومات تتبّع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تثبت بواسطة الانترنت إن يكون هناك تعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى وهذا كله يتم تحت تمكين السلطات المختصة بهذه الإجراءات بعدما يتم التوافق بين القانونيين².

¹ قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، عدد ممتاز 14 الوقائع الفلسطينية، المادة 43 فقرة 2/1

- نص المادة كالتالي:

1- تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية أو الإقليمية والثنائية المصادق عليها أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات بما في شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال وتقادي ارتكابها والمساعدة على تحقيق فيها وتتبع مرتكبيها.

2- يتوقف التعاون المشار إليه بالفقرة 1 من هذه المادة على الالتزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعد إحالتها إلى طرف آخر أو استغلالها لإغراض أخرى غير مكافحة الجرائم المعنية بهذا القرار بقانون.

² الاتفاقية العربية لمكافحة جرائم المعلومات الصادرة بتاريخ 2010/12/21 في جمهورية مصر العربية، من المادة الثانية والعشرون الى التاسعة والعشرون.

الخاتمة

بعد إنتهائي بفضل الله من كتابة هذا البحث، والذي كانت موضوعه البحث والتحري في الجرائم الإلكترونية، في ظل أن الجرائم الإلكترونية هي جرائم جديدة تدق أجراس الخطر في المجتمع الدولي، ولأعتبارات أن هذه الجرائم المستحدثة هي خطيرة أيضاً على الواقع الفلسطيني، أصدر الرئيس الفلسطيني محمود عباس قرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية للحد من هذه الجرائم على الواقع المحلي، ومن خلال الواقع العملي ومن خلال الاحصائيات الفلسطينية بات من المعروف بأن الجرائم الإلكترونية كبيرة نسبياً والتي تتظر أمام المحاكم الفلسطينية، ونظراً لأهمية هذا البحث موضعاً فيه عن البحث والتحري في الجرائم الإلكترونية من خلال الاجراءات التقليدية المتبعة مثل التبليغ والمراقبة والترصد الإلكتروني...، وبالإضافة تعاون مزودي الاتصالات مع النيابة أو المحكمة بأذن خطي من الجهات المختصة، ومن الوسائل الحديثة أيضاً الخبراء الإلكترونيين والتي يتم التعامل معهم من خلال سلطات التحقيق لكشف الحقيقة، حيث أنني أيضاً تطرقت الى وسائل التحقيق عن الجرائم الإلكترونية في الاتفاقات الدولية لأهمية وجود تعاون دولي مشترك لمكافحة هذه الجريمة كونها عابرة للقارات، فأن الباحث توصل لعدد من النتائج والتوصيات ومن أهمها:

أولاً: النتائج

1- نظراً لزيادة الجرائم الإلكترونية على الساحة الفلسطينية بشكل خاص وعلى الساحة الدولية بشكل عام صَدَرَ مؤخراً قرار بقانون ينظم الجرائم الإلكترونية ويحمل رقم (16) لسنة 2017 وبات هذا القانون فعالاً أمام المحاكم النظامية في فلسطين.

2- يوجد فرق كبير بين الضبط الإداري الضبط القضائي؛ فالأول مقتصر على رقابة المجتمع من المخاطر واجراءاته وقائية لحماية المجتمع أما مأمور الضبط القضائي يتولى سلطة الكشف عن مرتكبي المرتكبة من خلال البحث والتحري.

3- عند القيام بمأمور الضبط القضائي بالبحث والتحري عن وقوع جريمة أن يقوموا بإحترام مشروعة القانون والالتزام بالاجراءات المرسومه به وعدم تجاوزه، وأحترام خصوصيات المحفوظة على شبكة التواصل الاجتماعي أو على الحاسوب أو أي وسيلة أخرى وعدم العبث فيها.

4- أن دور سلطات الضبط القضائي يمكن له تفتيش الأدلة المادية ويمكن له الامتداد للبرامج والتي تعرف " بالسوفت وير"، وإنما يمكن أن يفتش "الهارد وير"، وما ينتج عن الجريمة الإلكترونية يضبط ويسجل وجاء المشرع الفلسطيني حاسم بهذه المسألة عند النظر فيها حيث نص على أنه لو كان الفاعل حسن النية يتم ضبطتها ومصادرتها.

5- أهم ميزات جرائم الإعتداء على نظم معالجة الآلية للمعطيات، أنها تنصب على محل من نوع خاص يختلف تماما عن محل الجرائم التقليدية، فهذه الجرائم تستهدف المساس بالمعلومات الإلكترونية المتواجدة في البيئة الرقمية على هيئة إشارات غير مرئية.

6- حديثا أصدر النائب العام المستشار أحمد براك تعليماته بإنشاء نيابة لمكافحة الجرائم الإلكترونية وكلفوا أعضاء النيابة العامة من وكلاء ومعاونين في كل نيابة جزائية بمختلف المحافظات، لأستقبال وتسجيل القضايا المرتكبة من قبل الجناة.

7- الكاملة لسلطات البحث والتحري حين الشروع بالتحقيق عند وقوع جريمة الالكترونية وأيضا المعرفة بالإجراءات اللازمة دون أي تقصير يذكر.

8- كل من بادر من الجناة بتبليغ السلطات المختصة عن وقوع جريمة الالكترونية أو قيد التخطيط لها يعفى من العقوبة المقررة، وهذا قبل وقوع الضرر وقبل علم السلطات المختصة فيها، لكن إذا تم التبليغ بعد وقوع الجريمة للمحكمة أن توقف العقوبة المقرر بحق من بادر بالتبليغ وأدى ذلك الى ضبط باقي الجناة.

9- معايير التمييز بين أعمال الضبط الإداري و أعمال الضبط القضائي يركز على طبيعة هذا الضبط وخلال فتره جمع الأدلة والاستدلالات الجريمة الالكترونية يعد ضبطاً قضائياً أما إذا صدر بصورة تدابير تسعى من خلالها الإدارة إلى الحفاظ على الأمن والنظام العام فإنه يعتبر ضبطاً

إدارياً، يمكن في بعض الحالات قد تكون المهمة مزدوجة وتحمل الصفتين معا - صفة السلطة الإدارية الضبطية و صفة السلطة القضائية الضبطية مثل شرطي المرور .

10- رأي الخبير يحتوي على امور فنية تعمل على كشف الجريمة الالكترونية، ولديه من العلم والدراية والخبرة العملية، بالإضافة إلى أن الخبير ينتدب ويراقب أثناء عملة بمعرفة الجهات التحقيق ويعمل تحت إشرافهم، وإلا إن أغلبية الفقهاء يرون أن حرية القاضي في تكوين قناعته برأي الخبير على جميع الأدلة المستخلصة.

11- يوجد اختلاف ملموس في الأدلة لكل من الجرائم التقليدية والجرائم الحديثة فالجرائم التقليدية يكون الدليل ظاهراً للعيان ومحسوساً ويمكن كشف، أما الأدلة في الجرائم الإلكترونية ليست بالصورة المذكورة في الجرائم التقليدية.

12- لأهمية البحث والتحري عن الجرائم الإلكترونية من الواجب على سلطات التحقيق الانتقال فوراً لمكان ارتكاب الجريمة والمحافظة على الأدلة والتعامل بحذر شديد مع الأدلة.

ثانياً: التوصيات

1- من الضروري إلى جهات التحقيق أن يتوفر لديهم كوادر بشرية تمكنها من سلطة البحث والتحري في الجرائم الإلكترونية بواسطة الوسائل الحديثة.

2- العمل على تدريب المحققين في معاهد مختصة؛ لأكتسابهم الخبرة في مجال البحث والتحري وإعطائهم دورات في هذا المجال.

3- ورد في القرار بقانون رقم (16) لسنة 2017 عقوبات صارمة، فلا تصلح تطبيقها على الواقع الفلسطيني؛ نظراً لشدتها من المفروض تخفيف هذه العقوبة حسب نوعية الجريمة وأيضاً حسب من هم مرتكبو الجرائم.

4- ضرورة التعاون المشترك من قبل سلطات التحقيق مع مزودي خدمة الاتصال وهذا يساعد عملية البحث والتحري عن الجرائم الإلكترونية.

5- العمل على توحيد قانون واحد بشأن الجرائم الإلكترونية في فلسطين (الضفة الغربية، وقطاع غزة).

6- ضرورة الحث على استخدام لفظ المشتبه فيه أمام سلطات البحث والتحري بدلا من الجاني لما له اثر متحقق في نفسية المشتبه فيه

قائمة المصادر والمراجع

المصادر:

- 1- اتفاقية بودابست لمكافحة الجرائم المعلوماتية 23 \ 11 \ 2001.
- 2- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية في القاهرة بتاريخ 2010/12/21،
- 3- القانون الكويتي رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات.
- 4- قانون الإجراءات الجزائية رقم (3) لسنة 2001 م.
- 5- قانون الاتصالات الفلسطيني رقم (3) لسنة 1996.
- 6- قانون السلطة القضائية الفلسطينية رقم (1) لسنة 2002م.
- 7- قانون الاجتماعات العامة رقم 12 لسنة 1998م.
- 8- قانون الجمارك والمكوس قانون رقم 1 لسنة 1962.
- 9- قانون المخابرات العامة رقم (17) لسنة 2005م.
- 10- قانون الدفاع المدني رقم 3 لسنة 1998 م.
- 11- قانون العقوبات الجزائري رقم 15 لسنة 2004 المؤرخ في 10/11/2004 المتمم والمعدل للأمر 156/66، وتم إضافة القسم السابع منه مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.
- 12- قرار بقانون الجرائم الإلكترونية رقم (16) لسنة 2017. عدد ممتاز 14 الوقائع الفلسطينية.

- 13- القرار بقانون الصادر حديثاً رقم (23) لسنة 2017 بشأن الشرطة الفلسطينية، الوقائع الفلسطينية عدد ممتاز رقم 15،
- 14- قرار بقانون بشأن الأمن الوقائي رقم (11) لسنة 2007 م.
- 15- قرار بقانون بشأن المعاملات التجارية رقم () لسنة 2017.
- 16- جرائم أنظمة المعلومات لسنة 2010 الأردني الصادر في الجريدة الرسمية بتاريخ 2010/9/16.
- 17- جرائم أنظمة المعلومات لسنة 2010 الأردني الصادر في الجريدة الرسمية بتاريخ 2010/9/16.
- 18- قانون جرائم المعلوماتية السوداني لسنة 2007.
- 19- قانون جرائم تقنية المعلومات العُماني، تاريخ الزيارة 2016-11-10 <http://www.omanlegal.net/vb/showthread.php?t=16297>
- 20- قانون بشأن جرائم تقنية المعلومات الصادر عن مملكة البحرين رقم (60) لسنة 2014 والصادر بتاريخ 30 سبتمبر 2014م.
- 21- قانون جرائم تقنية المعلومات الكويتي الصادر بداية من يوم 2016/1/12، وذلك بعد ما تم نشره في الجريدة الرسمية بتاريخ 2015/7/7.
- 22- مرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات صادر عن دولة الإمارات العربية المتحدة بتاريخ 13/ أغسطس/ 2012.
- 23- نظام مكافحة الجرائم المعلوماتية السعودي رقم 17 لسنة 2007

المراجع:

- 1- إبراهيم، خالد ممدوح: الجرائم المعلوماتية، ط1، الإسكندرية: دار الفكر الجامعي. 2002.
- 2- إبراهيم، خالد ممدوح: امن الجريمة الإلكترونية. لا يوجد طبعة. الإسكندرية: الدار الجامعية. 2008.
- 3- إبراهيم، راشد بشير: التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على اماره ابو ظبي. عدد131. لا يوجد طبعة. الإمارات: تصدر عن مركز الإمارات للدراسات والبحوث الإستراتيجية. لا يوجد سنة نشر.
- 4- احمد، هلاي عبد أله: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي. ط1. القاهرة: دار النهضة العربية. 1997.
- 5- ادعيس، معن : صلاحيات جهاز الشرطة. لا يوجد طبعة. الهيئة الفلسطينية المستقلة لحقوق المواطن رام الله- فلسطين.
- 6- احمد، هلاي عبد أله: حجية المخرجات الكمبيوترية في المواد الجمائية دراسة مقارنة. لا يوجد طبعة: لا يوجد دار نشر. 2000.
- 7- البقمي، ناصر بن محمد: جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، ط1: السعودية: مطابع الحميضي. 1430 هـ - 2009 م.
- 8- البشري، محمد امين: التحقيق في جرائم الحاسب الآلي والانترنت. المجلة العربية للدراسات الامنية والتدريب، عدد 30. مجلد 15. ط1. 2000.
- 9- البلوشي، راشد بن حمد: الدليل في الجريمة المعلوماتية. مجلة الحقوق للبحوث القانونية الاقتصادية. مجلد. 2008م.

- 10- البحر، ممدوح خليل: مبادئ أصول المحاكمات الجزائية. ط1. عمان: دار الثقافة للنشر والتوزيع. 1998.
- 11- أبو الروس، احمد: منهج البحث الجنائي. لا يوجد طبعة. الإسكندرية: المكتب الجامعي الحديث. 2009.
- 12- أبو عامر، محمد زكي: الإجراءات الجزائية. ط2. الإسكندرية: منشأة المعارف للنشر والتوزيع. 1997.
- 13- الحيارى، معن احمد: الركن المادي للجريمة، ط1. لبنان: منشورات الحلبي. 2010.
- 14- الدرة، ماهر عبد شويش: قانون العقوبات القسم الخاص، ط2. بغداد: المكتبة القانونية. لا يوجد سنة نشر.
- 15- السالك، كامل فريد 2000 نقلا عن: مؤتمر للجمعيات السوريات للمعلوماتية: 21-23 تشرين الأول 2000: حلب. الجمعية السورية للمعلوماتية.
- 16- الشالدة، محمد فهاد، وريعي، عبد الفتاح أمين: الجرائم الإلكترونية في دولة فلسطين المحتلة في ضوء التشريعات الوطنية والدولية. بحث مقدم إلى المؤتمر العلمي الحادي عشر لكلية القانون في جامعة جرش حول الجرائم المعلوماتية. فلسطين: 2015.
- 17- الشنفي، عبد الرحمن عبد العزيز: امن المعلومات وجرائم الحاسب الالى. الطبعة الأولى: بدون دار نشر. الرياض. السعودية 1414 هجري.
- 18- الصغير، جميل عبد الباقي عبد الوهاب: الجرائم الناجمة عن الحاسب الآلي والانترنت. المؤتمر الدولي الأول لقانون الانترنت (نحو علاقات قانونية وإدارية واقتصادية وسياسية واجتماعية جديدة). المنظمة العربية للتنمية الإدارية. المنظمة العربية للتنمية الإدارية. مؤتمر 1. مصر: المنظمة العربية للتنمية الإدارية. 2005.

- 19- الصغير، جميل عبد الباقي عبد الوهاب: *أدلة الإثبات الجنائي والتكنولوجيا الحديثة، الحاسبات الآلية دراسة مقارنة*. مجلة العلوم القانونية والاقتصادية كلية الحقوق جامعة عين شمس - مصر. عدد 1 مجلد 50. 2008.
- 20- الطهرأوي، هاني علي: *القانون الإداري*. ط1. عمان : دار العلمية الدولية ومكتبة دار الثقافة للنشر والتوزيع. 2001.
- 21- العدواني، محمد نافع فالح رشدان: *حجة الدليل الالكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية: دراسة مقارنة بين القانونين الكويتي والأردني*. رسالة ماجستير منشورة. جامعة الشرق الأوسط. الأردن. 2015.
- 22- العوجي: مصطفى: *دروس في العلم الجنائي*. ط2. بيروت: مؤسسة نوفل. 1987.
- 23- المالكي، محمد بن احمد: *رؤية إستراتيجية لربط شبكة المعلومات الأمنية بين دول مجلس التعاون لمكافحة الجرائم الإلكترونية*. (رسالة ماجستير منشورة). جامعة نايف العربية للعلوم الأمنية. الرياض. السعودية، 2015.
- 24- المقبل، صالح بن سعد: *بناء نموذج لمهارات التحقيق الاستدلالي في جرائم الابتزاز الالكتروني*. (رسالة ماجستير منشورة). جامعة نايف العربية للعلوم الأمنية. الرياض. السعودية. 2015.
- 25- المشجري، ليلي احمد سالم: *الجرائم الاقتصادية عبر الشبكة العالمية للمعلومات*. (رسالة ماجستير منشورة). كلية الدراسات الإسلامية العربية - دبي. 2014.
- 26- العريان، محمد علي: *الجرائم المعلوماتية*. لا يوجد طبعه. الإسكندرية: دار الجامعة الجديدة للنشر. 2004.
- 27- العبيدي: أسامة بن غانم: *التفتيش عن الدليل في الجرائم المعلوماتية*. المجلة العربية للأمنية والتدريب. عدد 58. مجلد 29. 2013.

- 28- العفيفي، يوسف خليل يوسف: الجرائم الإلكترونية في التشريع الفلسطيني. (رسالة ماجستير منشورة). الجامعة الإسلامية. غزة، 2013.
- 29- العنزي، سليمان مهجع: وسائل التحقيق في جرائم نظم المعلومات. رسالة ماجستير منشورة. أكاديمية نايف العربية للعلوم الأمنية. الرياض. السعودية. 2003.
- 30- المؤمني، نهلا عبد القادر: الجرائم المعلوماتية، ط1. عمان: دار الثقافة للنشر والتوزيع. 2008.
- 31- المضحكي، حنان ربحان مبارك: الجرائم المعلوماتية " دراسة مقارنة". ط1. بيروت: منشورات الحلبي الحقوقية. 2014.
- 32- الحيارى، معن احمد: الركن المادي للجريمة، ط1. لبنان: منشورات الحلبي. 2010.
- 33- السرحاني: محمد: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت. رسالة ماجستير منشورة. جامعة نايف العربية للعلوم الأمنية. السعودية. الرياض. 2004.
- 34- السموني: خالد الشرقاوي: مكافحة الجرائم الإلكترونية على ضوء التشريعين الوطني والدولي. المجلة المغربية للإدارة المحلية والتنمية.
- 35- الصبحي، دأود سليمان: إجراءات التحري والمراقبة والبحث الجنائي، جامعة نايف العربية للعلوم الأمنية. الرياض. 2012.
- 36- الحمامي، علاء حسين والحمامي، محمد علاء: مفاهيم وتطبيقات الأساليب الأمنية الحديثة في التحقيق الإلكتروني. لا يوجد طبعة، العدد 31، الإمارات: مركز الإمارات للدراسات والبحوث الإستراتيجية، لا وجد سنه نشر.
- 37- القاضيان، أسامة احمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، 2014.

- 38- القهوجي، علي عبد القادر: *الحماية الجنائية لبرامج الحاسوب*. مجلة الحقوق للبحوث القانونية الاقتصادية. مصر. ع1/1992.
- 39- القاضي: رامي متولي: *مكافحة الجرائم المعلوماتية*. طبعة 1. القاهرة: دار النهضة العربية. 2011. صفحة 109، مشار لقانون تحقيق الجنايات البلجيكي لسنة 2000
- 40- الحسبان، عطاء الله احمد: *نظم المعلومات المحاسبية*. الطبعة الاولى دار اليازوري للنشر. عمان. الاردن، 2013.
- 41- المعهد القضائي الفلسطيني. *التفتيش في قانون الاجراءات الجزائية الفلسطينية*. بحث منشور على موقع الدكتور احمد براك. رام الله. 2012.
- 42- الديري، عبد العال و إسماعيل، محمد صادر. *الجرائم الإلكترونية دراسة قانونية قضائية مقارنة*. القاهرة: المركز القومي للإصدارات القانونية. 2012. ط1.
- 43- الزين، إبراهيم بن سليمان بن محمد: *دور تقارير الخبراء في إثبات جرائم القتل*. رسالة ماجستير منشورة. جامعة نايف العربية للعلوم الأمنية. السعودية. 1430هـ.
- 44- الزرعوني، هشام عبد الرحمن: *المسؤولية المدنية لمأموري الضبط القضائي دراسة مقارنة*. طبعة اولى. حقوق الطبع محفوظة لشرطة الشارقة. الامارات العربية المتحدة. 2015
- 45- بن عبد العزيز، زينب: *الترصد الالكتروني وحماية الحرية الشخصية في قانون الفساد*، رسالة ماجستير منشورة. جامعة قاصدي مرباح. الجزائر. 2017/5/21
- 46- بن يونس، عمر محمد أبو بكر: *الجرائم الناشئة عن استخدام الانترنت*. بدون طبعة. مصر: جامعة المنصور كلية الحقوق. رقم الطبعة 2004.
- 47- بن بادرة، عبد الحليم: *إجراءات البحث والتحري عن الجريمة المعلوماتية الخصوصية والإشكالات*، مجلة الحقوق والعلوم الإنسانية. عدد 23. 2015م.

48- توبة: عبد الحكيم رشيد: جرائم تكنولوجيا المعلومات. عمان: دار المستقبل للنشر والتوزيع. 2008.

49- ثنيان، ناصر آل ثنيان: إثبات الجريمة الإلكترونية. (رسالة ماجستير منشورة). جامعة نايف العربية للعلوم الأمنية، ابو ظبي، الإمارات، 2012.

50- صغير، يوسف: الجريمة المرتكبة عبر الانترنت. (رسالة ماجستير منشورة). جامعة مولود معمري- تيزي وزو. 2013.

51- صالح، نائل عبد الرحمن: الجرائم الاقتصادية في التشريع الأردني، ط1: عمان - الأردن: دار الفكر للنشر والتوزيع. 1990.

52- فالي، علل: خصوصيات الجريمة المعلوماتية على ضوء التشريع و القضاء المغربي. مجلة القضاء التجاري. المغرب. ع1/2013. 20.

53- سعيداني، نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. (رسالة ماجستير منشورة). جامعة الحاج لخضر. باتنة. الجزائر، 2012-2013.

54- سقف الحيط، عادل: جرائم الدم والقذف والتحقيق المرتكبة عبر الوسائط الإلكترونية "دراسة قانونية مقارنة". ط1. عمان: دار الثقافة للنشر والتوزيع. 2011.

55- سلامة، مأمون: الإجراءات الجنائية في التشريع الليبي. ط1. ج 2، منشورات المكتبة الجامعة، 2000.

56- سعيداني، نعيم: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. (رسالة ماجستير منشورة). جامعة الحاج لخضر. باتنة. الجزائر، 2012-2013.

57- سقف الحيط، عادل: جرائم الدم والقذف والتحقيق المرتكبة عبر الوسائط الإلكترونية "دراسة قانونية مقارنة". ط1. عمان: دار الثقافة للنشر والتوزيع. 2011.

- 58- هروال، نبيلة هبة: الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات. ط1. الإسكندرية: دار الفكر الجامعي. 2007.
- 59- قشقوش، هدى حامد: جرائم الحاسب الالكتروني في التشريع المقارن. القاهرة: دار النهضة العربية، 1992.
- 60- قشقوش، هدى حامد: الجريمة المنظمة. لا يوجد طبعة. القاهرة: دار النهضة العربية. 2000.
- 61- حجازي، عبد الفتاح بيومي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت. ط1. الاسكندرية: دار الفكر الجامعي. 2006.
- 62- حجازي: عبد الفتاح بيومي: نحو صياغة نظرية عامة في علم الجريمة والمجرم الالكتروني. الطبعة الأولى: حقوق الطبع محفوظة للمؤلف. 2009
- 63- حسن: سعيد عبد اللطيف: اثبات جرائم الكمبيوتر والجرائم المرتكب عبر الانترنت. لا يوجد طبعة. القاهرة: دار النهضة العربية. 1999.
- 64- جبر، رُهام سائد احمد: جريمة الاحتيال الإلكترونية وإجراءات الضبط والتحقيق بها دراسة مقارنة. رسالة غير منشورة. جامعة القدس. القدس. فلسطين. 2015.
- 65- راسخ، إبراهيم: التحقيق الجنائي العلمي. الطبعة الأولى. مطبعة الفجيرة الوطنية: دبي. الإمارات. 1991.
- 66- زين الدين، بلال أمين: جرائم نظم المعالجة الآلية للبيانات، ط1. الإسكندرية: دار الفكر الجامعي، 2008.
- 67- زعنون، سالم. والحلي، محمد: شرح قانون الإجراءات الجزائية الفلسطينية. لا يوجد طبعه. مكتبة دار الفكر. 2002 م.

- 68- سرور، احمد فتحي: الوسيط في قانون الإجراءات الجزائية. القاهرة: دار النهضة العربية. 1996.
- 69- سالم، عبد الله حسن: أقوال الشهود في مرحلة التحري والتحقيق، مجلة الفكر الشرطي- مركز بحوث الشرطة القيادة العامة لشرطة الشارقة. عدد3. مجلد 1. 1992.
- 70- فضل، سليمان احمد: المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت. لا يوجد رقم طبعة. القاهرة: دار النهضة العربية. 2013.
- 71- لامين، سمير: مراقبة التليفون والتسجيلات الصوتية والمرئية، ط3، دار الكتاب الذهبي. مصر. 2000.
- 72- صورية، العاصمي : تأثير نظام الضبط الإداري على الحقوق والحريات العامة. رسالة ماجستير منشورة. جامعة الحاج لخضر بباتنة. 2011-2012 م.
- 73- رستم، هشام محمد فريد: الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة. طبعة 4: مصر- أسبوط: مكتبة الآلات الحديثة. 1994.
- 74- موسى، مصطفى محمد: المراقبة الإلكترونية عبر شبكة الانترنت. ط1. القاهرة: دار الكتب والوثائق المصرية. 2003.
- 75- مصطفى: محمود محمد: الإثبات في المواد الجنائية في القانون المقارن. ط1. القاهرة: مطبعة جامعة القاهرة. 1987.
- 76- عصفور: مي خميس: المواعيد والمدد في قانون الإجراءات الجزائية الفلسطيني (دراسة مقارنة). رسالة ماجستير منشورة. جامعة الأزهر. غزة. 2010.
- 77- عبد الهادي، محمد فتحي: مقدمة في علم المعلومات. ط1. القاهرة: مكتبة غريب. 1984.

- 78- عبد الحكيم، مولاي براهيم، *الجرائم الإلكترونية*. مجلة الحقوق والعلوم الإنسانية- جامعة زيان عاشور بالجلفة. الجزائر. عدد 23 / جوان 2015. 13.
- 79- عفيفي، كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "دراسة مقارنة". لا يوجد طبعة. الإسكندرية: منشأة وتوزيع المعارف بالإسكندرية. لا يوجد رقم سنة إصدار.
- 80- عطية، طارق إبراهيم الدسوقي: *إجراءات البحث الجنائي في ضبط الجريمة الإلكترونية في ضوء اتفاقية بودابست الموقعة في 23 نوفمبر سنة 2001 والمتعلقة بالإجرام الكوني*. مجلة الأمن والقانون أكاديمية شرطة دبي. عدد 2. مجلد 339. 2015.
- 81- عمري، محمد محمود: *الإثبات الجنائي الإلكتروني في الجرائم المعلوماتية دراسة مقارنة*. مجلة العلوم القانونية والسياسة. عدد 2. مجلد 216/12. 291-334.
- 82- علوني، هليل فرج: *التحقيق الجنائي والتصرف فيه*. لا يوجد طبعة. الإسكندرية: دار المطبوعات الجامعية. 2006.
- 83- عبد الحميد عبد المطلب، ممدوح: *البحث والتحقيق الجنائي في جرائم الكمبيوتر والانترنت*. لا يوجد طبعة. مصر: دار الكتب القانونية. 2006.
- 84- عمران، آية: *النيابة العامة الفلسطينية وفقا لقانون الاجراءات الجزائية رقم 3 لسنة 2001 وقانون السلطة القضائية رقم 1 لسنة 2002*، الهيئة المستقلة لحقوق الانسان (ديوان المظالم). سلسلة تقارير قانونية رقم 71 . تشرين الأول. 2009
- 85- خلفي، عبد الرحمن: *الاجراءات الجزائية في التشريع الجزائري المقرن، ط2*، دار بلقيس للنشر والتوزيع، الجزائر، 2016.
- 86- جرادة: عبد القادر صابر: *دستور الاستدلال والتحقيق الجنائي في التشريع الفلسطيني*. ط1. فلسطين. غزة: مكتبة افاق. 2012.

- 87- خليفة، خالد احمد إبراهيم: قبول وإجازة الأدلة الإلكترونية لجرائم الحاسوب في الدعوى الجنائية. المجلة العلمية جامعة الزعيم الأزهرى - السودان. عدد6. مجلد1. 2009.
- 88- حجازي، مصطفى احمد: المسؤولية المدنية للخبير القضائي. لا يوجد طبعة. مصر: دار الجامعة الجديدة للنشر. 2004.
- 89- فرغلي، عبد الناصر محمد محمود، و المسماري، محمد عبيد سيف سعيد: الاثبات الجنائي بالادلة الرقمية من الناحية القانونية والفنية دراسة تطبيقية مقارنة، (رسالة ماجستير منشورة) جامعة نايف العربية للعلوم الامنية. الرياض. السعودية.
- 90- قجاج، يوسف: الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والقانون. عدد28. 2015.
- 91- لموسخ، محمد : تنازع الاختصاص في الجرائم الإلكترونية، دفاثر السياسة والقانون. عدد2/143-157. لا يوجد سنة نشر.
- 92- محمد، ده شي صديق: القضاء الاداري وتنازع اختصاصاته مع القضاء العادي (دراسة تحليلية مقارنة). ط1. القاهرة: المركز القومي للإصدارات القانونية. 2016.
- 93- مراد، عبد الفتاح: التحقيق الجنائي التطبيقي. لا يوجد طبعة. الإسكندرية: دار الكتب والوثائق المصرية. لا يوجد سنة نشر.
- 94- مختاري، إكرام: الدليل في الجريمة الإلكترونية. مجلة المنارة للدراسات القانونية والادارية المغرب. عدد خاص. 2015.
- 95- مرسي، علاء زكي: سلطات النيابة العامة ومأمور الضبط القضائي في قانون الاجراءات الجزائية. طبعة اولى. المركز القومي للاصدارات القانونية. القاهرة. 2014.
- 96- موسى، مصطفى محمد: التحقيق الجنائي في الجرائم الالكترونية. ط1. القاهرة: مطابع الشرطة. 2008-2009.

97- مصطفى، يونس خالد عرب: جرائم الحاسوب دراسة مقارنة.(رسالة ماجستير منشورة). الجامعة الأردنية. عمان. الأردن. 1994.

98- نبيه، نسرين عبد الحميد: حقوق المتهم أمام سلطات الضبط القضائي. ط1. الإسكندرية: مكتبة الوفاء القانونية. 2010م.

99- نعيم جميل علاونة، فادي: مبدأ المشروعية في القانون الإداري و ضمانات تحقيقه. رسالة ماجستير منشورة. جامعة النجاح الوطنية. نابلس، فلسطين. 2011.

احكام المحاكم:

1- حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم 143 لسنة 2011

2- حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم 2014/1.

3- حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم 118 لسنة 2011.

4- قرار محكمة صلح قليلية جنح رقم 2016/1306

5- محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم 188 لسنة 2012

المراجع عن الشبكة العنكبوتية:

1- ارزقات، لؤي: الناطق الإعلامي باسم الشرطة الفلسطينية، فيديو منشور على موقع الشرطة الفلسطينية.

2- الشكري، عادل يوسف عبد النبي: الجريمة المعلوماتية وأزمة الشرعية الجزائية. الجريمة المعلوماتية. العدد السابع. 2008.

3- السموني: خالد الشرقاوي: *مكافحة الجرائم الإلكترونية على ضوء التشريعين الوطني والدولي*.
المجلة المغربية للإدارة المحلية والتنمية.

4- الأكاديمية العربية للعلوم المالية والمصرفية. *مسرح الجريمة والتحقيق فيها*،
عمان. 2016/8/31. الموقع الإلكتروني: <http://www.aabfs.org/ar>

5- العبودي، محسن. <http://www.eastlaws.com>. شبكة قوانين الشرق : 2016/9/5.

6- الشامل للأبحاث الإلكترونية، مبدأ المشروعية، بحث منشور على الانترنت
<http://droit.moontada.com/t70-topic>

7- جبريل، دانه: الجرائم الإلكترونية. الموقع الإلكتروني:
<http://7iber.com/society/facebook-cyber-crimes> .

8- جمال، فؤاد: *الجرائم المعلوماتية*، بحث منشور على الانترنت. www.lawofcrime.com

9- ريان، محمد عادل: *جرائم الحاسب الآلي وأمن البيانات*، مقال منشور على الانترنت على
الموقع التالي: www.anaharonline.com .

10- عرب، يونس: *جرائم الكمبيوتر والانترنت - المعنى والخصائص والصور وإستراتيجية
المواجهة القانونية*، بحث منشور على الانترنت على الموقع الإلكترونية: www.arablawn.org .

11- عقيدة، محمد أبو العلا: *التحقيق وجمع الأدلة في الجرائم الإلكترونية*. الموقع الإلكتروني:
www.kambota.forumarabia.net

12- قائد جهاز الضابطة الجمركية العميد إياد بركات ، تاريخ الزيارة 2016/9/25 على
الموقع الإلكتروني:

<http://www.palsafar.ps/%D8%A7%D9%84%D8%B3%D9%8A%D8%AF>

13- موقع المجلس القضاء الأعلى تاريخ الزيارة 2017/1/2، على الموقع الالكتروني:

<http://www.pgp.ps/ar/NC>

14- وكالة معا الإخبارية، تاريخ الزيارة 2017/1/2، على الموقع الالكتروني:

<http://www.maannnews.net/Content.aspx?id=884469>

15- موقع الشرطة الفلسطيني، التفتيش، تاريخ الزيارة 2017/6/15، الموقع الالكتروني:

<http://www.police.ps/ar/articles-action-show-id-105.htm>

16- موقع جريدة القدس، النيابة الالكترونية. تاريخ الزيارة 2018/5/2 الموقع الالكتروني

//http://www.alquds.com/articles/1484890275698412300 /الرشماوي في مقابلة

خاصة مع القدس.

17- موقع الحدث، الابلاغ عن الجرائم الالكترونية، تاريخ الزيارة 2018/5/2 الموقع

الالكتروني: <https://www.alhadath.ps/article/66802>

An-Najah National University
Faculty of Graduate Studies

Methods Of Exploring And Investigating Electronic Crimes

By
Adham Basem Nemer Baghdadi

Supervised
Dr. Anwar janem

**This Thesis is Submitted in Partial Fulfillment of the Requirements for
The Degree of Master of Public Law, Faculty of Graduate Studies,
An-Najah National University, Nablus – Palestine.**

2018

Methods Of Exploring And Investigating Electronic Crimes

By

Adham Basim Nimr Baghdadi

Supervised

Dr. Anwar janem

Abstract

After the spread of the use of the computer and the electronic network, and the proliferation of this increase in the level of the level of the ability of individuals to deal with these modern technologies to harness them to achieve their goals, show us the importance that enables police officers to deal with these techniques at the same level or better level and their ability to research and investigation On cybercrime. In this study, I will discuss the means of research and investigation of electronic crime from the perspective of the Palestinian laws, and the recent decision on electronic crimes No. 16 of 2017.

As electronic crime is emerging and the bells of danger are on its way, I will discuss in the first chapter the concept of cybercrime, its characteristics, and I will address the elements of cyber crime for its importance, the concept of research and investigation of cybercrime, and those who are authorized to investigate and investigate, Research and investigation and non-interference with the personal freedom of the person that laws and customs have preserved this human right.

In the second chapter, I will address the criminal investigation of traditional procedures for the investigation and investigation of electronic crimes, including the reporting of electronic crime, search and surveillance by various means, I will discuss the latest methods of criminal investigation through the cooperation of service providers with the investigative bodies to enable them to be easy to deal with computers and to inform them, and to intercept correspondence through electronic experts in case there was wearing a crime and this comes through allowing the objection of correspondence and registration and disclosure of confidentiality in case necessary Investigation and investigation, including some considered it a blatant attack on personal freedom And a means that can be useful in international cooperation to identify the offender because these crimes are intercontinental and can harm the economy and security of States. Recently, a law on cybercrime No. 16 of 2017 provides for cooperation with its theory in foreign countries with a view to accelerating the exchange of information. Which would ensure early warning of the discovery of cybercrime.

