



عمادة الدراسات العليا

جامعة القدس

التفتيش في الجرائم الإلكترونية

أشرف أحمد مصطفى عموري

رسالة ماجستير

القدس-فلسطين

1440هـ/2018م

التفتيش في الجرائم الإلكترونية

إعداد:

أشرف أحمد مصطفى عموري

بكالوريوس حقوق من جامعة تونس المنار / تونس

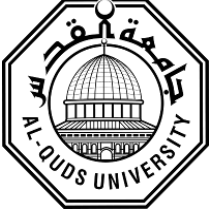
المشرف: د. حابس زيدات

قدمت هذه الرسالة استكمالاً لمتطلبات نيل الحصول على درجة الماجستير في

القانون الجنائي

كلية الدراسات العليا، جامعة القدس، فلسطين

1440 هـ / 2018 م



جامعة القدس
عمادة الدراسات العليا
برنامج الماجستير في القانون الجنائي

إجازة الرسالة

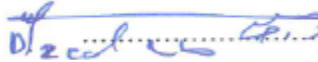


التفتيش في الجرائم الإلكترونية

اسم الطالب: أشرف أحمد مصطفى عموري

الرقم الجامعي: 21511955

المشرف: د. حابس زيدات

نوقشت هذه الرسالة بتاريخ: 8/12/2018، وأجيزت من قبل لجنة المناقشة المدرجة أسماؤهم وتوقيعاتهم:

1. رئيس لجنة المناقشة: د. حابس زيدات
التوقيع: 
2. ممتحناً داخلياً : د. عبد الله ناجرة
التوقيع: 
3. ممتحناً خارجياً : د. نائل طه
التوقيع: 

القدس – فلسطين

1440 هـ / 2018 م

الإهداء

أهدي هذا العمل المتواضع، إلى والدتي العزيزة، عنوان المحبة ومنبع الحنان الذي كان دعاؤها سر نجاحي، وإلى والدي العزيز، من زرع في قلبي روح الأمل والمثابرة،،،

وإلى أشقائي وزوجتي العزيزة

إلى من روت دماؤهم أرض فلسطين،،، الشهداء،،، رحمهم الله

إلى من ضحوا بحريتهم من أجل فلسطين،،، الأسرى الأبطال،،، فك الله قيدهم

أشرف أحمد عموري

إقرار:

أقر أنا معدة الرسالة أنها قدمت لجامعة القدس وأنها من نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد، وأنّ هذه الرسالة ككل، أو أي جزء منها لم يقدم لنيل أية درجة، أو لقب علمي، أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

التوقيع: _____

الاسم: أشرف أحمد مصطفى عموري

التاريخ: 2018 /12/8

الشكر والتقدير

قال الله تعالى في كتابه " لئن شكرتم لأزيدنكم " صدق الله العظيم

الآية(7) من سورة إبراهيم.

أشكر الله عز وجل أن أعانني ووفقني في كتابة هذه الرسالة.

كما أتقدم بجزيل الشكر والعرفان من أستاذي ومشرفي الدكتور حابس زيدات، أستاذ القانون الجنائي في جامعة القدس، لقبوله الإشراف على رسالتي، ومنحي من فكره الرشيد، ورأيه السديد، ولما بذله من جهد كان له الأثر الأكبر في إخراج هذه الدراسة إلى النور.

كما أشكر جميع أصدقائي وزملائي، كل بقلبه واسمه، الذين قدموا لي يد العون في إنجاز هذه الرسالة.

أشرف أحمد عموري

فهرس المحتويات

الصفحة	الموضوع
أ	الإقرار
ب	الشكر والتقدير
ج	فهرس المحتويات
ح	الملخص بالعربية
ي	الملخص بالإنجليزية
1	المقدمة
2	أهمية الدراسة
2	أهداف الدراسة
2	الإشكالية
3	منهج الدراسة
3	محددات الدراسة
3	الدراسات السابقة
4	تقسيم الدراسة
الفصل التمهيدي ماهية الجرائم الإلكترونية والتفتيش	
5	
6	المبحث الأول : ماهية الجرائم الإلكترونية
7	المطلب الأول : مفهوم الجريمة الإلكترونية
7	الفرع الأول : التعريفات التشريعية للجريمة الإلكترونية
8	الفرع الثاني : التعريفات الفقهية للجريمة الإلكترونية
9	المطلب الثاني : وسائل ارتكاب الجريمة الإلكترونية
10	الفرع الأول : الحاسوب
10	أولاً : نشأة الحاسوب
10	ثانياً : تسمية الحاسوب
10	ثالثاً : تسمية الحاسوب

11	رابعاً : مكونات الحاسوب
12	الفرع الثاني : الإنترنت
12	أولاً : ظهور الإنترنت.....
13	ثانياً : تعريف الإنترنت
13	المطلب الثالث : خصائص الجرائم الإلكترونية وطبيعتها القانونية
14	الفرع الأول : خصائص الجرائم الإلكترونية.....
14	الفرع الثاني : الطبيعة القانونية للجرائم الإلكترونية
14	أولاً : الجرائم الإلكترونية جرائم أموال
15	ثانياً : الجرائم الإلكترونية جرائم أشخاص
15	ثالثاً : الجرائم الإلكترونية جرائم إقتصادية
16	رابعاً : الجرائم الإلكترونية جرائم أمن دولة
16	خامساً : الجرائم الإلكترونية جرائم دولية
18	المبحث الثاني : ماهية التفتيش
19	المطلب الأول : مفهوم التفتيش وصوره
19	الفرع الأول : صور التفتيش
19	أولاً : التفتيش الوقائي
19	ثانياً : التفتيش الإداري
20	ثالثاً : التفتيش القضائي
20	الفرع الثاني : تعريف التفتيش
20	المطلب الثاني : الطبيعة القانونية للتفتيش وغايته وخصائصه
20	الفرع الأول : الطبيعة القانونية للتفتيش
20	أولاً : الطبيعة القانونية لتفتيش المنازل
21	ثانياً : الطبيعة القانونية لتفتيش الأشخاص
21	الفرع الثاني : خصائص التفتيش وغاية.....
21	أولاً : خصائص التفتيش
21	ثانياً : غاية التفتيش
23	الفصل الأول خصوصية التفتيش في الجرائم الإلكترونية

24	المبحث الأول : السلطة المختصة بالتفتيش في الجرائم الإلكترونية
25	المطلب الأول : تحديد السلطة المختصة بالتفتيش في الجرائم الإلكترونية
26	الفرع الأول : نيابة مكافحة الجرائم الإلكترونية
26	أولاً : تشكيل نيابة مكافحة الجرائم الإلكترونية
27	ثانياً : إختصاص نيابة مكافحة الجرائم الإلكترونية
32	الفرع الثاني : مأموري الضبط القضائي في الجرائم الإلكترونية
33	أولاً : وحدة مكافحة الجرائم الإلكترونية في جهاز الشرطة
34	ثانياً : وحدة مكافحة الجرائم الإلكترونية في الأجهزة الأخرى
35	ثالثاً : موظفو وزارة الإتصالات وتكنولوجيا المعلومات
35	المطلب الثاني : خصوصية السلطة المختصة في التفتيش بالجرائم الإلكترونية
36	الفرع الأول : خصوصية أعضاء نيابة مكافحة الجرائم الإلكترونية
37	أولاً : تأهيل قانوني
38	ثانياً : تأهيل فني
40	الفرع الثاني : خصوصية وحدات مكافحة الجرائم الإلكترونية
40	أولاً : أعضاء وحدة مكافحة الجرائم الإلكترونية
41	ثانياً : تأهيل فني
41	ثالثاً : تشكيل فريق للتفتيش في الجرائم الإلكترونية
42	رابعاً : التعاون مع الشرطة الدولية
43	خامساً : اللغة الانجليزية
45	المبحث الثاني : شروط التفتيش في الجرائم الإلكترونية
46	المطلب الأول : الضمانات المحددة للتفتيش في الجرائم الإلكترونية
46	الفرع الأول : سلطة التفتيش في الجرائم الإلكترونية
46	أولاً : السلطة الأصلية
48	ثانياً : السلطة المنابة
49	الفرع الثاني : سبب التفتيش في الجرائم الإلكترونية
49	أولاً : وقوع جريمة إلكترونية
50	ثانياً : تحديد المجرم الإلكتروني
51	ثالثاً : مبررات إجراء التفتيش
52	الفرع الثالث : محل التفتيش في الجرائم الإلكترونية

52	أولاً : تفتيش الأشخاص
55	ثانياً : تفتيش الأماكن
58	ثالثاً : تفتيش وسائل تكنولوجيا المعلومات
58	المطلب الثاني : الضمانات المقيدة للتفتيش في الجرائم الإلكترونية
59	الفرع الأول : تسبيب أمر التفتيش
59	أولاً : أمر التفتيش
59	ثانياً : مذكرة التفتيش
61	الفرع الثاني : وقت التفتيش
61	أولاً : التفتيش في النهار
62	ثانياً : التفتيش بالليل
65	الفرع الثالث : شهود ومحضر التفتيش
65	أولاً : شهود التفتيش
66	ثانياً : محضر التفتيش
70	الفصل الثاني خصوصية إجراءات التفتيش وأثاره في الجرائم الإلكترونية.
71	المبحث الأول : خصوصية إجراءات التفتيش في الجرائم الإلكترونية
72	المطلب الأول : الإجراءات التحضيرية للتفتيش في الجرائم الإلكترونية
72	الفرع الأول : تحديد محل التفتيش في الجرائم الإلكترونية
73	أولاً : تحديد وسائل تكنولوجيا المعلومات
74	ثانياً : تحديد مكان وجود وسائل تكنولوجيا المعلومات
75	الفرع الثاني : آلية التفتيش في الجرائم الإلكترونية
75	أولاً : الفريق الفني للتفتيش في الجرائم الإلكترونية
76	ثانياً : فريق الإقترحام للتفتيش في الجرائم الإلكترونية
78	المطلب الثاني : الإجراءات الفنية للتفتيش في الجرائم الإلكترونية
78	الفرع الأول : تفتيش مكونات وسائل تكنولوجيا المعلومات
79	أولاً : تفتيش المكونات المادية لوسائل تكنولوجيا المعلومات
79	ثانياً : تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات

82	الفرع الثاني : تحديات إجراءات تفتيش وسائل تكنولوجيا المعلومات
83	أولاً : صعوبات فنية تقنية
84	ثانياً : صعوبات جغرافية
88	المبحث الثاني : آثار التفتيش في الجرائم الإلكترونية
89	المطلب الأول : آثار التفتيش القانوني في الجرائم الإلكترونية
90	الفرع الأول : ضبط الأدلة الإلكترونية
91	أولاً : تعريف الضبط
93	ثانياً : ضبط الأدلة الإلكترونية المادية
94	ثالثاً : ضبط الأدلة الإلكترونية الغير مادية
95	الفرع الثاني : محضر الضبط وحفظ الأدلة في الجرائم الإلكترونية
96	أولاً : محضر الضبط في الجرائم الإلكترونية
97	ثانياً : حفظ الأدلة الإلكترونية
99	ثالثاً : التصرف بالأدلة الإلكترونية المضبوطة
100	المطلب الثاني : آثار التفتيش غير القانوني في الجرائم الإلكترونية
101	الفرع الأول : البطلان
101	أولاً : تعريف البطلان
102	ثانياً : مخالفة ضمانات التفتيش يرتب البطلان المطلق
103	ثالثاً : مخالفة ضمانات التفتيش يرتب البطلان النسبي
103	رابعاً : ضوابط التفرقة بين البطلان المطلق والنسبي
104	خامساً : آثار بطلان التفتيش
105	الفرع الثاني : العقوبات الجزائية والتأديبية
105	أولاً : العقوبات الجزائية
106	ثانياً : العقوبات التأديبية
108	الخاتمة
109	أولاً : النتائج
110	ثانياً : التوصيات
112	قائمة المصادر والمراجع

الملخص

شهد العالم في السنوات الأخيرة تطورا هائلا في مجال الإتصالات وتكنولوجيا المعلومات، وأصبح الإنسان يعتمد على هذه التكنولوجيا في حياته اليومية وتحفظ خصوصيته وسره، وقد أساء البعض استخدام هذه التكنولوجيا الحديثة بالإعتداء على المجتمع وتهديد أمنه وإستقراره، ممّا أظهر لنا جرائم جديدة وهي الجرائم الإلكترونية، " جرائم التقنية العالمية".

التفتيش، هو أحد الطرق للبحث عن الأدلة، وينصب في الجرائم الإلكترونية على وسائل تكنولوجيا المعلومات، وتفتيش هذه الوسائل بحاجة إلى سلطة متخصصة وأدوات تقنية مساعدة لإستخراج الأدلة الإلكترونية وضبطها وحفظها، وهذا العمل صعب وشاق لا يستطيع شخص واحد القيام به، وإنما يحتاج إلى فريق متخصص متكامل، مع ضرورة مراعاة الضمانات المقررة للتفتيش والتي أقرها الدستور والقانون، وجاءت بها الإتفاقيات الإقليمية والدولية.

إنّ هذه الدراسة بعنوان " التفتيش في الجرائم الإلكترونية "، وتكمن أهميتها في الكشف عن مدى إنترام السلطة المختصة بمراعاة الضمانات المقررة للتفتيش، وقد جاءت الإشكالية بالسؤال التالي، هل وفق المشرع الفلسطيني في وضع نظام قانوني متكامل يراعي خصوصية إجراءات التفتيش والضبط في الجرائم الإلكترونية، وخلق توازن بين حق الإنسان بالخصوصية وحق المجتمع في معاقبة المجرمين؟، والهدف من هذه الدراسة يتمثل بهدف عام هو، توضيح مفهوم التفتيش وصوره وبيان خصائصه وتحديد طبيعته القانونية والغاية منه، وأهداف خاصة تتمحور في إظهار خصوصية التفتيش في الجرائم الإلكترونية وبيان كيفية الحصول على الأدلة الإلكترونية وضبطها وتخزينها، وحتى يجيب الباحث عن إشكالية الدراسة إتبع المنهج الوصفي التحليلي المقارن، من خلال تحليل النصوص الخاصة بالتفتيش والضبط الواردة في القرار بقانون رقم (10) لسنة 2018، بشأن الجرائم الإلكترونية الفلسطيني، وقانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001، والقوانين المقارنة.

تناول الباحث في الفصل التمهيدي ماهية الجرائم الإلكترونية والتفتيش، وخصص المبحث الأول لتعريف الجرائم الإلكترونية التشريعية والفقهية، ووسائل إرتكابها، وبيان خصائصها ومميزاتها

وطبيعتها القانونية، وتناولنا في المبحث الثاني ماهية التفتيش، حيث قمنا بتعريفه، وبيننا صورته، وطبيعته القانونية وخصائصه والغاية من اللجوء إليه.

تناول الباحث في **الفصل الأول**، خصوصية التفتيش في الجرائم الإلكترونية، وبحثنا في **المبحث الأول** السلطة المختصة بالتفتيش في الجرائم الإلكترونية، وفي **المبحث الثاني** شروط التفتيش في الجرائم الإلكترونية، أما **الفصل الثاني** من الرسالة، تناولنا، خصوصية إجراءات التفتيش والضبط في الجرائم الإلكترونية، وبحثنا في **المبحث الأول** خصوصية إجراءات التفتيش في الجرائم الإلكترونية، وفي **المبحث الثاني** آثار التفتيش في الجرائم الإلكترونية.

وفي نهاية الدراسة توصل الباحث إلى **نتائج** أهمها، أن المشرع الفلسطيني في قانون الجرائم الإلكترونية لم يقر جميع ضمانات التفتيش التي نص عليها قانون الإجراءات الجزائية، وأن التفتيش في الجرائم الإلكترونية من أخطر وأدق إجراءات التحقيق كون أسرار الناس وخصوصيتهم أصبحت مخزنة في وسائل تكنولوجيا المعلومات، وهو بحاجة إلى نظام إجرائي متكامل، وسلطة متخصصة مدربة ومؤهلة فنيا تكون مسلحة بأدوات إلكترونية لإجرائه واستخراج الأدلة وضبطها وحفظها، والتغلب على الحراسة الإلكترونية، وهذا التفتيش إجراء صعب شاق يحتاج إلى فريق متكامل، ويمكن أن يمتد خارج حدود الدولة، ويحتاج إلى تعاون بين الدول، ولقد أوصى الباحث في نهاية دراسته إلى وضع نظام إجرائي خاص للتفتيش في الجرائم الإلكترونية يقر جميع ضمانات التفتيش، والنص صراحة في القانون على أن الوسائل غير المادية قابلة للتفتيش والضبط، وتحديد مكان تخزينها، والسماح للسلطة المختصة بتجاوز التفتيش لحدود الدولة، وإنشاء محكمة مختصة للنظر في الجرائم الإلكترونية يكون أعضائها مؤهلين، وإصدار دليل لإجراءات التفتيش والضبط في الجرائم الإلكترونية، وإنشاء مجلس وطني لمكافحة الجرائم الإلكترونية.

Inspection of Electronic Crimes

Preparation by: Ashraf Ahmad Mostafa Amouri

Supervised :Dr. Habes Zedat

Abstract

In recent years, the world has witnessed a tremendous development in the field of communications and information technology, and people are relying on this technology in their daily lives and preserving their privacy and happiness. Some have abused this modern technology to attack society and threaten its security and stability, “Crimes of global technology” .

Inspection is one of the ways to search for evidence. It focuses on electronic crimes on the means of information technology. The inspection of these means requires specialized authority and technical tools to assist in the extraction, control and preservation of electronic evidence. This work is difficult and hard that one person cannot do. Integrated, with the need to take into consideration the safeguards prescribed for inspection and approved by the Constitution and the law, and came by the regional and international conventions.

This study is entitled "Inspection of Electronic Crimes", whose importance lies in disclosing the extent of the obligation of the competent authority to take into account the guarantees of inspection, The problem has come up with the following question: Is the Palestinian legislator in the development of an integrated legal system that takes into account the specificity of the procedures of inspection and control of cybercrimes, and the creation of a balance between the human right to have privacy and the right of society to punish criminals? The aim of this study is to clarify the concept of inspection, its image, its characteristics, its legal nature and its purpose. The objectives of this study are to show the privacy of the inspection of electronic crimes and to explain how to obtain, and store electronic evidence through what was explained in Law No (10) for the year 2018, on the Palestinian electronic crimes, And Palestinian Penal Procedures Law No. (3) Of 2001, and the comparative laws.

The researcher dealt with the computer in the first section, the Internet in the second section, the electronic crime and its characteristics in the third section, its legal nature in section 4, and the methods of proving it to the inspection, which we identified, reviewed its characteristics, and determined its legal nature and purpose in section 5.

In the first chapter of the thesis, the researcher examined the specificity of the investigation of electronic crimes. In the first section the competent authority to inspect electronic crimes was examined.

The second part of the thesis dealt with the specificity of the procedures of the search and control of electronic crimes. In the first part, we discussed the specificity of the procedures for searching electronic crimes.

At the end of the study, the researcher concluded that the Palestinian legislator in the Electronic Crimes Law did not approve all the inspection guarantees stipulated in the Code of Criminal Procedure, and that the inspection of electronic crimes is one of the most serious and accurate procedures of investigation. The need of an integrated procedural system, and a specialized trained and technically qualified authority, armed with electronic tools to conduct, extract and maintain evidence, and overcome electronic custody. This inspection is a difficult procedure that needs an integrated team, and can extend beyond the borders of the state, and needs Li cooperation between States.

At the end of his study, the researcher also recommended the establishment of a special procedural system for the inspection of electronic crimes, which guarantees the inspection guarantees, the explicit provision in the law that the non-material means are subject to inspection and seizure, the location of their storage, the permission of the competent authority, and the creation of a manual for electronic crime investigation and seizure procedures and the establishment of a national council to combat cybercrime.

مقدمة.

إذا كان التفتيش أمراً ممقناً، فإن الجريمة تفوقه ممقناً⁽¹⁾، حيث تتطور أساليب إرتكاب الجريمة بتطور الحياة بنواحيها المختلفة، وفي عصرنا الحالي ومع تطور التكنولوجيا الحديثة أصبحت الجرائم التقليدية ترتكب بطرق غير تقليدية، وظهر في هذا الكون عالم خفي افتراضي أوجد لنا جرائم مستحدثة لم تكن معروفة سابقاً، مما أدى ذلك إلى ظهور فرع جديد في القانون الجزائي، وهو الجرائم الإلكترونية.

شهد العالم في نصف القرن العشرين تطوراً هائلاً في مجال الاتصالات وتكنولوجيا المعلومات، وتجلّى هذا التطور في اختراع الحاسوب، وتبعه ظهور الإنترنت الذي جعل البعيد قريباً، وأصبح العالم الكبير متصل مع بعضه البعض كأنه يجلس في حديقة صغيرة مليئة بالورود، وأستغل البعض هذه التقنيات الحديثة التي ظهرت لتسهيل حياة الناس، لزرع الأشواك في هذه الحديقة للقيام بأعمال تمس الأشخاص وحقوقهم وتعدي عليها من ناحية، والقيام بأعمال تمس أمن وسلامة الدول واقتصادها، والأمن والسلم العالمي من ناحية أخرى، مما دفع المشرعين في بعض دول العالم لتجريم تلك الأفعال كون قانون العقوبات العام والقوانين الجنائية الأخرى قاصرة عن معالجتها، فسارعت بعض الأنظمة إلى إدخال تعديلات على قانون العقوبات، وإضافة فصول لتجريم تلك الأعمال كقانون العقوبات الفرنسي⁽²⁾ والايطالي⁽³⁾، والبعض الأخر جرم تلك الأفعال بقوانين مستقلة كالقانون السعودي والأردني والقطري والفلسطيني، حيث سنتعرض لتلك القوانين لاحقاً، وما زال هناك بعض دول لم تصدر أي تشريعات تعالج تلك الجرائم محتجة بأن القوانين الجنائية النافذة قادرة على معالجة هذه الجرائم الحديثة كالقانون المصري واللبناني.

الجرائم الإلكترونية تُرتكب بواسطة وسائل تكنولوجيا المعلومات، وهذه الوسائل متعددة ومتنوعة ولكل منها خصوصية مختلفة عن الأخرى، وهي منتشرة في جميع أنحاء العالم ويمكن إرتكاب الجريمة الإلكترونية من خلال استخدامها من أي مكان في هذا العالم، لذلك تحتاج هذه الجرائم إلى طرق خاصة لجمع أدلتها نظراً لخصوصيتها التقنية سواء في مرحلة جمع الإستدلالات أو في

(1) عوض، رمزي رياض، الإجراءات الجنائية في القانون الأنجلوأمريكي، دار النهضة العربية، القاهرة، 2009، ص118.

(2) أنظر المادة (323) من قانون العقوبات الفرنسي. Code pénal français, 1992.

(3) أنظر المادة (615 / 3+4+5) من قانون العقوبات الإيطالي. Codice penale italiano, 1930.

مرحلة التحقيق الإبتدائي أو النهائي.

التفتيش في الجرائم الالكترونية، هو أحد الوسائل التي يمكن أن تستخدمها سلطة التحقيق للوصول إلى الأدلة، وقد أقرت الدساتير والقوانين ضمانات لإجراءات التفتيش يجب مراعاتها من قبل السلطات العامة، حفاظاً على حقوق الإنسان وحرياته الأساسية وحفاظاً على أسرارهِ وخصوصيته، بأن لا تمتد يد أعضاء السلطة العامة إلى هذه الأسرار إلا من خلال القانون.

إن وسائل تكنولوجيا المعلومات تحوي أسرار الناس وخصوصيتهم، وتفتيش هذه الوسائل يحتاج إلى سلطة متخصصة مؤهلة فنياً، وطرق خاصة وأدوات تقنية لإستخراج الأدلة الالكترونية، وهذه الأدلة تحتاج إلى طرق خاصة لضبطها وتخزينها.

• أهمية الدراسة.

تكمن أهمية الدراسة في تحديد النصوص القانونية الناظمة لإجراءات التفتيش في الجرائم الإلكترونية، لكشف مدى الإلتزام بضمانات التفتيش.

أهداف الدراسة.

الأهداف العامة: توضيح مفهوم التفتيش، وصوره، وخصائصه، وطبيعته القانونية، وإجراءاته، والغاية منه.

الأهداف الخاصة: إظهار خصوصية التفتيش في الجرائم الإلكترونية، وبيان كيفية الحصول على الأدلة الإلكترونية، وطرق ضبطها وحفظها.

• إشكالية الدراسة.

هل وفق المشرع الفلسطيني في وضع نظام قانوني متكامل يراعي خصوصية إجراءات التفتيش والضبط في الجرائم الإلكترونية، وخلق توازن بين حق الإنسان بالخصوصية وحق المجتمع في معاقبة المجرمين؟

• منهج الدراسة.

سيتبع الباحث المنهج الوصفي التحليلي المقارن، وهي دراسة تحليلية لنصوص القانون الخاصة بالتفتيش والضبط في الجرائم الإلكترونية، للوصول إلى معرفة مدى نجاح المشرع الفلسطيني في وضع نظام متكامل للتفتيش في الجرائم الإلكترونية، وبالتالي الوصول إلى إجابة على إشكالية البحث.

• محددات الدراسة.

محددات الدراسة هي قانون الإجراءات الجزائية وقانون الجرائم الإلكترونية الفلسطيني، والقوانين المقارنة، والإتفاقيات الدولية والإقليمية ذات العلاقة بالجرائم الإلكترونية، والقرارات القضائية، والآراء والنظريات الفقهية.

• الدراسات السابقة.

1- الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة، للباحث يوسف خليل يوسف العفيفي، الجامعة الإسلامية، غزة، فلسطين، رسالة ماجستير، 2013.

هدفت هذه الدراسة إلى التعريف بالجريمة الإلكترونية، وبيان خصائصها، وطبيعتها القانونية، وطرق جمع الأدلة في مرحلة الإستدلالات، والتحقيق الإبتدائي، والتعرف على آلية تفتيش مكونات الحاسوب المادية والغير مادية، وضبطها، والمشكلات التي تواجه القائم بالتفتيش.

2- المشكلات العلمية والقانونية للجرائم الإلكترونية، دراسة مقارنة، للباحث عبد الله دغش العجمي، جامعة الشرق الأوسط، عمان، الأردن، رسالة ماجستير، 2014.

هدفت هذه الدراسة إلى تحديد مفهوم الجريمة الإلكترونية، وطبيعتها القانونية، والحلول التشريعية لمواجهة الجريمة الإلكترونية، وضرورة التعاون الدولي لمواجهتها، والحلول العملية لمواجهة مشكلات التفتيش والضبط في تلك الجرائم.

3- خصوصية الجرائم المعلوماتية، للباحثة نداء نائل فايز المصري، جامعة النجاح الوطنية، نابلس، فلسطين، رسالة ماجستير، 2017.

هدفت هذه الدراسة إلى بيان خصوصية الجرائم الإلكترونية على المستوى الموضوعي (التجريم والعقاب)، وعلى المستوى الإجرائي (مرحلة التحقيق الابتدائي والنهائي).

• **تقتضي الإجابة على إشكالية الدراسة تقسيمها إلى:**

الفصل التمهيدي: ماهية الجرائم الإلكترونية والتفتيش.

الفصل الأول: خصوصية التفتيش في الجرائم الإلكترونية.

الفصل الثاني: خصوصية إجراءات التفتيش والضبط في الجرائم الإلكترونية.

الفصل التمهيدي

ماهية الجرائم الإلكترونية والتفتيش

تمهيد وتقسيم.

الجرائم الإلكترونية، عُرِفَت نتيجة التطور التكنولوجي الذي ظهر للبشرية لتيسير حياته، وأصبح الإنسان يستخدمها في جميع نواحي الحياة.

إن وسائل تكنولوجيا المعلومات متعددة ومتنوعة، وتتجلى صورها بالحاسوب، والهواتف النقالة الذكية التي تعمل بالتقنية الحديثة، والأجهزة الإلكترونية بشتى أنواعها، وإتصال تلك الوسائل ببعضها البعض عن طريق الشبكات العامة والخاصة أو الشبكات العالمية كشبكة الإنترنت، ووسائل تخزين المعلومات والبيانات الصلبة والمرنة، وأي وسائل الكترونية تعمل بالتقنية الحديثة.

نظراً لإنتشار وسائل تكنولوجيا المعلومات في جميع أرجاء العالم، قام البعض بإستغلال نقاط ضعفها للإعتداء عليها وتدميرها، أو الإعتداء على الناس وأموالهم، أو تعريض سلامة الدولة وإقتصادها للخطر، إمّا بقصد التسلية أو حباً للمعرفة، أو بقصد تحقيق مصالح شخصية، مما أدى إلى ظهور الجرائم الإلكترونية التي تمتاز بخصائص تستمدّها من طبيعة تلك الوسائل الإلكترونية وهي مختلفة تماماً عن الجرائم الأخرى.

إن التفتيش أحد الإجراءات التي قد تلجأ إليها سلطة التحقيق للوصول إلى الأدلة المطلوبة لإظهار الحقيقة، ولكن هذا الإجراء يمس خصوصية الناس بالاطلاع على أسرارهم المخزنة في وسائل تكنولوجيا المعلومات، ولكن يجب أن يتم هذا الإجراء وفق ما رسمه القانون. حيث يقتضي تقسيم المبحث التمهيدي إلى مطلبين.

المبحث الأول: ماهية الجرائم الإلكترونية.

المبحث الثاني: ماهية التفتيش.

المبحث الأول

ماهية الجرائم الإلكترونية

يختلف تعريف الجريمة الإلكترونية نظراً لإختلاف تسمياتها، فالإتفاقية العربية سمتها جرائم تقنية المعلومات⁽¹⁾، وسار على دريها المشرع العماني⁽²⁾ والبحريني⁽³⁾ والإماراتي⁽⁴⁾ والكويتي⁽⁵⁾، والبعض سماها جرائم المعلوماتية، كالمشرع السعودي⁽⁶⁾ والسوداني⁽⁷⁾ والسوري⁽⁸⁾، والبعض الآخر سماها الجرائم الإلكترونية، كالمشرع الفلسطيني⁽⁹⁾ والقطري⁽¹⁰⁾ والأردني⁽¹¹⁾، ولكن الإتفاقية الأوروبية سمتها سمتها الجرائم السيبرانية⁽¹²⁾.

أما المشرع الإنجليزي أطلق عليها جريمة إساءة إستخدام الحاسوب⁽¹³⁾، والبعض أطلق عليها مصطلح "جرائم التقنية العالمية" كون هذا المصطلح شامل ويدخل ضمنه كل التسميات السابقة⁽¹⁴⁾. الباحث سيستخدم مصطلح الجريمة الإلكترونية في البحث، للدلالة على كل التسميات السابقة، ويرى الباحث أن الإختلاف في تسمية الجريمة الإلكترونية طبيعي، كونها جريمة حديثة أوجدها المشرع لظروف تتعلق بتنظيم المجتمع الإلكتروني الحديث ويختلف النظر إليها من دولة

-
- (1) الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادرة عن جامعة الدول العربية، بتاريخ 2010/12/21، بالقاهرة، دخلت حيز النفاذ بتاريخ 2014/2/7، صادقت عليها دولة فلسطين بتاريخ 2013/5/21.
- (2) قانون مكافحة جرائم تقنية المعلومات العماني، الصادر بالمرسوم السلطاني، رقم (12) لسنة 2011.
- (3) قانون جرائم تقنية المعلومات البحريني، رقم (60) لسنة 2014.
- (4) قانون مكافحة جرائم تقنية المعلومات الإماراتي، رقم (5) لسنة 2012.
- (5) قانون مكافحة جرائم تقنية المعلومات الكويتي، رقم (63) لسنة 2015.
- (6) قانون نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم (م/17) لسنة 2007.
- (7) قانون جرائم المعلوماتية السوداني، رقم (13) لسنة 2007.
- (8) قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري، الصادر بالمرسوم التشريعي، رقم (17) لسنة 2012.
- (9) قرار بقانون بشأن الجرائم الإلكترونية الفلسطينية، رقم (10) لسنة 2018.
- (10) قانون مكافحة الجرائم الإلكترونية القطري، رقم (14) لسنة 2014.
- (11) قانون الجرائم الإلكترونية الأردني، رقم (27) لسنة 2015.
- (12) الإتفاقية الأوروبية لمكافحة الجرائم السيبرانية، اتفاقية بودابست، الصادرة عن الإتحاد الأوروبي بتاريخ 2001/11/23، بودابست، المجر.
- (13) قانون إساءة إستخدام الحاسوب البريطاني. Computer Misuse Act 1990
- (14) يوسف، أمير فرج، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2008، ص 107.

إلى دولة أخرى، لوجود تفاوت بين الدول في استخدام التكنولوجيا الحديثة، فبعض الدول متطورة في استخدامها، كالولايات المتحدة الأمريكية وبريطانيا وكندا والمانيا، والبعض الآخر أقل منها تطوراً كأغلب الدول العربية والآسيوية والإفريقية. حيث سنتناول مفهوم الجريمة الإلكترونية في المطلب الأول، ووسائل ارتكابها في المطلب الثاني، وخصائصها وطبيعتها القانونية في المطلب الثالث.

المطلب الأول

مفهوم الجريمة الإلكترونية.

الجريمة لغة، إشتقت من الجرم، وتعني التعدي أو الذنب⁽¹⁾، وعرفت الشريعة الإسلامية الجريمة، بأنها إتيان فعل محرم معاقب على فعله، أو ترك معاقب تركه، وله جزاء عاجل في الدنيا وجزاء أجل في الآخرة⁽²⁾، أما الجريمة فقهاً، عرفها الفقيه جازو بأنها " كل فعل أو ترك يعاقب عليه القانون بعقوبة جنائية ولا يبرره استعمال حق ولا أداء واجب"⁽³⁾. حيث سنتناول التعريفات التشريعية للجريمة الإلكترونية في الفرع الأول، والتعريفات الفقهية في الفرع الثاني.

الفرع الأول: التعريفات التشريعية للجريمة الإلكترونية.

الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لم تُعرف الجريمة الإلكترونية، وسار على نهجها المشرع الفلسطيني، والأردني والبحريني، والسوداني والإماراتي.

بعض القوانين العربية المقارنة عرفت الجريمة الإلكترونية، وأسهلها ما ورد في المادة (1/ج) من قانون مكافحة جرائم تقنية المعلومات العماني، والذي عرفها بأنها الجرائم المنصوص عليها في هذا القانون، ولكن المشرع الكويتي عرفها في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات

⁽¹⁾ لسان العرب، للإمام العلامة أبي الفضل، جمال الدين محمد بن مكرم ابن منظور الإفريقي المصري ، المجلد الثاني عشر، عشر، حرف الميم، فصل الجيم، دار صادر، بيروت، بدون سنة نشر، ص 91.

⁽²⁾ الحلبي، خالد عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 27.

⁽³⁾ مشار إليه في كتاب عبد الملك، جندي، الموسوعة الجنائية، ط2، ج3، دار العلم للجميع، بيروت، بدون سنة نشر، ص 6.

بأنها " كل فعل يرتكب من خلال إستخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات"، وبالتعمن في هذا النص نجد أن المشرع الكويتي إعتد على تعريفه للجريمة الإلكترونية على معيار وسيلة إرتكابها، وبالإعتماد على نفس المعيار عرفها المشرع السعودي في المادة(8/1) من قانون نظام مكافحة جرائم المعلوماتية، وبشكل مشابه عرفها المشرع القطري في المادة الأولى من قانون الجرائم الإلكترونية.

أما المشرع السوري إعتد في تعريفه للجريمة الإلكترونية على المعيار المزدوج، وهو وسيلة إرتكاب الجريمة ومحلها، فعرفها في المادة الأولى من قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية بأنها "جريمة ترتكب بإستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة"، وقد أكدت التعليمات التوضيحية والتنفيذية لهذا القانون على هذا المعيار⁽¹⁾.

الفرع الثاني: التعريفات الفقهية للجريمة الإلكترونية.

جاءت التعريفات الفقهية للجريمة الإلكترونية مختلفة، فالبعض إعتد في تعريفها على وسيلة إرتكابها وعرفها بأنها " أي سلوك غير مشروع يرتبط بإساءة إستخدام الحاسب الآلي ويؤدي إلى تحقيق أغراض غير مشروعة"⁽²⁾، وكذلك عرفت بأنها "السلوك الإجرامي الذي يرتكب عبر الفضاء الإلكتروني بالإستعانة بالخدمات المعلوماتية المضافة لجهاز الهاتف المحمول سواء بإستخدام شبكة الإنترنت أو شبكة إتصال الهاتف"⁽³⁾. والبعض الأخر، عرفها بالإستناد إلى موضوعها، حيث عرفها الفقيه ماس بأنها "الإعتداء القانوني الذي يرتكب بواسطة المعلومات الحاسوبية بغرض تحقيق الجريمة"⁽⁴⁾. وكذلك عرفت الجريمة الإلكترونية بشكل أقرب إلى التعريف العام للجريمة، بأنها " كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بإستخدام أية تكنولوجيا أو تقنية

(1) أنظر المادة (ت 15) من التعليمات التوضيحية والتنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري، الصادرة بالقرار رقم (290)، عن وزير الإتصالات والتقانة السوري، بتاريخ 2012/5/7.

(2) حجازي، عبد الفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية ودار شتات للنشر والبرمجيات، المحلة الكبرى، 2007، ص385.

(3) أحمد، طارق عفيفي صادق، الجرائم الإلكترونية، جرائم الهاتف المحمول، دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2015، ص33.

(4) مشار إليه في كتاب المناعسة، أسامة احمد، والزعيبي، جلال محمد، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، ط2، دار الثقافة للنشر والتوزيع، عمان، 2014، ص 70.

حديثاً لتحقيق النتيجة الإجرامية التي يؤتمها المشرع⁽¹⁾، ولكن البعض عرف الجريمة الإلكترونية بالإستناد إلى مدى معرفة إستخدام الحاسوب، ووضع تعريف للجريمة بالإعتماد على مدى قدرة الفاعل بإستخدام وسائل تكنولوجيا المعلومات، وعرفها بأنها "جريمة تتطلب لإقترافها أن تتوفر لدى فاعلها معرفة بتقنية النظام المعلوماتي⁽²⁾، وقد أخذت وزارة العدل الأمريكية بهذا الاتجاه عندما عرفت الجريمة المعلوماتية بأنها "أية جريمة يكون فاعلها ذا معرفة فنية بالحاسوب تمكنه من إرتكابها⁽³⁾. يرى الباحث وجود صعوبة في إيجاد تعريف شامل للجريمة الإلكترونية، ولكن نرى أن المشرع السوري كان موفقاً في تعريف الجريمة الإلكترونية، حيث جاءت صياغة النص شاملة، يستوعب جميع الجرائم التي ترتكب بواسطة تكنولوجيا المعلومات.

المطلب الثاني

وسائل إرتكاب الجريمة الإلكترونية

وسائل إرتكاب الجريمة الإلكترونية متعددة ومتنوعة، وهي متمثلة في وسائل تكنولوجيا المعلومات، التي عرفها المشرع الفلسطيني بالمادة الأولى من قانون الجرائم الإلكترونية بأنها " أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية أو أي وسيلة أخرى سواء كانت مادية أم غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أي قدرة تخزين بيانات أو إتصالات تتعلق أو تعمل بالإقتران مع مثل هذه الوسائل".

المجرم الإلكتروني⁽⁴⁾، يستخدم وسائل تكنولوجيا المعلومات لإرتكاب الجريمة الإلكترونية، والذي يعرف بأنه الشخص الذي لديه دراية ومهارات تقنية في مجال الحاسبات وأمن المعلومات تمكنه من

(1) الشناوي، محمد، جرائم النصب المستحدثة، الإنترنت وبطاقة الإئتمان والدعاية التجارية الكاذبة، دار الكتب القانونية، المحلة الكبرى، مصر، 2008، ص71.

(2) الملط، أحمد خليفة، الجرائم المعلوماتية، دراسة مقارنة، ط2، دار الفكر الجامعي، الإسكندرية، 2006، ص86.

(3) مشار إليه في كتاب حسين، سامي جلال فقي، التفيتش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، المحلة الكبرى، 2011، ص22.

(4) أحمد، هلاي عبد اللاه، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، القاهرة، 2015، ص176+177.

القيام بالإختراق والتخريب والتجسس وفك وكسر الشيفرات عبر شبكة الإنترنت وقد تم تصنف المجرمين الإلكترونيين إلى عدة أصناف، بالنظر إلى أهدافهم من إرتكاب الجريمة، فالمخترقون المتطفلين، صغار السن دافعهم هو التحدي، والمحترفون، يكون هدفهم تحقيق أغراض محددة، والهاقدون هدفهم الثار والإنتقام⁽¹⁾. حيث سنتناول الحاسوب في الفرع الأول، والإنترنت في الفرع الثاني.

الفرع الأول: الحاسوب. الحاسوب، هو أحد وسائل تكنولوجيا المعلومات التي يستخدمها المجرم لإرتكاب جريمة إلكترونية، ويمكن أن يكون الحاسوب محل للجريمة الإلكترونية. حيث سنتناول نشأة الحاسوب في الفقرة الأولى، والتسمية في الفقرة الثانية، وتعريفه في الفقرة الثالثة، ومكوناته في الفقرة الرابعة.

أولاً: نشأة الحاسوب. يعود نشأة الحاسوب إلى عام 1937 عندما صنعت جامعة هارفارد الأمريكية أول حاسوب آلي، وتم تطوير هذا الجهاز برعاية وزارة الدفاع الأمريكية، وأصبح منذ عام 1946 سر من أسرار الدفاع ويستخدم للأغراض الحربية وزنته (30 طناً)⁽²⁾، واستمر تطوير هذا الجهاز ومكوناته إلى أن وصل إلى أحجام صغيرة في وقتنا الحاضر.

ثانياً: تسمية الحاسوب. تعددت الترجمات العربية للمصطلح الانجليزي (computer)، حيث سمي بعدة تسميات منها كمبيوتر، حاسوب، حاسب آلي، ناظمة آلية، وقد أقرت المنظمة العربية للمواصفات والمقاييس كلمة حاسوب كمقابل لكلمة (computer)⁽³⁾، وأخذ المجمع اللغوي في الأردن بكلمة حاسوب، أما المجمع المصري للغة العربية إستخدم كلمة الحاسب⁽⁴⁾. الباحث سيستخدم كلمة حاسوب في البحث للدلالة على الكمبيوتر.

ثالثاً: تعريف الحاسوب. المشرع الفلسطيني لم يعرف الحاسوب في قانون الجرائم الإلكترونية، ولكن

(1) طه، محمود احمد، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، دراسة مقارنة، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2016/2017، ص14 وما بعدها.

(2) موقع ويكيبيديا، الموسوعة الحرة على الإنترنت، تاريخ الدخول 2018/3/1، الساعة 22:30.

(3) الديري، عبد العال وإسماعيل، محمد صادق، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة، مع أحدث التشريعات العربية في مجال مكافحة تكنولوجيا المعلومات، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص15.

(4) الطويلة، علي حسن محمد، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، عالم الكتب الحديث، اربد عمان، 2004، ص 17.

أشار إليه بشكل ضمنى في المادة الأولى عند تعريفه تكنولوجيا المعلومات كونه أحد هذه الوسائل، ولكن المشرع السوري عرف الحاسوب بشكل صريح في المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، بأنه "أي جهاز يستخدم التقانات الإلكترونية أو الكهروضوئية أو الضوئية أو الرقمية أو أي تقانات أخرى مشابهة بغرض توليد المعلومات أو جمعها أو حفظها أو الوصول إليها أو معالجتها أو توجيهها أو تبادلها"، وقد تم تفسير هذا التعريف الفني للحاسوب في المادة (1/ت1) من التعليمات التوضيحية والتنفيذية للقانون السوري، بأنه "كل ما يدل على أي جهاز سلكي أو لاسلكي مهما كان نوعه يملك معالجا للمعلومات مثل المخدم والحاسوب الشخصي والهاتف الذكي...".

وقد عرف المشرع الأمريكي الحاسوب بأنه "أداة إلكترونية مغناطيسية مرئية كهروكيميائية، أو أية أداة ذات سرعة عالية في معالجة البيانات، تؤدي عمليات منطقية رياضية أو عمليات تخزين وتتضمن أية تسهيلات لتخزين البيانات أو تسهيلات إتصالية ذات ارتباط مباشر ب /أو التشغيل"⁽¹⁾، وقد ورد التعريف الشامل للحاسوب، في الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني (دلنا كمبيوتر)، بأنه "جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات أو إخراج معلومات وإجراء عمليات حسابية أو منطقية، وهو يقوم بالكتابة على أجهزة الإخراج أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الحاسب عن طريق وحدات الإدخال مثل لوحة المفاتيح أو إسترجاعها من خلال وحدة المعالجة المركزية التي تقوم بإجراء العمليات الحسابية وكذلك العمليات المنطقية وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج مثل الطابعات أو وسائط التخزين المختلفة"⁽²⁾.

رابعاً: مكونات الحاسوب. يتكون الحاسوب من مكونات مادية، وأخرى غير مادية تسمى (منطقية أو معنوية)، ولكل منها عمل تقوم به.

1- المكونات المادية للحاسوب: تنقسم إلى وحدات الإدخال (لوحة المفاتيح والفارة) (الماوس) والماصح

⁽¹⁾ مشار إليه في كتاب بن يونس، عمر محمد أبوبكر، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، ط1، دار النهضة العربية، القاهرة، 2004، ص57.

⁽²⁾ مشار إليه في كتاب أحمد، هلاي عبدالله، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، ط2، بدون ناشر 2008، ص16+17.

الضوئي(الساكنر)، وتستخدم في إدخال البيانات والبرامج إلى وحدة التشغيل المركزية⁽¹⁾، والذاكرة الرئيسية، وهي التي تقوم بحفظ البيانات والمعلومات بشكل مؤقت، والذاكرة الثانوية، التي تقوم بدعم الذاكرة الرئيسية لتأمين مكان حفظ البرامج والبيانات⁽²⁾، ومكان تخزين المعلومات يتم إما في وحدات تخزين داخلية وخارجية، وتتمثل في الأقراص الصلبة، وتعد من مكونات الحاسوب كونها تتميز في سرعة التخزين، وتوفر حجم كبير للتخزين⁽³⁾.

2-المكونات الغير مادية (المنطقية) للحاسوب: عرفت المادة(1) من قانون مكافحة جرائم تقنية المعلومات الإماراتي بأنها "مجموعة من البيانات والتعليمات والأوامر القابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإنجاز مهمة معينة"، وقد عرّفها المنشور الفرنسي الصادر في 1981/11/22 بأنها "مجموعة من البرامج والأساليب والقواعد المتعلقة بتشغيل وحدة معالجة البيانات⁽⁴⁾، وبنفس المعنى عرفت الإتفاقية الأوروبية لمكافحة الجرائم السيبرانية⁽⁵⁾.

البرمجيات، تعتبر الكيان المنطقي للحاسوب، وهي كل البرامج الضرورية لعمل الحاسوب المدمجة بالجهاز ذاته والبرامج التي تمكن مستخدم الجهاز من أن ينفذ عملاً محدداً بدقة⁽⁶⁾.

الفرع الثاني: الإنترنت. إن وسائل تكنولوجيا المعلومات بحاجة إلى شبكات لربطها ببعضها، ومن هذه الشبكات شبكة الإنترنت، حيث سنتناول تاريخ ظهور الإنترنت في الفقرة الأولى، وتعريفه في الفقرة الثانية.

أولاً: ظهور الإنترنت. يعود ظهور الإنترنت إلى عام 1963 في الولايات المتحدة الأمريكية، لربط

(1) أحمد، هلاي عبدالله، المواجهة الجنائية لجرائم المعلوماتية، في النظامين المصري والبحريني، على ضوء إتفاقية بودابست، ط2، دار النهضة العربية، القاهرة ، 2013، ص56.

(2) سلامة، عماد محمد، الحماية القانونية لبرامج الحاسب الآلي، ومشكلة قرصنة البرامج، ط1، دار وائل للنشر والتوزيع، عمان 2005، ص31.

(3) الهيتي، محمد حمادة مرهج، جرائم الحاسوب، دراسة تحليلية، ط1، دار المناهج للنشر والتوزيع، عمان ، 2006، ص40.

(4) مشار إليه في كتاب الطولية، علي حسن، الجرائم الإلكترونية، ط1، جامعة العلوم التطبيقية، مملكة البحرين، 2008، ص22.

(5) انظر المادة (1/ب) من الإتفاقية الأوروبية لمكافحة الجرائم السيبرانية. ترجمة، أحمد، هلاي عبد اللاه، إتفاقية بودابست لمكافحة جرائم المعلوماتية، معلقاً عليها، ط1، دار النهضة العربية، القاهرة، 2011، ص17.

(6) الحسيناوي، علي جبار، جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، عمان، 2009، ص26.

مكاتب وزارة الدفاع الأمريكية مع بعضها البعض في شبكة محلية واحدة لتبادل المعلومات⁽¹⁾، وجرى تطوير الفكرة لربط الحواسيب ببعضها البعض في مناطق متباعدة، واستمر تطويرها إلى أن خرجت من الخدمة العسكرية في عام 1986، حيث ظهرت لأغراض مدنية ليستخدمها الإنسان في حياته اليومية⁽²⁾.

ثانياً: تعريف الإنترنت. المشرع الفلسطيني لم يعرف الإنترنت بشكل صريح في قانون الجرائم الإلكترونية، ولكن أشار إليه في تعريف الشبكة الإلكترونية بالمادة الأولى بإعتبره وسيلة لربط وسائل تكنولوجيا المعلومات داخل شبكة عامة أو عالمية، وهذا النص جاء بنفس العبارات التي وردت في المادة الأولى من قانون نظام مكافحة جرائم المعلوماتية السعودي، والمادة الأولى من قانون مكافحة الجرائم الإلكترونية القطري، والمادة (6/2) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وزير الإتصالات والتقانة السوري، كان أكثر جراءة، وعرف الإنترنت في المادة (1/ت4) من التعليمات التوضيحية والتنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية بأنه " ترابط من الأجهزة الحاسوبية والمنظومة المعلوماتية يسمح بتبادل المعلومات أو التشارك فيها بين مرسل ومستقبل أو مجموعة من المستقبلين وفق إجراءات محددة"، وتُعرف شبكة الإنترنت، بأنها عبارة عن مجموعة من الحاسبات المتصلة مع بعضها البعض والتي تعتبر المكونات المادية للشبكة بالإضافة إلى مكونات معنوية⁽³⁾.

المطلب الثالث

خصائص الجرائم الإلكترونية وطبيعتها القانونية.

الجريمة الإلكترونية لها خصائص تميزها عن غيرها من الجرائم، ولها طبيعة قانونية متعددة، حيث سنتناول خصائص الجرائم الإلكترونية في الفرع الأول، وطبيعتها القانونية في الفرع الثاني.

(1) الحلبي، خالد عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، مرجع سابق، ص 51.

(2) موقع ويكيبيديا، الموسوعة الحرة على شبكة الإنترنت، تاريخ الدخول 2018/3/2، الساعة 20:45.

(3) عزت، محمد فتحي محمد أنور، تفتيش شبكة الإنترنت لضبط جرائم الإعتداء على الآداب العامة والشرف والإعتبارات التي تقع بواسطتها، دراسة مقارنة، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 60.

الفرع الأول: خصائص الجرائم الإلكترونية. تتميز الجريمة الإلكترونية بخصائص تختلف عنها في الجرائم التقليدية، فهي جرائم سهلة وسريعة التنفيذ ترتكب بكبسة زر رغم أنها تحتاج لتحضير قبل إرتكابها⁽¹⁾، وهي جرائم تنفذ عن بعد، كون أنها لا تحتاج وجود الفاعل في مسرح الجريمة، وتلاحظ أثارها فقط كونها مخفية وجاذبة ومغرية لإستثمار الأموال وغسلها⁽²⁾، وتسمى جرائم ناعمة كونها لا تحتاج إلى عنف، ولا تترك أي اثر خارجي⁽³⁾، وهي جرائم عابرة للحدود، غير مقيدة بمنطقة جغرافية معينة، يمكن إرتكابها من أي مكان في هذا العالم وتتحقق نتيجتها الإجرامية في مكان آخر أو أكثر.

يرى الباحث من خلال استعراض خصائص الجرائم الإلكترونية، أن لها مميزات مختلفة تماما عن الجرائم التقليدية، وصعوبة بالغة في إكتشافها ومعرفة فاعلها، وكذلك صعوبة في جمع الأدلة الإلكترونية كون أنه يمكن تدميرها وإخفائها بسهولة، مما يجعل نسبتها إلى الفاعل إن عُرفَ أمر في غاية الصعوبة.

الفرع الثاني: الطبيعة القانونية للجرائم الإلكترونية. لتحديد الطبيعة القانونية للجرائم الإلكترونية، لابد بداية من الإشارة إلى التقسيمات الواردة في قانون

العقوبات النافذ، حيث ورد في الباب الأول من الكتاب الثاني، الجرائم التي تقع على أمن الدولة الداخلي والخارجي، و في الباب الثامن، الجرائم التي تقع على الإنسان، وفي الباب الحادي عشر، الجرائم التي تقع على الأموال⁽⁴⁾، ولكن أين تقع الجرائم الإلكترونية من هذه التقسيمات.

أولاً: الجرائم الإلكترونية جرائم أموال. عرفت المادة الأولى من قانون مكافحة غسل الأموال وتمويل الإرهاب الفلسطيني⁽⁵⁾، الأموال بأنها "الأصول من كل نوع سواء كانت مادية أم معنوية، منقولة أم غير منقولة، والوثائق أو المستندات القانونية أيا كان شكلها بما فيها الإلكترونية أو الرقمية....". حيث تستخدم وسائل تكنولوجيا المعلومات في سرقة الأموال، وتدمير المكونات المادية والمعنوية

(1) أحمد، طارق عفيفي صادق، الجرائم الإلكترونية، جرائم الهاتف المحمول، مرجع سابق، ص 34.

(2) الديري عبد العال، و الأستاذ. إسماعيل محمد صادق، الجرائم الإلكترونية، مرجع سابق، ص 55.

(3) الشناوي، محمد، جرائم النصب المستحدثة، مرجع سابق، ص 73.

(4) قانون العقوبات الأردني النافذ في المحافظات الشمالية (الضفة الغربية)، رقم (16) لسنة 1960.

(5) قرار بقانون بشأن غسل الأموال وتمويل الإرهاب الفلسطيني، رقم (20) لسنة 2015.

لنتلك الوسائل، ولا إشكال في الطبيعة القانونية للمكونات المادية لتكنولوجيا المعلومات كونها تقدر بثمان، ولكن ما هي الطبيعة القانونية للبيانات والبرامج والمكونات المنطقية لتكنولوجيا المعلومات؟ هل الإعتداء عليها يدخل ضمن جرائم الأموال كونها غير ملموسة؟.

عرفت الإتفاقية العربية لمكافحة الجريمة المنظمة عبر الوطنية، الممتلكات بأنها " الموجودات سواء كانت مادية أم غير مادية، ملموسة أم غير ملموسة "(1)، وهذا النص مطابق للتعريف الوارد بإتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية(2). والمكونات المنطقية لتكنولوجيا المعلومات، لها قيمة مادية وتقدر بثمان مادي، كونها تأخذ شكل نبضات إلكترونية، وهي بذلك تشبه التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبل الأشياء المادية(3)، وبالتبصر في المواد(6/12+4/13+14) من قانون الجرائم الإلكترونية الفلسطيني نجدها جرائم أموال.

ثانيا: الجرائم الإلكترونية جرائم أشخاص. الجرائم الإلكترونية جرائم أشخاص، عندما يكون محل الجريمة أحد الأشخاص، وتتجلى هذه الجرائم بشكل واضح في جرائم الذم والقبح والتحقيق والإبتزاز والتهديد وجرائم إفساد الأخلاق والإباحية والاستغلال الجنسي للأطفال، بإستخدام وسائل التقنية الحديثة، وشواهد ذلك كثيرة بالقانون(4).

ثالثا: الجرائم الإلكترونية جرائم إقتصادية. إنتشار التجارة الإلكترونية في أرجاء المعمورة، أدى إلى ظهور جرائم إلكترونية تمس الإقتصاد، وهذه الجرائم على درجة كبيرة من الخطورة، لأنها تمس إقتصاد الدولة، ويمكن أن تؤدي إلى إنهيار الإقتصاد الوطني.

وقد عرفت المادة(3) من قانون الجرائم الإقتصادية الأردني(5)، الجريمة الإقتصادية بأنها " الجرائم التي تتعلق بالأموال العامة، وتلحق الضرر بالمركز الإقتصادي للبلاد أو بالنقطة العامة بالإقتصاد

(1) انظر المادة (8/2) من الإتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، الصادرة عن جامعة الدول العربية بتاريخ 2010/12/21، دخلت حيز التنفيذ بتاريخ 2013/10/5، صادقت عليها دولة فلسطين بتاريخ 2013/5/21.

(2) أنظر المادة(2/د) من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، الصادرة عن الجمعية العامة للأمم المتحدة، بتاريخ 2000/11/15.

(3) الطوالبه، علي حسن، الجرائم الإلكترونية، مرجع سابق، ص85، في الهامش.

(4) انظر المواد(7+15+16+22) من قانون الجرائم الإلكترونية الفلسطيني.

- كذلك انظر المادة (18) من قانون مكافحة جرائم تقنية المعلومات العماني.

(5) قانون الجرائم الإقتصادية الأردني رقم(11) لسنة 1993، والمعدل بالقانون رقم (20) لسنة 2004.

الوطني أو العملة الوطنية أو السهم أو السندات أو الأوراق المالية المتداولة".

وتعرف الجريمة الاقتصادية بأنها " كل تصرف أو إمتناع يخالف أحكام النشاط الإقتصادي رتب عليه القانون جزاء"⁽¹⁾، وقد نص قانون الجرائم الإلكترونية الأردني في المادة(12/ج) صراحة على تجريم الأعمال التي تمس الإقتصاد الوطني، وهو القانون العربي الوحيد الذي تميز بهذا النص في الجرائم الإلكترونية.

يرى الباحث أن المشرع الفلسطيني لم يكن موفقا في عدم إدراج نص مماثل لما جاء بالنص الأردني في تجريم الأعمال التي تمس الإقتصاد الوطني، وذلك لعدم وجود قانون خاص بالجرائم الاقتصادية في فلسطين، ولكن يمكن فهم قصد المشرع الفلسطيني أن قانون الجرائم الإلكترونية شمل الجرائم الاقتصادية بشكل ضمني، من خلال المواد(44+45) التي جرمت إرتكاب الجرائم المنصوص عليها بالتشريع النافذ بإستخدام وسائل تكنولوجيا المعلومات، وإشارته بالمادة(18) إلى جرائم غسل الأموال وتمويل الإرهاب، ورغم ذلك نرى أنه من الضروري إدراج نص صريح يخص الجرائم الاقتصادية كما فعل المشرع الأردني.

رابعا: الجرائم الإلكترونية جرائم أمن دولة. بعض الجرائم الإلكترونية تعتبر إعتداء على أمن الدولة الداخلي والخارجي، وتتمثل في الدخول على الحاسوب الخاص بالدولة والإطلاع على الأسرار السياسية والعسكرية، وإثارة الفتن الطائفية، وقد شددت القوانين الإلكترونية العقوبات المقررة للجرائم التي تدخل تحت الجرائم الماسة بأمن الدولة⁽²⁾.

خامسا: الجرائم الإلكترونية جرائم دولية. من خصائص الجرائم الإلكترونية أنها عابرة للقارات وتدخل تحت تصنيف جرائم دولية، والتي تعرف بأنها "كل فعل أو سلوك يحظره القانون الدولي الجنائي ويقرر لمرتكبه جزاءً جنائياً"⁽³⁾، ويصدر هذا الفعل عن شخص ذو إرادة معتبرة قانونيا وتطبق

⁽¹⁾ صالح، نائل عبد الرحمن، الجرائم الاقتصادية في التشريع الأردني، ط1، ج1، دار الفكر للنشر والتوزيع، عمان، 1990، ص17.

⁽²⁾ أنظر المواد(4+2/4) من قانون الجرائم الإلكترونية الفلسطيني.

- وكذلك أنظر المادة (44) من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

⁽³⁾ القهوجي، علي عبد القادر، القانون الدولي الجنائي، أهم الجرائم والمحاكم الدولية الجنائية، ط1، منشورات الحلبي الحقوقية، بيروت، 2001، ص7.

عليه العقوبة باسم الجماعة الدولية⁽¹⁾.

قانون الجرائم الإلكترونية الفلسطيني جرم في المواد (24+25) إنشاء مواقع إلكترونية بقصد إثارة النعرات العنصرية أو للتحريض على أعمال الإبادة الجماعية أو جرائم ضد الإنسانية التي نصت عليها القوانين الدولية، وبالرجوع إلى نص المادة (5) من القانون الأساسي للمحكمة الجنائية الدولية⁽²⁾، التي عدت الجرائم الدولية التي تختص بها المحكمة، نجد من ضمنها جرائم الإبادة الجماعية والجرائم ضد الإنسانية، وأكدت المادة (25) من قانون المحكمة على إختصاصها في معاقبة الأشخاص الذين يحرضون بشكل مباشر وعلمي على ارتكاب تلك الجرائم، وكون أن دولة فلسطين إنضمت إلى القانون الأساسي للمحكمة الجنائية الدولية وأصبحت عضو في الجمعية العامة للمحكمة، مما يترتب عليها مع هذا الوضع القانوني الجديد التزامات قانونية، منها موافقة تشريعاتها الداخلية، والنص على الجرائم المذكورة في القانون الأساسي للمحكمة الجنائية الدولية، وهذا ما أكدته المحكمة الدستورية الفلسطينية في قرارها الذي أكدت فيه على سمو الإتفاقيات الدولية على التشريعات الداخلية⁽³⁾.

يرى الباحث إن المشرع الفلسطيني كان موفقاً في إدراج هذا النص لتجريم الدعوة أو التحريض على ارتكاب جرائم ضد الإنسانية أو جرائم الإبادة الجماعية عبر المواقع الإلكترونية متماشياً بذلك مع القانون الجنائي الدولي، ولم يجد الباحث أي نص مماثل للنص الفلسطيني في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات والقوانين العربية المقارنة التي تم الإشارة إليها، ولكن نجد أن أغلبها جرم إنشاء مواقع لجمعيات أو لجماعات إرهابية وترويج المخدرات والإتجار بالبشر. وكذلك نرى أن الجرائم الإلكترونية ليس لها طبيعة قانونية واحدة، وإنما لها طبيعة قانونية متعددة.

(1) إبراهيم، هشام مصطفى محمد، التحقيق والمحاكمة أمام المحكمة الجنائية الدولية الدائمة، دار المطبوعات الجامعية، الإسكندرية، 2015، ص60.

(2) القانون الأساسي للمحكمة الجنائية الدولية، نظام روما الأساسي، الذي إعتده مؤتمر الأمم المتحدة المعنى بإنشاء محكمة جنائية دولية بتاريخ 17/7/1998، دخل حيز النفاذ بتاريخ 1/7/2002، وأصبحت فلسطين عضو في المحكمة الجنائية من تاريخ 1/4/2015.

(3) أنظر قرار المحكمة الدستورية العليا الفلسطينية، قضية رقم (12)، لسنة (2) قضائية، الصادر بتاريخ 19/11/2017، منشور بالجريدة الرسمية، بتاريخ 29/11/2017، بالعدد (138).

المبحث الثاني

ماهية التفتيش

قانون الإجراءات الجزائية الفلسطيني⁽¹⁾، هو القانون الذي يرسم خط سير الدعوى الجزائية من لحظة وقوع الجريمة حتى تنفيذ الحكم، ويعتبر من أدق القوانين في حياة الدولة القانونية، كونه يتعين على المشرع تحقيق التوازن بين مصلحتين متعارضتين المصلحة العامة والمصلحة الخاصة⁽²⁾، وقد رسم هذا القانون الطرق القانونية الواجب إتباعها لجمع الأدلة القانونية من قبل مأموري الضبط القضائي أو سلطة التحقيق.

التفتيش يعتبر أخطر إجراء تقوم به السلطة العامة لما فيه مساس بالحياة الخاصة للإنسان، وله خصوصية أكثر في الجرائم الإلكترونية، كون أهم أسرار الناس محفوظة بوسائل التكنولوجيا الحديثة، التي حمتها الشريعة الإسلامية⁽³⁾، وكذلك القانون الأساسي الفلسطيني⁽⁴⁾، والمواثيق الدولية⁽⁵⁾.

المشرع الفلسطيني نظم إجراءات التفتيش في الفصل الرابع من الباب الأول من قانون الإجراءات الجزائية، وكذلك أفرد المشرع الفلسطيني في قانون الجرائم الإلكترونية بعض نصوص القانون للتفتيش، معتبراً بذلك أن نصوص قانون الإجراءات الجزائية غير قادرة لوحدها على معالجة إجراءات التفتيش في الجرائم الإلكترونية. حيث سنتناول مفهوم التفتيش وصوره في المطلب الأول، وطبيعته القانونية في المطلب الثاني.

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

(2) سرور، أحمد فتحي، الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية، طبعة معدلة، دار النهضة العربية، القاهرة، 1995، ص3.

(3) لقوله تعالى (يا أيها الذين امنوا لا تدخلوا بيوتا غير بيوتكم حتى تستأسوا وتسلموا على أهلها ذلك خير لكم لعلكم تذكرون) الآية (27) من سورة النور.

(4) أنظر المواد(11+17) من القانون الأساسي الفلسطيني.

(5) انظر المواد(1/3+3/1+1/13+ب/55/ج) من ميثاق الأمم المتحدة، الصادر بتاريخ 1945/6/26، دخل حيز النفاذ بتاريخ 1945/10/24.

- كذلك أنظر المادة(12) من الإعلان العالمي لحقوق الإنسان، الصادر عن الجمعية العامة للأمم المتحدة بتاريخ 1948/12/10.

المطلب الأول

مفهوم التفتيش وصوره.

التفتيش المباح، هو الذي يحقق التوازن بين حقوق الأفراد في الحرية الشخصية والخصوصية وبين حق المجتمع في المحافظة على كيانه واستقراره⁽¹⁾، وللتفتيش أهمية كبيرة سواء في إثبات الجريمة ونسبتها إلى المشتبه به أو نفيها عنه. لذلك سنتناول صور التفتيش في الفرع الأول، وتعريفه في الفرع الثاني.

الفرع الأول: صور التفتيش. للتفتيش عدة صور، حيث سنتناول التفتيش الوقائي في الفقرة الأولى، والإداري بالفقرة الثانية، والتفتيش الوقائي بالفقرة الثالثة.

أولاً: التفتيش الوقائي. هو إجراء يقوم به مأموري الضبط القضائي بناءً على القوانين واللوائح، ويعتبر التفتيش الوقائي، مجرد إجراء احتياطي للحيلولة دون إعتداء الشخص على نفسه أو غيره، وللحفاظ على الأمن العام، وتنفيذ أوامر القانون واللوائح التنفيذية⁽²⁾، وتطبيقاً لصور التفتيش الوقائي، نصت المادة(6) من قانون الأمن الوقائي الفلسطيني⁽³⁾، على أنه من مهام الإدارة العامة للأمن الوقائي حماية الأمن الداخلي والعمل على منع وقوع الجرائم، وتتجلى صورته العملية للتفتيش الذي يخضع له المسافرين في المطارات ونقاط العبور، والفنادق وبعض الأماكن الأخرى، وهذا التفتيش يكون وقائي، لمنع الجريمة قبل ارتكابها حماية للأمن والنظام العام.

ثانياً: التفتيش الإداري. هو إجراء تحفظي إداري، يقوم به موظفاً عاماً بتفتيش شخص لكي يتحرى إذا كان قد ارتكب جريمة أم لا ويهدف إلى حسن سير العمل⁽⁴⁾، وتظهر صورته في ما نصت عليه المادة(2) من قانون الضابطة الجمركية⁽⁵⁾، على أن مرجعية الضابطة الجمركية الفنية والعملية إلى وزارة المالية والتخطيط، وأكد القانون في المادة(6) على أن مجلس الوزراء يصدر الأنظمة

(1) عوض، رمزي رياض، الإجراءات الجنائية في القانون الأنجلوأمريكي، مرجع سابق، ص83.

(2) الشهاوي، قنري عبد الفتاح، مناهج التفتيش، قيوده وضوابطه، ط1، دار النهضة العربية، القاهرة، 2006، ص25.

(3) قرار بقانون بشأن الأمن الوقائي الفلسطيني رقم (11) لسنة 2007.

(4) الكواري، منى جاسم، التفتيش، شروطه وحالات بطلانه، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت، 2008، ص 26.

(5) قرار بقانون بشأن الضابطة الجمركية الفلسطيني، رقم (2) لسنة 2016.

اللازمة لتنفيذ أحكام القانون، ويعتبر قيام أفراد الضابطة الجمركية بتفتيش المسافرين وأمتعتهم وناقلي البضائع لمنع التهريب هو تفتيش إداري.

ثالثاً: التفتيش القضائي. هو التفتيش الذي سنبحثه في الفرع الثاني، لنصل إلى موضوع بحثنا وهو التفتيش بالجرائم الالكترونية.

الفرع الثاني: تعريف التفتيش. التفتيش لغةً، يعني الطلب والبحث، ويقال فتشت الشيء فتشاً أي سألت عنه واستقصاه⁽¹⁾، والتفتيش فقهاً، إجراء تحقيق، يقوم به موظف مختص، للبحث عن أدلة مادية لجناية أو جنحة، وذلك في محل خاص أو لدى شخص، وفقاً للأحكام المقررة قانوناً⁽²⁾، وهو الإطلاع على محل منحه القانون حرمة خاصة، بإعتباره مستودع سر صاحبه، لضبط ما عسى قد يوجد به مما يفيد في كشف الحقيقة عن جريمة معينة⁽³⁾. والحرمة، هي ذلك الشيء الواجب الإحتزام، وهو موضع حماية من القانون فالجسم والمسكن والرسائل لها حرمة لأنها مستودع الأسرار⁽⁴⁾.

المطلب الثاني

الطبيعة القانونية للتفتيش وغايته وخصائصه.

الطبيعة القانونية للتفتيش والغاية منه حددها القانون، حيث سنتناول الطبيعة القانونية للتفتيش في الفرع الأول، والغاية منه بالفرع الثاني.

الفرع الأول: الطبيعة القانونية للتفتيش. القانون نص على الطبيعة القانونية لتفتيش المنازل، ولكنه لم ينص على الطبيعة القانونية لتفتيش الأشخاص.

أولاً: الطبيعة القانونية لتفتيش المنازل. نصت المادة(39) من قانون الإجراءات الجزائية الفلسطيني

(1) لسان العرب، المجلد السادس، حرف الشين، فصل الفاء، مصدر سابق، ص 325.

(2) مصطفى، محمود محمود، الإثبات في المواد الجنائية في القانون المقارن، ط1، ج 2، التفتيش والضبط، مطبعة جامعة القاهرة والكتاب الجامعي، 1978، ص 14.

(3) المرصفاوي، حسن صادق، المرصفاوي في أصول الإجراءات الجنائية، منشأة المعارف، الإسكندرية، 2000، ص 438.

(4) ثروت، جلال، نظم الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، 1997، ص 465.

على الطبيعة القانونية لتفتيش المنازل بأنه عمل من أعمال التحقيق، والسلطة المختصة بالتحقيق بالجرائم في فلسطين هي النيابة العامة.

ثانياً: الطبيعة القانونية لتفتيش الأشخاص. القانون لم يحدد الطبيعة القانونية لتفتيش الأشخاص، والأصل أن تفتيش الأشخاص عمل تحقيق، تمارسه السلطة المختصة بالتحقيق، وإستثناءً خول القانون لمأموري الضبط القضائي إجراء تفتيش الأشخاص في حالات معينة⁽¹⁾، وهذا الإستثناء ممنوعون من إجرائه إلا إذا رخص لهم القانون ترخيصاً خاصاً في أحوال معينة أو كان بيدهم إذن من السلطة القضائية المختصة⁽²⁾.

الفرع الثاني: خصائص وغاية التفتيش. التفتيش كإجراء من إجراءات التحقيق له خصائص يتميز بها، وله غاية من اللجوء إليه.

أولاً: خصائص التفتيش. أجازت المادة(42) من قانون الإجراءات الجزائية الفلسطيني، تنفيذ التفتيش بالقوة إذا رفض المقيم بالمنزل أو المسئول عن المكان المراد تفتيشه السماح بالدخول، وهنا نجد أن من خصائص التفتيش، الجبر والإكراه، بغض النظر عن إرادة من يقع عليه في شخصه أو مسكنه⁽³⁾.

ثانياً: غاية التفتيش. نصت المادة(50) من قانون الإجراءات الجزائية الفلسطيني على غاية التفتيش، البحث عن الأشياء الخاصة بالجريمة الجاري التحقيق بشأنها، ونصت المادة(32) على أن الغاية من التفتيش الحصول على وسائل ذات صلة بالجريمة الإلكترونية.

والغاية من إجراء التفتيش في الجرائم الإلكترونية، هو البحث عن أدلة تفيد التحقيق سواء كانت ضد المشتبه به أو في صالحه، ويتم البحث عن وسائل تكنولوجيا المعلومات ذات الصلة بالجريمة الإلكترونية، سواء كانت تلك الوسائل مادية أو غير مادية.

(1) السعيد، كامل، شرح قانون أصول المحاكمات الجزائية، دراسة تحليلية تأصيلية مقارنة، في القوانين الأردنية والمصرية والسورية وغيرها، دار الثقافة للنشر والتوزيع، عمان، 2005، ص392.

(2) عبد الملك، جندي، الموسوعة الجنائية، ج4، مرجع سابق، ص565.

(3) عطية، كاظم السيد، الحماية الجنائية لحق المتهم في الخصوصية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2007، ص605.

الفصل الأول

خصوصية التفتيش في الجرائم الإلكترونية

الفصل الأول

خصوصية التفتيش في الجرائم الإلكترونية

تمهيد وتقسيم.

التفتيش في الجرائم الإلكترونية، له خصوصية تميزه عن التفتيش بالجرائم العادية، كون أن تلك الجرائم لها خصائص وبيئة مختلفة، وهي بحاجة إلى سلطة متخصصة، تكون مؤهلة، لرفع قدرتها على التعامل مع هذه الجرائم الحديثة، وإستخراج الأدلة المقبولة قانوناً.

الجرائم الإلكترونية، بحاجة إلى سلطة مختصة تكون مؤهلة فنياً ومدربة على التعامل مع الطبيعة الخاصة للجرائم الإلكترونية، كون السلطات العادية المختصة بالتحقيق بالجرائم غير قادرة على التعامل مع الجرائم الإلكترونية، مما يتطلب وجود سلطة مختصة للتحقيق في تلك الجرائم، وهذه السلطة المختصة تكون مؤهلة للتفتيش في الجرائم الإلكترونية، وعلى علم في إستخراج الأدلة الإلكترونية.

ويجب على السلطة المختصة في التفتيش بالجرائم الإلكترونية أن تراعي الضمانات الدستورية والقانونية الخاصة بالتفتيش، كون التفتيش في الجرائم الإلكترونية يمس خصوصية الناس والإطلاع على أسرارهم المخزنة في وسائل تكنولوجيا المعلومات. حيث ينقسم الفصل إلى مبحثين.

المبحث الأول: السلطة المختصة في التفتيش بالجرائم الإلكترونية.

المبحث الثاني: شروط التفتيش بالجرائم الإلكترونية.

المبحث الأول

السلطة المختصة بالتفتيش في الجرائم الإلكترونية

أوصى المؤتمر الدولي لقانون العقوبات، بضرورة الإشارة بوضوح إلى السلطة المختصة، بإجراءات التفتيش والضبط في بيئة تكنولوجيا المعلومات⁽¹⁾، وإن هذه التوصية بوجوب تحديد السلطة المختصة بالتفتيش في الجرائم الإلكترونية، يدل على أن هذه المهمة لا تستطيع السلطات العادية القيام بها، وإنما تحتاج إلى سلطة متخصصة مؤهلة للتعامل مع نوعية تلك الجرائم.

أخذت إتفاقية بودابست لمكافحة الجرائم الإلكترونية بتوصية المؤتمر الدولي لقانون العقوبات في المادة(14)، ونصت على ضرورة إنشاء سلطات مختصة للتقيب والقيام بالإجراءات الجنائية اللازمة في الجرائم الإلكترونية، ووضحت المذكرة التفسيرية لإتفاقية بودابست، أن المقصود بتحديد السلطة المختصة تعني، سلطة قضائية، أو إدارية، أو بوليسية، مؤهلة قانوناً في القانون الداخلي، يناط بها الأمر في تنفيذ إجراءات جمع الأدلة المرتبطة بالتنقيبات⁽²⁾.

المشرع الفلسطيني، أخذ بتلك التوصيات كذلك في قانون الجرائم الإلكترونية، وحدد بوضوح السلطة المختصة بالتفتيش في الجرائم الإلكترونية، بالمادة(2/3+32) وأسند المهمة للنيابة العامة، وكذلك القانون الكويتي، والسعودي، والأردني، والبحريني، والقطري⁽³⁾، إلا أن بعض القوانين أسندت مهمة التفتيش بالجرائم الإلكترونية إلى مأموري الضبط القضائي الذين يتم تسميتهم من الوزير المختص، كالمشرع السوري⁽⁴⁾، والبعض الآخر لم يحدد السلطة المختصة بالتفتيش في الجرائم الإلكترونية،

⁽¹⁾ أنظر البند(3/أ)، من توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات، حول القواعد الإجرائية في بيئة جرائم الكمبيوتر، الشق الإجرائي، المنعقد بتاريخ 4 إلى 9/10/1994، في ريو دي جانيرو، البرازيل.

⁽²⁾ المذكرة التفسيرية للإتفاقية الأوروبية للجرائم السيبرانية، ترجمة أحمد، هلاي عبد اللاه، إتفاقية بودابست لمكافحة جرائم المعلوماتية، معلقاً عليها، مرجع سابق، ص165.

⁽³⁾ أنظر المادة (17) من قانون مكافحة جرائم تقنية المعلومات الكويتي.

- كذلك أنظر المادة(15) من قانون نظام مكافحة جرائم المعلوماتية السعودي.

- كذلك أنظر المادة(13) من قانون الجرائم الإلكترونية الأردني.

- كذلك أنظر المادة(15) من قانون جرائم تقنية المعلومات البحريني.

- كذلك أنظر المادة(14) من قانون الجرائم الإلكترونية القطري.

⁽⁴⁾ أنظر المادة (26) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

كقانون مكافحة جرائم تقنية المعلومات العماني والإماراتي⁽¹⁾، معتبرة بأن قانون الإجراءات الجزائية يعالج هذه المسألة.

كما أسلفنا في المقدمة، واستعرضنا خصائص الجرائم الإلكترونية، فهي بتلك الخصائص والمميزات لا بد أن تكون السلطة المختصة بالتحقيق والتفتيش لها مميزات تؤهلها للقيام بهذه المهمة. حيث سنتناول في هذا المبحث تحديد السلطة المختصة بالتفتيش في الجرائم الإلكترونية بالمطلب الأول، وخصوصية تلك السلطة في المطلب الثاني.

المطلب الأول

تحديد السلطة المختصة بالتفتيش في الجرائم الإلكترونية.

نص المشرع الفلسطيني بالمادة (32) من قانون الجرائم الإلكترونية، على السلطة المختصة في التفتيش بالجرائم الإلكترونية هي النيابة العامة⁽²⁾، ولم يُنشئ القانون الفلسطيني نيابة متخصصة للجرائم الإلكترونية كما فعل المشرع السوداني الذي أمر بالمادة (29) من قانون جرائم المعلوماتية بإنشاء نيابة متخصصة لجرائم المعلوماتية.

إن العلة من وضع إجراء التفتيش بيد النيابة، باعتبارها سلطة قضائية⁽³⁾، وأن التفتيش لا يجوز قانوناً إلا بأمر قضائي تطبيقاً للمواد (11+17) الواردة بالقانون الأساسي الفلسطيني، والإتفاقيات

(1) أنظر المادة (34) من قانون مكافحة جرائم تقنية المعلومات العماني.

- كذلك أنظر المادة (49) من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

(2) النيابة العامة في فلسطين، مشكلة بقاعدة تسلسلية على رأسها النائب العام، يساعده نائب عام مساعد أو أكثر، وعلى رأس كل مكتب للنيابة العامة في المحافظات رئيس نيابة وعدد كافي من وكلاء النيابة ومعاوني النيابة، أنظر في تشكيل النيابة العامة في فلسطين، الباب الخامس من قانون السلطة القضائية، رقم (1) لسنة 2002.

- وكذلك يوجد نيابة عسكرية متخصصة بالتحقيق في الجرائم التي يرتكبها العسكريين، أنظر الباب الثاني من الكتاب الأول من قانون أصول المحاكمات الجزائية الثوري، الصادر عن المجلس الوطني الفلسطيني لمنظمة التحرير الفلسطينية، بالقرار التشريعي رقم (5) بتاريخ 1979/7/11، بيروت، وكذلك أنظر الباب السادس من قرار بقانون بشأن الهيئة القضائية لقوى الأمن الفلسطيني، رقم (2) لسنة 2018.

(3) صالح، نبيه، شرح قانون الإجراءات الجزائية الفلسطيني، دراسة مقارنة، ط 2، ج 1، دار الفكر، القدس، 2006، ص 90.

والمبادئ الدولية الخاصة بحقوق الإنسان⁽¹⁾، لضمان الحفاظ على عدم المس بالحقوق والحريات الأساسية للإنسان إلا من خلال سلطة قضائية، كون التفتيش يمس خصوصية الأفراد بالإطلاع على أسرارهم

النيابة العامة، مختصة في التفتيش بجميع الجرائم، وأعضاء النيابة موزعين جغرافياً داخل حدود الدولة، وكل له منطقة جغرافية محددة يمارس صلاحياته بها⁽²⁾، ولكن التفتيش في الجرائم الإلكترونية يمتاز بصعوبة بالغة في أغلب الأحيان، وإن لم يكن إجراءه مستحيل أحياناً، وهو بحاجة إلى جهود مضاعفة من قبل السلطة المختصة به، ولعدم قدرة أعضاء النيابة العاديين على القيام بهذه المهمة، دعت الحاجة إلى وجود أعضاء نيابة متخصصين للتعامل مع تلك الجرائم. حيث سنبحث في نيابة مكافحة الجرائم الإلكترونية بالفرع الأول، وبالفرع الثاني، مأموري الضبط القضائي.

الفرع الأول: نيابة مكافحة الجرائم الإلكترونية.

التفتيش في الجرائم الإلكترونية هو من إجراءات التحقيق الصعبة، كونه يهدف إلى التفتيش عن الأدلة في البيئة الإلكترونية، ولذلك ظهرت حاجة ملحة لإنشاء نيابة متخصصة لمكافحة الجرائم الإلكترونية، حيث سنبحث تشكيلها في الفقرة الأولى، وإختصاصها بالفقرة الثانية.

أولاً: تشكيل نيابة مكافحة الجرائم الإلكترونية.

أنشأت نيابة مكافحة الجرائم الإلكترونية في فلسطين بقرار من النائب العام بتاريخ 2016/3/20 لمتابعة الجرائم الإلكترونية⁽³⁾، ولكن ما هي تشكيلات نيابة الجرائم الإلكترونية؟.

⁽¹⁾ أنظر المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية، الصادرة عن الجمعية العامة للأمم المتحدة، بتاريخ 1966/12/16. وأصبحت فلسطين طرف فيه من تاريخ 2014/4/2.

- كذلك أنظر المادة (8) من الإتفاقية الأوروبية لحقوق الإنسان، الصادرة عن مجلس أوروبا بتاريخ 1950/11/4، روما.
- كذلك أنظر المادة (18) من إعلان القاهرة، حول حقوق الإنسان في الإسلام، الصادر عن منظمة المؤتمر الإسلامي، بتاريخ 1990/8/5، القاهرة، مصر.

⁽²⁾ أنظر المادة (1/19) من قانون الإجراءات الجزائية الفلسطيني.

⁽³⁾ مقابلة بحثية، مع الأستاذة نسرين زينة، رئيسة نيابة مكافحة الجرائم الإلكترونية، أجريت بتاريخ 2018/5/2، الساعة العاشرة صباحاً، في مكتب نيابة مكافحة الجرائم الإلكترونية، مقر النائب العام، رام الله، فلسطين.

1- رئيس نيابة مكافحة الجرائم الإلكترونية. في مقابلي مع رئيس نيابة مكافحة الجرائم الإلكترونية أفادت، أن النائب العام لدولة فلسطين كلف بتاريخ 2016/3/27 رئيس نيابة على رأس نيابة مكافحة الجرائم الإلكترونية، ومقره مكتب النائب العام رام الله، مهمته متابعة قضايا الجرائم الإلكترونية الواردة إلى النيابة العامة، وتكمن مهمة رئيس نيابة مكافحة الجرائم الإلكترونية في استقبال طلب الإحتياج المرفوع من أعضاء النيابة المتخصصين والمنتشرين في المحافظات، (معرفة الخطوط التي إرتكبت منها الجريمة الإلكترونية)، وإحالة الطلبات إلى وحدة الجرائم الإلكترونية في جهاز الشرطة، وعند الحصول على المعلومات المطلوبة، يقوم رئيس النيابة بإرسال النتائج إلى عضو النيابة الذي طلبها، وفي بعض الأحيان ولإعتبارات خاصة يتم إرسال النتائج مع إحالة الملف إلى عضو نيابة آخر.

يرى الباحث أنه بالنظر إلى الأعمال التي يقوم بها رئيس نيابة مكافحة الجرائم الإلكترونية في مكتب النائب العام، وظيفته تعتبر حلقة وصل بين أعضاء النيابة المنتشرين بالمحافظات الذين يمارسون إختصاصهم داخل حدود جغرافية محددة، وبين وحدة الجرائم الإلكترونية الرئيسية في جهاز الشرطة.

2- أعضاء نيابة مكافحة الجرائم الإلكترونية. أعضاء النيابة العامة مكلفين بحكم القانون في التحقيق بالجرائم والتصرف بها⁽¹⁾، وبعد قرار إنشاء نيابة الجرائم الإلكترونية، وتكليف رئيس نيابة على رأسها، أصدر النائب العام بتاريخ 2017/1/2، قرار بتخصيص عضو نيابة في كل مكتب للنيابة العامة المنتشرة في المحافظات، وعضو النيابة الذي تم تكليفه، متخصص في متابعة قضايا الجرائم الإلكترونية الواردة على مكتب النيابة⁽²⁾، ولكن ما هو إختصاص نيابة مكافحة الجرائم الإلكترونية؟.

ثانياً: إختصاص نيابة مكافحة الجرائم الإلكترونية.

ينقسم أعضاء النيابة العامة إلى أعضاء ذو إختصاص عام لهم صلاحية التحقيق في جميع الجرائم، وأعضاء ذو إختصاص خاص لهم صلاحية التحقيق في بعض الجرائم المحددة دون غيرها

(1) أنظر المادة(55) من قانون الإجراءات الجزائية الفلسطيني.

(2) مقابلة بحثية مع رئيس نيابة الجرائم الإلكترونية، مصدر سابق.

ويكون إختصاصهم بمكان جغرافي محدود، أو على كامل أراضي الدولة⁽¹⁾، وبذلك يكون لأعضاء نيابة مكافحة الجرائم الإلكترونية إختصاص نوعي ومكاني.

1- الإختصاص النوعي. الإختصاص النوعي يعني، أنه يجب على من يقوم بالتفتيش أن يكون مختص بالتحقيق بالجريمة من حيث نوعها أو موضوعها⁽²⁾، وهذا الشرط من متطلبات الشرعية الإجرائية، حيث أن بعض أعضاء النيابة العامة يكون لهم إختصاص بالتحقيق في نوعية معينة من الجرائم تكون محددة، وفي الجرائم الإلكترونية التي تفرض أن يكون عضو النيابة الذي يقوم بالتحقيق فيها متخصص ومدرب نظرا لخصوصيتها.

تشكيل نيابة متخصصة في مكافحة الجرائم الإلكترونية، وتحديد أعضائها، أصبح لهم صلاحية الإختصاص النوعي المحدد⁽³⁾ بالتحقيق بالجرائم المنصوص عليها في قانون الجرائم الإلكترونية، وجميع الجرائم التي ترتكب بواسطة تكنولوجيا المعلومات، ولا يجوز لسلطة أخرى التحقيق بنوعية تلك الجرائم، وبالتالي الإختصاص ينعقد لهم في التفتيش بتلك الجرائم.

يرى الباحث أن قانون الجرائم الإلكترونية لم ينشئ نيابة متخصصة لمكافحة الجرائم الإلكترونية، ولكن تم تشكيلها بقرار من النائب العام، وهذا القرار هو قرار إداري تنظيمي، لتوزيع العمل بين أعضاء النيابة العامة، بموجبه يمنح بعض أعضاء النيابة إختصاص نوعي في التحقيق بالجرائم الإلكترونية، ولكن ليس من شأن هذا القرار الإداري التنظيمي أن يجرّد أعضاء النيابة الآخرين من صلاحياتهم بالتحقيق في الجرائم الإلكترونية، كون أن القرارات الإدارية لا تقوى على القانون⁽⁴⁾، وجائز قانوناً أن يقوم أي عضو نيابة عامة بالتحقيق بجريمة تدخل نوعياً في إختصاص عضو نيابة ذوو الإختصاص الخاص⁽⁵⁾. لذلك فإن أي عضو من أعضاء النيابة العامة له صلاحية التحقيق في الجرائم الإلكترونية ولا مخالفة قانونية لهذا الإجراء.

(1) الجوخدار، حسن، شرح قانون أصول المحاكمات الجزائية، ط2، مكتبة دار الثقافة للنشر والتوزيع، عمان، 1997، ص219+220.

(2) أحمد، هلالى عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص137.

(3) هروال، نبيلة هبة، الجوانب الإجرائية لجرائم الإنترنت، في مرحلة جمع الإستدلالات، دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2007، ص95.

(4) راسخ، إبراهيم، التحقيق الجنائي العلمي، ط1، أكاديمية شرطة دبي، الإمارات العربية المتحدة، 1991، ص389.

(5) طنطاوي، إبراهيم حامد، الدفع ببطلان إذن النيابة العامة بالتفتيش، دار النهضة العربية، القاهرة، 1997، ص30.

2-الإختصاص المكاني. يتحدد الإختصاص المكاني في التحقيق بالجرائم بشكل عام، بمكان وقوع الجريمة، أو المكان الذي يقيم فيه المتهم، أو المكان الذي يتم إلقاء القبض عليه⁽¹⁾، وقد حدد قانون الجرائم الإلكترونية الفلسطيني في المادة الثانية ميدان تطبيق أحكامه، والذي جاء فيها " تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتُكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو إمتد أثرها داخل فلسطين... مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ"

الجرائم الإلكترونية، يصعب معرفة فاعلها، أو مكان ارتكابها، كونها جرائم مستترة⁽²⁾، ويمكن أن ترتكب من داخل الدولة أو من خارجها، وفي مقابلي مع رئيس نيابة مكافحة الجرائم الإلكترونية، حول الإختصاص المكاني في الجرائم الإلكترونية، أكدت على أن عضو النيابة المتخصص بالجرائم الإلكترونية في منطقتة، يقوم بتلقي البلاغات، وإستقبال الشكاوي بوقوع جريمة إلكترونية، وسماع الشهود للحصول على المعلومات الإلكترونية الأولية اللازمة والضرورية، وإرسال طلب إحتياج إلى رئيس نيابة مكافحة الجرائم الإلكترونية في مكتب النائب العام، يطلب فيه معرفة الخطوط والشبكات التي إستخدمت في إرتكاب هذه الجريمة، وينتظر نتائج الفحص، لمحاولة تحديد نقطة الشبكة والوسيلة الإلكترونية المستخدمة للوصول إلى الفاعل، سواء إرتُكبت الجريمة من داخل الدولة أو خارجها.

أ-الإختصاص الداخلي بالتفتيش. عضو النيابة المختص بالتفتيش، مقيد داخل نطاق مكاني محدد⁽³⁾، فإذا كانت نتائج الفحص الواردة إليه، تؤكد أن الفاعل استخدم شبكات محلية داخل الدولة، وتم حصر هذه الشبكة في منطقة إختصاصه، يستكمل عضو النيابة التحقيق بالقضية، ومنها إجراء التفتيش إذا ظهرت ضرورة لإجرائه، سواء في تفتيش الأشخاص، أو الأماكن، لغاية البحث عن وسائل تكنولوجيا المعلومات، ولا يجوز النفاذ المباشر إلى تلك الوسائل الإلكترونية وتفتيشها إلا بأذن من عضو النيابة تطبيقاً لنص المادة (4/32) من قانون الجرائم الإلكترونية.

(1) أنظر المادة (163) من قانون الإجراءات الجزائية الفلسطيني.

(2) المضحكي، حنان ربحان مبارك، الجرائم المعلوماتية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014، ص360.

(3) عطية، طارق إبراهيم الدسوقي، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص423.

ب-الإختصاص الخارجي في التفتيش. الأصل أن التفتيش لا يتخطى حدود الدولة، حفاظاً على السيادة الإقليمية للدول، هذا ما أكدت عليه المادة (4) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذلك المادة(4) من الإتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، والتي نهت عن ممارسة أي دولة ولايتها القضائية على إقليم دولة أخرى.

رئيسة نيابة مكافحة الجرائم الإلكترونية في مقابلتي معها أفادت، على أنه في حال تبين لعضو النيابة أن الجريمة الإلكترونية التي يحقق بها إرتكبت من خارج الدولة، وتم تحديد هذه الدولة، يقوم عضو النيابة بإعداد مذكرة يرفعها إلى النائب العام، يبلغه بما وصل إليه التحقيق، ويطلب القيام بإجراء تفتيش في الدولة التي إرتكبت منها الجريمة عن طريق طلب المساعدة القانونية، للحصول على الأدلة اللازمة، وفي هذه الحالة يخضع تقدير الموقف بطلب المساعدة القانونية للنائب العام.

نظم المشرع الفلسطيني طلب المساعدة القانونية المتبادلة في المادة(43) من قانون الجرائم الإلكترونية، في حالة وجود إتفاقيات ثنائية، أو متعددة الأطراف، تكون فلسطين طرف فيها، أو بالإستناد إلى مبدأ المعاملة بالمثل في حالة عدم وجود إتفاقيات، وقد أقرت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المساعدة القانونية في المادة(32)، وكذلك الإتفاقية العربية لمكافحة الجريمة عبر الحدود الوطنية⁽¹⁾، وتكون المساعدة القضائية عن طريق وزارة العدل أو الإنترنت أو بدونهما.

1.المساعدة القضائية عن طريق وزارة العدل. نصت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، على ضرورة تحديد كل طرف سلطة مركزية تكون مسؤولة عن إرسال طلبات المساعدة القانونية⁽²⁾، وأفادت رئيس نيابة الجرائم الإلكترونية في مقابلتي معها، أنّ الجهة المختصة بإرسال وإستقبال طلبات المساعدة في فلسطين هي دائرة التعاون القضائي الدولي في مكتب النائب العام، وقد نظمت إتفاقية الرياض للتعاون القضائي، آلية إرسال طلب المساعدة عن طريق وزارة العدل، وإنابة طرف آخر للقيام بإقليمه بأي إجراء قضائي⁽³⁾، ومن ضمنها التفتيش، وفي الحالات العاجلة، أجازت المادة (1/8/34) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، إرسال طلب

⁽¹⁾ أنظر المادة (26) من الإتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

⁽²⁾ أنظر المادة(2/34) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

⁽³⁾ أنظر المواد(14 +15/ب) من إتفاقية الرياض للتعاون القضائي، الصادرة عن جامعة الدول العربية، بتاريخ 1983/4/6، بالرياض، المملكة العربية السعودية، صادقت عليها دولة فلسطين بتاريخ 1983/11/28.

المساعدة القانونية مباشرة إلى السلطات القضائية في الدولة الطرف، مع إرسال نسخة عن طريق وزارة العدل.

2. المساعدة القضائية عن طريق الشرطة الدولية (الإنتربول) . من أهداف إنشاء المنظمة الدولية للشرطة الجنائية (الإنتربول)⁽¹⁾، تأمين وتنمية المساعدة المتبادلة بين الدول للوقاية من الجرائم الدولية ومكافحتها، ونصت المادة الثانية من القانون الأساسي للمنظمة على أهداف إنشائها وجاء فيها بان أهداف المنظمة " تأمين وتنمية المساعدة المتبادلة على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان وبروح الإعلان العالمي لحقوق الإنسان، والوقاية من جرائم القانون العام ومكافحتها.

الإتفاقية العربية لمكافحة جرائم تقنية المعلومات أجازت في المادة(8/34/ب) تقديم طلب المساعدة القانونية عن طريق الشرطة الدولية، وبذلك تكون دائرة التعاون القضائي الدولي في مكتب النائب العام لها الخيار بطلب المساعدة القانونية إما عن طريق وزارة العدل، أو عن طريق منظمة الشرطة الجنائية الدولية، التي لها فرع في فلسطين.

3. التفتيش بدون مساعدة قانونية. قانون الجرائم الإلكترونية الفلسطيني لم يجيز إمتداد التفتيش خارج حدود الدولة، ولكن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة(40)، أجازت لأي دولة وبدون تفويض، الوصول إلى معلومات تقنية بغض النظر عن موقعها الجغرافي، بشرط أن تكون هذه المعلومات متوفرة للعامة(مصدر مفتوح)، أو أن تكون حاصلة على الموافقة القانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات، وأن المعلومات المطلوبة ضرورية للتحقيق، وهذا النص مشابه لنص المادة(32) من الإتفاقية الأوربية لمكافحة الجرائم السيبرانية، حيث يجب أن تمنح السلطة المختصة في الجرائم الإلكترونية، إختصاص بالتفتيش خارج حدود الدولة، إذا كان مرتكب الجريمة أجنبياً، وإستهدف مؤسسات الدولة⁽²⁾، وكذلك بتجاوز التفتيش لحدود

⁽¹⁾ أنظر المادة(2) من القانون الأساسي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، الصادر بتاريخ 13/6/1956، فيينا، وأصبحت فلسطين عضو في الجمعية العامة للمنظمة، بتاريخ 27/9/2017، في الدورة (86) المنعقدة في بكين.
⁽²⁾ بوزوجة، عبد الحكيم، موقف المشرع الجزائري من الجريمة المعلوماتية، بحث مقدم للمؤتمر العلمي الحادي عشر، كلية الحقوق، جامعة جرش، 5-7/5/2015، ص 8.

لحدود الدولة، في حالات المطاردة الفورية⁽¹⁾.

يرى الباحث أنّ التفتيش في الجرائم الإلكترونية داخل الدولة يمكن إجراءه بسرعة بعد الحصول على الإذن بذلك، والعثور على الأدلة المطلوبة ونسبتها إلى الفاعل، ولكن المشرع الفلسطيني لم يجيز إمتداد التفتيش خارج حدود الدولة، ونظم إجراءه عن طريق طلب المساعدة القضائية سواء تم عن طريق وزارة العدل أو الشرطة الدولية، وهذا الإجراء لا يمكن القيام به بالسرعة الملائمة للجرائم الإلكترونية، كون الإجراءات والمخاطبات اللازمة بحاجة إلى وقت حتى تصل إلى الجهات المختصة لتنفيذها، وهذا يؤدي إلى فقدان وتدمير الأدلة اللازمة خلال تلك الفترة، وبالتالي يفقد التفتيش غايته، وتعتمد تلك الإجراءات على علاقات الدول فيما بينها، فإذا كانت العلاقات جيدة جرى التفتيش على وجه السرعة، أمام إذا كانت العلاقة متوترة فإن التفتيش يتم ببطء أو لا يتم إجراءه، وبناء على ذلك وكون أن الجريمة الإلكترونية عابره للحدود، ويمكن إجرائها من أي مكان على وجه الأرض، يؤيد الباحث الآراء التي تقر بضرورة توسيع التفتيش على وسائل تكنولوجيا ليمتد إلى خارج حدود الدولة في الجرائم الإلكترونية.

الفرع الثاني: مأموري الضبط القضائي في الجرائم الإلكترونية.

مأمور الضبط القضائي، هو كل من أوكل إليه القانون مسؤولية ضبط الوقائع التي جرمها القانون ووضع لها جزاءً جنائياً وجمع الأدلة عليها⁽²⁾، والقانون هو الذي يحدد من هم مأموري الضبط القضائي، ومنحهم سلطة واسعة، فلا يريد القانون أن يباشر مهام الضبط القضائي إلا أشخاص وثق فيهم إبتداءً⁽³⁾.

أجاز قانون الجرائم الإلكترونية الفلسطيني بالمادة (1/32) ندب مأموري الضبط القضائي للقيام بتفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات المستخدمة وذات الصلة بالجريمة، ولكن في الجرائم الإلكترونية نظراً لخصوصيتها ولطبيعتها الرقمية، يحتاج التفتيش إلى مأمور ضبط

⁽¹⁾ الطوالبة، علي حسن محمد، التفتيش الجنائي على نظم الحاسوب والإنترنت، مرجع سابق، ص94.

⁽²⁾ علام، حسن، قانون الإجراءات الجنائية، ج1، م1 مطابع روز اليوسف، القاهرة، 1982، ص80.

⁽³⁾ حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، الدعاوي الناشئة عن الجريمة، الإستدلال، التحقيق الإبتدائي، ط3، دار النهضة العربية، القاهرة، 1995، ص382.

قضائي متخصص في البيئة الرقمية، للبحث عن الأدلة الإلكترونية⁽¹⁾.

أنشأ قانون الجرائم الإلكترونية الفلسطيني بنص المادة (1/3)، وحدة متخصصة بالجرائم الإلكترونية في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي، وقد عدد قانون الإجراءات الجزائية الفلسطيني في المادة (21) مأموري الضبط القضائي⁽²⁾، وكذلك قانون الشرطة⁽³⁾، والقوانين الخاصة الأخرى. حيث سنبحث وحدة مكافحة الجرائم الإلكترونية بالشرطة في الفقرة الأولى، والأجهزة الأخرى في الفقرة الثانية، وموظفو وزارة الإتصالات وتكنولوجيا المعلومات في الفقرة الثالثة.

أولاً: وحدة مكافحة الجرائم الإلكترونية في جهاز الشرطة.

أنشأت وحدة مكافحة الجرائم الإلكترونية وتكنولوجيا المعلومات والإتصالات في جهاز الشرطة في منتصف عام 2013، بقرار من مدير عام الشرطة، وتتبع هذه الوحدة إدارة المباحث العامة في جهاز الشرطة، ومكتبها الرئيسي في مقر قيادة الشرطة برام الله⁽⁴⁾، وأضحى عمل لهذه الوحدة والإجراءات التي تقوم بها شرعية مع دخول القرار بقانون بشأن الجرائم الإلكترونية حيز التنفيذ.

قانون الجرائم الإلكترونية هو الذي أنشاء وحدة مكافحة الجرائم الإلكترونية، والعلة من إنشائها هو عدم مقدرة مأموري الضبط العاديين على التعامل مع البيئة الإلكترونية، ويعتبر إنشائها نوع من الإجراءات والضمانات للمحافظة على أموال الغير وأسرارهم⁽⁵⁾، وأصبح لتلك الوحدة إختصاص نوعي محدد، لا يجوز لغيرهم القيام بالتفتيش بالجرائم الإلكترونية. حيث سنبحث في تشكيلات تلك الوحدة وتحديد أعضائها.

1- الوحدة الرئيسية. رئيس وحدة مكافحة الجرائم الإلكترونية في الشرطة في مقابلي معه أفاد، أن الوحدة تتكون من عدة أقسام، على رأسها مدير يدير شؤونها، ونائب له في حالة غيابه، وأقسام

(1) موسى، مصطفى محمد، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة، القاهرة، 2009، ص166.

(2) وهم مدير الشرطة ونوابه ومساعديه، ومديرو المحافظات، وضباط وضباط صف الشرطة في دائرة إختصاصهم، رؤساء المراكب البحرية والجوية.

(3) أنظر المادة (6) من قرار بقانون بشأن الشرطة، رقم (23) لسنة 2017.

(4) مقابلة بحثية، مع المقدم/ سامر الهندي، رئيس وحدة مكافحة الجرائم الإلكترونية وتكنولوجيا المعلومات والإتصالات في جهاز الشرطة، أجريت بتاريخ 2018/5/6، الساعة الخامسة والنصف مساءً، في مكتب وحدة مكافحة الجرائم الإلكترونية، رام الله، فلسطين.

(5) الصغير، جميل عبد الباقي، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002، ص77.

متخصصة هي، قسم جرائم الإنترنت وجرائم التقنية، وقسم الأدلة الرقمية الذي ينقسم إلى (مختبر الأدلة الرقمية، ومخزن الأدلة الرقمية)، وهو القسم المختص بالتفتيش وضبط الأدلة وتخزينها، وقسم التوعية والإرشاد، وقسم الإتصالات وتأمين المعلومات، وقسم التحقيق والدائرة القانونية.

إن إختصاص الوحدة الرئيسية كما أفاد رئيسها، يتمثل أولاً في إستقبال الإحتياج الوارد من رئيس نيابة مكافحة الجرائم الإلكترونية، لتحديد وسائل تكنولوجيا المعلومات، والإتصالات، التي إرتكبت بواسطتها الجريمة الإلكترونية، وتزويد رئيس النيابة بتقرير فني بالمعلومات المطلوبة، وثاني مهامها، تنفيذ أمر النيابة بالنفذ المباشر إلى وسائل تكنولوجيا المعلومات المضبوطة وتفتيشها، للحصول على المعلومات والأدلة المطلوبة، وثالثاً وفي حالات معينة متابعة بعض القضايا المعقدة التي لا يقدر عليها ضباط الشرطة بالمحافظات.

2-أعضاء وحدة مكافحة الجرائم الإلكترونية . إختيار أعضاء وحدة الجرائم الإلكترونية يجب أن يتم بعناية، ويكونوا من النخبة المتخصصة في مجال تكنولوجيا المعلومات، لهم موهبة التحقيق والإبداع والقدرة على الاستنتاج والتحليل وسرعة التصرف وقوة الملاحظة والهدوء وضبط النفس وحفظ الأسرار⁽¹⁾.

رئيس وحدة مكافحة الجرائم الإلكترونية في جهاز الشرطة أفاد في مقابلي معه، على وجود إثنين إلى ثلاثة ضباط شرطة بقسم المباحث في كل محافظة، مدربين على التعامل ومتابعة قضايا الجرائم الإلكترونية الواردة إلى الشرطة في مناطقهم، ويمارسون عملهم تحت إشراف عضو النيابة المختص، وتنفيذ قراراته.

ثانياً: وحدات مكافحة الجرائم الإلكترونية في الأجهزة الأخرى.

وحدات مكافحة الجرائم الإلكترونية في قوى الأمن، نص على إنشائها قانون الجرائم الإلكترونية في المادة(1/3) كما في جهاز الشرطة، على أن تكون هذه القوى من مأموري الضبط القضائي.

القانون الأساسي الفلسطيني في المادة(84) حدد قوى الأمن، وفصل قانون الخدمة في قوى الأمن

(1) إبراهيم، خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، ط1، دار الفكر الجامعي، الإسكندرية، 2010، ص 95 ما بعدها.

السلطانية تشكياتها⁽¹⁾، حيث منح القانون بعض هذه القوى صفة الضابطة القضائية كجهاز الأمن الوقائي⁽²⁾، والمخابرات العامة⁽³⁾، والاستخبارات العسكرية⁽⁴⁾، وهذه الصفة تمكنهم من إنشاء وحدات متخصصة لمكافحة الجرائم الإلكترونية وفق القانون، ولكن هذه الوحدات تحتاج إلى كوادر بشرية متخصصة، ومعدات تقنية فنية للقيام بعملها كما في جهاز الشرطة.

ثالثاً: موظفو وزارة الإتصالات وتكنولوجيا المعلومات.

مأموري الضبط القضائي، بعضهم من رجال الأمن، والبعض الآخر من غير رجال الأمن، والقانون هو الذي يحدد من هم مأموري الضبط القضائي بشكل مباشر، أو بطريقة غير مباشرة عن طريق تفويض الوزير المختص منح هذه الصفة لبعض موظفيه بالنسبة لبعض الجرائم المرتبطة بوظائفهم.

قانون الجرائم الإلكترونية الفلسطيني في المادة (54) منح موظفي وزارة الإتصالات وتكنولوجيا المعلومات الذين يعينهم الوزير صفة مأموري الضبط القضائي، لتقديم الدعم والمساعدة الفنية لوحدات مكافحة الجرائم الإلكترونية في قوى الأمن، وبهذه الصفة يجوز إنداب موظفي وزارة الإتصالات وتكنولوجيا المعلومات للقيام بإجراءات التفتيش على وسائل تكنولوجيا المعلومات.

المطلب الثاني

خصوصية السلطة المختصة في التفتيش بالجرائم الإلكترونية.

يمتاز أعضاء السلطة المختصة بالتفتيش بالجرائم الإلكترونية بخصائص تميزهم عن زملائهم، على صعيد التدريب والتأهيل الفني الذي يخضعوا له.

التفتيش في الجرائم الإلكترونية عمل من أعمال التحقيق الإبتدائي، والتحقيق الإبتدائي هو مجموعة من الإجراءات تباشرها السلطة المختصة لكشف الحقيقة عن جريمة ارتُكبت، بالبحث والتفتيش عن

(1) أنظر المواد (3+7+12+13) من قانون الخدمة في قوى الأمن الفلسطينية، رقم (8) لسنة 2005.

(2) أنظر المادة (7) من قرار بقانون بشأن الأمن الوقائي الفلسطيني.

(3) انظر المادة (12) من قانون المخابرات العامة الفلسطيني، رقم (17) لسنة 2005.

(4) أنظر المادة (1) من قرار بقانون بشأن الإستخبارات العسكرية الفلسطيني، رقم (34) لسنة 20014.

الأدلة وتجميعها⁽¹⁾، وهي المرحلة الأولى والمهمة بالخصوصة الجنائية، والتي يتم من خلالها جمع الأدلة، وتحديد مدى جدوى تقديم المتهم للمحكمة لإقرار حق الدولة في العقاب⁽²⁾، ويتولى ذلك عضو النيابة الذي يعد المحقق في الدعوى الجزائية، والمحقق، هو كل من عهد إليه القانون بتحري الحقيقة في الحوادث الجنائية⁽³⁾، ويمكن أن يفوض عضو النيابة بعض من صلاحياته في التحقيق إلى مأمور الضبط القضائي، ومنها إجراء تفتيش، ولكن يجب على أعضاء السلطة المختصة بالتفتيش بالجرائم الإلكترونية أن يكونوا مؤهلين للتعامل مع نوعية تلك الجرائم، كون هذا العمل هو عمل دقيق، وحساس، ويمس خصوصية الناس، بالإطلاع على أسرارهم، ومن الممكن أن تكون نتائجه عكسية بإضاعة الأدلة وتدميرها. حيث سنبحث في خصوصية أعضاء نيابة مكافحة الجرائم الإلكترونية بالفرع الأول، وبالفرع الثاني خصوصية مأموري الضبط القضائي.

الفرع الأول: خصوصية أعضاء نيابة مكافحة الجرائم الإلكترونية.

إن إجراء التفتيش بالجرائم الإلكترونية علم وفن⁽⁴⁾، ومن هنا تظهر خصوصية أعضاء نيابة مكافحة الجرائم الإلكترونية، في خبراتهم، وتأهيلهم، للتعامل مع البيئة الإلكترونية، كون التفتيش يعتبر أحد أعمدة التحقيق الابتدائي، وهو أخطر إجراء للكشف عن الأدلة ونسبتها إلى الفاعل أو نفيها عنه.

لخطورة إجراءات التفتيش في الجرائم الإلكترونية، لا بد لمن منح هذه السلطة أن يكون على دراية تامة في بيئة تكنولوجيا المعلومات، والتمتع بقدرات تؤهله للتعرف على آلية عمل هذه البيئة وطرق ارتكاب الجرائم الإلكترونية، كون التفتيش في البيئة الرقمية يعد أهم وأصعب مرحلة في التحقيق الابتدائي، لذلك لا بد أن يمتاز أعضاء نيابة الجرائم الإلكترونية بمؤهلات تميزهم عن غيرهم من أعضاء النيابة الآخرين، وبقدرات تؤهلهم للتعامل مع تكنولوجيا المعلومات، حيث سنبحث تأهيلهم القانوني في الفقرة الأولى، وتأهيلهم الفني في الفقرة الثانية.

(1) حسن، سعيد عبد اللطيف، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر شبكة الإنترنت، ط1، دار النهضة العربية، القاهرة، 1999، ص 133.

(2) سرور، احمد فتحي، الوسيط في قانون الإجراءات الجنائية، ط7، دار النهضة العربية، القاهرة، 1996، ص456.

(3) جاد، نبيل عبد المنعم، أسس التحقيق الجنائي العلمي، بدون ناشر، 1991، ص11.

(4) بن يونس، عمر محمد، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، ترجمة ودراسة المرشد الفدرالي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، ط2، دار النهضة العربية، القاهرة، 2006/2005، ص 18.

أولاً: تأهيل قانوني.

يشترط فيمن يعين عضواً في النيابة العامة، أن يكون حاصلًا على إجازة الحقوق، أو إجازة الشريعة والقانون، من إحدى الجامعات المعترف بها⁽¹⁾، وبعد إخضاعه للتدريب اللازم على إجراءات التحقيق، يكون على معرفة في قوانين الدولة، وخاصة القوانين الإجرائية الجزائية.

1- القوانين الوطنية. الجرائم الإلكترونية بحاجة إلى رجال قانون على دراية تامة بالقوانين المحلية، وقادرين على التعامل مع الجريمة الإلكترونية بمنظور يجمع بين علم الإجرام وعلم ضحايا الجريمة وتكنولوجيا المعلومات⁽²⁾.

يرى الباحث أنّ أعضاء نيابة مكافحة الجرائم الإلكترونية المختصين بالتفتيش في الجرائم الإلكترونية، يجب أن يكونوا على دراية تامة بالنصوص الدستورية المقررة للتفتيش، والتعمق في معرفة نصوص القانون الإجرائي العام وقانون الجرائم الإلكترونية المتعلقة بالتفتيش، لدقتها، وخطورتها، كون التفتيش في الجرائم الإلكترونية من أشد إجراءات التحقيق مساساً بالحرية الشخصية، والمتمثل بالاطلاع عن خصوصية الناس المخزنة في وسائل تكنولوجيا المعلومات، وكذلك ضرورة أن يكون أعضاء نيابة مكافحة الجرائم الإلكترونية على دراية تامة في القوانين الوطنية ذات العلاقة بوسائل تكنولوجيا المعلومات، إضافة إلى قانون الجرائم الإلكترونية، قانون مكافحة غسل الأموال وتمويل الإرهاب، وقانون الاتصالات السلكية واللاسلكية، وقانون الهيئة الفلسطينية لتنظيم قطاع الاتصالات، وقانون المعاملات الإلكترونية، وجميع القوانين ذات العلاقة بالتكنولوجيا الحديثة.

2- الإتفاقيات الخاصة بالجرائم الإلكترونية. ملاحقة المجرم الإلكتروني تكون بلا جدوى، بدون التعاون القضائي بين الدول، وخاصة في إجراءات التفتيش⁽³⁾، وهذا ما أكدت عليه المادة (42) من قانون الجرائم الإلكترونية الفلسطيني، على تيسير التعاون مع البلاد الأجنبية في إطار الإتفاقيات

(1) أنظر المواد (16 + 61) من قانون السلطة القضائية الفلسطيني.

(2) توصيات المؤتمر الثاني للرابطة الدولية للقانون الجنائي، حول الجرائم الرقمية، الذي عقد في عام 2000، أمستردام، هولندا.

(3) قشقوش، هدى حامد، الجريمة المنظمة، القواعد الموضوعية والإجرائية والتعاون الدولي، ط1، دار النهضة العربية، القاهرة، 1997، ص85.

المصادق عليها، أو على مبدأ المعاملة بالمثل.

يرى الباحث أنه واجب على عضو النيابة أن يكون على معرفة ودراية تامة بالإتفاقيات الثنائية ومتعددة الأطراف، الموقعة عليها الدولة في مجال تكنولوجيا المعلومات، وخاصة الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، والإتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، وقانون الإمارات العربي الإسترشادي لمكافحة تقنية المعلومات وما في حكمها، وإتفاقية الرياض العربية للتعاون القضائي، لمعرفة الجرائم الإلكترونية المشتركة بين الدول العربية، وطرق طلب المساعدة القضائية وإجراءاتها، وكذلك الاطلاع على شروط تجاوز التفتيش لحدود الدولة.

وكذلك يرى الباحث أنه يجب على عضو النيابة الإطلاع على الإتفاقيات الخاصة بحقوق الإنسان، الموقعة عليها الدولة، كالميثاق العربي لحقوق الإنسان، والإعلان العالمي لحقوق الإنسان، والعهد الدولي الخاص بالحقوق المدنية والسياسية، لتكون هذه الإتفاقيات سداً منيعاً بعدم تجاوز القانون في التفتيش، والإطلاع على ميثاق الأمم المتحدة، والإتفاقية الأوروبية لحقوق الإنسان كون أن المراقبين الأوروبيين يراقبوا باستمرار مدى إحترام حقوق الإنسان ببلادنا، والاطلاع على إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، والقوانين العربية المقارنة في الجرائم الإلكترونية، وإذا أمكن الإطلاع على القوانين الأجنبية، وقراءة كتب شراح القانون الغربيين في مجال تكنولوجيا المعلومات للإطلاع على إجراء التفتيش، وملاحقة التطورات الخاصة بالجريمة الإلكترونية في الدول المتقدمة.

ثانياً: التأهيل الفني.

التفتيش في الجرائم الإلكترونية، يحتاج إلى نيابة لمكافحة تلك الجرائم يكون أعضائها متميزين ومدربين تدريب فني يساعدهم في السير بخطى ثابتة في التحقيق في الجرائم الإلكترونية.

التأهيل الفني لأعضاء النيابة المختصين بالتفتيش بالجرائم الإلكترونية، له أهمية بالغة في تطوير معلوماتهم في مجال تكنولوجيا المعلومات⁽¹⁾، والرفع من قدرتهم على الإشراف على إجراءات التفتيش، ومعرفة طرق التفتيش في البيئة الإلكترونية، وطرق إستخراج الأدلة، وهذا يؤدي إلى فهم

⁽¹⁾ رمضان، مدحت، جرائم الإعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000، ص82.

الأدلة المتحصلة عن التفتيش في الجرائم الإلكترونية⁽¹⁾، وأعضاء نيابة مكافحة الجرائم الإلكترونية بحاجة إلى تدريب فني مستمر، وإطلاع دائم، ليلتحقوا بالتطورات التقنية المستمرة والمتجددة⁽²⁾.

1- وسائل ارتكاب الجريمة الإلكترونية. يجب تدريب أعضاء النيابة المختصين بالتحقيق بالجرائم الإلكترونية على معرفة جميع وسائل تكنولوجيا المعلومات التي ترتكب من خلالها الجريمة الإلكترونية، وأن يكون عضو النيابة المختص على علم كامل بالمكونات المادية وغير المادية للحاسب الآلي، وكيفية عمله، ومعرفة بالشبكات المحلية، والعالمية، وطريقة عملها، ومعرفة طرق ارتكاب الجريمة الإلكترونية⁽³⁾.

2- اللغة الإنجليزية. يجب تدريب أعضاء النيابة المختصين بالتحقيق بالجرائم الإلكترونية، على لغة الإنترنت، ولغة البرامج، ووظائفها، وإختصاصاتها المتنوعة، وطرق معالجة البيانات، والمخاطر التي يمكن أن تتعرض لها⁽⁴⁾.

إن اللغة العربية، هي اللغة المعتمدة في التحقيق⁽⁵⁾، كونها اللغة الرئيسية للدولة، ولكن في الجرائم الإلكترونية يجب على عضو النيابة أن يكون على إطلاع ومعرفة باللغة الإنجليزية، لفهم المصطلحات العلمية الخاصة بوسائل تكنولوجيا المعلومات، وفهم أليه عملها ووظائفها⁽⁶⁾، كون أن أغلب هذه المصطلحات تكتب بلغتها الأم ويصعب تعريبها، ويجب كتابتها كما هي في محضر التحقيق والضبط، وكذلك يستفاد من المعرفة باللغة الإنجليزية، الإطلاع على آخر ما وصل إليه العلم في طرق التفتيش بمجال تكنولوجيا المعلومات في الدول المتقدمة.

رئيس نيابة مكافحة الجرائم الإلكترونية، في فلسطين، في مقابلي معها أفادت، انه تم إعطاء

(1) سقف الحيط، عادل عزام، جرائم الدم والقذح والتحقير المرتكبة عبر الوسائط الإلكترونية، ط2، دار الثقافة للنشر والتوزيع، عمان، 2015، ص232.

(2) الصاعدي، محمد، جرائم الإنترنت وجهود المملكة العربية السعودية في مكافحتها، بحث مقدم إلى ندوة "مكافحة الجريمة عبر الإنترنت على المستوى العربي، ابريل/2008، شرم الشيخ، مصر، ص 7.

(3) الغافري، حسين بن سعيد، السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009، ص504 وما بعدها.

(4) رستم، هشام محمد فريد، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني والية التدريب التخصصي للمحققين، مقالة منشورة في مجلة الأمن والقانون، كلية شرطة دبي، العدد الثاني، 1999، ص30 وما بعدها.

(5) أنظر المادة(60) من قانون الإجراءات الجزائية الفلسطيني.

(6) إبراهيم، خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 69.

جميع أعضاء النيابة العامة في فلسطين، دورات بشكل عام، لتعريفهم بمفهوم الجرائم الإلكترونية وكيفية التعامل معها وطرق إرتكابها، وبشكل خاص تم إعطاء أعضاء نيابة مكافحة الجرائم الإلكترونية، دورات تدريبية متخصصة في أدوات التقنية الرقمية التي يمكن الحصول منها على الدليل الرقمي، وتحليله، لرفع كفاءتهم في التحقيق بالجرائم الإلكترونية، وسيتم إعطائهم مزيد من الدورات المتخصصة في البيئة الإلكترونية.

الفرع الثاني: خصوصية وحدات مكافحة الجرائم الإلكترونية.

الأصل، أن يقوم عضو النيابة المختص بإجراء التفتيش بنفسه، ولكن في أغلب الأحيان يقوم به مأموري الضبط القضائي بناءً على نداء من عضو النيابة، ولكن في الجرائم الإلكترونية لا يستطيع عضو النيابة القيام في التفتيش بنفسه، كون أن إجراءاته معقد لا يستطيعه سوى المتخصص⁽¹⁾.

إنداب مأموري الضبط القضائي للتفتيش في الجرائم الإلكترونية يتم من وحدات مكافحة الجرائم الإلكترونية، كون تلك الوحدات تضم كوادر بشرية مدربة تدريباً خاصاً للتعامل مع البيئة الرقمية، وكون التفتيش بالجرائم الإلكترونية عمل شاق يحتاج إلى خبرة فنية عميقة، لا يستطيع القيام بها إلا الخبير المتخصص، وهذا ما أكدت عليه المادة (5/32) من قانون الجرائم الإلكترونية الفلسطيني، عندما اشترط أن يكون مأمور الضبط القضائي مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية، ولكن القانون لم يفسر طبيعة هذا التأهيل. لذلك سنبحث أعضائها في الفقرة الأولى، وتأهيلهم الفني في الفقرة الثانية، وفريق التفتيش في الفقرة الثالثة، وطرق تعاونهم مع الشرطة الدولية في الفقرة الرابعة، ومعرفتهم باللغة الإنجليزية في الفقرة الخامسة.

أولاً: أعضاء وحدة مكافحة الجرائم الإلكترونية.

يجب أن تتوافر في من يتم إختياره من مأمور الضبط القضائي للعمل في وحدة مكافحة الجرائم الإلكترونية، خبرة في التحقيق في القضايا المعقدة، والدراسة الفنية لتكنولوجيا المعلومات للقيام بالتفتيش⁽²⁾، وأن تجمع الوحدة أعضاء متخصصين في جميع مجالات تكنولوجيا المعلومات، وأن

(1) عزت، محمد فتحي محمد أنور، تفتيش شبكة الإنترنت، مرجع سابق، ص 349+350.

(2) داود، حسن طاهر، جرائم نظم المعلومات، ط1، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص 222.

يكون أعضاؤها ممن يملك مهارات فنية تميزه عن غيره، حتى يستطيع القيام بالتفتيش في البيئة الرقمية⁽¹⁾.

ثانياً: تأهيل فني.

التأهيل الفني لمأموري الضبط القضائي المختص بالتفتيش بالجرائم الإلكترونية، أهم بكثير من تأهيل أعضاء النيابة، كون أنهم هم الذين يجرون التفتيش بأنفسهم، بناءً على ندب من عضو النيابة، ويجب أن يحصل أعضاء الوحدة على تدريب متخصص على تقنيات تكنولوجيا المعلومات وأساليب التفتيش فيها وجمع الأدلة⁽²⁾، وكلما كان تأهيل مأمور الضبط القضائي على تقنية تكنولوجيا المعلومات عالياً فإنه يؤدي إلى نجاح مهمة التفتيش، وإذا كان ينقصه الخبرة يؤدي إلى تدمير الأدلة وضياعتها⁽³⁾.

يقع على عاتق الدولة دعم إعداد برامج علمية وفنية مستمرة لتأهيل وتدريب مأموري الضبط القضائي على تقنية تكنولوجيا المعلومات وتزويد الوحدات بالأجهزة والتقنيات الحديثة لتساعدهم في إجراء التفتيش على وسائل تكنولوجيا المعلومات والحصول على الأدلة.

ثالثاً: تشكيل فريق للتفتيش في الجرائم الإلكترونية.

إن تشكيل فريق للتفتيش في الجرائم الإلكترونية، له أهمية كبرى في نجاح المهمة والحصول على الأدلة المطلوبة، كون التفتيش في البيئة الرقمية أكبر من أن يتولاه شخص واحد بمفرده، لأن الجريمة الإلكترونية لها عدة أنواع ونماذج، وبحاجة إلى تخصصات علمية وفنية دقيقة ومتنوعة ومتطورة ومتلاحقة، لدرجة يصعب على المختص تتبعها لوحده⁽⁴⁾، ولا يوجد خبير واحد قادر على التعامل مع كافة أنماط الجرائم الإلكترونية ومعرفة كافة المصطلحات التي يتم استخدامها⁽⁵⁾.

فريق التفتيش، يجمع بين أعضائه جميع التخصصات في البيئة الإلكترونية، كمختصين في

(1) الحلبي، خالد عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، مرجع سابق، ص 155.

(2) الحسيناوي، علي جبار، جرائم الحاسوب والإنترنت، مرجع سابق، ص 130.

(3) أحمد، هلاي عبد اللاه، تفتيش نظم الحاسب الآلي، مرجع سابق، ص 146+147.

(4) الديري، عبد العال، وإسماعيل، محمد صادق، الجرائم الإلكترونية، مرجع سابق، ص 317.

(5) حجازي، عبد الفتاح بيومي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، ط 1، بدون ناشر، 2009، ص 232.

الحاسوب بجميع أنواعه، والأجهزة الخلوية بأنواعها المختلفة، والشبكات المحلية والدولية، ومختصين في البرامج المختلفة، والتحليل و الصوت، وشبكة الإنترنت⁽¹⁾، معتمدا على البناء العلمي والتكنولوجي لأفراده، تؤهلهم لإجراء مطاردة إلكترونية تخصصية للمجرمين⁽²⁾، وكل واحد من أعضاء الفريق متخصص في قسم معين بتقنيات المعلومات، يعملون مع بعضهم البعض بروح الفريق الواحد، منهم للمداومة وآخر لإجراء تفتيش وجمع للأدلة وضبطها.

يجب تكوين محققين مختصين في الجريمة الإلكترونية، وإحداث خلايا متخصصة على مستوى المحافظات، وإلحاق مهندسي تقنيين مختصين بتكنولوجيا المعلومات، وتزويدهم بأحدث التقنيات والوسائل اللازمة لانجاز مهامهم⁽³⁾، ولا يقتصر ذلك على الوحدة الرئيسية.

رابعاً: التعاون مع الشرطة الدولية.

إن التفتيش بالجرائم الإلكترونية، خارج حدود الدولة لا يتحقق في أغلب الأحيان إلا بتعاون مع الشرطة الدولية، ويسمح به بين أجهزة الشرطة في الدول المختلفة⁽⁴⁾، ويجب أن تشمل الوحدات على أشخاص للتواصل مع الأجهزة الشرطة في دول العالم، وخاصة، الشرطة الدولية (الإنتربول).

إن مواجهة الجرائم الإلكترونية يستحيل على أي دولة أن تقوم به بمفردها، ومكافحة هذه الجرائم بحاجة إلى القيام ببعض العمليات الشرطة والأمنية المشتركة للقيام بالتفتيش العابر للحدود بحثاً عن الأدلة، كون شرطة الدولة لا تستطيع لوحدها تعقب المجرمين وملاحقتهم⁽⁵⁾، وخاصة في المطاردة أو التتبع الإلكتروني، والذي يعتبر من قبيل التلبس الإعتباري للجاني⁽⁶⁾.

(1) موسى، مصطفى محمد، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 221 وما بعدها.

(2) الغافري، حسين بن سعيد، السياسة الجنائية في مواجهة جرائم الإنترنت، مرجع سابق، ص 450.

(3) فالي، علل، حجبة الأدلة الرقمية أمام القاضي الجزائري، بحث مقدم إلى المؤتمر العلمي الحادي عشر، المنعقد من 5 إلى 2015/5/7، جامعة جرش، الأردن، ص 12.

(4) عفيفي، كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ودور الشرطة والقانون، دراسة مقارنة، بدون ناشر، 2000، ص 325.

(5) القبالي، سعيد حماد صالح، الجهود الدولية في مواجهة الجرائم المعلوماتية، بحث مقدم إلى المؤتمر العلمي الحادي عشر، تحت عنوان الجرائم المعلوماتية، 5 إلى 2015/5/7 جامعة جرش، عمان، ص 12+13.

(6) بن يونس، عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 848.

خامساً: اللغة الإنجليزية.

كما أسلفنا، ولنفس الأسباب التي تم شرحها في تأهيل أعضاء نيابة مكافحة الجرائم الإلكترونية ورفع قدرته في اللغة الإنجليزية، يجب رفع قدرات أعضاء وحدة الجرائم الإلكترونية في اللغة الإنجليزية، ولكن بشكل أعمق لمأموري الضبط القضائي، كون أنهم يقومون بالتفتيش والضبط وتنظيم المحاضر بأنفسهم، ولسبب آخر لا يقل أهمية، متمثل في إتصالهم مع الشرطة الدولية، أو الأجنبية، سواء شفاهة أو كتابة، ويجب على من يقوم بهذه المهمة إتقان اللغة الإنجليزية بطلاقة.

رئيس وحدة الجرائم الإلكترونية في جهاز الشرطة، أفاد في مقابلي معه، أن أعضاء وحدة الجرائم الإلكترونية، جميعهم من منتسبي جهاز الشرطة، وتم اختيارهم من الأكاديميين والهواة في المجال الإلكتروني، وحصلوا على تدريب داخلي وخارجي بكل نواحي الجرائم الإلكترونية، ومنها التفتيش والضبط في البيئة الرقمية، واللغة الإنجليزية للتعامل مع المصطلحات الإلكترونية، ولم يتم الإستعانة بأي خبراء من خارج جهاز الشرطة، وأن الوحدة تقوم بأعمالها وفق القانون، وتحت إشراف رئيس نيابة مكافحة الجرائم الإلكترونية، ولا يمكن النفاذ المباشر إلى وسائل تكنولوجيا المعلومات وإجراء تفتيش عليها إلا بإذن من النيابة، وأن الإتصال مع مكتب الشرطة الدولية في فلسطين يتم عبر النيابة لإعطاء شرعية قانونية للإجراء.

يرى الباحث انه يتوجب على وحدات مكافحة الجرائم الإلكترونية، إستقطاب الهاكرز والكرارز⁽¹⁾، وإستصلاحهم، وتوظيفهم للعمل في الوحدات الإلكترونية، لما يملكوه من مهارات فنية عالية في إستخدام تكنولوجيا المعلومات، ومعرفة متطورة بطرق إرتكاب الجرائم الإلكترونية وكشفها، ومكافحتها، والطرق الخفية بالنفاذ المباشر إلى الوسائل الإلكترونية، وتفتيشها، والحصول على الأدلة منها، ويجب وضع عمليات التفتيش تحت الدراسة والتقييم بإستمرار من حيث عوامل النجاح وعوامل الفشل.

كذلك نرى ضرورة إنشاء مجلس وطني لمكافحة الجرائم الإلكترونية، ويكون لهذا المجلس سلطة

⁽¹⁾ Hacker: يطلق على الشخص الذي يقوم بعمليات الاختراق والتخريب والتجسس عبر شبكة الإنترنت.

Cracher: يطلق على الشخص المتخصص في فك أو كسر شفرات البرامج أو كلمات السر.

ورد في كتاب أحمد، هلاي عبد اللاه، جرائم الحاسوب والإنترنت بين التجريم الجنائي واليات المواجهة، مرجع سابق، ص

قانونية وتقنية وأمنية، يضم بين أعضائه، ممثل عن نيابة مكافحة الجرائم الإلكترونية، وممثل عن وحدات الجرائم الإلكترونية في قوى الأمن المتخصصة، وممثل عن وزارة الإتصالات وتكنولوجيا المعلومات، وخبراء فنيين وأكاديميين في البيئة الرقمية، وخبراء في القانون المحلي والدولي، ويكون من مهام هذا المجلس وضع معايير السياسة الجنائية في الميدان الإلكتروني، ودراسة القوانين المتعلقة في الميدان الإلكتروني وتقييمها، وإقتراح التعديلات اللازمة عليها، ودراسة وتقييم الإتفاقيات الدولية أو الثنائية أو الإقليمية الخاصة بالجرائم الإلكترونية، قبل المصادقة عليها من الجهة المختصة في الدولة.

المبحث الثاني

شروط التفتيش في الجرائم الإلكترونية

أحاط المشرع إجراءات التفتيش بمجموعة من الشروط والضمانات، ليكفل إجراءه بشكل صحيح ولتحقيق الغاية منه، ولضمان عدم التعسف في إستعماله، وتجاوز حدوده، في الاعتداء على خصوصية الناس، وكشف أسرارهم التي حماها الدستور والقانون.

نص القانون الأساسي الفلسطيني في المادة (2/11) على ضمانات تفتيش الأشخاص، حيث جاء بالنص على أنه " لا يجوز القبض على احد أو تفتيشه ... إلا بأمر قضائي..."، وكذلك نص بالمادة (1/17) على ضمانات تفتيش المساكن وجاء بالنص على انه " للمساكن حرمة، فلا تجوز مراقبتها أو دخولها أو تفتيشها إلا بأمر قضائي مسبب وفقا لأحكام القانون". وهذه النصوص أقرت ضمانات دستورية لتفتيش الأشخاص والأماكن.

وعلى هدي القانون الأساسي وتطبيقا لنصوصه، جاء قانون الإجراءات الجزائية الفلسطيني ليؤكد على الضمانات الدستورية ويضيف ضمانات وشروط أخرى لإجراءات التفتيش، حيث نصت المادة (38) على ضمانات تفتيش الأشخاص، وبالفصل الرابع من الباب الثاني على ضمانات تفتيش المساكن، كون أن التفتيش من أكثر إجراءات التحقيق خطورة، كونه يمس حق الإنسان المقدس في خصوصيته، بالإعتداء القانوني على حرمة الشخصية أو حرمة مسكنه، بالاطلاع على أسرار وخصوصياته.

المشرع الفلسطيني أقر في المادة (32) من قانون الجرائم الإلكترونية بعض الضمانات للتفتيش في الجرائم الإلكترونية، ولم ينص على الضمانات الأخرى التي وردت في قانون الإجراءات الجزائية، والسؤال هنا، هل المشرع الفلسطيني إكتفى بضمانات التفتيش التي أقرها في قانون الجرائم الإلكترونية نظرا لخصوصيتها، تاركا الضمانات الأخرى كون أنها يمكن أن تكون عائقا على إجراء التفتيش؟. حيث سنبحث في المطلب الأول الضمانات المحددة للتفتيش بالجرائم الإلكترونية، وفي المطلب الثاني الضمانات المقيدة.

المطلب الأول

الضمانات المحددة للتفتيش في الجرائم الإلكترونية.

الضمانات المحددة للتفتيش في الجرائم بشكل عام، نجدها في نص الدستور، أو قانون الإجراءات الجزائية، أو القوانين الجزائية الأخرى كقانون الجرائم الإلكترونية.

إن الضمانات الخاصة بالتفتيش في الجرائم الإلكترونية أقرت للأشخاص والأماكن ووسائل تكنولوجيا المعلومات، كون أن التفتيش لا يجوز إجراءه إلا بأمر من السلطة القضائية المختصة، بإعتبارها الأمانة على حياة الناس وحفظ أسرارهم. حيث سنتناول سلطة التفتيش في الجرائم الإلكترونية بالفرع الأول، وسبب التفتيش في الفرع الثاني، ومحل التفتيش بالفرع الثالث.

الفرع الأول: سلطة التفتيش بالجرائم الإلكترونية.

من الضمانات الدستورية التي أقرها القانون الأساسي الفلسطيني في المواد (11+17)، لتفتيش الأشخاص والمساكن، أن يجري التفتيش بأمر من السلطة القضائية المختصة، سواء أثناء مرحلة التحقيق الابتدائي أو النهائي. لذلك سنبحث السلطة الأصلية في الفقرة الأولى ، والسلطة المنابة في الفقرة الثانية.

أولاً: السلطة الأصلية.

السلطة الأصلية، التي أناطها القانون بالتفتيش هي السلطة القضائية، والسلطة القضائية تتمثل في النيابة العامة الموكل إليها التحقيق الابتدائي، وقضاة المحاكم، الموكل إليهم بحكم القانون الأساسي إجراء التحقيق النهائي وإصدار الأحكام عنوان الحقيقة وإصدارها باسم الشعب العربي الفلسطيني.

1- النيابة العامة. كما أسلفنا، أنّ النيابة العامة المختصة بالتفتيش في الجرائم الإلكترونية، بالدرجة الأولى نيابة مكافحة الجرائم الإلكترونية، وبالدرجة الثانية يعود الإختصاص إلى جميع أعضاء النيابة العامة الآخرين.

الأصل، أن يقوم عضو نيابة مكافحة الجرائم الإلكترونية المختص مكانيا بإجراء التفتيش بنفسه، بمرافقة مأموري الضبط القضائي، بالانتقال إلى محل التفتيش بصحبة كاتباً⁽¹⁾، ليقوم الكاتب بتدوين جميع الإجراءات التي يقوم بها عضو النيابة، ويتقيد عضو النيابة عند قيامه بإجراء التفتيش بالقيود والضمانات التي يتقيد بها مأمور الضبط القضائي⁽²⁾، ولكن التفتيش في الجرائم الإلكترونية يصعب على عضو النيابة القيام به في أغلب الأحيان إن لم يكن في جميعها، كونه يحتاج إلى مختصين فنيين لإجرائه، وبالتالي يقوم عضو النيابة بنذب أحد مأموري الضبط القضائي من وحدة الجرائم الإلكترونية في قوى الأمن المتخصصة للقيام به.

2- المحكمة. لم يعطيها القانون سلطة إجراء التفتيش أثناء نظرها للدعوى، كون التفتيش ينفرد عن باقي طرق الإثبات بأنه إجراء تحقيق ابتدائي بينما الطرق الأخرى جائزة في مرحلة المحاكمة⁽³⁾، ولكن ليس هناك ما يمنع المحكمة أثناء نظرها الدعوى من نذب أحد أعضائها للقيام بالتفتيش إذا رأت ضرورة لذلك⁽⁴⁾.

نصت المادة (208) من قانون الإجراءات الجزائية الفلسطيني على انه " للمحكمة بناء على طلب الخصوم، أو من تلقاء نفسها أثناء سير الدعوى أن تأمر بتقديم أي دليل تراه لازماً لظهور الحقيقة..."، وكلمة أي دليل الوارد في النص يستوعب أن يكون من ضمنها إجراء تفتيش للحصول على دليل يؤيد التهمة أو ينفيها عن المتهم.

الباحث يرى أن للمحكمة الحق بإجراء تفتيش أثناء نظرها الدعوى، كون القانون منحها صلاحية واسعة للقيام بأي إجراء تراه مناسباً لظهور الحقيقة، ولعدم وجود مانع قانوني يحد من سلطتها لإجراء التفتيش، ويمكن تصور حالة تتمثل في ظهور شاهد لم يكن قد سمع بمرحلة التحقيق الابتدائي، وأدلى بمعلومات أمام المحكمة تفيد بوجود أدلة في مكان ما تؤيد التهمة أو تنفيها عن المتهم، وفي هذه الحالة للمحكمة أن تقوم بإجراء التفتيش بنفسها بتكليف أحد أعضائها، أو أن تنتدب أحد أعضاء النيابة العامة أو أحد مأموري الضبط القضائي لإجراء التفتيش.

(1) أنظر المادة (58) من قانون الإجراءات الجزائية الفلسطيني.

(2) راشد، حامد، أحكام تفتيش المسكن في التشريعات الإجرائية العربية، دراسة مقارنة، ط 1، دار النهضة العربية، القاهرة، 1998، ص 367 .

(3) مصطفى، محمود محمود، الإثبات في المواد الجنائية، الجزء الثاني، التفتيش والضبط، مرجع سابق، ص 3.

(4) السعيد، كامل، شرح قانون أصول المحاكمات الجزائية، مرجع سابق، ص 457.

ونرى كذلك أنه في الجرائم الإلكترونية، وبالنظر إلى خصائصها ومميزاتها الخاصة، يمكن أن تفرض نوعية هذه الجرائم على المحكمة القيام بإجراء تفتيش أثناء نظرها الدعوى على وسائل تكنولوجيا المعلومات، كون هذه الوسائل تمتاز بأنها توثق وتحفظ أي حركة يتم القيام بها من قبل أي شخص، لإمكانية استخدام برامج أو وسائل تقنية لإسترجاع كل الأشياء التي تم حذفها من هذه الوسائل.

ثانياً: السلطة النيابة.

أجاز المشرع الفلسطيني إنتداب مأموري الضبط القضائي لإجراء تفتيش بدل أعضاء النيابة العامة، حيث نصت المادة (1/32) من قانون الجرائم الإلكترونية الفلسطيني على أنه " للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة".

الإنيابة أو الندب بالتحقيق، يعرف بأنه " إجراء يصدر من قضاء إلى أحد مأموري الضبط القضائي لكي يقوم بدلاً منه بنفس الشروط التي يتقيد بها بمباشرة إجراء معين من إجراءات التحقيق التي تدخل في سلطته⁽¹⁾.

نظراً لخصوصية الجرائم الإلكترونية، يصعب على أعضاء السلطة القضائية القيام بإجراءات التفتيش بأنفسهم، حيث أجاز القانون لهم إنتداب احد مأموري الضبط القضائي من وحدة الجرائم الإلكترونية في قوى الأمن لإجرائه، سواء على الأشخاص والأماكن أو على وسائل تكنولوجيا المعلومات، ولكن يجب أن يكون المنتدب له صفة الضبط القضائي ومختص نوعياً ومكانياً⁽²⁾، والقانون نظم شروط التفويض وحدوده⁽³⁾، وحجة اللجوء إليه، لسرعة اتخاذ الإجراءات، أو لكون أن الإجراء يلزم للقيام به الخروج عن دائرة الاختصاص⁽⁴⁾، ويجب أن يكون الندب كتابي للقيام بعمل أو بعض أعمال محددة من أعمال التحقيق⁽⁵⁾.

(1) الشواربي، عبد الحميد، إذن التفتيش في ضوء القضاء والفقهاء، منشأة المعارف، الإسكندرية، بدون سنة نشر، ص 61.

(2) طنطاوي، إبراهيم حامد، الدفع ببطلان إذن النيابة العامة بالتفتيش، مرجع سابق، ص 25 وما بعدها.

(3) أنظر المادة(55) من قانون الإجراءات الجزائية الفلسطيني.

(4) الرخاوي، كمال كمال، إذن التفتيش فقهاً وقضائياً، ط1، دار الفكر والقانون، المنصورة، 2000، ص 25.

(5) القهوجي، علي عبد القادر، الندب للتحقيق، دار الجامعة الجديدة للنشر، الإسكندرية، 1997، ص 2.

يرى الباحث أن المنتدب للتفتيش بالجرائم الإلكترونية، هم مأموري الضبط القضائي من أعضاء وحدة مكافحة الجرائم الإلكترونية، وموظفو وزارة الإتصالات وتكنولوجيا المعلومات الممنوحين صفة مأمور الضبط القضائي من قبل الوزير المختص فقط ولا يمتد إلى غيرهم.

الفرع الثاني: سبب التفتيش في الجرائم الإلكترونية.

سبب التفتيش، من الشروط الموضوعية الجوهرية الواجب تحققها للقيام بالتفتيش، وهو من الضمانات القانونية التي أقرها قانون الإجراءات الجزائية الفلسطيني في صلب المادة(39) والتي أوجبت أن التفتيش لا يتم إلا بناءً على إتهام موجه إلى شخص بإرتكاب جناية أو جنحة أو لوجود قرائن قوية على أنه يحوز أشياء تتعلق بالجريمة ، وعبر عنه المشرع الفلسطيني في قانون الجرائم الإلكترونية بالمادة(2/32) بوسائل تكنولوجيا المعلومات ذات الصلة بالجريمة، وأجاز التفتيش للبحث عنها.

لا يصح إصدار إذن التفتيش إلا لضبط جريمة -جناية أو جنحة- وقعت بالفعل وترجحت نسبتها إلى متهم معين أو هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرية الشخصية⁽¹⁾. حيث سنبحث في وقوع جريمة إلكترونية بالفقرة الأولى، ومعرفة المجرم الإلكتروني في الفقرة الثانية، ومبررات التفتيش في الفقرة الثالثة.

أولاً: وقوع جريمة إلكترونية.

وقوع جريمة إلكترونية أول شرط من أسباب التفتيش في الجرائم الإلكترونية، وهذا مستقى من طبيعة التفتيش كعمل من أعمال التحقيق، كون التحقيق لا يبدأ إلا بعد أن تكون الجريمة قد وقعت، ولا يجوز التفتيش لجريمة مستقبلية محتملة الوقوع⁽²⁾، ويعد باطلا التفتيش الذي يتقرر بالنسبة لجريمة

(1) نقض جنائي مصري، بتاريخ 1987/11/11، أحكام النقض، س 38، ق 153، ص 943، مشار إليه في كتاب المرصفاوي، حسن صادق، المرصفاوي في القانون الجنائي، قانون الإجراءات الجنائية تشريعا وقضاء في مائة عام. ج3، منشأة المعارف، بدون سنة نشر، ص 372.

(2) الجوخدار، حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، دراسة مقارنة، ط2، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 131.

لم تقع بعد، ولو توافرت دلائل جديّة على أنها ستقع فعلا في المستقبل⁽¹⁾.

المشرع حصر التفتيش في جرائم الجرح والجنايات فقط، وبذلك يكون قد إستبعد التفتيش في المخالفات لتفاهتها، وتحدد نوعية الجرائم بالإعتماد على نوع ومقدار العقوبة وجسامتها، أشدها الجنايات وأخفها المخالفات و أوسطها الجرح⁽²⁾، وقد حدد قانون العقوبات النافذ، أنواع الجرائم بالنظر إلى العقوبات المقررة لها، فالجرح هي الجرائم التي تتراوح عقوبتها من أسبوع حتى ثلاث سنوات، والجنايات الجرائم التي تفوق عقوبتها الثلاث سنوات⁽³⁾، ولكن المشرع الفلسطيني في قانون الجرائم الإلكترونية لم ينص صراحة على نوعية الجرائم التي يجوز التفتيش فيها.

يرى الباحث أن المشرع الفلسطيني لم ينص على نوعية الجرائم الإلكترونية التي يجوز التفتيش فيها، كون أن جميع الجرائم الواردة في قانون الجرائم الإلكترونية من نوعية الجرح والجنايات، وكذلك نرى، أن شرط ضرورة وقوع جريمة إلكترونية قبل إجراء التفتيش يتفق مع القواعد العامة.

ثانياً: تحديد المجرم الإلكتروني.

المجرم الإلكتروني يتم تحديده بعد وقوع الجريمة، وهو الشرط الثاني من أسباب التفتيش، ويتمثل بإسناد التهمة إلى شخص معين، ولكن يجب أن يكون هذا الإتهام جدي ويحوز في شخصه أو في مسكنه أشياء متعلقة بالجريمة⁽⁴⁾.

تحديد الفاعل، عبر عنه المشرع الفلسطيني بالمادة (1/39) من قانون الإجراءات الجزائية بوجود إتهام موجه إلى شخص، والدلائل الكافية هي مجموعة المظاهر والإمارات التي تقوم على المضمون العقلي والمنطقي لملايسات الواقعة، وتؤديها حرفية الخبرة الفنية بنسبة الجريمة الإلكترونية إلى شخص معين⁽⁵⁾، وعلّة هذا الشرط بأن توجيه إتهام إلى شخص معين بالذات يبرر

(1) مصطفى، محمود محمود، الإثبات في المواد الجنائية في القانون المقارن، مرجع سابق، ص 16.

(2) حسني، محمود نجيب، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، والنظرية العامة للعقوبة والتدبير الإحترازي، ط 7، دار النهضة العربية، القاهرة، 2012، ص 60+59.

(3) أنظر، الفصل الأول، من الباب الثاني، من الكتاب الأول، المادة (14) وما بعدها، من قانون العقوبات النافذ.

(4) الجوخدار، حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، مرجع سابق، ص 133.

(5) حجازي، عبد الفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 387.

القيام بالتفتيش⁽¹⁾، ولكن المشرع الفلسطيني في قانون الجرائم الإلكترونية لم يقر هذا الشرط في نصوصه.

يرى الباحث أن الأمر يختلف في الجرائم الإلكترونية عنه في الجرائم العادية، كون الفاعل في الجريمة الإلكترونية في أغلب الجرائم إن لم يكن في جميعها مجهول، ويصعب معرفته بعد ارتكابه الجريمة الإلكترونية، وقبل إجراء التفتيش، وهذا يرجع إلى خصائص تلك الجريمة، ويكون التفتيش في وسائل تكنولوجيا المعلومات عنصراً مهماً في التحقيق لمعرفة الفاعل، وهذا يبرر خروج السلطة المختصة بالتفتيش عن القواعد العامة في شرط تحديد الفاعل قبل إجراء التفتيش في تكنولوجيا المعلومات.

ثالثاً: مبررات إجراء التفتيش.

إن مبررات إجراء تفتيش، عبر عنها المشرع الفلسطيني في المادة(1/39) من قانون الإجراءات الجزائية، بضرورة وجود قرائن قوية على أن المشتبه به يحوز أشياء تتعلق بالجريمة، وفي قانون الجرائم الإلكترونية الفلسطيني عبر عنها المشرع بالمادة(1/32) بأشياء ذات صلة بالجريمة الإلكترونية، بشرط أن تكون هذه الأشياء مفيدة للتحقيق وضرورية لإظهار الحقيقة، وإلا أصبح التفتيش بانتهاك حرمة الناس غير مبرر⁽²⁾.

مبررات إجراء التفتيش على وسائل تكنولوجيا المعلومات، هو توافر دلائل قوية على أن المشتبه به هو من قام بارتكاب الجريمة الإلكترونية، ويجري التفتيش في البيئة الإلكترونية للحصول على دليل يفيد التحقيق وينسب التهمة للمتهم أو يفيها عنه.

يرى الباحث أن شرط توافر مبررات للتفتيش، تنطبق على الجرائم الإلكترونية، وهذه من الضمانات الواجب التدقيق فيها قبل إجراء عملية التفتيش في وسائل تكنولوجيا، لتفادي الإطلاع على أسرار الناس وخصوصيتهم الموجودة والمخزنة في وسائل تكنولوجيا المعلومات المختلفة بشكل عشوائي، بحيث يجب الإعتماد على محاضر إستدلال أوليه جدية ومعقولة، تؤكد بأن الأماكن تحتوي على

(1) تاوضروس، جمال جرجس مجلع، الشرعية الدستورية لأعمال الضبطية القضائية، النسر الذهبي للطباعة، مصر، 2005، ص182 .

(2) عوض، محمد محيي الدين، حقوق الإنسان في الإجراءات الجنائية، بدون ناشر، 1989، ص 227.

الوسائل الإلكترونية المنوي تفتيشها والتي يمكن أن يتم الحصول منها على أدلة تفيد التحقيق.

الفرع الثالث: محل التفتيش في الجرائم الإلكترونية.

محل التفتيش في الجرائم الإلكترونية، الأشخاص والأماكن للبحث عن وسائل تكنولوجيا المعلومات التي تحتوي أفكار الشخص وأفعاله سواء كانت ضده أو لصالحه. حيث سنبحث في تفتيش الأشخاص في الفقرة الأولى، والأماكن في الفقرة الثانية، ووسائل تكنولوجيا المعلومات في الفقرة الثالثة.

أولاً: تفتيش الأشخاص.

في الحالات التي أجاز القانون فيها التعرض لحرية الشخص فإنه يجوز تفتيشه⁽¹⁾، والشخص كمحل للتفتيش رسم القانون الأساسي طرق تفتيشه بالمادة (11) في باب الحقوق والحريات العامة حيث نهى النص الدستوري تفتيش الشخص إلا بإذن قضائي، وكذلك نصت المادة(38) من قانون الإجراءات الجزائية على انه لا يجوز تفتيش الشخص إلا إذا كان مقبوضا عليه بشكل قانوني، وهذه الضمانات أقرت لتفتيش شخص المتهم، وغيره.

1-تفتيش شخص المتهم. تفتيش شخص المتهم، يعني البحث في جسم الشخص وملابسه عن الأشياء التي توجد بحوزته وعن أدلة متعلقة بالجريمة تفيد في كشف الحقيقة ونسبتها إليه⁽²⁾، ويشمل تفتيش الشخص توابعه، المنقولة كالأمتعة والأكياس والسيارات ووسائل تكنولوجيا المعلومات.

نظم المشرع الفلسطيني طرق تفتيش شخص المتهم المقبوض عليه قانونا⁽³⁾، وحالات القبض القانوني تتمثل في التلبس بالجريمة، وأمر من السلطة القضائية، وحالات التفتيش الوقائي والإداري.

أ-تفتيش شخص المتهم بناء على أمر قبض: القبض الصحيح، أشار إليه المشرع في المادة (2/31) من قانون الإجراءات الجزائية، وهو الذي يكون بأمر من السلطة القضائية المختصة بناءً على وجود دلائل كافية بإتهام شخص بإرتكاب جناية أو جنحة، وهذا هو القبض القانوني الذي

(1) مصطفى، محمود محمود، الإثبات في المواد الجنائية في القانون المقارن، مرجع سابق، ص21.

(2) عقيدة، محمد أبو العلا، شرح قانون الإجراءات الجنائية، ط2، دار النهضة العربية، القاهرة، 2001، ص 377.

(3) أنظر المادة(38) من قانون الإجراءات الجزائية الفلسطيني.

يخول مأمور الضبط القضائي تفتيش شخص المتهم على معنى المادة(38).

ب-تفتيش شخص المتهم في حالة التلبس: إستثناءً، وبدون أمر من السلطة القضائية، أجاز قانون الإجراءات الجزائية الفلسطيني في المادة (30)، إلقاء القبض على شخص المتهم في حالة التلبس بإرتكاب الجريمة، وذكر المشرع صور التلبس في المادة(26) من ذات القانون، وكذلك فعل المشرع الأردني والمصري⁽¹⁾.

التلبس بإرتكاب الجريمة له صورتين، الأولى ما يعبر عنه بالتلبس الواضح أو الحقيقي، والذي يتحقق عند مشاهدة الجاني أثناء ارتكابه الأفعال التي يتكون منها الركن المادي للجريمة أو جزء منه⁽²⁾، ويمتد نطاقه إلى كل حالة يتم فيها إدراك إرتكاب الجريمة عن طريق حاسة من الحواس على سبيل اليقين⁽³⁾، والثانية ما يعبر عنه بالتلبس الحكمي، ويتحقق عند عدم مشاهدة إرتكاب الجريمة، وإنما عند رؤية أثارها، وتتبع المجني عليه، أو العامة، مرتكبها بالصياح أثر وقوعها، أو وجد مرتكبها حاملاً أشياء تفيد أنه مساهم فيها أو عليه آثار أو علامات تفيد بذلك⁽⁴⁾، والقبض في حالة التلبس، هو قبض صحيح متفق مع القانون، وهذا القبض يخول مأمور الضبط القضائي تفتيش شخص المتهم على معنى المادة(38).

ت-التفتيش الوقائي والإداري: كما أسلفنا في هذا البحث وبيننا صور التفتيش ومنها التفتيش الوقائي والإداري، فإن هذا التفتيش الذي يجري للأشخاص، ويقومون به مأموري الضبط القضائي المختصين، يعتبر تفتيش صحيح متفق والقانون، على معنى المادة(38).

2-تفتيش شخص غير المتهم. تفتيش شخص غير المتهم وشروطه نظمه قانون الإجراءات الجزائية الفلسطيني في المادة(44)، وتتمثل هذه الشروط، في وجود هذه الشخص في المكان الذي يجري تفتيشه واشتبه بأنه يخفي شيء من الأشياء التي يجري التفتيش عنها، وهذا الإجراء يعتمد على ذكاء القائم على التفتيش، وفطنته في التخمين والشك في شخص غير المتهم بأن يكون حائز

(1) أنظر المادة(28) من قانون أصول المحاكمات الجزائية الأردني، رقم(9) لسنة 1961.

- كذلك أنظر المادة(30) من قانون الإجراءات الجنائية المصري، رقم(150) لسنة 1950.

(2) عبد الستار، فوزية، شرح قانون الإجراءات الجنائية، وفقاً لأحدث التعديلات، ط2، ج1، دار النهضة العربية، القاهرة، 2010، ص311.

(3) أبو الروس، احمد، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، المكتب الجامعي الحديث، الإسكندرية، 2008، ص107.

(4) الشهاوي، قديري عبد الفتاح، مناط التفتيش قيودة وضوابطه، مرجع سابق، ص87.

لأشياء متعلقة بالجريمة.

3-تفتيش الأنثى. من الضمانات التي أقرها القانون، بأن يجري تفتيش الأنثى بمعرفة أنثى ينتدبها لذلك القائم بالتفتيش⁽¹⁾، وهذه القاعدة تتعلق بالنظام العام، الهدف منها الحفاظ على الآداب العامة، وحدودها عورات المرأة التي تخدش حياءها إذا مُست⁽²⁾، وتطبيقاً لأحكام القانون، تم إلحاق عنصر نسائي متخصص في وحدة مكافحة الجرائم الإلكترونية بجهاز الشرطة، من مهامها الأساسية إجراء تفتيش على وسائل تكنولوجيا المعلومات إذا كانت تلك الوسائل تخص أنثى، للحفاظ على خصوصيتها⁽³⁾، علماً أن قانون الجرائم الإلكترونية الفلسطيني لم ينص على ضمانات تفتيش الأنثى.

يرى الباحث أن الأشخاص كمحل للتفتيش في الجرائم الإلكترونية يكون الهدف منه البحث في ملابس الشخص وتوابعه على وسائل تكنولوجيا المعلومات لتفتيشها، ومثال هذه الأشياء، الهاتف النقال، جهاز الحاسوب الشخصي، وغيرها من وسائل تكنولوجيا المعلومات التي يمكن أن يخفيها الشخص في ملابسه، أو في الحقائب التي يحملها بيده، ولا خلاف على تفتيش الشخص المقبوض عليه بأمر من السلطة القضائية المختصة، أو في حالات التفتيش الإداري والوقائي، ولكن هل يتصور حالة التلبس في الجرائم الإلكترونية؟.

الإجابة على هذا السؤال، جاءت على لسان رئيس وحدة مكافحة الجرائم الإلكترونية في جهاز الشرطة الفلسطينية، والذي أفاد أثناء مقابلاتي معه، أن حالة التلبس بالجريمة الإلكترونية غير متصورة، وانه مضى أكثر من ثلاث سنوات على إنشاء الوحدة في مكافحة الجرائم الإلكترونية لم يقبض على أي شخص في حالة تلبس في جريمة إلكترونية.

ونرى أنه يمكن تصور حالات تلبس في الجريمة الإلكترونية، ومثالها أن يشاهد مأمور الضبط القضائي المختص شخص يجلس في مكان عام يقوم بإرتكاب جريمة إلكترونية من هاتفه النقال، أو إرتكاب جريمة إلكترونية أثناء استخدام وسائل تكنولوجيا المعلومات في الأماكن العامة للإنترنت، أو مشاهدة الجاني وهو يقوم بسرقة بيانات أو معلومات من جهاز حاسوب خاص بمؤسسه حكومية، أو خاصة، ووضعها على وسيلة تخزين (فلاشه) وتخبيتها في ملابسه، أو تدمير

(1) أنظر المادة(47) من قانون الإجراءات الجزائية الفلسطيني.

(2) عبد الستار، فوزية، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 306.

(3) مقابلة بحثية، مع رئيس وحدة مكافحة الجرائم الإلكترونية في جهاز الشرطة، مصدر سابق.

البرامج داخل تلك الأجهزة، كذلك يمكن تصور حالات أخرى للتلبس في ارتكاب جريمة إلكترونية برأينا ستكون الأكثر شيوعاً، وهي حالات التلبس الافتراضية في البيئة الإلكترونية، ومثالها قيام مأمور الضبط القضائي بإجراء تفتيش إداري على المواقع الإلكترونية المتاحة على الشبكات المختلفة وهو يجلس في مكتبه داخل الوحدة الإلكترونية المجهزة بوسائل تكنولوجية حديثة، ولاحظ أثناء التفتيش الإداري قيام أحد الأشخاص بإرتكاب إحدى الجرائم المنصوص عليها في قانون الجرائم الإلكترونية عبر الشبكة، ولا خلاف إذا تمكن من معرفته وتحديد مكانه وتبليغ مأموري الضبط المختص مكانياً بإلقاء القبض عليه وتفتيشه إذا كان في مكان عام، وطلب إذن تفتيش إذا كان في مكان خاص، ولكن في أغلب الجرائم الإلكترونية يصعب معرفة الفاعل، ومكانه، بوقت قصير لتوافر حالة التلبس، ويمكن أن يستغرق معرفة الجاني ومكان ارتكاب الجريمة وقت طويل، وحالة التلبس التي تتيح لمأمور الضبط إلقاء القبض على الجاني وتفتيشه هي معاصرة لإرتكاب الجريمة، وتكون هناك ملاحقة مادية، تعقبها صراخ الناس، وهذا غير متصور في هذه الحالة وبالتالي في أغلب الحالات.

ثانياً: تفتيش الأماكن.

قانون الجرائم الإلكترونية الفلسطيني أجاز تفتيش الأماكن في المادة (1/32)، ولكن لم يحدد هذه الأماكن، فجاءت عبارات النص مطلقة، وهي تشمل الأماكن العامة والخاصة.

1- الأماكن العامة. المكان العام⁽¹⁾، هو كل مكان مباح للجمهور الدخول إليه في كل وقت وبغير قيد أو بمقابل مادي، والعبرة بالمكان العام ليس بالأسماء التي تعطى لها وإنما بحقيقة الواقع من أمرها⁽²⁾، وتفتيشها ليس بحاجة إلى إذن قضائي كون القانون لم يقر لها ضمانات في التفتيش، لأنها لا تعتبر مكان خاص لخصوصية الإنسان، وبالتالي ليس لها الحرمة كما المساكن.

يرى الباحث أن الأماكن العامة في البيئة الإلكترونية كثيرة، سواء كانت حقيقية أو افتراضية، وتتمثل الأماكن الحقيقية، في الأماكن العامة لاستخدام الإنترنت، والتي يستطيع أي أحد

⁽¹⁾ عرف قانون العقوبات النافذ، بالمادة (2) المكان العام أو المحل العام بأنه " كل طريق عام، أو مكان، أو ممر، يباح للجمهور المرور به، أو الدخول إليه، في كل وقت وبغير قيد، أو كان مقيداً بدفع مبلغ من النقود، وكل بناء، أو مكان، يستعمل إذ ذاك لأي اجتماع، أو حفل عمومي، أو ديني، أو كساحة مكشوفة.

⁽²⁾ نقض جنائي مصري، بتاريخ 1976/2/16، أحكام النقض، س 27، ق 45، ص 225.

الدخول إليها واستخدام وسائل تكنولوجيا المعلومات الموجودة فيها بمقابل مادي، رغم تقلص عددها في هذه الأيام بسبب إنتشار شبكة الإنترنت، وأصبح الإنترنت في اغلب البيوت والأماكن الخاصة، والأماكن العامة الافتراضية على الشبكات، تتمثل في المواقع الإلكترونية المفتوحة، والتي يستطيع أي شخص الدخول عليها بواسطة وسائل تكنولوجيا المعلومات، بأي وقت وبدون قيد وان كان بمقابل مادي.

2- المساكن. هي التي وفر لها القانون ضمانات من إجراءات التفتيش، كونها المكان الذي له حرمة، ورسم القانون طرق خرق حرمتها وتفتيشها.

المنزل، كل مكان مخصص للسكن لأحد الأشخاص ولعائلته وضيوفه وخدمه، وتوابعه وملحقاته، وإن لم يكن مسكونا فعلا⁽¹⁾، ويمكن أن يكون خيمة، أو عربة كبيرة يسكنها بشكل مؤقت ومخصص للزهره ولكنها تكون مخزن أسرار⁽²⁾، ولكن يجب أن يكون المسكن المراد تفتيشه محدد بالذات.

في الجرائم العادية، تفتيش المنزل يجيز تفتيش ما به من أشياء منقولة أو غير منقولة، ولكن يختلف الأمر في الجرائم الإلكترونية، فتفتيش المنزل يكون لضبط وسائل تكنولوجيا المعلومات التي إستخدمت في ارتكاب الجريمة، كالحاسوب وملحقاتها، أو وسائل تخزين المعلومات وغيرها، فان إذن تفتيش المنزل لا يبيح لمأمور الضبط القضائي تفتيش الوسائل الإلكترونية المضبوطة، ولا بد للحصول على إذن خاص من النيابة للنفاد المباشر لتلك الوسائل وتفتيشها للحصول على المعلومات المطلوبة، وهذا ما أشار إليه المشرع بوضوح في المادة (4/32) من قانون الجرائم الإلكترونية، وأكد عليه رئيس نيابة مكافحة الجرائم الإلكترونية، ورئيس وحدة مكافحة الجرائم الإلكترونية بالشرطة، ولكن بنفس الضمانات والشروط المقررة له.

3- الأماكن الخاصة. المكان الخاص، هو المكان الذي يعتبره صاحبه مستودعا لسره، وليس لإقامته، فتلك الأماكن تخضع لقواعد تفتيش الأشخاص، كمكاتب المحامين، ورجال الأعمال، وعيادات الأطباء⁽³⁾، فجواز تفتيش الشخص يرتبط به جواز تفتيش ما يحوزه من أشياء و أماكن

(1) السعيد، كامل، شرح قانون أصول المحاكمات الجزائية، مرجع سابق، ص446.

(2) عزيز، سردار علي، النطاق القانوني لإجراءات التحقيق الابتدائي، دراسة مقارنة، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، 2011، ص396.

(3) الجوخدار، حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، مرجع سابق، ص 145.

خاصة⁽¹⁾.

القانون الأساسي الفلسطيني إشتراط إجراءات محددة لتفتيش بعض الأماكن الخاصة، بأعضاء المجلس التشريعي، ونظم إجراءات التحقيق مع الوزراء⁽²⁾، كونهم يتمتعون بحصانة أقرت لهم، والقانون نظم إجراءات التحقيق مع القضاة⁽³⁾، وألزم حضور نقيب المحامين أو من يمثله عند تفتيش مكتب المحامي⁽⁴⁾، ويستثني من التفتيش المساكن والأماكن الخاصة المشمولة بالحصانة، كمقر البعثات الدبلوماسية والقنصلية⁽⁵⁾. ولكن ما هو حكم تفتيش السيارة؟.

يختلف الفقهاء في حكم تفتيش السيارة، فمنهم من يرى أنها تخضع لقواعد تفتيش الأماكن، ومنهم من يرى أنها تخضع لقواعد تفتيش الأشخاص، حيث سنستعرض تلك الآراء على النحو التالي:

الرأي الأول: يرى الأستاذ علي زكي العرابي، أن السيارة مكان خاص تتمتع بحرمة، وتخضع لقواعد تفتيش المنازل، سواء كانت داخل المنزل أم خارجه⁽⁶⁾.

الرأي الثاني: يرى الدكتور سامي حسني الحسيني، أن تفتيش السيارة الخاصة ترتبط بتفتيش شخص صاحبها أو حائزها، كونها تستمد حرمتها منه⁽⁷⁾.

الباحث يرى بأن السيارة الخاصة تخضع لقواعد تفتيش المنازل إذا كانت داخل المنزل، أما إذا كانت السيارة بحوزة صاحبها أو حائزها خارج المنزل تخضع لقواعد تفتيش الأشخاص.

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 546.

(2) أنظر المادة (76+75+2/53) من القانون الأساسي الفلسطيني.

(3) أنظر المادة (56) من قانون السلطة القضائية الفلسطيني.

(4) أنظر المادة (20/د) من قانون تنظيم مهنة المحاماة الفلسطيني رقم (3) لسنة 1999.

(5) أنظر المادة (30) من إتفاقية فينا للعلاقات الدبلوماسية، الصادرة بتاريخ 18/4/1961، فينا.

(6) علي زكي العرابي، المبادئ الأساسية للتحقيقات والإجراءات الجنائية، ج1، مطبعة التأليف والترجمة والنشر، 1940، ص254، ورد في كتاب أحمد، هلالى عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص127.

(7) الحسيني، سامي حسني، النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، جامعة عين شمس، دار النهضة العربية، القاهرة، 1972، ورد في كتاب الجوخدار، حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، مرجع سابق، ص153.

ثالثاً: تفتيش وسائل تكنولوجيا المعلومات.

قانون الجرائم الإلكترونية الفلسطيني اشترط في المادة(32) إجراء التفتيش على وسائل تكنولوجيا المعلومات والنفاد المباشر إليها بعد إذن من النيابة العامة، وهذه الوسائل تكون مادية وغير مادية كما عرفها المشرع الفلسطيني بالمادة الأولى من قانون الجرائم الإلكترونية.

تكنولوجيا المعلومات، كمحل للتفتيش، ذات معنى كبير وواسع، تشمل جميع الوسائل الإلكترونية الحديثة، كأجهزة الكمبيوتر، والهواتف النقالة الحديثة وما بداخلها، والشبكات العامة والخاصة، وشبكات الإنترنت الداخلية والعالمية، والمواقع الإلكترونية الخاصة والعامة، والبريد الإلكتروني، ووسائل تخزين المعلومات، أو أي وسيلة تعمل بالتقنية الرقمية.

يرى الباحث أنه يجب عند إعطاء الإذن بالنفاد المباشر إلى وسائل تكنولوجيا المعلومات بإجراء تفتيش عليها، أن يتم التحديد بدقة ووضوح على وسيلة تكنولوجيا المعلومات المراد تفتيشها، تطبيقاً لنص المادة(2/32) من قانون الجرائم الإلكترونية الفلسطيني، والتي أكدت على أن أمر التفتيش يجب أن يكون مسبباً ومحدداً، وإلا تم تفتيش جميع الوسائل الإلكترونية وبالتالي يؤدي إلى خرق الضمانات المقررة لحماية خصوصية الناس وحرمتهم بالإطلاع على أسرهم بدون وجه حق.

المطلب الثاني

الضمانات المقيدة للتفتيش في الجرائم الإلكترونية.

الضمانات المقيدة في التفتيش بالجرائم الإلكترونية، تتمثل في شروط شكلية، أقرها المشرع، لا تقل أهمية عن الضمانات المحددة، ويجب مراعاتها بالتفتيش. حيث سنبحث تسبباً أمر التفتيش في الفرع الأول، وقت التفتيش بالفرع الثاني، وشهود ومحضر التفتيش بالفرع الثالث.

الفرع الأول: تسبب أمر التفتيش.

القانون الأساسي الفلسطيني في المادة (17) أوجب أن يصدر أمر التفتيش عن السلطة القضائية، وإن يكون هذه الأمر مسبب، وعلى هدي القانون الأساسي جاءت المادة (2/39) من قانون الإجراءات الجزائية الفلسطيني، والمادة (2/32) من قانون الجرائم الإلكترونية الفلسطيني وأكدت على هذا الشرط في التفتيش، ولكن هذا الشرط أُفِر لتفتيش المنازل، ولم يُقره المشرع لتفتيش الأشخاص. لذلك سنتناول أمر التفتيش في الفقرة الأولى، ومذكرة التفتيش في الفقرة الثانية.

أولاً: أمر التفتيش .

أمر التفتيش، هو تفويض يصدر من سلطة التحقيق المختصة إلى احد مأموري الضبط القضائي مخولاً بإياه التفتيش الذي تختص به تلك السلطة⁽¹⁾.

القانون لم يرسم شكل خاص لتسبب الأمر، ولكن يكفي أن يسبب بالإعتماد على الدلائل التي إستخلصتها سلطة الإستدلال من تحرياتها⁽²⁾، وتقدير جدية التحريات وكفايتها من المسائل الموضوعية التي يوكل الأمر فيها إلى سلطة التحقيق تحت إشراف محكمة الموضوع⁽³⁾.

ثانياً: مذكرة التفتيش.

بعد صدور أمر التفتيش المسبب من السلطة المختصة، يجب أن يكون أمر التفتيش مكتوباً، ولا قيمة له إذا صدر شفاهة أو بالهاتف أو بالوسائل الإلكترونية الحديثة قبل أن يكتب⁽⁴⁾، ولا يشترط أن يكون الأمر بيد مأمور الضبط القضائي المنتدب، ولكن يجب أن يكون فحوى الإذن ثابت بالكتابة في الأوراق⁽⁵⁾، ويجب إن تحتوي المذكرة على بيانات إلزامية عددها المشرع.

1-بيانات مذكرة التفتيش. القانون لم يشترط شكل معين للمذكرة، ولكن قانون الإجراءات الجزائية

الفلسطيني إشتراط بالمادة(40) وجود بيانات واجب ذكرها في مذكرة التفتيش وهي:

(1) الكواري، منى جاسم، التفتيش، شروطه وحالاته وبطلانه، مرجع سابق، ص 49.

(2) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، مرجع سابق، ص551.

(3) نقض جنائي مصري، بتاريخ 1976/1/11، أحكام النقض، س 27، ق 9، ص 52.

(4) الطوالبية، علي حسن محمد، التفتيش الجنائي على نظم الحاسوب والإنترنت، مرجع سابق، ص112.

(5) نقض جنائي مصري، بتاريخ 1981/11/19، أحكام النقض، س 32، ق 163، ص 944.

أ-اسم الشخص: يجب أن تشمل مذكرة التفتيش على إسم الشخص المراد تفتيشه، أو تفتيش منزله، وأي إسم أو لقب يدل عليه.

ب-عنوان المنزل: يجب أن يكتب بالمذكرة عنوان المنزل المراد تفتيشه بكل دقة.

ت-غرض التفتيش: يجب أن يكتب بالمذكرة الغرض من تفتيش الشخص أو الغرض من تفتيش منزله، ولكن يجب أن يكون الغرض محددًا نافيًا للجهالة⁽¹⁾.

ث-مأمور الضبط القضائي: يجب أن يكتب بالمذكرة اسم مأمور الضبط القضائي المكلف بإجراء التفتيش.

ج-مدة سريان المذكرة: يجب أن يكتب بالمذكرة مدة سريان مذكرة التفتيش، محدد بمدة معينة يتم التفتيش خلالها، سواء بالساعات أو بالأيام.

القانون لم يقيد سلطة التفتيش بمدة محددة عند إصدار مذكرة التفتيش، وينبغي أن لا تطول إلى حد طويل يجعل المتهم مهددًا بالتفتيش لفترة طويلة⁽²⁾، أما التفتيش في الجرائم الإلكترونية، منح قانون الجرائم الإلكترونية الفلسطيني في المادة (2/33) النيابة العامة حق تجديد أمر التفتيش أكثر من مره ما دامت مبررات التفتيش قائمة.

ح-تاريخ وساعة إصدار المذكرة: يجب أن يكتب في المذكرة ساعة وتاريخ إصدارها، وعلة ذلك، بان التفتيش يجب أن يتم بعد وقوع الجريمة، وفي خلال مدة سريان المذكرة، وكتابة تاريخ وساعة إصدار المذكرة يظهر مدى صحة إجراء التفتيش⁽³⁾.

2-بيانات مصدر المذكرة: من الشروط الجوهرية التي أوجبها القانون، توقيع مذكرة التفتيش من عضو النيابة الذي أصدرها، وتطبيقا لنص القانون يجب أن يكتب في مذكرة التفتيش إسم عضو النيابة وصفته وتوقيعه، لبيان الإختصاص المكاني والنوعي لعضو النيابة⁽⁴⁾، كون المذكرة ورقة

(1) عطية، كاظم السيد، الحماية الجنائية لحق المتهم في الخصوصية، مرجع سابق، ص 664.

(2) راسخ، إبراهيم، التحقيق الجنائي العلمي، مرجع سابق، ص 336.

(3) الشواربي، عبد الحميد، إذن التفتيش في ضوء الفقه والقضاء، مرجع سابق، ص 43.

(4) طنطاوي، إبراهيم حامد، الدفع ببطلان إذن النيابة العامة بالتفتيش، مرجع سابق، ص 56+57.

رسمية يجب أن تحمل بذاتها دليل صحتها ومقومات وجودها لأن التوقيع عليها يشهد بصورها
عن صدرت منه⁽¹⁾.

يرى الباحث أن المشرع الفلسطيني أوجب تسبب أمر التفتيش، لأن التسبب من الضمانات التي
يجب مراعاتها في التفتيش بالجرائم الإلكترونية، وكون وسائل تكنولوجيا المعلومات الموجودة بحوزة
الأشخاص أو في المنازل تخزن بها خصوصيتهم، وتعتبر مستودع للسر "البيت الافتراضي"، لا
تقل أهمية عن البيوت الحقيقية، مع ضرورة وجود مذكرة تفتيش تحتوي على البيانات الإلزامية التي
ذكرناها، وتحديد الوسيلة الإلكترونية المراد تفتيشها بدقة.

الفرع الثاني: وقت التفتيش.

وقت التفتيش لم ينص عليه قانون الجرائم الإلكترونية، وهو من الشروط التي أقرها المشرع لتفتيش
المنازل في قانون الإجراءات الجزائية الفلسطيني بالمادة (41)، وحصر وقت تفتيش المنازل في فترة
النهار، وفي حالات محصورة ليلاً، حيث سنتناول التفتيش نهاراً في الفقرة الأولى، وليلاً في الفقرة
الثانية.

أولاً: التفتيش في النهار.

المشرع الفلسطيني أجاز بالمادة (41) من قانون الإجراءات الجزائية تفتيش المنازل نهاراً، ولكنه لم
يحدد ساعات النهار رغم إختلافها خلال فصول السنة، كون النهار أطول في فصل الصيف منه
في الشتاء، ولكن قانون العقوبات النافذ عرف النهار أو الليل بالمادة(2) بأنها "الفترة التي تقع بين
غروب الشمس وشروقها".

النهار لغة، هو ضياء ما بين طلوع الفجر إلى غروب الشمس، ويقال انه انتشار ضوء البصر
واجتماعه⁽²⁾.

بعض القوانين المقارنة حددت ساعات النهار ووضحتها، فالبعض حدد ساعات النهار من السادسة

(1) نقض جنائي مصري، بتاريخ 1967/11/13، أحكام النقض، س 18، ق 229، ص 1101.

(2) لسان العرب، المجلد الخامس، حرف الراء، فصل النون، مصدر سابق، ص 238.

صباحاً حتى الثامنة مساءً⁽¹⁾، أو من الساعة السادسة صباحاً حتى التاسعة مساءً⁽²⁾، أو من الخامسة صباحاً حتى الثامنة مساءً⁽³⁾، ولكن البعض الآخر حدد ساعات النهار بشكل ضمني، عندما حدد بالنص ساعات الليل التي لا يجوز التفتيش فيها وراعت تغييرها خلال فصول السنة⁽⁴⁾.

قانون أصول المحاكمات الجزائية الأردني، وقانون الإجراءات الجنائية المصري، لم تحدد تلك القوانين أوقات التفتيش، ولكن قضت محكمة التمييز الأردنية، بأنه لا يجوز تفتيش المنازل في منتصف الليل، ولا يجوز تفتيش البيوت إلا نهاراً⁽⁵⁾، وعلى عكس ذلك، قضت محكمة النقض المصرية، بأن تحديد الوقت المناسب للقيام بالتفتيش ترك للقائم به، لإجرائه بطريقة مثمرة، وفي الوقت الذي يراه مناسب، مادام ذلك خلال الفترة المحددة بالإذن، وأجازت التفتيش ليلاً⁽⁶⁾.

ثانياً: التفتيش بالليل.

نهى المشرع الفلسطيني في المادة(41) من قانون الإجراءات الجزائية عن تفتيش البيوت ليلاً إلا في حالات إستثنائية حددها على سبيل الحصر، وهي حالة التلبس في الجريمة وظروف الإستعجال.

1- حالة التلبس في الجريمة. حالة التلبس كما أسلفنا، الإستثناء الأول الذي أورده المشرع الفلسطيني في المادة(41) من قانون الإجراءات الجزائية، وأجاز تفتيش منزل المتهم ليلاً في حال تم إلقاء القبض عليه متلبساً بالجريمة.

(1) أنظر المادة(95) من مجلة الإجراءات الجزائية التونسية، قانون رقم(23) لسنة 1968.

(2) أنظر المادة(62) من المسطرة الجنائية المغربية، قانون رقم(22/1) لسنة 2002.

- كذلك أنظر المادة(1/59) من قانون الإجراءات الجنائية الفرنسي، Code de procédure pénale.

(3) أنظر المادة(47) من قانون الإجراءات الجزائية الجزائري، الصادر بالأمر رقم(155/66) لسنة 1966.

(4) أنظر المادة(3/104) من قانون الإجراءات الجنائية الألماني، لسنة 1950.

Strafprozeßordnung (StPO). Ausfertigungsdatum: 12.09.1950.

- المشرع الألماني، حدد ساعات الليل من (تاريخ 1/ ابريل إلى 30/ سبتمبر) من الساعة التاسعة مساءً إلى الساعة الرابعة فجراً، و من (1/ أكتوبر إلى 31/ مارس) من الساعة التاسعة مساءً حتى الساعة السادسة فجراً.

(5) تمييز جزاء أردني، رقم 97/697، س 1998، ع 2 و 4، ص 941، وتميز جزاء أردني رقم 99/420، س 2000، ص 1147، مجلة نقابة المحامين.

(6) نقض جنائي مصري، بتاريخ 1979/3/18، أحكام النقض، س 30، رقم 72، ص 351، ونقض جنائي مصري، بتاريخ 1979/11/8، س 30، رقم 170، ص 799.

والسؤال الذي يطرح، هل التلبس بالجريمة يبيح لمأمور الضبط القضائي تفتيش منزل المتهم المقبوض عليه بدون أمر من السلطة القضائية؟ أم يجب الحصول على أمر منها؟.

نصت المادة(47) من قانون الإجراءات الجنائية المصري على انه " لمأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن يفتش منزل المتهم..."، ولكن قضت المحكمة الدستورية العليا في مصر بعدم دستورية هذا النص، وحكمت بعدم جواز تفتيش منزل المتهم المقبوض عليه متلبسا بالجريمة إلا بأمر قضائي، وأجازت تفتيش الأشخاص فقط في حالة التلبس⁽¹⁾.

يرى الباحث أنه بالرجوع إلى المادة(11) من القانون الأساسي الفلسطيني، التي نصت على انه " لا يجوز تفتيش الأشخاص إلا بأمر قضائي"، وكذلك بالرجوع إلى نص المادة(17) التي نصت على انه " لا يجوز تفتيش المساكن إلا بأمر قضائي" فإننا نجد أن النص الدستوري لم يستثني حالة التلبس من الحصول على الأمر القضائي لإجراء التفتيش، وبالتالي فإن التفتيش في حالة التلبس بالتشريع الفلسطيني بحاجة إلى أمر قضائي قبل إجراءه، ويؤيد الباحث ما ذهب إليه المحكمة الدستورية العليا في مصر بان تفتيش منزل المتهم المقبوض عليه متلبسا بالجريمة لايجوز إلا بأمر من السلطة القضائية المختصة فقط، وإقتصار التفتيش بدون إذن قضائي على شخص المقبوض عليه متلبسا بالجريمة.

2-ظروف الاستعجال. ظروف الاستعجال، هي الإستثناء الثاني لتفتيش المنازل ليلاً، ولكن المشرع لم يوضح ما هي ظروف الاستعجال الموجبة لتفتيش المنازل في الليل.

المشرع الفلسطيني أجاز في المادة(98) من قانون الإجراءات الجزائية، إستجواب المتهم بمعزل عن محاميه في حالات الضرورة والإستعجال، وذكر منها الخوف من ضياع الأدلة مع ضرورة ذكرها في المحضر، وهذه الظروف تخضع لتقدير السلطة المختصة.

الجرائم الإلكترونية تكثر في ساعات الليل، كون المجرم الإلكتروني ينشط ليلاً مستغلاً عدم وجود الموظفين في المؤسسات العامة والخاصة، محاولاً ارتكاب جريمته⁽²⁾، ونظراً لخصوصية الجرائم

(1) دستورية عليا، بتاريخ 1984/2/2، القضية رقم 5، س 4 قضائية، أحكام المحكمة الدستورية العليا المصرية، ج 3، رقم 13، ص 67.

(2) الطوالة، علي حسن محمد، التفتيش الجنائي على نظم الحاسوب والإنترنت، مرجع سابق، ص61.

الإلكترونية فإن التفتيش فيها لا يخضع لوقت محدد⁽¹⁾.

يرى الباحث أنه بالقياس على ظروف الإستعجال التي أوردها المشرع في باب الإستجواب، فإن ظروف الإستعجال يخضع توافرها وتقديرها إلى السلطة المختصة بالتفتيش، وفي الجرائم الإلكترونية فإن ظروف الإستعجال ستكون متحققة دوما نظرا لخصوصية تلك الجرائم، وسيكون الهدف من تفتيش المنازل ليلاً الخوف من ضياع الأدلة الإلكترونية وتدميرها والتخلص منها، ويجب تدوين ظروف الإستعجال في أمر التفتيش.

3- التفتيش بناءً على موافقة المتهم. المشرع الفلسطيني لم ينص في قانون الإجراءات الجزائية وقانون الجرائم الإلكترونية على حالة رضا المتهم أو حائز المنزل على التفتيش، ولكن يمكن أن نلمس هذه الحالة من آراء الفقهاء.

تفتيش المنزل لا يجوز ليلاً إلا برضا صاحب المنزل⁽²⁾، ويجب أن يكون الرضا صريحاً ومكتوباً خالي من الخداع والزيف وبدون عنف أو إكراه لإجبار أحد على إصدار تلك الموافقة⁽³⁾، ويترتب عليه نتائج صحيحة، إذا كان على علم بان من يريد التفتيش لا يملكه قانوناً⁽⁴⁾، ويجب أن يصدر عن صاحب الحق وليس عن ممثله، ولا يعتد به إذا كان صادر عن معدوم الأهلية أو ناقصها⁽⁵⁾.

البعض⁽⁶⁾ لا يؤيد الأخذ بالرضا في التفتيش، معللاً ذلك بأن المسكن قلعة الإنسان، كفل الدستور حمايته، لرفعة الشعور بالعزة والكرامة، الذي يرقى بها المجتمع الحر الغيور على أمان وسكينة أبنائه، مما يستدعي عدم انتظار تنازل الأبرياء عن حرمتهم وعدم المساس بهم أو التعرض إليهم.

الباحث يؤيد الرأي الذي يعارض الإستناد إلى الرضا بالتفتيش ليلاً، كون أنه لا يتصور أن يتخلى الإنسان كامل الأهلية عن حماية دستورية وقانونية أُقرت له، إلا بالخوف والتهديد والخديعة من قبل مأموري الضبط القضائي. ونرى أن وقت التفتيش في الجرائم الإلكترونية على درجة كبيرة من

(1) هروال، نبيلة هبة، الجوانب الإجرائية لجرائم الانترنت، مرجع سابق. ص 262.

(2) جارو، 3، ن 906، مشار إليه في عبد الملك، جندي، الموسوعة الجنائية، ج 2، مرجع سابق، ص 262.

(3) عطية، طارق إبراهيم الدسوقي، الأمن المعلوماتي، مرجع سابق، ص 440+439.

(4) عبد الملك، جندي، الموسوعة الجنائية، ج 4، مرجع سابق، ص 588.

(5) حجازي، عبد الفتاح بيومي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، مرجع سابق، ص 635.

(6) الدسوقي، ناينتي ناين أحمد، الرضا كتكأة في التفتيش الجنائي، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 2008،

الأهمية، وإن تقييد وقت التفتيش يتعارض مع خصوصية تلك الجرائم، كونها ترتكب بكل الأوقات، وتنشط في ساعات الليل، وأي تأخير على إجراء التفتيش يعرقل سير التحقيق لسهولة التخلص من الأدلة، وإعتبار ظروف الإستعجال متحققا دائماً، وأن يُترك إختيار الوقت المناسب لإجراء التفتيش لتقدير مأمور الضبط القضائي المختص، ولهذه الأسباب نرى أن المشرع الفلسطيني لم يقيد التفتيش بالجرائم الإلكترونية بوقت محدد.

الفرع الثالث: شهود ومحضر التفتيش.

شهود ومحضر التفتيش، ضمانات أقرها قانون الإجراءات الجزائية الفلسطيني في المواد (43+50/4)، وعلّة ذلك حماية الخاضع للتفتيش وصيانة حقه في الدفاع وتقوية الدليل الذي يتم الحصول عليه ويعزز الثقة به⁽¹⁾. لذلك سنبحث في شهود التفتيش بالفقرة الأولى، ومحضر التفتيش بالفقرة الثانية.

أولاً: شهود التفتيش.

نص قانون الإجراءات الجزائية الفلسطيني في المادة (43) على ضرورة إجراء تفتيش المنزل بحضور المتهم، أو حائز المنزل، وإذا تعذر حضورهم، وأوجب حضور شاهدين من أقاربهم، أو جيرانهم، ولكن المشرع الفلسطيني في قانون الجرائم الإلكترونية لم ينص على ضرورة حضور المتهم أو غيره إجراءات التفتيش، وإنما نص في المادة (6/33) على حضور المتهم أو من وجد لديه المضبوط عند تحرير محضر بالمضبوطات إذا أمكن ذلك.

إن علة حضور المتهم أو غيره إجراءات التفتيش، هو إدخال الاطمئنان إلى نفس من يجري تفتيش مسكنه بان الإجراءات تسير وفق القانون⁽²⁾، ولتفادي التعسف في تنفيذ التفتيش⁽³⁾، ولم يقر المشرع الفلسطيني حضور شهود عند تفتيش الأشخاص، وعلّة ذلك أن حضور بعض الأشخاص ينطوي على إمتهان للشخص أمام غيره⁽⁴⁾، أما إذا كان متعذراً حضور المتهم أو غيره إجراءات التفتيش

(1) تاوضروس، جمال جرجس مجلع، الشرعية الدستورية لأعمال الضبطية القضائية، مرجع سابق، ص 187.

(2) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 551 + 552.

(3) عزت، محمد فتحي محمد أنور، تفتيش شبكة الإنترنت، مرجع سابق، ص 367.

(4) ثروت، جلال، نظم الإجراءات الجنائية، مرجع سابق، ص 476.

صح التفتيش في غيبتهما ولا يشترط في هذه الحالة حضور شهود⁽¹⁾، كون حضورهم ليس شرطا
جوهريا لصحة التفتيش⁽²⁾.

يرى الباحث أن حضور المتهم، المجرم الإلكتروني، إجراءات تفتيش وسائل تكنولوجيا المعلومات
أمر مستوعب، كونه على معرفه باستخدام وسائل تكنولوجيا المعلومات وقادر على فهم ما يقوم به
القائم بالتفتيش، رغم أنه يمكن أن يكون حضور المتهم سبب في إعاقة إجراءات التفتيش وتدمير
الأدلة إذا سمح له استخدام تلك الوسائل أو تضليل القائم بالتفتيش، وكذلك لا يتصور حضور
المتهم لإجراءات التفتيش إذا حصل التفتيش عن بعد من مكتب القائم به بالنفذ المباشر على
وسائل تكنولوجيا المعلومات الخاصة بالمتهم، وهو غير مقبوض عليه، أو لعدم القدرة على
إحضاره، ولكن نرى أن شرط حضور أشخاص كشهود على إجراءات التفتيش في الجرائم
الإلكترونية، غير مقنع، كون أن وجودهم لا يفيد العدالة، لأنهم أناس عاديين، ليسوا أصحاب خبرة
في وسائل تكنولوجيا المعلومات، وغير قادرين على معرفة ما يجريه القائم بالتفتيش، لذلك نرى
ضرورة الخروج عن القواعد العامة في حضور التفتيش، وأن يقتصر الحضور على شخص المتهم
فقط إذا أمكن ذلك ولا يمتد إلى غيره، لان المشرع منح مأموري الضبط القضائي هذه الصفة كونه
وثق بهم بأنهم لا يخالفون القانون، ويحافظون على أسرار الناس وخصوصياتهم.

ثانياً: محضر التفتيش.

قانون الإجراءات الجزائية الفلسطيني بالمادة(4/50) ألزم القائم بالتفتيش تحرير محضر بالإجراءات
التي قام بها، والتي جاء بها " يحرر محضر التفتيش من قبل القائم عليه، ويذكر فيه الأشياء التي
تم ضبطها والأمكنة التي وجدت فيها ويوقع عليه ومن حضر إجراءات التفتيش".

لم يقر المشرع الفلسطيني في قانون الجرائم الإلكترونية تحرير محضر التفتيش، والذي يقصد به
جميع التدابير والإجراءات التي اتخذها القائم بالتفتيش أثناء إجراء التفتيش⁽³⁾، وهو الصورة المكتوبة
لنتيجة التفتيش، سواء أسفر عن ضبط، أم لم يسفر عن شيء⁽⁴⁾، والغرض من تحرير المحضر، هو

(1) عوض، محمد محيي الدين، حقوق الإنسان في الإجراءات الجنائية، مرجع سابق، ص 227.

(2) نقض جنائي مصري، بتاريخ 1972/6/19، أحكام النقض، س 23، ق 209، ص 936.

(3) حسين، سامي جلال فقي، التفتيش في الجرائم المعلوماتية، مرجع سابق، ص 171.

(4) ثروت، جلال، نظم الإجراءات الجنائية، مرجع سابق، ص 478.

تدوين ما عسى أن يبيده المتهم من ملاحظات على التفتيش، ولا يبطل التفتيش إذا اغفل تحرير هذا المحضر⁽¹⁾.

1- لغة المحضر: كما أسلفنا، يدون المحضر باللغة العربية، كونها اللغة الرسمية للدولة، مع مراعاة المصطلحات الأجنبية في الجرائم الالكترونية، وإذا كان من يجري تفتيشه أو تفتيش منزله يجهل اللغة العربية، أجازت له المادة(60) من قانون الإجراءات الجزائية الفلسطيني الاستعانة بمترجم.

2- تدوين المحضر: إذا كان القائم بالتفتيش عضو النيابة، ألزمه القانون في المادة(58) من قانون الإجراءات الجزائية الفلسطيني إصطحاب كاتباً حتى يتفرغ فكره في مجريات التفتيش، ويقوم الكاتب بتدوين كل الإجراءات التي يقوم بها عضو النيابة ومنها محضر التفتيش، أما إذا قام عضو النيابة بكتابة محضر التفتيش بنفسه إعتبر محضر التفتيش محضر جمع إستدلالات كالذي ينظمه مأمور الضبط القضائي بنفسه⁽²⁾.

3- تغيير محتوى المحضر: تغيير محتوى محضر التفتيش لم يُشر المشرع الفلسطيني إليه صراحة، ولكن في باب سماع الشهود بمتن المادة(91) من قانون الإجراءات الجزائية، نهى المشرع عن فعل حك أو شطب في المحضر، وإذا حصل ذلك وجب التوقيع على أي تغيير من جميع الأطراف.

تتفق غالبية التشريعات العربية المقارنة⁽³⁾، على عدم وجود شطب أو كشط في المحاضر، وإذا دعت الضرورة لذلك يجب التوقيع على هذا التغيير من قبل القائم به والكاتب والشهود.

يرى الباحث أن ما ينطبق على محاضر شهادة الشهود، ينطبق على محاضر التفتيش كون إنها ذات طبيعة واحدة وهي عمل من أعمال التحقيق، وبالتالي لا يجوز شطب أو إضافة أي كلمات على محضر التفتيش إلا إذا قام الحاضرين بالتوقيع على هذا التغيير، وإلا بطل محضر التفتيش.

4- توقيع المحضر: القانون أوجب توقيع المحضر من قبل القائم به، ومن حضر إجراءات التفتيش⁽⁴⁾، فإذا كان القائم بالتفتيش عضو النيابة يجب أن يقوم بالتوقيع على المحضر مع الكاتب

(1) نقض جنائي مصري، بتاريخ 1957/6/10، أحكام النقض، س 8، ق 173، ص 633.

(2) نقض جنائي مصري، 1961/2/20، أحكام النقض، س 12، رقم 40، ص 233.

(3) أنظر المادة(73) من قانون أصول المحاكمات الجزائية الأردني، والمادة(113) من قانون الإجراءات الجنائية المصري.

(4) أنظر المواد(4/22) و (4/50) من قانون الإجراءات الجزائية الفلسطيني.

ومن حضر التفتيش، سواء المتهم أو حائز البيت أو الشهود الحاضرين، وإذا رفض أحد الحاضرين التوقيع على المحضر يكتب ذلك بالمحضر.

5- وقت إجراء التفتيش: يرى الباحث ضرورة كتابة تاريخ ووقت إجراء التفتيش في المحضر، رغم أن القانون لم يأمر بذلك، كون أن وقت إجراء التفتيش تستدل منه المحكمة على تاريخ إجراء التفتيش، وتثبت من انه وقع قبل ارتكاب الجريمة أم بعدها، وهل جرى التفتيش أثناء سريان المذكرة أم لا، وأن التفتيش جرى في النهار أو الليل.

6- ملاحظات التفتيش: يرى الباحث أنه يجب على القائم بالتفتيش تدوين في المحضر كل الملاحظات التي يبديها من حضروا التفتيش، وكذلك تدوين كيفية إجراء التفتيش، وهل تم التفتيش بالرضا أو بموافقة المتهم أو بالعنف، وفي الجرائم الإلكترونية يتم تدوين كيفية الدخول إلى وسيلة تكنولوجيا المعلومات، وتفتيشها.

يرى الباحث أن محضر التفتيش من الضمانات التي أقرها قانون الإجراءات الجزائية، ولم يقرها قانون الجرائم الإلكترونية، ولهذا المحضر أهمية عملية لأنه يدون فيه جميع إجراءات التفتيش منذ بدايتها حتى نهايتها، وتسجل به جميع الملاحظات، وملاحظات من حضروا التفتيش، ولكن المشرع الفلسطيني بالمادة (6/33) من قانون الجرائم الإلكترونية ذكر حضور المتهم أو حائز المضبوط عند تحرير قائمة بالمضبوطات فقط، وهذا يعني أن القانون لم يقر ضرورة حضور أحد عند إجراء التفتيش.

الفصل الثاني

خصوصية إجراءات التفتيش وآثاره في الجرائم الإلكترونية

الفصل الثاني

خصوصية إجراءات التفتيش وآثاره في الجرائم الإلكترونية

تمهيد وتقسيم.

إجراءات التفتيش والضبط في الجرائم الإلكترونية بحاجة إلى إجراءات خاصة، وطرق فنية إلكترونية للقيام به للوصول إلى الدليل الإلكتروني، وضبطه، وهذه الإجراءات مختلفة عن ما هو مألوف في التفتيش في الجرائم العادية.

إن التفتيش والضبط بالجرائم الإلكترونية له طرق خاصة، وإتباع هذه الطرق يؤدي إلى الوصول للأدلة المطلوبة وضبطها بالطرق الفنية الصحيحة، وكذلك يحتاج القائم بالتفتيش إلى وسائل إلكترونية خاصة للقيام بالتفتيش، ووسائل أخرى لضبط الأدلة كون أنها بحاجة إلى طرق تقنية.

إن الأدلة الإلكترونية ذات طبيعة حساسة، لا تحتمل الخشونة والقوة بالتعامل معها، وكذلك تحتاج إلى أماكن وطرق خاصة لحفظها، كون أنه يمكن تدميرها أو مسح محتواها بسهولة، وكذلك يمكن استبدالها بقطع إلكترونية مشابهة لها، مما يجعل إثبات الجريمة الإلكترونية ونسبتها إلى الفاعل أمر صعب.

حيث سنتناول في هذا الفصل، خصوصية إجراءات التفتيش في الجرائم الإلكترونية للتعرف على الطرق الفنية الملائمة لاستخراج الأدلة الإلكترونية، وكذلك سنبحث في آثار التفتيش سواء تم إجراءه وفق القانون أم بخلافه. حيث ينقسم الفصل الثاني إلى مبحثين.

المبحث الأول: خصوصية إجراءات التفتيش في الجرائم الإلكترونية.

المبحث الثاني: آثار التفتيش في الجرائم الإلكترونية.

المبحث الأول

خصوصية إجراءات التفتيش في الجرائم الإلكترونية

للجرائم الإلكترونية إجراءات تفتيش خاصة، وذلك لخصوصية هذه الجرائم التي تمتاز بسرعة إرتكابها وتدمير أدلتها، حيث أنها تمتاز عن غيرها من الجرائم الأخرى، وتحتاج لعدة مراحل لتنفيذها.

إن وسائل تكنولوجيا المعلومات، تتكون من وسائل كهرومغناطيسية بصرية كهروكيميائية، مادية وغير مادية⁽¹⁾، وكلمة كهرومغناطيسي تشمل، كل نظام لنقل الإشارات بواسطة الأسلاك الكهربائية والموجات اللاسلكية وكل مصدر أخر للطاقة⁽²⁾، وهذه الإجراءات بالغة الصعوبة، كون أن وسائل تكنولوجيا المعلومات تتكون من مجموعة وسائل مترابطة وغير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتبادلها، وتشمل جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لاسلكيا⁽³⁾، وهذه مميزات خاصة بالتقنية الحديثة، يحتاج تفتيشها إضافة إلى أشخاص متخصصين بالتعامل مع مكوناتها إلى وسائل تقنية حديثة.

تظهر خصوصية إجراءات التفتيش في الجرائم الإلكترونية في أنها تنقسم إلى إجراءات يجب مراعاتها قبل القيام بالتفتيش، وإجراء معاصر له، وإجراءات لاحقة له، وتختلف هذه الإجراءات باختلاف محل التفتيش، سواء كان التفتيش منصب على وسائل تكنولوجيا المعلومات الموجودة بحوزة شخص أو بأماكن عامة أو خاصة، داخل حدود الدولة أو خارجها.

حيث سنتناول في المطلب الأول، الإجراءات التحضيرية للتفتيش في الجرائم الإلكترونية، وفي المطلب الثاني، الإجراءات الفنية للتفتيش بالجرائم الإلكترونية.

(1) أنظر المادة الأولى من قانون الجرائم الإلكترونية الفلسطيني.

(2) أنظر المادة الأولى من قانون الإتصالات السلكية واللاسلكية الفلسطيني، رقم (3) لسنة 1996.

(3) أنظر المادة الأولى من قانون مكافحة الجرائم الإلكترونية القطري.

المطلب الأول

الإجراءات التحضيرية للتفتيش في الجرائم الإلكترونية.

إجراءات التفتيش في الجرائم الإلكترونية، بحاجة إلى إجراءات تحضيرية، وهذه الإجراءات لازمة وضرورية لنجاح التفتيش، وتكون هذه الإجراءات التحضيرية مساعدة للقائم بالتفتيش لضمان نجاحه في الحصول على الأدلة المطلوبة. حيث سنتناول تحديد محل التفتيش في الفرع الأول، والية التفتيش في الفرع الثاني.

الفرع الأول: تحديد محل التفتيش في الجرائم الإلكترونية.

تحديد محل التفتيش في الجرائم الإلكترونية، هو أول الأعمال التحضيرية الهامة لإجراء التفتيش، حيث يتم تحديد وسائل تكنولوجيا المعلومات المراد تفتيشها والمستخدم في ارتكاب الجريمة الإلكترونية، وتحديد مكانها، سواء بحوزة أشخاص أو في أماكن خاصة أو عامة، بهدف معرفة الفاعل وإجراء تفتيش عليها للحصول على الأدلة المطلوبة.

إن تحديد وسائل تكنولوجيا المعلومات المستخدمة في ارتكاب الجريمة الإلكترونية، يتم من خلال الحصول على المعلومات والبيانات الإلكترونية للأشخاص و للشبكات، والتي يتم الحصول عليها من شركات مزودي الخدمة أو شركات الاتصالات، وهذا من أهم الإجراءات التحضيرية التي يجب الحصول عليه، لكشف الوسائل الإلكترونية والشبكات المستخدمة في ارتكاب الجريمة الإلكترونية، وتعتبر هذه المعلومات الإلكترونية أساسية وضرورية لإجراء التفتيش.

قانون الجرائم الإلكترونية الفلسطيني عرف معلومات المشترك بالمادة الأولى بأنها " أي معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات، بما في ذلك نوع خدمة الإتصالات المستخدمة وهوية المشترك وعنوانه الجغرافي وهاتفه وأي معلومات أخرى، وهذه المعلومات تكون مخزنة لدى الجهات المختصة في الإتصالات ومزودي الخدمات، وقد ألزم قانون الجرائم الإلكترونية الفلسطيني⁽¹⁾ مزود الخدمة بتزويد الجهات القضائية المختصة بجميع البيانات

(1) أنظر المادة (1/31) من قانون الجرائم الإلكترونية الفلسطيني.

والمعلومات اللازمة والتي تساعد في كشف الحقيقة، وتطبيقاً لهذا النص فإن مزود الخدمات ملزم بحكم القانون تزويد الجهات القضائية المختصة بجميع البيانات والمعلومات اللازمة لمعرفة وسائل تكنولوجيا المعلومات والشبكات المستخدمة في ارتكاب الجريمة الإلكترونية، للوصول إلى مكانها ومعرفة فاعلها وإجراء تفتيش عليها للحصول على الأدلة المطلوبة، وكذلك ألزم المشرع السوري مقدمي الخدمات على الشبكة تقديم أي معلومات تطلبها السلطات القضائية المختصة⁽¹⁾، كما أجبر القانون الفلسطيني، مزودي الخدمة بالإحتفاظ بالمعلومات الشخصية والإلكترونية للمشاركين لديه لمدة لا تقل عن ثلاثة سنوات⁽²⁾، ولكن المشرع القطري حدد المدة بسنة واحدة فقط⁽³⁾. حيث سنبحث في تحديد وسائل تكنولوجيا المعلومات المستخدمة لإرتكاب الجريمة الإلكترونية في الفقرة الأولى، وتحديد مكان وجودها في الفقرة الثانية.

أولاً: تحديد وسائل تكنولوجيا المعلومات.

تحديد وسائل تكنولوجيا المعلومات يتم من خلال المعلومات التي يتم الحصول عليها من شركات الإتصالات ومزودي الخدمات، وكذلك يتم تحديد الشبكات المستخدمة، سواء كانت داخلية أم خارجية.

عرفت المادة الأولى من قانون الجرائم الإلكترونية الفلسطيني الشبكة الإلكترونية بأنها " إرتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية الإنترنت"، وهذا التعريف يشمل جميع الشبكات سواء كانت عامة أو خاصة، محلية أو دولية، وأن وسائل تكنولوجيا المعلومات يتم تحديدها إذا استخدمت تلك الشبكات، سواء كانت أجهزة حاسوب أو هواتف نقالة أو غيرها من الوسائل الإلكترونية التي تعمل بالتقنية الحديثة، وهذا التعريف متناغم مع التعريف الوارد في المادة (6/2) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وقد ألزمت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، كل دولة بتبني الإجراءات الضرورية

(1) أنظر المادة(2/ب) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

(2) أنظر المادة(3/31) من قانون الجرائم الإلكترونية الفلسطيني.

(3) أنظر المادة (3/21) من قانون مكافحة الجرائم الإلكترونية القطري.

لتمكين السلطات من إصدار الأوامر إلى مزودي الخدمة لتسليم معلومات المشترك⁽¹⁾، وبالعودة إلى المادة (31) من قانون الجرائم الإلكترونية نجد أن المشرع الفلسطيني ألزم مزودي الخدمات تزويد الجهات المختصة بجميع المعلومات اللازمة لكشف الحقيقة، ومنح النيابة العامة بالمادة (1/33) الحق في الحصول على الأجهزة والأدوات والوسائل الإلكترونية وحركة الإتصالات وبمستعملها أو معلومات المحتوى ذات الصلة بالجريمة الإلكترونية.

إن تحديد وسائل تكنولوجيا المعلومات المستخدمة في ارتكاب الجريمة الإلكترونية، لها أهمية كبيرة كون التفتيش ينصب عليها للحصول على الأدلة المطلوبة، وهذا الشرط من الشروط الموضوعية للتفتيش كما أسلفنا، وقد ألزم القانون مزودي الخدمات الإلكترونية تقديم الدعم الفني اللازم لجهات التحقيق للوصول إلى المعلومات المطلوبة والتي تفيد في كشف الحقيقة.

ثانياً: تحديد مكان وجود وسائل تكنولوجيا المعلومات.

تحديد مكان وجود وسائل تكنولوجيا المعلومات المستخدمة في ارتكاب الجريمة الإلكترونية، يكون إما بحوزة شخص أو الأشخاص الذين ارتكبوا تلك الجريمة تمهيدا للقيام بالتفتيش.

1- تحديد الأشخاص. يجب أن يتم تحديد الشخص أو الأشخاص المراد تفتيشهم بكل دقة، سواء من حيث الإسم والأوصاف والوظيفة والعمر ومحل إقامته وعمله، وهذه المعلومات تنفي مظنة الخطأ من تفتيش شخص آخر⁽²⁾.

2- تحديد الأماكن. يجب على القائم بالتفتيش التعرف على الأماكن المراد تفتيشها والطرق المؤدية إليها، ومعرفة مداخلها ومخارجها والمسالك المخفية، بناءً على معاينة سرية، لتحقيق عنصر المفاجأة خوفاً من التخلص من الأدلة⁽³⁾.

إن آلية تحديد المكان الموجودة بداخله وسائل تكنولوجيا المعلومات المراد تفتيشها يتم عن طريق إتصال تلك الوسائل بالشبكات، سواء كان إتصالها بالشبكات سلكي أو لاسلكي، مع ضرورة معرفة

(1) أنظر المادة (1/25) من الإتفاقية العربية لمكافحة تقنية المعلومات.

(2) راسخ، إبراهيم، التحقيق الجنائي العلمي، مرجع سابق، ص 392+393.

(3) راسخ، إبراهيم، المصدر نفسه، ص 293+294.

إذا كان هناك أكثر من شخص أو جهة تستخدم تلك الشبكات⁽¹⁾.

الفرع الثاني: آلية التفتيش في الجرائم الإلكترونية.

إن السلطة القائمة بالتفتيش في الجرائم الإلكترونية تضع آلية للتفتيش بعد حصولها على المعلومات الضرورية واللازمة والتي من خلالها حددت وسائل تكنولوجيا المعلومات التي إرتكبت بواسطتها الجريمة الإلكترونية، سواء كانت تلك الوسائل بحوزة أشخاص، أو داخل الأماكن.

إن التفتيش في الجرائم الإلكترونية يحتاج إلى فريق متكامل يكون له دور في نجاح التفتيش والحصول على الأدلة، كونه يتكون من عدد كاف من الأشخاص المتخصصين في وسائل تكنولوجيا المعلومات، ويكون تشكيله ملائم مع خصوصية الجرائم الإلكترونية، وتحديدًا لمكافحة سرعة تدمير الأدلة الإلكترونية والتخلص منها.

التفتيش غير مقصور على شخص واحد محدد، ولا يقدح في صحة التفتيش أن ينفذه أي واحد من مأموري الضبط القضائي⁽²⁾، إن إجراءات التفتيش في الجرائم الإلكترونية لا يمكن لشخص واحد القيام بها، بل بحاجة إلى تعاون عدة أشخاص لضمان نجاحه، كون إجراءات التفتيش بحاجة إلى أشخاص فنيين متخصصين في تفتيش وسائل تكنولوجيا المعلومات، يساندهم فريق أمني متخصص لفرض السيطرة الأمنية على المكان المراد تفتيشه لضبط مداخله ومخارجه. حيث سنتناول الفريق الفني للتفتيش بالجرائم الإلكترونية في الفقرة الأولى، وفريق الاقتحام في الفقرة الثانية.

أولاً: الفريق الفني للتفتيش في الجرائم الإلكترونية.

الفريق الفني للتفتيش بالجرائم الإلكترونية، يتكون من عدة أشخاص كل واحد منهم له دور محدد في إجراءات التفتيش، وتلك الأدوار محددة بناءً على دليل معد مسبقاً، وهذا الدليل يحدد الهدف من التفتيش والتنبؤ بوجود الوسائل الإلكترونية وتحديد أدوار كل عضو بالفريق⁽³⁾.

يتكون الفريق الفني للتفتيش، من مشرف على التفتيش، مهمته الإشراف على إجراءات التفتيش

(1) مقابلة مع رئيس وحدة مكافحة الجرائم الإلكترونية في جهاز الشرطة، مصدر سابق.

(2) نقض جنائي مصري، بتاريخ 1972/5/22، أحكام النقض، س 23، ق 177، ص 786.

(3) موسى، مصطفى محمد، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 245+246.

وخبراء في وسائل التكنولوجيا الحديثة⁽¹⁾، وخبراء مختصين في مسرح الجريمة الإلكترونية، مهمتهم البحث والتدقيق في مسرح الجريمة، وفحص جميع الغرف والمخازن والمخابئ⁽²⁾، وأشخاص مختصين بضبط وتحريز الأدلة، وهم ذو خبرة في التقنية الإلكترونية⁽³⁾، وكذلك يضم أشخاص للرسم والتصوير، مهمتهم رسم الخرائط (الكروكة) لمسرح الجريمة وتحديد مواقع الأجهزة والملفات والأشخاص والتقاط الصور الفوتوغرافية والتصوير بالفيديو⁽⁴⁾.

ثانياً: فريق الإقتحام للتفتيش في الجرائم الإلكترونية.

فريق الإقتحام للتفتيش في الجرائم الإلكترونية، هو القوة التي تكون معدة ومجهزة لمراقبة الفريق الفني المتخصص⁽⁵⁾، ويتم تجهيز هذا الفريق باختيار أعضائه من قوات مسلحة ومدربة على تأمين المكان المراد تفتيشه بالسرعة المطلوبة للحفاظ على الوسائل الإلكترونية من التدمير.

أجاز المشرع الفلسطيني في المادة (43) من قانون الإجراءات الجزائية، تنفيذ التفتيش باستخدام القوة إذا رفض المقيم بالمنزل أو المسؤول عن المكان السماح للقائم بالتفتيش بالدخول، ولم يشير المشرع الفلسطيني في قانون الجرائم الإلكترونية إلى آلية تنفيذ التفتيش، ولكن التفتيش في الجرائم الإلكترونية ليحقق أهدافه يجب أن يعتمد على عنصر المفاجئة والسرعة في السيطرة على المكان لتنفيذ التفتيش تماشياً مع طبيعة تلك الجرائم.

ويجب أن يتم دخول المكان المراد تفتيشه في الجرائم الإلكترونية عن طريق فريق الإقتحام بدون إذن من صاحب البيت لتحقيق عنصر المفاجئة، ولمنع المجرم الإلكتروني من إخفاء الأدلة أو تدميرها⁽⁶⁾، وهذا الأسلوب مطابق للأسلوب الأمريكي للتفتيش بالجرائم الإلكترونية، الذي يتم عبر قيام الشرطة في إقتحام المكان بصورة سريعة ومن كافة المنافذ في وقت واحد، ويتم إستبعاد الجميع

(1) حجازي، عبد الفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 392.

(2) البشري، محمد الأمين، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، بتاريخ 1 إلى 3 / 2000/5، ط 3، م 3، ص 1057.

(3) حسين، سامي جلال فقي، التفتيش في الجرائم المعلوماتية، مرجع سابق، ص 199.

(4) الديري، عبد العال، وإسماعيل محمد صادق، الجرائم الإلكترونية، مرجع سابق، ص 310.

(5) راسخ، إبراهيم، التحقيق الجنائي العلمي، مرجع سابق، ص 396.

(6) محاضرات للخبير البريطاني Jon Blake، بعنوان التحقيق بالجرائم الإلكترونية، أعطيت في مقر هيئة قضاء قوى الأمن، بتاريخ 24 - 25 / 2 / 2018، رام الله، فلسطين.

عن وسائل تكنولوجيا المعلومات وإدخال الجميع إلى غرفة لا توجد بها وسائل إلكترونية وبعد ذلك يتم تقديم إذن التفتيش، والبحث عن وسائل تكنولوجيا المعلومات المطلوبة⁽¹⁾.

ترجع طريقة تنفيذ التفتيش لتقدير القائم به، لما يكون منتجا وما لا يكون، مادام التفتيش في ذاته حصل بناء على أمر قانوني⁽²⁾، والأصل أن الدخول للأماكن يتم من بابيه، ولكن يجوز لمأموري الضبط القضائي بعد الحصول على إذن بالتفتيش أن يتخذوا لتنفيذه ما يرونه كفيلا بتحقيق الغرض منه دون أن يلتزموا في ذلك طريقة معينة بعينها ما داموا لا يخرجون عن القانون⁽³⁾، ويجوز الدخول سرا أو خلسة إلى المكان المراد تفتيشه، وإعلام الشخص المراد تفتيشه وتفتيش ممتلكاته بعد ذلك كون أن الإعلام ربما يكون له تأثيرا عكسيا في الجرائم الإلكترونية لما يعرض التفتيش للخطر لمحاولة العبث بالدليل ومحوه⁽⁴⁾.

للمشرف على التفتيش بالجرائم الإلكترونية، أن يصدر أوامره للقوة المرافقة التحفظ على أفراد أسرة الجاري تفتيش مسكنه ريثما ينتهي من التفتيش، وهذا ليس قبضاً، وإنما من الإجراءات التحفظية لتساعده على إجراء مهمته⁽⁵⁾، وإذا صدر الإذن بالتفتيش لمأموري الضبط بإجراء التفتيش واستعان الضابط بزملائه لمساعدته لإجراء التفتيش، فإن كل ما أجراه كل منهم من تفتيش بمفرده صحيحا لوقوعه في حدود الإذن⁽⁶⁾.

يرى الباحث أن الطرق التقليدية للدخول إلى الأماكن يحتاج إلى قرع الجرس، وعرض إذن التفتيش على الموجود بالمكان المراد تفتيشه، وطلب الإذن منه لإجراء تفتيش، فإذا رفض يجوز استخدام القوة لتنفيذ التفتيش، وهذا يحتاج إلى وقت، ولكن هذا الوقت يعتبر كبير في التفتيش بالجرائم الإلكترونية نظراً لخصوصيتها، وهذا الوقت كافي لأي مجرم إلكتروني بتدمير الأدلة الإلكترونية أو إخفائها، وهذا لا يتفق مع خصوصية الجرائم الإلكترونية التي تحتاج إلى سرعه فائقة في الدخول إلى المكان المراد تفتيشه والسيطرة على الوسائل الإلكترونية.

(1) حجازي، عبد الفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 384.

(2) عبد الملك، جندي، الموسوعة الجنائية، ج4، مرجع سابق، ص 587.

(3) نقض جنائي مصري، بتاريخ 1972/5/29، أحكام النقض، س 23، ق 188، ص 830.

(4) بن يونس، عمر محمد، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، مرجع سابق، ص 207.

(5) طنطاوي إبراهيم حامد، الدفع ببطان إذن النيابة العامة بالتفتيش، مرجع سابق، ص 81.

(6) نقض جنائي مصري، بتاريخ 1957/5/7، أحكام النقض، س 8، ق 130، ص 471.

المطلب الثاني

الإجراءات الفنية للتفتيش في الجرائم الإلكترونية.

التفتيش التقليدي، هو الذي يهدف إلى البحث عن الأشياء المادية المتعلقة بالجريمة وتفيد في كشف الحقيقة، ولكن التفتيش في الجرائم الإلكترونية يهدف إلى البحث عن أشياء مادية وغير مادية لوسائل تكنولوجيا المعلومات، كون أن الأدلة الإلكترونية تحفظ وتخزن داخل تلك الوسائل الإلكترونية المتعددة.

التفتيش في الجرائم الإلكترونية يحتاج إلى وسائل وأدوات إلكترونية خاصة، للبحث في وسائل تكنولوجيا المعلومات عن الأدلة المطلوبة⁽¹⁾. لذلك سنتناول تفتيش مكونات وسائل تكنولوجيا المعلومات في الفرع الأول، ونبحث بالصعوبات والتحديات التي تواجه القائم بالتفتيش عند إجراء تفتيش على تلك المكونات في الفرع الثاني.

الفرع الأول: تفتيش مكونات وسائل تكنولوجيا المعلومات.

تفتيش مكونات وسائل تكنولوجيا المعلومات يحتاج إلى أشخاص ذوي خبرة في تلك الوسائل كونها تتكون من مكونات مادية وأخرى غير مادية، وتسمى كذلك (منطقية أو معنوية)، ويمكن أن تكون هذه الوسائل الإلكترونية متصلة بشبكات سلكية أو لا سلكية، ومتصلة بأجهزة وشبكات داخل الدولة أو خارجها⁽²⁾.

إجراء تفتيش على مكونات وسائل تكنولوجيا المعلومات، يخضع لصفة مكان وجودها، سواء بحوزة الأشخاص أو داخل الأماكن، سواء كانت منعزلة، أو متصلة بأجهزة أخرى عن طريق الشبكات الخاصة والعامة، داخل الدولة أو خارجها، لذلك سنبحث بتفتيش المكونات المادية لوسائل تكنولوجيا

(1) جابر، محمود محمد محمود، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة، جرائم نظم الاتصالات والمعلومات، دراسة مقارنة في التشريع المصري والفرنسي والأمريكي والإتفاقيات الدولية والإقليمية، الكتاب الثاني، المكتب الجامعي الحديث، الإسكندرية، 2018/2017، ص 164.

(2) حمودة، علي محمود علي، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في أكاديمية شرطة دبي، في شهر 4/2003، المجلد الأول، ص 272.

المعلومات في الفقرة الأولى، وتفتيش المكونات المعنوية في الفقرة الثانية.

أولاً: تفتيش المكونات المادية لوسائل لتكنولوجيا المعلومات.

كما أسلفنا، المكونات المادية لوسائل تكنولوجيا المعلومات متعددة ومتنوعة، منها ما يستخدم في عمليات إدخال المعلومات والبيانات وإخراجها، ومنها ما يستخدم لعمليات التخزين الإلكترونية.

المكونات المادية لوسائل تكنولوجيا المعلومات، هي عبارة عن المواد والأجسام التي توجد بمكان الحادث أو ذات صلة بالحادث ويمكن إدراكها وإحساسها بأحد الحواس⁽¹⁾، ويهدف تفتيش المكونات المادية لوسائل تكنولوجيا المعلومات إلى البحث عن شي يتصل بجريمة إلكترونية وقعت ويفيد بكشف الحقيقة عنها وعن مرتكبها⁽²⁾.

إن تفتيش المكونات المادية لوسائل تكنولوجيا المعلومات، لا يثير أي مشكلة قانونية عند تفتيشها⁽³⁾، طالما تمت وفق الإجراءات القانونية وتطبق عليها القواعد التقليدية للتفتيش، ولكن مكان وجودها له أهمية، حيث يتوقف تفتيشها على طبيعة المكان الموجودة فيه، فإذا كانت بحيازة الشخص فإنها تخضع لقواعد لتفتيش الأشخاص، وإذا كانت موجودة في مكان فان تفتيشها يخضع لقواعد تفتيش الأماكن بنفس الضمانات والشروط المقررة.

يرى الباحث عدم وجود مشكلة قانونية في تفتيش المكونات المادية لوسائل تكنولوجيا المعلومات، كون أن تلك المكونات لها طبيعة مادية ملموسة، وتطبق عليها القواعد العامة للتفتيش، ورغم ذلك كان لا بد على المشرع وضع نص في القانون لتعريفها وتحديدتها.

ثانياً: تفتيش المكونات الغير مادية لوسائل لتكنولوجيا المعلومات.

إن تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات، والتي تسمى كذلك المكونات المنطقية أو المعنوية، يثير صعوبات ومشاكل قانونية نظرا لطبيعتها الغير ملموس، ونظراً لخصوصيتها وطرق تخزينها وأماكن وجودها.

(1) أبو الروس، احمد، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، مرجع سابق، ص 317.

(2) الفيل، علي عدنان، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، 2012، ص 41.

(3) أحمد، هلاي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص 73.

المشرع الفلسطيني أجاز في المادة(1/32) من قانون الجرائم الإلكترونية تفتيش وسائل تكنولوجيا المعلومات، التي عرفها في المادة الأولى على أنها تتكون من وسائل مادية و غير مادية، وقد نصت المادة(1/50) من قانون الإجراءات الجزائية الفلسطيني، على أنه لا يجوز التفتيش إلا على الأشياء الخاصة بالجريمة، ولكن المشرع البحريني كان أكثر جرأة ووضوحا عندما عرف كلمة شيء أو أشياء بالمادة(2/22) من قانون جرائم تقنية المعلومات، على أنها تشمل نظام تقنية المعلومات أو أي جزء منه، وبيانات تقنية المعلومات، وأي من وسائط تخزين بيانات وسيلة تقنية المعلومات، أما المشرع الفرنسي أضاف كلمة المعطيات المعلوماتية إلى كلمة أشياء الواردة بالنص، لتشمل المكونات الغير مادية لوسائل تكنولوجيا المعلومات⁽¹⁾.

إختلف الفقهاء على إمكانية تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات، منهم من أنكر إمكانية تفتيشها لطبيعتها الغير ملموسة، ومنهم من أقر إمكانية تفتيشها، حيث سنستعرض تلك الآراء بشكل من البيان على النحو التالي:-

الرأي الأول: يرى (Vassilaki)، انه يجوز تفتيش المكونات المنطقية الإلكترونية بمختلف أشكالها مستندا إلى القوانين الإجرائية التي تنص في إذن التفتيش على ضبط "أي شيء"، وكلمة أي شيء تشمل المكونات المعنوية المحسوسة وغير المحسوسة⁽²⁾، وكلمة "الشيء" تشمل المكونات المادية والغير مادية لوسائل تكنولوجيا المعلومات⁽³⁾، والمكونات الغير مادية تفسر على أنها تشمل على البيانات المخزنة أو المعالجة الكترونيا⁽⁴⁾.

إن الوصول إلى معرفة المكونات الغير مادية لوسائل تكنولوجيا المعلومات يمكن من خلال البحث في تعريف المادة، حيث تعرف المادة بأنها " كل ما شغل حيزاً مادياً في فراغ معين، وأن الحيز يمكن قياسه والتحكم فيه" وإن الكيانات المنطقية لوسائل تكنولوجيا المعلومات تأخذ حيزاً مادياً في

(1) انظر المادة(94) من قانون الإجراءات الجنائية الفرنسي، Code de procédure pénale.

(2) Article by, Dr. Vassilaki (irini), Computer Crimes and Other Crimes Against Information Technology In Greec.1993. P 371. مشار إليه في كتاب أحمد، طارق عفيفي صادق، الجرائم الإلكترونية وجرائم

الهاتف المحمول، مرجع سابق، ص 218.

(3) الفهوجي، علي عبد القادر، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد في جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، بتاريخ 1 إلى 3/5/2000، م 2، ط 3، ص 561.

(4) سقف الحيط، عادل عزام، جرائم الدم والقدح والتحقيق المرتكبة عبر الوسائط الإلكترونية، مرجع سابق، ص 244.

الذاكرة ويمكن قياسها بمقياس معين، وتأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، وطبقاً لذلك تعد كيان مادي تشابه التيار الكهربائي⁽¹⁾.

الرأي الثاني: يرى (Piragoff) أن كلمة "أي شيء" لا تنطبق على المكونات المنطقية الإلكترونية، ويجب مواجهه هذا القصور التشريعي بالإضافة إلى كلمة شيء كلمة المكونات المعنوية الإلكترونية⁽²⁾، كما فعل المشرع الفرنسي.

الرأي الثالث: يرى (Mohrenschlager) أن هدف التفتيش هو ضبط الأدلة، وإن الضبط لا يقع إلا على الأشياء المادية، ويمكن ضبط الأدلة التي تتخذ شكلاً مادياً، عن طريق تصويرها أو طبعها أو نقلها على حافظة بيانات مادية⁽³⁾.

ولكن يجب التمييز بين المعلومات والبيانات، كون أن المعلومات ليس شيئاً مادياً ولا يرد عليها تفتيش، ولكن البيانات المعالجة إلكترونياً هي نبضات أو ذبذبات إلكترونية قابلة للتسجيل والتخزين على وسائط معينة ويمكن نقلها ويمكن تقديرها كمياً وقياسها وهي بذلك شيء ملموس للعالم الخارجي له وجود مادي ويرد عليها التفتيش⁽⁴⁾، وهذه البيانات والمعلومات المخزنة في وسائل التكنولوجيا تصلح لأن تكون محلاً للتفتيش إذا تم تسجيلها على ورق أو على الأقراص أو أية دعامة أخرى⁽⁵⁾.

إن تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات، هو تفتيش للفضاء الافتراضي غير الملموس في أغلب الأحيان بما يصعب معه تحريز الأدلة إلا من خلال تجميده على شكل مادي

(1) الفيل، علي عدنان، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، مرجع سابق، ص 43.

(2) Article by, Dr. Piragoff (Donald K), Computer Crimes and Other Crimes Against Information

Technology In Canda, 1993, P 241. مشار إليه في كتاب الغافري، حسين بن سعيد، السياسة الجنائية في مواجهة

جرائم الإنترنت، مرجع سابق، ص 477.

(3) Article by, Dr. Mohrenschlager (Manfred), Computer Crimes and Other Crimes Against

Information Technology In Germany, 1993, P 351. مشار إليه في كتاب أحمد، هلالى عبد اللاه، تفتيش نظم

الحاسب الآلي، مرجع سابق، ص 85.

(4) جابر، محمود محمد محمود، الأحكام الإجرائية الناشئة عن استخدام الهواتف النقالة، مرجع سابق، ص 168.

(5) الحلبي، خالد عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، مرجع سابق، ص 160.

ملموس⁽¹⁾، وهو أمر صعب إذا بقيت على صورتها المعنوية في شكل نبضات أو ذبذبات، أما إذا حولت إلى مستخرجات أو مستندات أو سجلات فإنه يسهل الوصول إلى الجرائم التي تُرتكب عليها⁽²⁾.

يرى الباحث أنه رغم الخلاف الدائر على إمكانية تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات، نرى عدم وجود مشكلة قانونية وعملية في تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات في التشريع الفلسطيني، كون أن المشرع نص صراحة على تفتيش تلك المكونات سواء كانت مادية أم غير مادية، وأن كلمة الأشياء الواردة في المادة (1/50) من قانون الإجراءات الجزائية الفلسطيني واسعة وتستوعب الوسائل الغير مادية لتكنولوجيا المعلومات، ومع ذلك كان لا بد على المشرع الفلسطيني أن ينص صراحة على تفتيش المكونات المعنوية لوسائل تكنولوجيا المعلومات، كما فعل المشرع السوري في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، بنص المادة (26/ب) والذي أكد فيها أن البرمجيات الحاسوبية خاضعة للتفتيش كما هي الأشياء المادية.

الفرع الثاني: تحديات إجراءات تفتيش وسائل تكنولوجيا المعلومات.

إن تفتيش وسائل تكنولوجيا المعلومات لا يتم بسهولة كما في الجرائم التقليدية، كون التفتيش في البيئة الإلكترونية له خصوصيته التي تخلق صعوبات ومعوقات للقائم بالتفتيش لمنعه من القيام بالتفتيش على وسائل تكنولوجيا المعلومات، وحرمانه من الوصول إلى الأدلة الإلكترونية.

منع المشرع الفلسطيني في المادة (3/50) من قانون الإجراءات الجزائية، مأموري الضبط القضائي الذين يقومون بالتفتيش من الإطلاع على الأوراق المختومة أو المغلقة التي يتم العثور عليها في المكان الذي يتم تفتيشه، وهذا النص مشابه للنص المصري⁽³⁾، وكرر المشرع الفلسطيني هذا المنع مرة أخرى في المادة (4/32) من قانون الجرائم الإلكترونية، وحظر على مأموري الضبط القضائي النفاذ المباشر إلى وسائل تكنولوجيا المعلومات وتفتيشها إلا بعد الحصول على إذن خاص من

(1) ربيعة، عبد اللطيف محمود، الجرائم الإلكترونية، التجريم والملاحقة والإثبات، بحث مقدم إلى المؤتمر الأول للجرائم الإلكترونية في فلسطين، المنعقد في جامعة النجاح الوطنية، بتاريخ 2016/4/17، نابلس، فلسطين، ص 15.

(2) إبراهيم، خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 199+200.

(3) أنظر المادة (52) من قانون الإجراءات الجنائية المصري.

النيابة العامة لإجراء تفتيش عليها، كون أن الأوراق والصور أصبحت تحفظ في وعاء إلكتروني غير تقليدي.

إن أغلب وسائل تكنولوجيا المعلومات تكون محمية عن طريق نظام حماية سواء برقم سري أو برنامج حماية لمنع الدخول إليها أو الاطلاع على محتوياتها، وأن الدخول إليها أو الإطلاع على ما بداخلها لا يجوز بغير تصريح من القانون⁽¹⁾، ويمنع على مأموري الضبط القضائي الإطلاع على البيانات والمعلومات والصور المخزنة إلكترونياً في وسائل تكنولوجيا المعلومات سواء توافرت لديه القدرة الفنية على ذلك، أو عن طريق أهل الخبرة لفك الحماية أو عن طريق الاختراق⁽²⁾، إلا بعد الحصول على إذن تفتيش من الجهات المختصة، ويستطيع بعدها مأمور الضبط القضائي القيام بتفتيش تلك الوسائل والتجول داخلها بحثاً عن الأدلة، وبناءً على هذه الخصوصية التي تتمتع بها وسائل تكنولوجيا المعلومات تظهر صعوبات ومعوقات تواجه القائم بالتفتيش، حيث سنبحث بالمعوقات الفنية في الفقرة الأولى، والصعوبات الجغرافية في الفقرة الثانية.

أولاً: صعوبات فنية تقنية.

القائم بالتفتيش يواجه أثناء قيامه بإجراء تفتيش على وسائل تكنولوجيا المعلومات صعوبات فنية تقنية، وتلك المعوقات يمكن أن تكون مانعاً إلكترونياً لإجراء تفتيش على تلك الوسائل.

عرف المشرع الفلسطيني في المادة الأولى من قانون الجرائم الإلكترونية كلمة السر بأنها "كل ما يستخدم للولوج لنظم تكنولوجيا المعلومات، وما في حكمها، للتأكد من هويته، وهي جزء من بيانات المرور، وتشمل الرموز وبصمة العين أو الوجه أو الأصبع أو ما في حكمها، وكذلك عرف الشفرة بأنها " مفتاح أو مفاتيح سرية خاصة لشخص أو لجهة معينة تُستخدم لتشفير البيانات الحاسوبية بالأرقام والحروف والرموز والبصمات أو ما في حكمها".

إن وسائل تكنولوجيا المعلومات، يمكن حمايتها بأرقام سرية لمنع الوصول إلى البيانات والمعلومات المخزنة داخلها، وهذه الأرقام لا يعرفها إلا صاحب تلك الوسائل أو مستخدمها، ولا يمكن إجباره

(1) عطية، طارق إبراهيم الدسوقي، الأمن المعلوماتي، مرجع سابق، ص 472.

(2) رستم، هشام محمد فريد، أصول التحقيق الجنائي الفني، واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، بتاريخ 1-3 / 5 / 2000م، م 2، ط 3، ص 427.

على البوح بها⁽¹⁾، وقد أجاز المشرع الفلسطيني بالمادة (1/33) من قانون الجرائم الإلكترونية للنيابة العامة الحصول على بيانات المرور الخاصة بالمشاركين، كون انه لا يمكن إجراء تفتيش على وسائل تكنولوجيا المعلومات دون الكشف عن أرقام الحماية، ولكن إذا لم يتم الحصول عليها أو لم يفصح المتهم عنها، يجوز للمفتش أن يستخدم برامج خاصة لفك الشيفرة والنفاذ إلى وسائل تكنولوجيا المعلومات وإجراء تفتيش عليها⁽²⁾.

يرى الباحث أن اغلب وسائل تكنولوجيا المعلومات محمية بأرقام سرية ولا يمكن النفاذ إلى تلك الوسائل إلا بعد معرفة الأرقام السرية سواء تم الحصول عليها من شخص المتهم، أو عن طريق استخدام القائم بالتفتيش لبرامج خاصة قادرة على معرفة الرقم السري، وكذلك نرى انه من غير المتصور أن يقوم المتهم بإرادته بإعطاء الرقم السري للقائم بالتفتيش إلا بعد الضغط عليه وإجباره من قبل مأموري الضبط القضائي على إعطاء الأرقام السرية، كون انه لا يعقل أن يقدم المتهم دليل على نفسه، وأن استخدام القائم بالتفتيش لبرامج ووسائل خاصة لفك الشيفرة يحتاج إلى وقت وجهد كبير، ويمكن أن يكون لهذا الفعل نتائج عكسية بتدمير الوسيلة المراد تفتيشها وإتلاف الأدلة المخزنة بداخلها، كون أن المجرم الإلكتروني يمكن أن يضع نظام تدمير ذاتي للوسيلة الإلكترونية إذا حاول أي شخص الدخول عليها وإختراقها، لذلك فان النفاذ المباشر إلى وسائل تكنولوجيا المعلومات المحمية بأرقام سرية لتفتيشها أمر صعب وبحاجة إلى خبراء ومتخصصين في تلك الوسائل وهي مخاطرة مجهولة النتيجة.

ثانياً: صعوبات جغرافية.

إضافة إلى الصعوبات الفنية التقنية لإجراء تفتيش على وسائل تكنولوجيا المعلومات، يواجه القائم بالتفتيش صعوبات أخرى جغرافية، تحتاج إلى وقت وجهد لا يقل أهمية عن الصعوبات التقنية.

وسائل تكنولوجيا المعلومات يمكن أن تكون منعزلة، ويمكن أن تكون متصلة بوسائل أخرى نهايتها في مكان آخر غير المكان المراد تفتيشه، ويخضع تفتيشها لنفس الضمانات المقررة بالقانون⁽³⁾،

(1) يوسف، أمير فرج، الجرائم المعلوماتية على شبكة الإنترنت، مرجع سابق، ص 234.

(2) حسين، سامي جلال فقي، التفتيش في الجرائم المعلوماتية، مرجع سابق، ص 223.

(3) الديري، عبد العال، وإسماعيل محمد صادق، الجرائم الإلكترونية، مرجع سابق، ص 299.

وإتصال وسائل تكنولوجيا المعلومات ببعضها من الصعوبات الجغرافية التي تواجه القائم بالتفتيش، سواء كانت هذه الوسائل متصلة ببعضها داخل الدولة أو مع وسائل أخرى خارج الدولة.

1- معوقات جغرافية داخل الدولة. من الصعوبات التي تواجه القائم بالتفتيش بالجرائم الإلكترونية، وجود المعلومات والأدلة التي يتم البحث عنها مخزنة في وسائل إلكترونية متواجدة في مكان آخر داخل حدود الدولة غير المكان الذي يتم البحث فيه.

المشرع الفلسطيني، أجاز لوكيل النيابة إذا اقتضى الأمر اتخاذ إجراء من الإجراءات خارج دائرة الإختصاص الجغرافي أن يُنيب عنه وكيل نيابة تلك الدائرة⁽¹⁾، وهذا النص يسمح للقائم بالتفتيش بالجرائم الإلكترونية في حال أن الأدلة المطلوبة مخزنة خارج دائرة إختصاصه أن ينيب عنه من هو مختص بالتفتيش في المكان الأخر التي توجد به الأدلة المطلوبة، وهذا بحاجة إلى أدون إضافية لكل مكان تتواجد به البيانات لإجراء تفتيش عليه⁽²⁾.

يرى الباحث أن التفتيش في الجرائم الإلكترونية يحتاج إلى سرعة في تنفيذه للطبيعة الخاصة لتلك الجرائم، وأن وجود الأدلة التي يتم البحث عنها المخزنة في وسائل تكنولوجيا المعلومات بمكان آخر غير المكان الذي يتم البحث فيه، فإنه والحالة تلك تكون هذه من معوقات التفتيش بالجرائم الإلكترونية، ولكن يمكن التغلب على تلك المعوقات إذا كان هناك سرعة في الحصول على الأدون القانونية المطلوبة من الجهات القضائية المختصة إستناداً إلى الإنابة في التحقيق، وسرعة تحرك مأموري الضبط القضائي إلى المكان المحدد والسيطرة عليه ومنع التخلص من الوسائل والأدلة، ورغم ذلك فإن مسح وتدمير الأدلة يكون أقرب من الوصول إليها.

2- معوقات جغرافية خارج الدولة. المعوقات الجغرافية بالتفتيش بالجرائم الإلكترونية ليست داخلية فقط، وإنما يوجد معوقات خارجية كذلك تواجه القائم بالتفتيش.

نظراً إلى خصوصية الجرائم الإلكترونية وطبيعتها العالمية، فإن القائم بالتفتيش يواجه مشاكل وصعوبات جغرافية لإجراء تفتيش على وسائل تكنولوجيا المعلومات التي تكون متصلة مع وسائل أخرى خارج الدولة، لأن الأدلة والمعلومات يمكن تخزينها خارج حدود الدولة عن طريق الشبكات

(1) أنظر المادة(57) من قانون الإجراءات الجزائية الفلسطيني.

(2) بن يونس، عمر محمد، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، مرجع سابق، ص 202.

العالمية، بهدف عرقلة سلطات التحقيق من الوصول إليها⁽¹⁾.

ومن أصعب المشاكل التي تواجه القائم بالتفتيش في الجرائم الإلكترونية قيام المجرمين بتخزين بياناتهم في أنظمة تقنية خارج حدود الدولة، مستخدمين في ذلك شبكات الإتصال الإلكترونية لعرقلة سلطة التفتيش من جمع الأدلة، وبسبب ذلك يتعذر إجراء تفتيش على تلك الوسائل إلزاماً بمبدأ عدم الإعتداء على سيادة دولة أخرى.

المشرع الفلسطيني في قانون الجرائم الإلكترونية لم يُشر إلى إمكانية تجاوز التفتيش لحدود الدولة، إلزاماً منه بمبدأ الإقليمية بعدم الإعتداء على سيادة دولة أخرى، كون التفتيش العابر للحدود لا يجوز القيام به إلا من خلال إتفاقيات ثنائية أو دولية عن طريق التعاون القضائي أو بعد الحصول على إذن الدولة⁽²⁾، وفي هذه الحالة فإن يد القائم بالتفتيش تبقى مقيدة بأن لا تمتد إلى تلك الأدلة.

الإتفاقية العربية لمكافحة جرائم تقنية المعلومات أجازت في المادة(40) إجراء تفتيش على وسائل تكنولوجيا المعلومات المتواجدة في دولة أخرى دون تفويض من تلك الدولة، ولكن وضعت شرطين لإجراء هذا التفتيش دون النظر إلى الموقع الجغرافي المتواجدة فيه، الأول أن يكون الوصول إلى المعلومات مفتوح ومصروح به، والثاني وجود موافقة طوعية من الشخص الذي يملك السلطة القانونية على تلك المعلومات، وهي نفس الشروط التي وردت في المادة(32) من الإتفاقية الأوروبية للجرائم السبيرانية، وهذه الشروط توصل إليها واضعوا الإتفاقية الأوروبية بعد مخاض عسير، كون أنهم وجدوا أنه ليس من الممكن إعداد نظام قانوني عالمي ملزم يمكن تطبيقه في المجال الإلكتروني، وتراعى الظروف الخاصة بكل حالة فردية على حدى⁽³⁾.

المشرع البحريني، أجاز إمتداد الدخول والتفتيش إلى نظام تقني آخر إذا كان هناك إمارات قوية بان البيانات المتصلة بالجريمة مخزنه عليه، وتكون قابله للدخول إليها من النظام الأول وتكون متاحة على نحو مشروع⁽⁴⁾، وكذلك فعل المشرع الفرنسي وأجاز لرجال الضبط القضائي أن يدخلوا على البيانات التي تهم التحقيق والمخزنة في النظام أو في أي نظام معلوماتي آخر مادامت متصلة

(1) حجازي، عبد الفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 382.

(2) الفيل، علي عدنان، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، مرجع سابق، ص 46.

(3) أحمد، هلاي عبد اللاه، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، مرجع سابق، ص 379.

(4) أنظر المادة(2/15) من قانون جرائم تقنية المعلومات البحريني.

شبكة واحدة مع النظام الرئيسي وتكون متاحة⁽¹⁾.

نظم المشرع الفلسطيني بالمادة (43) من قانون الجرائم الإلكترونية طرق طلب المساعدة القانونية من الدول الأخرى للحصول على الأدلة المطلوبة الموجودة على أراضيها، وقد تناولنا طرق طلب المساعدة القانونية، حيث منح المشرع الفلسطيني في المادة(38) من قانون الجرائم الإلكترونية شرعية لتلك الأدلة طالما أن الحصول عليها قد تم وفقا للإجراءات القانونية والقضائية بالتعاون الدولي.

إن الوضع الغالب بالتفتيش بالجرائم الإلكترونية، أن يتجاوز التفتيش المكان الذي يجري تفتيشه إلى مكان آخر، في ظل شبك الأجهزة وربطها ببعضها سواء محليا أو إقليميا⁽²⁾، كون انه لا وجود لحدود جغرافية محددة في الجرائم الإلكترونية ولا يشترط الحصول على موافقة طرف ثالثا⁽³⁾.

يرى الباحث أن المشرع الفلسطيني في قانون الجرائم الإلكترونية، لم يأخذ بالمادة(40) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات كما فعل المشرع البحريني، والتي أجازت تجاوز التفتيش لحدود الدولة للبحث عن الأدلة والمعلومات المطلوبة للتحقيق والمخزنة في وسائل إلكترونية بدولة أخرى أو عدة دول في حالات معينة، وبالتالي لم يجيز المشرع الفلسطيني تجاوز التفتيش لحدود الدولة، واكتفى بالحصول على الأدلة المطلوبة من دولة أخرى من خلال طلب المساعدة القانونية بالطرق القضائية المحددة بالقانون والإتفاقيات الموقعة فقط، وبذلك يكون إمتداد التفتيش خارج حدود الدولة بغير سند من القانون، ولكن نرى أن المشرع الفلسطيني لم يكن موقفا في ذلك، كون الجرائم الإلكترونية لا تعترف بالحدود الجغرافية للدول، وأن السلطة القائمة بالتفتيش يجب عليها ملاحقة المجرمين الإلكترونيين من دولة إلى دولة وبالتالي فإن الباحث يؤيد تجاوز التفتيش حدود الدولة في الجرائم الإلكترونية للحصول على المعلومات والأدلة التي تقيد التحقيق.

(1) أنظر المادة(1/57) من قانون الإجراءات الجنائية الفرنسي. .Code de procédure pénale.

(2) طه، محمود احمد، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، مرجع سابق، ص 211.

(3) الفيل، علي عدنان، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، مرجع سابق، ص 45.

المبحث الثاني

أثار التفتيش في الجرائم الإلكترونية

العثور على الأدلة وضبطها من أهم أثار التفتيش، لذلك وضع المشرع الفلسطيني شروط لإجراء التفتيش، ويجب أن يتم إجراء التفتيش وفق تلك القواعد التي رسمها المشرع، حتى يتم العثور على الأدلة المطلوبة لفائدة التحقيق، وضبطها بالشكل الذي يتفق ونص القانون.

إن البيئة في الدعاوي الجزائية بفلسطين تقام بجميع طرق الإثبات، إلا إذا نص القانون على طريقة معينة للإثبات⁽¹⁾، وهذا نظام الإثبات الحر في المادة الجزائية، والذي يعني أن القاضي الجزائي له حرية في تكوين قناعته، بأن يقبل بالأدلة التي يطمئن إليها ويستبعد أي دليل لا يطمئن إليه، فلا وجود لأدلة مفروضة عليه، وله السلطة الكاملة في وزن قيمة كل دليل⁽²⁾.

نصت المادة (37) من قانون الجرائم الإلكترونية الفلسطيني، على انه " يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات"، ونصت المادة(38) من ذات القانون على أن الأدلة المتحصلة من جهات التحقيق من دولة أخرى تعتبر أدلة إثبات، وهذا يعني أن الأدلة الإلكترونية تخضع لتقدير القاضي الجزائي كغيرها من الأدلة الأخرى، ولكن المشرع السوري كعادته كان أكثر وضوحا عندما نص بشكل صريح بالمادة(25) من قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، أن الدليل الإلكتروني يعود تقديره للمحكمة.

الدليل الإلكتروني المأخوذ من وسائل تكنولوجيا المعلومات كغيره من الأدلة يجب الحصول عليه بطرق مشروعة، مع إمكانية مناقشته، ويكون غير قابل للشك⁽³⁾، وبذلك يصبح دليل يمكن إعماله أمام القضاء، سواء في حالة الإدانة أو البراءة.

(1) انظر المادة(1/206) من قانون الإجراءات الجزائية الفلسطيني.

(2) Rached. مشار إليه في كتاب عزات، محمد فتحي محمد أنور، تفتيش شبكة الإنترنت، مرجع سابق، ص 319.

(3) عبد المطلب، ممدوح عبد الحميد، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2006، ص 88.

كما أسلفنا، قانون الجرائم الإلكترونية الفلسطيني لم ينص على ضرورة إنشاء محكمة مختصة للنظر بالجرائم الإلكترونية، على عكس قانون الجرائم المعلوماتية السوداني، الذي اوجب بالمادة(28) إنشاء محكمة مختصة للنظر بالجرائم الإلكترونية، ولكن نظرا لخصوصية تلك الجرائم التي يغلب عليها الطابع التقني، فهي بحاجة إلى قضاء مؤهلين للنظر بها، حتى يستطيعوا فهم فحوى هذه التقنية، وأن يكونوا على معرفة بطبيعتها، ويجب أن يتفهم القاضي الجزائي خصائص الدليل الإلكترونية وطرق إستخراجه، الذي يغلب عليه الطابع الفني⁽¹⁾، حتى يكون له دوراً مهماً في مكافحة الجرائم الإلكترونية.

تناولنا في المبحث الثاني من الفصل الأول من هذا البحث ضمانات التفتيش، فإذا تم مراعاتها من قبل القائم بالتفتيش، فإن التفتيش ينتج آثار قانونية، وفي حال تم مخالفتها يكون البطلان مصير التفتيش، وقد رسم المشرع الفلسطيني في قانون الإجراءات الجزائية طرق ضبط الأدلة، وحفظها، والتصرف فيها، وكذلك فعل في قانون الجرائم الإلكترونية، كون الأدلة الإلكترونية لها خصوصية، فهي بحاجة إلى طرق فنية للتعامل معها وطرق لحفظها. لذلك سنتناول في المطلب الأول، آثار التفتيش القانوني، وبالمطلب الثاني آثار التفتيش غير القانوني .

المطلب الأول

آثار التفتيش القانوني في الجرائم الإلكترونية.

التفتيش القانوني في الجرائم الإلكترونية الذي يجري وفق ما رسمه القانون يعطي مشروعية قانونية لأهم آثاره وهو ضبط الأدلة الإلكترونية، ولهذه الأدلة صلة مباشرة في كشف الحقيقة بنسب الجريمة للفاعل أو نفيها عنه، ويمكن أن تكون الأدلة المضبوطة في ذاتها دليل على الجريمة، أو يظهر منها هذا الدليل، أو قد تكون تلك الأشياء المضبوطة هي التي إستعملت في ارتكاب الجريمة أو تكون السبب الذي إرتكبت لأجله الجريمة⁽²⁾.

(1) يوسف، أمير فرج، الجرائم المعلوماتية على شبكة الإنترنت، مرجع سابق، ص 238.

(2) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 481.

نصت المادة (1/50) من قانون الإجراءات الجزائية الفلسطيني، على أنه "لا يجوز التفتيش إلا عن الأشياء الخاصة بالجريمة الجاري التحقيق بشأنها، وإذا ظهر عرضاً أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة في جريمة أخرى جاز لمأمور الضبط القضائي ضبطها"، وكذلك نصت المادة (1/32) من قانون الجرائم الإلكترونية، على أن التفتيش يتم على وسائل تكنولوجيا المعلومات ذات الصلة بالجريمة الإلكترونية، وهذه النصوص حددت الغاية من التفتيش وهي البحث عن الأدلة المرتبطة بالجريمة وضبطها، وفي حال تمت إجراءات التفتيش بمراعاة الضمانات المقررة له، يكون ضبط الأشياء الخاصة بالجريمة والأشياء التي تظهر عرضاً ضبطاً قانونياً⁽¹⁾.

إن التفتيش في الجرائم الإلكترونية يسعى إلى ضبط الأدلة الإلكترونية، ولكن بطرق مختلفة عن ما يتم بالجرائم التقليدية نظراً لخصوصيتها، حيث سنتناول ضبط الأدلة الإلكترونية في الفرع الأول، وبالفرع الثاني محضر الضبط وحفظ الأدلة.

الفرع الأول: ضبط الأدلة الإلكترونية .

ضبط الأدلة الإلكترونية سواء كانت أدلة مادية أم غير مادية، هو غاية التفتيش في الجرائم الإلكترونية.

أوصت اللجنة الدولية لقانون العقوبات، أن يتم التحديد بوضوح على السلطات التي تقوم بالتفتيش والضبط في بيئة تكنولوجيا المعلومات، وخاصة ضبط الأشياء غير المحسوسة، وشبكات الحاسوب⁽²⁾، كما أن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة (1/27)، أوجبت على كل دولة تبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين المعلومات الإلكترونية التي يتم الوصول إليها، وهذا النص مشابه لنص المادة (3/19) من الإتفاقية الأوروبية لمكافحة الجرائم السيبرانية.

قانون الإجراءات الجزائية الفلسطيني، أوجب في المادة (2/50) على ضرورة ضبط جميع الأشياء التي يعثر عليها أثناء إجراء التفتيش والمتعلقة بالجريمة، ولكن المشرع الأردني ذكر بالمادة (87)

(1) عوض، محمد محيي الدين، حقوق الإنسان في الإجراءات الجنائية، مرجع سابق، ص 232.

(2) انظر البند (1/3) من قرار وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات، حول القواعد الإجرائية في بيئة جرائم الكمبيوتر، الشق الإجرائي، مصدر سابق.

من قانون أصول المحاكمات الجزائية مصطلح ضبط جميع الأشياء التي يراها المدعي العام ضرورة لإظهار الحقيقة، واستخدم المشرع المصري في المادة(55) من قانون الإجراءات الجنائية كلمة ضبط كل ما يفيد في كشف الحقيقة.

المشرع الفلسطيني، نظم ضبط الأدلة الإلكترونية المادية في المادة(3/32) من قانون الجرائم الإلكترونية، حيث نص على انه " إذا أسفر التفتيش على ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة يتعين على مأمور الضبط القضائي تنظيم محضر ضبط بالمضبوطات وعرضها على النيابة لاتخاذ ما يلزم بشأنها "، وهذا النص مشابه لما جاء في قانون الجرائم الإلكترونية الأردني⁽¹⁾، وكذلك نص المشرع الفلسطيني في متن المادة (4+3+2/33) من قانون الجرائم الإلكترونية، على ضبط الأدلة الإلكترونية غير المادية، حيث جاء بالفقرة الأولى على أنه " للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام معلومات، أو جزء منه، أو أية وسيلة إلكترونية، ونص بالفقرة الثالثة على انه إذا تعذر إجراء الضبط والتحفظ ، يتم نسخ البيانات أو المعلومات التي لها علاقة بالجريمة على وسيلة إلكترونية من وسائل تكنولوجيا المعلومات، ونص بالفقرة الرابعة، في حال إستحالة الضبط والتحفظ بصفة فعلية، يتم إستعمال كافة الوسائل المناسبة لمنع الوصول والنفاد إلى البيانات المخزنة بنظام المعلومات، وأشترط المشرع الفلسطيني بالمادة(6/33) أن يتم تحرير قائمة بالمضبوطات بحضور المتهم أو من وجدت لديه إذا أمكن ذلك.

المشرع الفلسطيني، لم يستخدم بقانون الجرائم الإلكترونية وخاصة بالنصوص المتعلقة بالضبط كلمة الأدلة غير المادية بشكل مباشر، ولكنه إستخدمها عند تعريف وسائل تكنولوجيا المعلومات في المادة الأولى، عندما أكد على أن وسائل تكنولوجيا المعلومات تتكون من وسائل مادية وغير مادية. لذلك سنبحث بتعريف الضبط في الفقرة الأولى، وضبط الأدلة الإلكترونية المادية في الفقرة الثانية، والغير مادية في الفقرة الثالثة.

أولاً: تعريف الضبط.

الضبط القضائي، هو إجراء تحقيقي، بوضع اليد على الشيء وحبسه والمحافظة عليه لمصلحة

(1) أنظر المادة(13/ب) من قانون الجرائم الإلكترونية الأردني.

التحقيق⁽¹⁾، وينصب على الأشياء التي تفيد في كشف الحقيقة وكذلك الأشياء التي تعد حيازتها جريمة⁽²⁾، وهو الوسيلة القانونية التي تضع بواسطتها سلطة التحقيق يدها على الأشياء التي تساعد على ظهور الحقيقة⁽³⁾.

إن مصطلح كشف الحقيقة يعني، أن يكون مأمور الضبط موضوعيا في أداء واجبه، فلا يقتصر الضبط على الأشياء التي تفيد في إدانة المتهم وإنما يجب أن يمتد إلى تبرئته⁽⁴⁾، ومعيار ضبط الأشياء، هو أن تكون مفيدة في شأن حقيقة الجريمة الجاري التحقيق بشأنها حتى لو لم تعد حيازتها جريمة ما دام أنها تفيد الحقيقة⁽⁵⁾، ويجب أن يكون الضبط في مكان معين، أو لدى شخص معين، وينصب على أشياء معينة، تفيد في كشف الحقيقة إثباتا ونفيا، وتكون تلك الأشياء مرتبطة بالجريمة التي أمر فيها الضبط⁽⁶⁾، والأصل في الأشياء التي يجوز ضبطها أن تكون مادية، ولكن يجوز أن يرد الضبط على أشياء أخرى في مدلولها الواسع كالمحادثات السلوكية أو اللاسلوكية، أو أشياء في حيازة غير المتهم⁽⁷⁾.

الضبط بالجرائم الإلكترونية، هو وضع اليد على المكونات المادية لوسائل تكنولوجيا المعلومات والأدلة الإلكترونية المخزنة فيها، والتي تفيد في كشف الحقيقة في جريمة إلكترونية قد وقعت وجاري التحقيق فيها⁽⁸⁾، ويقع الضبط على المكونات المادية والغير مادية لوسائل تكنولوجيا المعلومات، كونها تشكل أدلة إلكترونية⁽⁹⁾

الدليل الإلكتروني غير المادي يقصد به، معلومات يقبلها العقل والمنطق ويعتمدها العلم، يتم الحصول عليها بإجراءات علمية وقانونية ويتم إستخدامها لإثبات حقيقة فعل أو شيء أو شخص له

(1) ثروت جلال، نظم الإجراءات الجنائية، مرجع سابق، ص 457.

(2) الشواربي، عبد الحميد، إذن التفتيش، مرجع سابق، ص 86.

(3) Vidal(Georges) et Magnol,(Joseph) Cours de droit criminel et de science penitentiaire,

tome11,Procédure pe-nale,9 edition, Rousseau, Paris,1949.no,807,p,1157. مشار إليه في كتاب

الجوخدار، حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، مرجع سابق، ص 186.

(4) عبد الستار، فوزية، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات، مرجع سابق، ص 309.

(5) السعيد كامل، شرح قانون أصول المحاكمات الجزائية، مرجع سابق، ص 467.

(6) مصطفى، محمود محمود، الإثبات في المواد الجنائية في القانون المقارن، مرجع سابق، ص 81.

(7) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 560.

(8) حسين، سامي جلال فقي، التفتيش في الجرائم المعلوماتية، مرجع سابق، ص 263.

(9) إبراهيم، خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 275.

علاقة بالجريمة⁽¹⁾.

ثانياً: ضبط الأدلة الإلكترونية المادية.

الأدلة المادية الإلكترونية التي يجوز ضبطها، هي الأشياء المنقولة التي تفيد في كشف الحقيقة، وكل الأشياء التي توجد في مكان وقوع الجريمة، أو غيره من الأماكن، والتي تؤدي إلى معرفة الفاعل والمساهمين كون أنها بطبيعتها المادية تمثل دلائل تفيد التحقيق⁽²⁾.

المشرع الفلسطيني، عبر في قانون الجرائم الإلكترونية عن الوسائل المادية بالمادة (3/32) بأنها الأجهزة، والأدوات، أو أي وسائل لها صلة بالجريمة الإلكترونية، والوسائل المادية لتكنولوجيا المعلومات، هي الأدوات الفنية التي غالباً ما تستخدم في بنية نظم المعلومات وتثبت وقوع الجريمة الإلكترونية وتساعد على تحديد هوية مرتكبها⁽³⁾، وهي عبارة عن أجسام توجد بمكان الحادث أو ذات صلة بالجريمة الإلكترونية، ويمكن إدراكها وإحساسها بأحد الحواس، وتؤدي إلى معرفة طرق ارتكاب الجريمة، ومعرفة شخصية المتهم⁽⁴⁾، وهي التي يقع عليها الضبط، سواء كانت حيازتها تعد تعد جريمة، أو أن تلك القطع أداة لارتكاب الجريمة الإلكترونية⁽⁵⁾.

ويمكن أن تكون الأدلة المادية الإلكترونية وسائل منقولة، أي يمكن نقلها من مكان لآخر لحفظها، وكذلك يمكن أن تكون عقار إلكتروني لا يمكن نقله ويحتوي على الأدلة المطلوبة، يتم ضبط هذا العقار عن طريق وضع أختام أو تعيين حراس عليه بما تحويه⁽⁶⁾.

يرى الباحث أن ضبط الأدلة المادية الإلكترونية لا يشكل أي مشكلة لدى القائم بالتفتيش، كون أنها مادية ويتم ضبطها كما في الجرائم التقليدية، وتطبق عليها قواعد الضبط المنصوص عليها بالقواعد العامة، ولكن مع ضرورة اتخاذ الحذر في التعامل معها لحساسيتها وهي بحاجة إلى رقة

(1) البشري، محمد الأمين، التحقيق في الجرائم المستحدثة، ط1، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 234.

(2) الشهاوي، قدري عبد الفتاح، مناهج التفتيش، قيوده وضوابطه، مرجع سابق، ص 169.

(3) العنزى، سليمان بن مهجع، وسائل التحقيق في جرائم نظم المعلومات، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003، ص 98.

(4) أبو الروس، احمد، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، مرجع سابق، ص 317+318.

(5) بن يونس، عمر محمد، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، مرجع سابق، ص 219.

(6) الشهاوي، قدري عبد الفتاح، مناهج التفتيش، قيوده وضوابطه، مرجع سابق، ص 180.

بالتعامل، ولا تلزم أي نوع من القوة.

ثالثاً: ضبط الأدلة الإلكترونية الغير مادية.

التفتيش بالجرائم الإلكترونية، يقع على الأشياء المادية والغير المادية لوسائل تكنولوجيا المعلومات، والضبط لا يرد إلا على شي مادي، والأشياء المعنوية لا تصلح بطبيعتها لان تكون محلا للضبط⁽¹⁾.

كما أسلفنا، أن المشرع الفلسطيني إستخدم في المادة (50) من قانون الإجراءات الجزائية، مصطلح ضبط جميع الأشياء المتعلقة بالجريمة، والمشرع المصري إستخدم بالمادة(55) من قانون الإجراءات الجنائية مصطلح ضبط كل ما يفيد في كشف الحقيقة، والمشرع الأردني إستخدم في المادة(87) من قانون أصول المحاكمات الجزائية، ضبط جميع الأشياء الضرورية لإظهار الحقيقة، ولكن في قانون الجرائم الإلكترونية إستخدم المشرع الفلسطيني بالمادة(32) مصطلح ضبط وسائل تكنولوجيا المعلومات ذات الصلة بالجريمة، وإن كلمة الأشياء، التي استخدمها المشرعين، تسمح بضبط الأدلة الإلكترونية غير المحسوسة⁽²⁾.

المشرع السوري عرف الدليل الرقمي بالمادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية بأنه "البيانات الرقمية المخزنة في الأجهزة الحاسوبية، أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتي يمكن إستخدامها في إثبات أو نفي جريمة معلوماتية، ونص المشرع السوري بشكل صريح بالمادة(26/ب) من ذات القانون على ضبط الأشياء غير المادية لوسائل تكنولوجيا المعلومات، حيث جاء فيها أنه " تعد البرمجيات الحاسوبية من الأشياء المادية التي يجوز ضبطها وفق القواعد المنصوص عليها في قانون أصول المحاكمات الجزائية، وذكرت التعليمات التوضيحية والتنفيذية للقانون السوري، أن الغرض من هذه الفقرة هو أن البرمجيات الحاسوبية إلى جانب الأشياء المادية الأخرى تكون خاضعة للضبط.

إلا أن المشرع البحريني، أخذ نهجاً اخرأً، ونص بالمادة(2/22) من قانون جرائم تقنية المعلومات،

(1) حجازي، عبد الفتاح بيومي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم الإلكترونية، مرجع سابق، ص 670.

(2) حمود، علي محمود علي، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى مؤتمر حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، مرجع سابق، ص 14.

على أن كلمة شيء، أو أشياء، تشمل نظام تقنية المعلومات أو أي جزء منه، وبيانات وسيلة تقنية المعلومات، وأي من وسائط تخزين بيانات وسيلة تقنية المعلومات.

الدليل الإلكتروني، دليل غير ملموس، ولكن البرامج والمعلومات والملفات المخزنة في الذاكرة الإلكترونية يحتاج ضبطها إلى إجراءات خاصة مناسبة تراعي خصوصيتها⁽¹⁾، كون تلك الأدلة مخزنة بشكل إلكتروني بالقطع الصلبة لوسائل تكنولوجيا المعلومات⁽²⁾، وان البيانات والمعلومات المخزنة لا تعتبر أدلة مادية، ولكن يمكن ضبط حاملة البيانات (الدعامة التي تم تخزين البيانات عليها) وأخذ نسخة ورقية لتأخذ شكلا ماديا⁽³⁾، ولها قيمة قانونية لأنها من قبيل الأدلة الفنية المستمدة من الوسائل الإلكترونية.

إن الضبط، يمتد إلى الأشياء الغير مادية، ولكن بعد تفريغها في كيان مادي ملموس⁽⁴⁾، كطباعتها على ورق أو إفراغ البيانات على الأقراص المدمجة أو المرنة⁽⁵⁾.

يرى الباحث أن ضبط الأدلة الإلكترونية الغير مادية لوسائل تكنولوجيا المعلومات، لا يشكل أي مشكلة في التشريع الفلسطيني، كون أن المشرع في تعريفه لوسائل تكنولوجيا المعلومات أشار إلى أنها تتكون من وسائل مادية وغير مادية، وان كلمة جميع الأشياء، أو ذات صلة بالجريمة التي إستخدامها المشرع الفلسطيني تشمل الأدلة الإلكترونية غير المادية، وأجاز المشرع الفلسطيني في المادة(3/33) من قانون الجرائم الإلكترونية نسخ البيانات والمعلومات المخزنة في وسائل تكنولوجيا المعلومات ولها علاقة بالجريمة الإلكترونية، ورغم ذلك كان لابد على المشرع النص بوضوح على قابلية البرمجيات الإلكترونية وغيرها من الأشياء الغير مادية لوسائل لتكنولوجيا المعلومات للضبط.

الفرع الثاني: محضر الضبط وحفظ الأدلة في الجرائم الإلكترونية.

أوجب المشرع الفلسطيني في المادة(50) من قانون الإجراءات الجزائية، والمادة(3/32) من قانون

(1) أحمد، طارق عفيفي صادق، الجرائم الإلكترونية، جرائم الهاتف المحمول، مرجع سابق، ص 225 وما بعدها.

(2) بن يونس، عمر محمد، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، مرجع سابق، ص 230 وما بعدها.

(3) أحمد، هلالى عبد اللاه، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني، على ضوء اتفاقية بودابست، مرجع سابق، ص 206 وما بعدها.

(4) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسبوط، 1994، ص 93.

(5) الطوالة، علي حسن محمد، التفتيش الجنائي على نظم الحاسوب والإنترنت، مرجع سابق، ص 149.

الجرائم الإلكترونية، تنظيم محضر ضبط بالمضبوبات التي يتم العثور عليها أثناء التفتيش، وكذلك رسم طرق وأماكن حفظها.

القائم بالتفتيش ملزم بنص القانون في حال العثور على أدلة أن يقوم بتحرير محضر ضبط بتلك الأدلة والمحافظة عليها ومنع محاولة العبث بها، وعلة هذا الإجراء يكمن في ضمان الإطلاع على الأشياء المضبوطة لإستخلاص الدليل منها⁽¹⁾، ويجب أن يوضع المضبوط في حرز مغلق ويختم عليه وإذا كان المضبوط عقارا يتم وضع الأختام عليه وغلقه وختمه ووضع حارس عليه ولضمان التعرف عليها⁽²⁾. حيث سنتناول محضر الضبط في الفقرة الأولى، وحفظ الأدلة في الفقرة الثانية، والتصرف بها في الفقرة الثالثة.

أولاً: محضر الضبط في الجرائم الإلكترونية.

الضبط، هو الصورة المادية لنتيجة التفتيش، أما محضر الضبط فهو الصورة المكتوبة له⁽³⁾، لذلك يجب على القائم بالتفتيش أن يحرر محضر ضبط بالأشياء المضبوطة.

من الضمانات التي أوردها المشرع الفلسطيني بالمادة (2/50) من قانون الإجراءات الجزائية، ضبط جميع الأشياء وتحريزها، وتثبيتها بمحضر وحفظها وإحالتها إلى الجهات المختصة، وكذلك بالمادة (3/32) من قانون الجرائم الإلكترونية الفلسطيني، والتي نصت على ضرورة تنظيم محضر ضبط بالمضبوبات وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها، وأشترط المشرع الفلسطيني بالمادة (6/33) من قانون الجرائم الإلكترونية أن يتم تحرير قائمة بالمضبوبات بحضور المتهم أو من وجدت لديه إذا أمكن ذلك، ولكن المشرع المصري أضاف في المادة (55) من قانون الإجراءات الجنائية ضرورة قيام مأمور الضبط القضائي بعرض الأشياء المضبوطة على المتهم لإبداء ملاحظته عليها والتوقيع على المحضر، أما المشرع الفلسطيني لم ينص صراحة على هذا الإجراء الأخير، ولكن يمكن استنتاجه من المادة (94) من قانون الإجراءات الجزائية عند إستجواب المتهم، ومواجهته بالأدلة وسماع أقواله حولها وتدوين ذلك بمحضر التحقيق.

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 568.

(2) عبد الستار، فوزية، شرح قانون الإجراءات الجنائية وفقاً لأحدث التعديلات، مرجع سابق، ص 310.

(3) ثروت جلال، نظم الإجراءات الجنائية، مرجع سابق، ص 477.

المشرع الفلسطيني، أمر بتنظيم محضر ضبط بالمضبوطات، ولكن لم يحدد شكل معين لهذا المحضر، ولكنه أورد ثلاثة شروط كي يكتسب المحضر قوة ثبوتية في متن المادة(213) من قانون الإجراءات الجزائية، وهذه الشروط متمثلة في أن يكون المحضر صحيحا بالشكل، ومحرره عاين الواقعة بنفسه أو أبلغ عنها، وأن يكون محرره قد دونه ضمن حدود إختصاصه وأثناء قيامه بمهام وظيفته، ولكن يجب على القائم بالتفتيش الإطلاع على الأشياء المضبوطة بنفسه، وأن ينتدب خبير إذا كان الإطلاع عليها وإستخلاص الدليل منها يتطلب خبرة فنية، وينظم محضر ضبط بها⁽¹⁾.

يرى الباحث إن تنظيم محضر الضبط من الضمانات التي أقرها المشرع الفلسطيني في الجرائم الإلكترونية، حتى يتم تسجيل بيانات جميع الأدلة الإلكترونية المضبوطة في المحضر، وذكر تفاصيلها، ووظائفها التقنية، ولهذا المحضر أهمية بالغة في الجرائم الإلكترونية، ليتم التعرف على الأدلة الإلكترونية المضبوطة وليتم تمييزها عن غيرها، ومنعا من إستبدالها كون انه يوجد وسائل إلكترونية لها نفس الشكل إذا كانت من نفس النوع ونتاجة عن نفس الشركة المصنعة، وبهذه الخصوصية يمكن تغييرها بسهولة بوضع وسائل أخرى مشابهة، يصعب تمييزها عن بعضها.

ثانياً: حفظ الأدلة الإلكترونية.

الأدلة الإلكترونية التي يتم ضبطها تحتاج إلى طرق خاصة لحفظها نظرا لخصوصيتها التقنية، التي تجعل منها أدلة حساسة تحتاج إلى طرق ومعاملة لينة لحفظها، كون إتلافها أو إتلاف ما تحتويه أمر سهل.

رسم المشرع الفلسطيني طرق حفظ الأدلة في قانون الإجراءات الجزائية، حيث نصت المادة(2/50) على أن المضبوطات تحرز وتحفظ وتحال إلى الجهات المختصة، وحدد المشرع في المادة(1/72) من ذات القانون على أن يتم وضع المضبوطات في حرز مغلق وتكتب عليها بياناتها وتودع في مخزن النيابة أو المكان الذي تقرر لذلك.

المشرع الأردني نص على طرق حفظ الأدلة بالمادة(1/35) من قانون أصول المحاكمات الجزائية، والتي جاء فيها انه يعنى بحفظ الأشياء المضبوطة بالحالة التي كانت عليها، فتحزم أو توضع في وعاء إذا اقتضت ماهيتها ذلك وتختم بختم رسمي، ووضح المشرع المصري بالمادة(56)

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، مرجع سابق، ص 568.

من قانون الإجراءات الجنائية آلية حفظ الأشياء المضبوطة، وأمر بوضعها في حرز مغلق وربطها وختمها ويكتب على شريط داخل الختم تاريخ المحضر المحرر بضبط تلك الأشياء ويشار إلى الموضوع الذي حصل الضبط من أجله.

قانون الجرائم الإلكترونية الفلسطيني، نص في المادة (3/32) على ضرورة ضبط الأدلة وإحالتها إلى النيابة العامة لإتخاذ ما يلزم بشأنها، ونظم طرق حفظها في المادة (6/33) من ذات القانون والذي جاء فيها " يحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف، أو في مغلف مختوم، وتكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.

حفظ الأدلة بشكل يمنع الوصول إليها وتغييرها، هو ضمان ذاتية الأشياء المضبوطة لصونها من يد العبث⁽¹⁾، ويتم وضع المضبوطات في وعاء تناسب حجمها، وختمها بوجود الأشخاص الذين حضروا التفتيش، للمحافظة عليها بالحالة التي كانت عليها لمنع التلاعب بها أو تحريف معالمها⁽²⁾.

إن قواعد حفظ الأدلة، هي قواعد إرشادية تنظيمية لا ترتب البطلان وإنما تؤدي إلى إثارة الشك حول الدليل⁽³⁾، ويترتب عدم تحريز الأدلة إهمال الدليل غير المحرز⁽⁴⁾.

كما أسلفنا، أن الأدلة الإلكترونية تحتاج إلى طرق فنية لحفظها نظر لطبيعتها وخصوصيتها الحساسة، وهي بحاجة إلى لطف بالتعامل لا تحتمل أي خشونة، وكذلك تحتاج إلى أشخاص متخصصين ومؤهلين لحفظها، وكذلك تحتاج أماكن مخصصة لحفظها⁽⁵⁾، ويجب إبعادها عن درجات الحرارة العالية والرطوبة ومعاملة لينة بعيدة عن العنف ووضعها في صناديق معدنية مغلقة⁽⁶⁾، ويجب أن لا يكون تحريز الدليل الإلكتروني سبب في تغيير طبيعته، وأن أي تعامل معه يجب أن يكون مؤثقا⁽⁷⁾.

الأدلة الإلكترونية المضبوطة في دولة فلسطين، تحفظ في قسم الأدلة الرقمية التابع لوحدة مكافحة

(1) السعيد كامل، شرح قانون أصول المحاكمات الجزائية، مرجع سابق، ص 471.

(2) الجوخدار، حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، مرجع سابق، ص 194.

(3) طنطاوي، إبراهيم حامد، الدفع ببطلان إذن النيابة العامة بالتفتيش، مرجع سابق، ص 92 وما بعدها.

(4) عوض، محمد محيي الدين، حقوق الإنسان في الإجراءات الجنائية، مرجع سابق، ص 264.

(5) بن يونس، عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 872.

(6) هروال، نبيلة هبة، الجوانب الإجرائية لجرائم الإنترنت، مرجع سابق، ص 273+274.

(7) جابر، محمود محمد محمود، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة، مرجع سابق، ص 204.

الجرائم الإلكترونية في جهاز الشرطة، كون هذا القسم يحتوي على مختبر الأدلة الرقمية، ومخزن الأدلة الرقمية، وهذا المخزن مجهز لحفظ الأدلة الإلكترونية على الحالة التي ضبطت فيها، ولضمان منع العبث فيها أو إتلافها⁽¹⁾، وقد رتب المشرع الفلسطيني في صلب المادة(47) من قانون الجرائم الإلكترونية عقوبات جزائية على كل من يقوم بالعبث بالأدلة القضائية الإلكترونية.

يرى الباحث انه بالنظر إلى خصوصية الأدلة الإلكترونية فان مخازن النيابة التي تحفظ بها الأدلة المضبوطة غير مهيأة لحفظ الأدلة الإلكترونية بها، وبالتالي فان المكان الأنسب لحفظها هو مخزن الأدلة الرقمية في وحدة مكافحة الجرائم الإلكترونية في جهاز الشرطة.

ثالثاً: التصرف بالأدلة الإلكترونية المضبوطة.

المشرع الفلسطيني، نظم آلية التصرف بالأدلة الإلكترونية المضبوطة، والمحفوظة تحت تصرف سلطة التحقيق إلى حين صدور قرار بالدعوى.

قانون الإجراءات الجزائية الفلسطيني، حدد آلية وطرق التصرف بالمضبوطات في الفصل الثالث من الباب الثالث، حيث ورد بالمادة(2/72) على إمكانية بيع المضبوطات إذا كانت من الأشياء القابلة للتلف بمرور الزمن، وكذلك سمح بالمادة(73) للنيابة أو المحكمة برد المضبوطات إذا لم تكن لازمة لسير الدعوى، ولم تكن محلاً للمصادرة الوجوبية، ولو قبل النطق بالحكم.

المشرع الأردني أجاز في نص المادة(90) من قانون أصول المحاكمات الجزائية مصادرة المضبوطات لصالح الدولة في حال لم يطلبها أصحابها في ميعاد ثلاثة سنوات من تاريخ إنتهاء الدعوى المتعلقة بغير حاجة إلى حكم يصدر بذلك.

المشرع الفلسطيني في قانون الجرائم الإلكترونية لم ينص على الخيارات التي أوردها في قانون الإجراءات الجزائية، ولكن أمر في نص المادة(2/50)، على وجوب مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجرائم الإلكترونية، مع عدم الإخلال بحقوق حسن النية، وهذا النص مشابه للنص السعودي⁽²⁾.

(1) مقابلة مع رئيس وحدة مكافحة الجرائم الإلكترونية في جهاز الشرطة، مصدر سابق.

(2) أنظر المادة(13) من قانون مكافحة جرائم المعلوماتية السعودي.

الأصل، أن يتم الاحتفاظ بالأشياء المضبوطة كلما كان ذلك لازماً لإظهار الحقيقة، وعملية التحقيق، وإطلاع المحكمة، ولكن إذا لم يقتض ذلك يجوز ردها⁽¹⁾، تماشياً مع القاعدة العامة التي تبيح رد الأشياء التي ضبطت أثناء التحقيق ولو قبل الحكم، ويستثنى من ذلك الأشياء المضبوطة التي تكون لازمة للسير بالدعوى، والأشياء التي تكون محلاً للمصادرة⁽²⁾.

يرى الباحث إن الخيارات التي منحها المشرع الفلسطيني في قانون الإجراءات الجزائية للتصرف بالمضبوطات لم ينص عليها قانون الجرائم الإلكترونية، وجعل مصادرتها أمر وجوبي إذا استخدمت في ارتكاب جريمة إلكترونية، وهذه إشارة واضحة من المشرع الفلسطيني على أن التصرف بالأدلة الإلكترونية لا تنطبق عليها القواعد العامة، ونرى أن حيازة وسائل تكنولوجيا المعلومات لا يعد جريمة، ويمكن لأي شخص حيازتها، وكان أولى بالمشرع وضع خيارات للنيابة أو المحكمة للتصرف بالمضبوطات إما بردها أو مصادرتها، وتقتصر المصادرة على الأجهزة الإلكترونية الخطيرة إن وجدت والتي تكون مصخرة لإرتكاب جرائم إلكترونية.

المطلب الثاني

أثار التفتيش غير القانوني في الجرائم الإلكترونية.

ينتج عن التفتيش القانوني أثار قانونية، ولكن التفتيش الغير قانوني الذي يجري بدون مراعاة الضمانات الدستورية والقانونية فان إجراءاته باطلة، وتبطل جميع أثاره.

نصت المادة (17) من القانون الأساسي الفلسطيني بالفقرة الأولى على ما يلي " للمساكن حرمة فلا تجوز مراقبتها أو دخولها أو تفتيشها إلا بأمر قضائي مسبب وفقاً لأحكام القانون"، ونصت الفقرة الثانية من ذات المادة على ما يلي " يقع باطلاً كل ما يترتب على مخالفة أحكام هذه المادة، ولمن تضرر من جراء ذلك الحق في تعويض عادل تضمنه السلطة الوطنية الفلسطينية"، وكذلك نص قانون الإجراءات الجزائية الفلسطيني على البطلان في الباب الرابع، وأنزل البطلان على أي إجراء مخالفة لنص القانون، ولكن المشرع الفلسطيني لم ينص على البطلان في حال مخالفة

(1) الجوخدار، حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، مرجع سابق، ص 195.

(2) مصطفى، محمود محمود، الإثبات في المواد الجنائية في القانون المقارن، مرجع سابق، ص 97.

إجراءات التفتيش في قانون الجرائم الإلكترونية، حيث أن البطلان هو النتيجة الحتمية لعدم مراعاة أي نص من تلك النصوص القانونية. لذلك سنبحث في البطلان بالفرع الأول، والجزاءات التي يتعرض لها المخالف بالفرع الثاني.

الفرع الأول: البطلان.

البطلان، هو عقوبة فرضها المشرع على الإجراءات المخالفة لنصوص القانون، ويبطل جميع آثار هذا الإجراء الباطل. حيث سنتناول تعريف البطلان في الفقرة الأولى، وتحديد البطلان الذي يلحق بمخالفة ضمانات التفتيش في الفقرات الثانية والثالثة والرابعة، وآثار البطلان في الفقرة الخامسة.

أولاً: تعريف البطلان.

البطلان، هو أحد صور الجزاءات التي تلحق بالإجراء المعيب، متى افتقر العمل إلى أحد مقوماته الموضوعية، أو تجريده من أحد شروطه الشكلية، وبطلان البطلان آثاره القانونية⁽¹⁾.

كما أسلفنا، القانون الأساسي الفلسطيني نص بالمادة (2/17) على بطلان كل إجراء يخالف النصوص المخصصة لتفتيش المنازل، وقد نصت المادة (474) من قانون الإجراءات الجزائية الفلسطيني، على أنه " يعتبر الإجراء باطلاً إذا نص القانون صراحة على بطلانه أو إذا شابته عيب أدى إلى عدم تحقيق الغاية منه "، وقد ذكر المشرع في النصوص اللاحقة نوعين من البطلان، الأول هو البطلان المتعلق بالنظام العام، والذي نصت عليه المادة (475) من قانون الإجراءات الجزائية الفلسطيني، وذكر المشرع مثال على هذا البطلان، وهو عدم مراعاة أحكام القانون المتعلقة بتشكيل المحاكم أو بولايتها، أو باختصاصها، وأية أحكام متعلقة بالنظام العام، وهذا البطلان يجوز إثارته في أي مرحلة من مراحل الدعوى وتقضي به المحكمة من تلقاء نفسها، وهذا النص مشابه لما جاء به المشرع المصري في نص المادة (331) من قانون الإجراءات الجنائية. والثاني هو البطلان المتعلق بمصلحة الخصوم، والذي نصت عليه المادة (476) من قانون الإجراءات الجزائية الفلسطيني، وهذا البطلان لا يجوز إثارته إلا ممن شرع لمصلحته، ما لم يكن قد تسبب فيه أو تنازل عنه صراحة أو ضمناً.

(1) عبد المنعم، سليمان، بطلان الإجراءات الجنائية، محاولة تأصيل أسباب البطلان في ظل قضاء النقض في مصر ولبنان وفرنسا، دار الجامعة الجديدة، الإسكندرية، 2008، ص 17.

المشرع الفلسطيني، نص صراحة على البطلان في حال مخالفة قواعد تفتيش المنازل، في متن المادة (52) من قانون الإجراءات الجزائية، والتي جاء فيها انه "يترتب البطلان على عدم مراعاة أي حكم من أحكام الفصل الرابع من الباب الثاني، وهذا الفصل نظم إجراءات تفتيش المنازل وحدوده المواد (39 إلى 50)، ولكن المشرع لم يحدد طبيعة هذا البطلان سواء ما أورده في القانون الأساسي أو قانون الإجراءات الجزائية، والتساؤل الذي يطرح، هل قواعد التفتيش تعتبر من النظام العام على معنى المواد (2/17) من القانون الأساسي الفلسطيني، والمادة (475) من قانون الإجراءات الجزائية الفلسطيني؟، أم هي قواعد خاصة وجدت لمصلحة الخصوم على معنى المادة (476) من قانون الإجراءات الجزائية الفلسطيني؟.

ثانياً: مخالفة ضمانات التفتيش يترتب البطلان المطلق.

المشرع الفلسطيني ذكر بالمادة (475) من قانون الإجراءات الجزائية على أنه يترتب البطلان على عدم مراعاة أحكام القانون المتعلقة بتشكيل المحاكم وإختصاصها وولايتها، أو مما هو متعلق بالنظام العام، ولم يذكر المشرع الفلسطيني قواعد التفتيش بشكل صريح على أنها متعلقة بالنظام العام، ولكي نتمكن من معرفة فيما إذا كانت قواعد التفتيش من النظام العام يجب أولاً تحديد مفهوم مصطلح النظام العام الذي ذكره المشرع.

مصطلح النظام العام، مصطلح غامض يستمد عظمته من ذلك الغموض الذي يحيط به، فمن مظاهر سموه انه ظل متعالياً على كل الجهود التي بذلها الفقهاء لتعريفه⁽¹⁾.

إن القواعد الموضوعية والشكلية للتفتيش من القواعد الجوهرية، وهي متعلقة بالنظام العام بلا شبهة، ويترتب على مخالفتها بطلان مطلق، وينسحب البطلان على الدليل المستمد منها⁽²⁾، ويجوز الإحتجاج به في أي مرحلة من مراحل الدعوى، ولكن لا يجوز الإحتجاج به أمام محكمة النقض، كون أن الدفع ببطلان التفتيش يختلط فيه الواقع بالقانون ويقتضي تحقيقاً موضوعياً لا تختص به محكمة النقض⁽³⁾.

(1) عرفة، محمد علي، مبادئ العلوم القانونية، ط2، 1951، ص 98، مشار إليه في كتاب أحمد، هلاي عبد اللاه، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي، مرجع سابق، ص 227.

(2) مصطفى، محمود محمود، الإثبات في المواد الجنائية في القانون المقارن، مرجع سابق، ص 106+108.

(3) نقض جنائي مصري، بتاريخ 1983/10/2، مجموعة أحكام محكمة النقض، س 34، رقم 167، ص 841.

ثالثاً: مخالفة ضمانات التفتيش يرتب البطلان النسبي.

البطلان النسبي، هو كل بطلان ينشأ عن مخالفة قاعدة غير متعلقة بالنظام العام وإن كانت جوهرية في إظهار الحقيقة⁽¹⁾.

المشرع الفلسطيني ذكر بالمادة(476) من قانون الإجراءات الجزائية، على أنه فيما عدا حالات البطلان المتعلقة بالنظام العام لا يجوز الدفع بالبطلان إلا ممن شرع لمصلحته ما لم يكن قد تنازل عنه صراحة أو ضمناً، وذكر المشرع بالمادة(478) من ذات القانون حالات التنازل عن البطلان وهو القيام بالإجراء بوجود محامي للمتهم دون إعتراض منه.

إن مخالفة قواعد التفتيش الموضوعية والشكلية يرتب بطلان يتعلق بمصلحة جوهرية للخصوم، ولا يتعلق بالنظام العام⁽²⁾، ويترتب عليه بطلان نسبي، ولا يجوز الدفع به إلا من صاحب الشأن، ويجب الدفع به بمرحلة جمع الاستدلالات أو التحقيق الابتدائي أو بالتحقيق بالجلسة على معنى المادة(478) من قانون الإجراءات الجزائية الفلسطيني، والرضا بالتفتيش يسقط هذا البطلان، كون أنه يجوز التنازل عنه صراحة أو ضمناً⁽³⁾، كون قواعد التفتيش لا تتعلق بالنظام العام⁽⁴⁾، وإن قول محكمة النقض بأن الدفع ببطلان التفتيش لا يجوز أن يبدي لأول مرة في النقض يشير بحد ذاته إلى أن هذا البطلان نسبي وليس مطلقاً⁽⁵⁾.

رابعاً: ضوابط التفرقة بين البطلان المطلق والنسبي.

إن الضابط في التفرقة بين البطلان المطلق والبطلان النسبي، هو نوع المصلحة التي تحميها القاعدة الإجرائية، فإذا كانت المصلحة التي يحميها القانون عامة يترتب على مخالفتها بطلان مطلق، وإذا كانت قاعدة مقررّة لمصلحة الخصوم يترتب على مخالفتها بطلان نسبي⁽⁶⁾، وبالنتيجة

(1) الشواربي، عبد الحميد، إذن التفتيش، مرجع سابق، ص 146.

(2) سلامة، مأمون محمد، الإجراءات الجنائية في التشريع المصري، ج2، دار الفكر العربي، القاهرة، 1988، ص 623.

(3) السعيد كامل، شرح قانون أصول المحاكمات الجزائية، مرجع سابق، ص 461 وما بعدها.

(4) عبد الستار، فوزية، شرح قانون الإجراءات الجنائية وفقاً لأحدث التعديلات، مرجع سابق، ص 308+358.

(5) عبيد، رؤوف، المشكلات العلمية الهامة في الإجراءات الجنائية، ج 1، مكتبة الوفاء القانونية، الإسكندرية، 2015، ص

196.

(6) الجوخدار، حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، مرجع سابق، ص 183.

فإن مخالفة الشروط الموضوعية للتفتيش، يتصل بالنظام العام، مما يترتب البطلان المطلق⁽¹⁾، أما مخالفة الشروط الشكلية للتفتيش، فهو متعلق بمصلحة الخصوم، مما يترتب البطلان النسبي⁽²⁾.

الباحث يرى أن ضمانات تفتيش المنازل سواء كانت شكلية أم موضوعية هي قواعد جوهرية متصلة بالنظام العام، لا يجوز مخالفتها، ويترتب على مخالفتها البطلان المطلق، وذلك بالاستناد إلى نص بالمادة (2/17) من القانون الأساسي الفلسطيني، والمواد (475+474+52) من قانون الإجراءات الجزائية الفلسطيني، كون أن تلك المواد أنزلت حكم البطلان بشكل صريح على مخالفة النصوص المتعلقة بتفتيش المنازل، وهي تحمي المصلحة العامة ومصلحة الخصوم معاً، أمام قواعد تفتيش الأشخاص نرى أنها متعلقة بمصلحة جوهرية للخصوم وغير متعلقة بالنظام العام، كون القانون الأساسي وقانون الإجراءات الجزائية الفلسطيني لم ينص على بطلان تفتيش الأشخاص في حال مخالفة قواعده كما فعل في تفتيش المنازل.

خامساً : آثار بطلان التفتيش.

إن بطلان إجراءات التفتيش لمخالفتها ضمانات التفتيش، سواء كان البطلان مطلق متعلق بالنظام العام، أو متعلق بمصلحة الخصوم، وتم الدفع ببطلانه فإن ما ينتج عن هذا التفتيش يكون باطل.

نصت المادة(477) من قانون الإجراءات الجزائية الفلسطيني، على انه" لا يترتب على بطلان الإجراء بطلان الإجراءات السابقة عليه، أو بطلان الإجراءات اللاحقة له إذا لم تكن مبنية عليه، وإذا كان الإجراء باطلاً في جزء منه فإن هذا الجزء وحده هو الذي يبطل".

بطلان التفتيش، يؤدي إلى بطلان الدليل المستمد منه، وبطلان أهم آثاره وهو ضبط الأشياء التي أسفرت عن التفتيش⁽³⁾، ويجب على المحكمة أن تستبعد الدليل المستمد منه، ولا يؤثر هذا البطلان على الإجراءات السابقة واللاحقة عليه على معنى المادة(477) من قانون الإجراءات الجزائية.

إن التفتيش الباطل، يترتب عليه إستبعاد الدليل المستمد منه، ولا تستطيع المحكمة الإعتماد على

(1) الحسيني، سامي حسني، النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، جامعة عين شمس، دار النهضة العربية، القاهرة، 1972، ص 416، مشار إليه في الجوخدار، التحقيق الإبتدائي في قانون أصول المحاكمات الجزائية حسن، ص 183.

(2) الشهاوي، قدرتي عبد الفتاح، مناط التفتيش، قيوده وضوابطه، مرجع سابق، ص 119.

(3) السعيد كامل، شرح قانون أصول المحاكمات الجزائية، مرجع سابق، ص 465.

شهادة الأشخاص الذين قاموا به، لأن معلوماتهم إستقيت من إجراء مخالف للقانون⁽¹⁾، ولا يؤثر البطلان على الأدلة المنفصلة عن الإجراء الباطل⁽²⁾، وإذا جرى التفتيش بحضور محامي المتهم وبدون اعتراض منه لا يحق الدفع ببطلان التفتيش⁽³⁾.

يرى الباحث أن كل الأدلة الإلكترونية التي يتم العثور عليها وضبطها تكون باطلة، كونها ناتجة عن إجراءات تفتيش لم تراعى الضمانات الأساسية والقانونية، ولا يجوز الإعتماد عليها ويجب إستبعادها من الأدلة.

الفرع الثاني: العقوبات الجزائية والتأديبية.

إن مخالفة ضمانات التفتيش يترتب بطلان إجراءاته، وإستبعاد الأدلة الناتجة عنه، وكذلك رتب المشرع عقوبات جزائية وتأديبية بحق مأموري الضبط القضائي الذين يخالفون قواعد القانون.

إن عدم مراعاة قواعد التفتيش يترتب عليه البطلان كجزاء إجرائي، ويترتب عليه كذلك عقاب جزائي وتعويض مدني⁽⁴⁾، وهذا الجزاء الذي فرضه المشرع على مأموري الضبط القضائي حتى يكون رادع مسلط عليهم، في حال قيامهم بتفتيش الأماكن الخاصة للناس والإعتداء على خصوصيتهم والإطلاع على أسرارهم بدون إذن من القانون. لذلك سنتناول العقوبات الجزائية بالفقرة الأولى، والعقوبات التأديبية بالفقرة الثانية.

أولاً: العقوبات الجزائية.

إن فرض عقوبات جزائية على مأموري الضبط القضائي، هدفه منعهم من مخالفة نصوص القانون، وإلا إعتبروا أنفسهم فوق القانون، بقيامهم بالإعتداء على حريات الناس الأساسية التي كفلها القانون الأساسي والقوانين والمواثيق والإتفاقيات الدولية، بالإطلاع على أسرار الناس بدون وجه حق، مستغلين وظائفهم ومناصبهم.

نصت المادة (1/27) من قانون الجرائم الإلكترونية الفلسطيني، على أنه " كل موظف إرتكب أيا

(1) المرصفاوي، حسن صادق، المرصفاوي في أصول الإجراءات الجنائية، مرجع سابق، ص 467.

(2) الشواربي، عبد الحميد، إذن التفتيش، مرجع سابق، ص 151.

(3) ثروت جلال، نظم الإجراءات الجنائية، مرجع سابق، ص 479.

(4) عوض، محمد محيي الدين، حقوق الإنسان في الإجراءات الجنائية، مرجع سابق، ص 264.

من الجرائم المنصوص عليها في هذا القانون، مستغلاً صلاحياته وسلطاته أثناء تأديته عمله أو بسببها أو سهل ذلك لغيره يعاقب بالحبس لمدة سنة..."، وبالرجوع إلى تعريف الموظف الوارد بالمادة الأولى من قانون الجرائم الإلكترونية الفلسطيني، نجد أن الموظف المقصود هو كل من يعمل بالقطاع العام، وأن مأموري الضبط القضائي هم موظفين عموميين، وقد شدد المشرع الفلسطيني في ذات المادة (1/27) العقوبة على الموظف بمقدار الثلث.

وكذلك أكدت المادة (25) من قانون الشرطة الفلسطيني، على أن المسؤول المباشر يتحمل المسؤوليات القانونية عن أي أمر مخالف للقانون، فيما أمر أو أشار بتنفيذه، ونصت المادة (42) من ذات القانون، على أن مجالس التأديب تقوم بإحالة القضايا الجزائية إلى المدير العام للشرطة ليقوم بدوره بإحالتها إلى النيابة العامة لإتخاذ المقتضى القانوني وفق أحكام قانون الإجراءات النافذ، وقد نصت المادة (53) من ذات القانون، على أن عناصر الشرطة تخضع للمساءلة الجزائية أمام القضاء في حال ارتكاب أي منهم لجريمة معاقب عليها وفقاً للقوانين النافذة، سواء أمام القضاء النظامي أو القضاء العسكري وفقاً لإختصاصاتهما.

يرى الباحث أن المشرع الفلسطيني كان موفقاً في تشديد العقوبة على مأموري الضبط القضائي الذين يرتكبون أي من الجرائم الإلكترونية، كونهم مكلفين بحكم القانون بتنفيذ أحكامه، ومؤتمنين على أسرار الناس وأعراضهم، وأن وسائل تكنولوجيا المعلومات تحتوي على أسرار الناس وخصوصياتهم، ولا يجوز لمأمور الضبط القضائي الإطلاع على تلك الأسرار مستغلاً وظيفته وما وفرت له الدولة من وسائل تكنولوجيا حديثة لخدمة القانون بالإطلاع على ما تحتويه تلك الوسائل الإلكترونية الخاصة بالناس إلا بعد الحصول على إذن القانون.

ثانياً: العقوبات التأديبية.

أقر المشرع الفلسطيني، إضافة إلى العقوبات الجزائية التي فرضها على مأموري الضبط القضائي عقوبات تأديبية، يوقعها عليهم رؤوسهم في حال مخالفتهم لواجباتهم ومخالفتهم لنصوص القانون.

نصت المادة (20) من قانون الإجراءات الجزائية الفلسطيني، على أن النائب العام يشرف على مأموري الضبط القضائي ومراقبتهم فيما يتعلق بأعمال وظيفتهم، ومنحت للنائب العام أن يطلب من الجهات المختصة إتخاذ الإجراءات التأديبية بحق كل من يقع منه مخالفة لواجباته أو تقصيره في

عمله. وهذه نصت بوضوح على وجود عقوبات تأديبية تقع على مأمور الضبط القضائي، وهذا ما أكد عليه قانون الشرطة الفلسطيني، في متن المادة(6) على أن عناصر الشرطة يباشرون أعمالهم تحت إشراف النائب العام، وأمر القانون في المواد (27+38) على تشكيل مجالس تأديبية لعناصر الشرطة، ونظم في المادة(24) آلية معاقبة المخالفين تأديبياً كل حسب رتبته العسكرية، في حال مخالفة واجباتهم المنصوص عليها بالقوانين النافذة، دون الإخلال بالدعوى الجزائية والمدنية.

وكذلك يوجد عقوبات تأديبية تفرض على مأموري الضبط القضائي، نظماً قانون العقوبات العسكري الفلسطيني النافذ، حيث نصت المادة(189) على عقوبات تأديبية تفرض على الضباط وضباط صف قوى الأمن، ومنها التنبيه والإنذار، تأخير الأقدمية، وتنزيل الرتبة، والحجز بالوحدة العسكرية، والحرمان من الإجازات الأسبوعية، والحبس لمدة لا تتجاوز ثلاثة أشهر.

وكذلك نص قانون الخدمة في قوى الأمن الفلسطينية، على عقوبات تأديبية أخرى في صلب المادة(96)، وهذه العقوبات التأديبية توقع على الضباط في حال مخالفتهم أحكام القانون، ومن تلك العقوبات التأديبية الإحالة على الاستيداع، والترك بالرتبة، والحرمان من العلاوة الدورية وعلاوة القيادة، ونظمت المادة(174) العقوبات التأديبية التي توقع على صف الضباط والأفراد.

الخاتمة.

في العصر الحديث، أصبحت أسرار الناس وخصوصيتهم تحفظ في مخزن إلكتروني، وهذا المخزن الإلكتروني متمثل في وسائل تكنولوجيا المعلومات التي أصبح الإنسان يستخدمها في حياته اليومية، وقد نظم القانون طرق الوصول إليها وتفتيشها، وأحاطها بمجموعة من الضمانات لحماية أسرار الناس وخصوصيتهم من العبث.

التقنية الحديثة ظهرت لخدمة الإنسان، إلا أن البعض أساء استخدامها بالاعتداء على المجتمع والدولة، ومع إزدياد استخدام وسائل تكنولوجيا المعلومات ظهرت جرائم جديد هي الجرائم الإلكترونية، وهذه الجرائم عابرة للقارات، لا تعترف بالحدود الجغرافية للدول، وترتكب عن بعد، لا تحتاج إلى مجهود لإرتكابها، ونتائجها تظهر في مكان آخر أو عدة أماكن سواء داخل حدود الدولة أو خارجها أو في عدة دول، وتصيب كل مناحي الحياة داخل الدولة، فتتطال الأشخاص والأموال، وتهدد أمن الدولة واقتصادها.

التفتيش في الجرائم الإلكترونية يحتاج إلى نظام إجرائي خاص، وسلطة مختصة به، تكون مدربة ومؤهلة فنيا، كون عملية استخراج الأدلة الإلكترونية عمل شاق وطريق مليء بالصعوبات والتحديات ويحتاج جهد كبير.

لقد تناول الباحث في هذه الدراسة، التفتيش في الجرائم الإلكترونية، وقام ببحث خصوصية التفتيش في الجرائم الإلكترونية بالفصل الأول، وبالفصل الثاني خصوصية إجراءات التفتيش والضبط في الجرائم الإلكترونية.

وقد عالَجَ الباحث إشكالية الدراسة وهي، هل وفق المشرع الفلسطيني في وضع نظام متكامل يراعي خصوصية التفتيش في الجرائم الإلكترونية، وإقامة توازن بين حق الإنسان في الخصوصية وحق المجتمع في العقاب من المجرمين؟،

وقد توصل الباحث إلى العديد من النتائج، وعلى ضوء تلك النتائج إقترح عدة توصيات وهي على النحو التالي:

أولاً: النتائج.

1-التفتيش في الجرائم الإلكترونية من أدق وأخطر إجراءات التحقيق، كونه يمس خصوصية الناس بالإطلاع على أسرارهم المخزنة في وسائل تكنولوجيا المعلومات.

2-الجرائم الإلكترونية جرائم مستترة، يصعب معرفة فاعلها، ترتكب من أي مكان في هذا العالم، وتتحقق أثارها في مكان آخر، والتفتيش بتلك الجرائم بحاجة إلى نظام إجرائي خاص يراعي خصوصيتها، وبحاجة إلى أشخاص مؤهلين ومدربين تدريباً قانونياً وفنياً، للتعامل مع وسائل تكنولوجيا المعلومات والتغلب على التحديات الفنية التي تمتاز بها.

3-التفتيش في الجرائم الإلكترونية من إختصاص السلطة الأصلية المتمثلة في نيابة مكافحة الجرائم الإلكترونية بالدرجة الأولى، والسلطة المناوبة المتمثلة في وحدات مكافحة الجرائم الإلكترونية في قوى الأمن المتخصصة فقط.

4-محل التفتيش في الجرائم الإلكترونية، هو وسائل تكنولوجيا المعلومات سواء كانت بحوزة أشخاص أو داخل الأماكن، وهذه الوسائل يمكن حمايتها بأرقام سرية لمنع الوصول إليها ويصعب إختراقها، وتحتاج إلى أجهزة ومعدات تقنية لإستخراج الأدلة، وهذا إجراء شاق وصعب ومجهول النتيجة.

5-التفتيش في الجرائم الإلكترونية بحاجة إلى فريق فني للقيام به، وهذا الفريق يضم جميع التخصصات على وسائل تكنولوجيا المعلومات، يرافقه فريق أمني للاقتحام للسيطرة والقبض على وسائل تكنولوجيا المعلومات المستخدمة في ارتكاب الجريمة الإلكترونية بالسرعة المطلوبة.

6-التفتيش في الجرائم الإلكترونية يكون داخل حدود الدولة أو يمتد إلى خارجها.

7-التفتيش في الجرائم الإلكترونية بحاجة إلى تعاون ومساعدة بين الدول، كون أنه لا تستطيع دولة واحدة بمفردها مكافحة تلك الجرائم لوحدها.

8-الأدلة الإلكترونية تتكون من أدلة مادية وغير مادية، وهي أدلة حساسة بحاجة إلى معاملة لينة وإجراءات خاصة لضبطها، وكذلك تحتاج إلى أماكن مخصصة لحفظها على الحالة التي ضبط عليها.

9- قانون الجرائم الإلكترونية الفلسطيني، نص على بعض ضمانات التفتيش، ولم ينص على الضمانات الأخرى التي اقراها قانون الإجراءات الجزائية للتفتيش في الجرائم العادية، منها حضور المتهم وغيره إجراء التفتيش، ووقت للتفتيش، وضمان تفتيش الأنثى، ولم يأمر بتنظيم محضر التفتيش، ولم يحيل الأمر إلى قانون الإجراءات الجزائية النافذ.

ثانياً: التوصيات.

1-النص بوضوح على أن التفتيش في الجرائم الإلكترونية يخضع لنفس الضمانات الواردة في القانون الأساسي وقانون الإجراءات الجزائية النافذ، أو إدراج نصوص شاملة في القرار بقانون بشأن الجرائم الإلكترونية تقرر جميع ضمانات التفتيش.

2-النص بوضوح على أن تكون مذكرة التفتيش مكتوبة، وتحتوي على جميع بياناتها الإلزامية، والتحديد بوضوح الوسيلة الإلكترونية المراد تفتيش، وأي جزء من هذه الوسيلة المراد تفتيشه.

3-النص بوضوح على قابلية المكونات الغير مادية لوسائل تكنولوجيا المعلومات للتفتيش والضبط، وبيان طرق ضبطها.

4-النص بوضوح على ضرورة حضور المتهم أو شهود أثناء إجراء التفتيش على وسائل تكنولوجيا المعلومات.

5-النص بوضوح على ضرورة تنظيم محضر بإجراءات التفتيش، لتدوين جميع الإجراءات التي تمت على وسائل تكنولوجيا المعلومات، وطرق إجرائها، والوسائل المستخدمة، وتاريخها وساعتها، والتدوين في المحضر جميع الملاحظات التي يبديها المتهم أو الشهود.

6-النص بوضوح على أن السيارة الخاصة تخضع لضمانات تفتيش الأشخاص إذا كانت بحوزة صاحبها أو حائزها، وتخضع لضمانات تفتيش المنازل إذا كانت داخل المساكن.

7-النص بوضوح على أن تقوم أنثى بتفتيش وسائل تكنولوجيا المعلومات الخاصة بالأنثى.

8-النص بوضوح على مكان حفظ الأدلة الإلكترونية المضبوطة، لضمان الحفاظ عليها على الحالة التي ضبطت بها، ولضمان عدم العبث بها أو تغيير محتواها.

9-النص بوضوح على طرق التصرف بالمضبوبات الإلكترونية، ومنح السلطة القضائية خيارات التصرف بها إما بردها إلى أصحابها أو مصادرتها بقرار مسبب، سواء تم تحريك دعوى الحق العام أم تم حفظ أوراق الدعوى لدى النيابة العامة.

10-النص بوضوح على تجريم الأعمال التي تمس الاقتصاد الوطني بواسطة تكنولوجيا المعلومات.

11-إنشاء نيابة متخصصة للجرائم الإلكترونية بنص القانون.

12-إنشاء محكمة متخصصة للنظر في الجرائم الإلكترونية بنص القانون.

13-النص بوضوح على أن الدليل الإلكتروني يعود تقدير قيمته للمحكمة، ليكون بإمكان المحكمة التيقن من سلامته.

14-النص بوضوح على الجهة المختصة بالتعاون الدولي وطلب المساعدة القضائية في التفتيش بالجرائم الإلكترونية، والجهة المختصة بالتعامل مع الشرطة الدولية.

15-السماح للسلطات المختصة بالتفتيش في الجرائم الإلكترونية بتجاوز حدود الدولة في الحالات والشروط الواردة بالمادة (40) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

16-إصدار مرشد للتفتيش والضبط في الجرائم الإلكترونية، يكون دليل للقائم بالتفتيش.

17-إنشاء مجلس وطني لمكافحة الجرائم الإلكترونية، يضم بين أعضائه ممثل عن نيابة مكافحة الجرائم الإلكترونية، وممثل عن وحدات مكافحة الجرائم الإلكترونية في قوى الأمن، وممثل عن وزارة الإتصالات وتكنولوجيا المعلومات، وخبراء وأكاديميين فنيين في البيئة الرقمية، وخبراء في القانون الإلكتروني المحلي والدولي، ويكون لهذه المجلس صلاحية وضع معايير السياسة الجنائية في الميدان الإلكتروني، ودراسة القوانين المتعلقة به، وتقييمها، وإقتراح التعديلات اللازمة عليها، ودراسة الإتفاقيات الثنائية والإقليمية والدولية الخاصة بالجرائم الإلكترونية قبل المصادقة عليها من الجهة المختصة.

تم بحمد الله

المصادر والمراجع.

أولاً : المصادر.

- 1- القرآن الكريم.
 - 2- لسان العرب للإمام العلامة أبي الفضل جمال الدين محمد بن مكرم ابن منظور الإفريقي المصري، دار صادر، بيروت، بدون سنة نشر.
 - 3- التشريعات الفلسطينية.
- قانون العقوبات الأردني النافذ في المحافظات الشمالية (الضفة الغربية)، رقم(16) لسنة 1960.
 - قانون أصول المحاكمات الجزائية الثوري الصادر عن المجلس الوطني الفلسطيني لمنظمة التحرير الفلسطينية، بالقرار التشريعي رقم(5) لسنة 1979، بيروت.
 - قانون الإتصالات السلكية واللاسلكية رقم (3) لسنة 1996.
 - قانون تنظيم مهنة المحاماه رقم(3) لسنة 1999.
 - قانون الإجراءات الجزائية رقم(3) لسنة 2001.
 - قانون السلطة القضائية رقم(1) لسنة 2002.
 - القانون الأساسي الصادر بتاريخ 2002/5/29، والمعدل بتاريخ 2003/3/18.
 - قانون الخدمة في قوى الأمن رقم(8) لسنة 2005.
 - قانون المخابرات العامة رقم(17) لسنة 2005.
 - قرار بقانون بشأن الأمن الوقائي رقم(11) لسنة 2007.
 - قرار بقانون بشأن الاستخبارات العسكرية رقم(34) لسنة 2014.
 - قرار بقانون بشأن غسل الأموال وتمويل الإرهاب رقم(20) لسنة 2015.
 - قرار بقانون بشأن الضابطة الجمركية رقم(2) لسنة 2016.
 - قرار بقانون بشأن الشرطة رقم(23) لسنة 2017.
 - قرار بقانون بشأن الهيئة القضائية لقوى الأمن رقم (2) لسنة 2018.
 - قرار بقانون بشأن الجرائم الإلكترونية رقم (10) لسنة 2018.

4- التشريعات العربية.

- قانون الإجراءات الجنائية المصري رقم(150)، لسنة 1950.
- قانون أصول المحاكمات الجزائية الأردني رقم(9)، لسنة 1961.
- قانون الإجراءات الجزائية الجزائري الصادر بالأمر رقم(155/66)، لسنة 1966.
- مجلة الإجراءات الجزائية التونسية القانون رقم(23) لسنة 1968.
- المسطرة الجنائية المغربية القانون رقم (22/1) لسنة 2002.
- قانون الجرائم الاقتصادية الأردني رقم(11) لسنة 1993، والمعدل بالقانون رقم(20) لسنة 2004.
- قانون نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم (م/17)، لسنة 2007.
- قانون جرائم المعلوماتية السوداني رقم (13) لسنة 2007.
- قانون مكافحة جرائم تقنية المعلومات العماني الصادر بالمرسوم السلطاني، رقم(2011/12)، لسنة 2011.
- قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري الصادر بالمرسوم التشريعي، رقم 2012/17، بلسنة 2012.
- التعليمات التوضيحية والتنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري، الصادرة بالقرار رقم (290)، عن وزير الاتصالات والتقانة السوري.
- قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (5) لسنة 2012.
- قانون مكافحة الجرائم الإلكترونية القطري رقم(14) لسنة 2014.
- قانون جرائم تقنية المعلومات البحريني رقم (60) لسنة 2014.
- قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015.
- قانون مكافحة جرائم تقنية المعلومات الكويتي رقم(63) لسنة 2015.

5- التشريعات الأجنبية.

- قانون العقوبات الايطالي لسنة 1930 . Codice penale italiano, 1930.
- قانون إساءة استخدام الحاسوب الانجليزي . Computer Misuse Act 1990.
- قانون العقوبات الفرنسي لسنة 1992 . Code pénal français, 1992.

- قانون الإجراءات الجنائية الفرنسي. Code de procédure pénale.
- قانون الإجراءات الجنائية الألماني.

Strafprozeßordnung (StPO). Ausfertigungsdatum: 1950.

ثانياً : المراجع

- 1- المراجع القانونية العامة.
 - الدكتور إبراهيم حامد طنطاوي.
الدفع ببطلان إذن النيابة العامة بالتفتيش، دار النهضة العربية، القاهرة، 1997.
 - إبراهيم راسخ.
التحقيق الجنائي العلمي، الطبعة الأولى، أكاديمية شرطة دبي، الإمارات العربية المتحدة، 1991.
 - أحمد أبو الروس.
التحقيق الجنائي والتصرف فيه والأدلة الجنائية، المكتب الجامعي الحديث، الإسكندرية، 2008.
 - الدكتور أحمد فتحي سرور.
 - الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية، طبعة معدلة، دار النهضة العربية، القاهرة، 1995.
 - الوسيط في قانون الإجراءات الجنائية، الطبعة السابعة، دار النهضة العربية، القاهرة، 1996.
 - الدكتور جندي عبد الملك.
الموسوعة الجنائية، الطبعة الثانية، دار العلم للجميع، الجزء الثاني، والثالث، والرابع، بدون سنة نشر، بيروت، لبنان.
 - الدكتور جلال ثروت.
نظم الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، 1997.

- **الدكتور جمال جرجس مجلع تاوضروس.**
الشرعية الدستورية لأعمال الضبطية القضائية، النسر الذهبي للطباعة، مصر،
2006.
- **الدكتور حامد راشد.**
أحكام تفتيش المسكن في التشريعات الإجرائية العربية، دراسة مقارنة، الطبعة الأولى،
دار النهضة العربية، القاهرة، 1998.
- **الدكتور حسن الجوخدار.**
• شرح قانون أصول المحاكمات الجزائية، الطبعة الثانية، مكتبة دار الثقافة للنشر
والتوزيع، عمان، 1997.
• التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، دراسة مقارنة، دار الثقافة
للنشر والتوزيع، عمان، 2011.
- **الدكتور حسن صادق المرصفاوي.**
• المرصفاوي في القانون الجنائي، قانون الإجراءات الجنائية، تشريعا وقضاء في مائة
عام، الجزء الثالث، منشأة المعارف، بدون سنة نشر.
• المرصفاوي في أصول الإجراءات الجنائية، منشأة المعارف، الإسكندرية، 2000.
- **الدكتور حسن علام.**
قانون الإجراءات الجنائية، الجزء الأول، مطابع روز اليوسف، القاهرة، 1982.
- **الدكتور رؤوف عبيد.**
المشكلات العملية الهامة في الإجراءات الجنائية، الجزء الأول، مكتبة الوفاء القانونية،
الإسكندرية، 2015.
- **الدكتور رمزي رياض عوض.**
الإجراءات الجنائية في القانون الانجلوامريكي، دار النهضة العربية، القاهرة، 2009.
- **سردار علي عزيز.**
النطاق القانوني لإجراءات التحقيق الابتدائي، دراسة مقارنة، دار الكتب القانونية، ودار
شنتات للنشر والبرمجيات، مصر، 2011.

- **الدكتور سليمان عبد المنعم.**
بطلان الإجراء الجنائي، محاولة تأصيل أسباب البطلان في ظل قضاء النقض في مصر ولبنان وفرنسا، دار الجامعة الجديدة، الإسكندرية، 2008.
- **الدكتور عبد الحميد الشواربي.**
إذن التفتيش في ضوء القضاء والفقهاء، منشأة المعارف، الإسكندرية، 1995.
- **الدكتور علي عبد القادر القهوجي.**
 - الندب للتحقيق، دار الجامعة الجديدة للنشر، الإسكندرية، 1997.
 - القانون الدولي الجنائي، أهم الجرائم الدولية، المحاكم الدولية الجنائية، الطبعة الأولى، منشورات الحلبي الحقوقية، 2001.
- **الدكتورة فوزية عبد الستار.**
شرح قانون الإجراءات الجنائية، وفقا لأحدث التعديلات، الطبعة الثانية، الجزء الأول، دار النهضة العربية، القاهرة، 2010.
- **الدكتور قدري عبد الفتاح الشهاوي.**
مناط التفتيش، قيوده وضوابطه، الطبعة الأولى، دار النهضة العربية، القاهرة، 2006.
- **الدكتور كاظم السيد عطية.**
الحماية الجنائية لحق المتهم في الخصوصية، دراسة مقارنة بين القانون المصري والفرنسي والأمريكي والانجليزي، دار النهضة العربية، القاهرة، 2007.
- **الدكتور كامل السعيد.**
شرح قانون أصول المحاكمات الجزائية، دراسة تحليلية تأصيلية مقارنة، في القوانين الأردنية والمصرية والسورية وغيرها، دار الثقافة للنشر والتوزيع، عمان، 2005.
- **الدكتور كمال كمال الرخاوي.**
إذن التفتيش فقهاً وقضائياً، الطبعة الأولى، دار الفكر والقانون، المنصورة، 2000.
- **الدكتور مأمون محمد سلامة.**
الإجراءات الجنائية في التشريع المصري، الجزء الثاني، دار الفكر العربي، القاهرة، 1988.

- الدكتور محمد أبو العلا عقيدة.
شرح قانون الإجراءات الجنائية، دار النهضة العربية، الطبعة الثانية، دار النهضة العربية، القاهرة، 2001.
- الدكتور محمد محيي الدين عوض.
حقوق الإنسان في الإجراءات الجنائية، بدون ناشر، 1989.
- الدكتور محمود محمود مصطفى.
الإثبات في المواد الجنائية، الجزء الثاني، التفتيش والضبط، الطبعة الأولى، مطبعة جامعة القاهرة والكتاب الجامعي، 1978.
- الدكتور محمود نجيب حسني.
• شرح قانون الإجراءات الجنائية، الدعاوي الناشئة عن الجريمة، الاستدلال والتحقيق الابتدائي، الطبعة الثالثة، دار النهضة العربية و مطبعة جامعة القاهرة، القاهرة، 1995.
- شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي، الطبعة السابعة، دار النهضة العربية، القاهرة، 2012.
- القاضية منى جاسم الكواري.
التفتيش، شروطه وحالات بطلانه، دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2008.
- الدكتور نائل عبد الرحمن صالح.
الجرائم الاقتصادية في التشريع الأردني، الطبعة الأولى، الجزء الأول، دار الفكر للنشر والتوزيع، عمان، 1990.
- الدكتور ناينتي ناين احمد الدسوقي.
الرضا كتكأة في التفتيش الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2008.
- الدكتور نبيل عبد المنعم جاد.
أسس التحقيق الجنائي العلمي، بدون ناشر، 1991.

- الدكتور نبيه صالح.
شرح مبادئ قانون الإجراءات الجزائية الفلسطيني، دراسة مقارنة، الطبعة الثانية، الجزء الأول، مكتبة دار الفكر، القدس، 2006.
 - الدكتورة هدى حامد قشقوش.
الجريمة المنظمة، القواعد الموضوعية والإجرائية والتعاون الدولي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997.
 - الدكتور هشام مصطفى محمد إبراهيم.
التحقيق والمحاكمة، أمام المحكمة الجنائية الدولية الدائمة، دار المطبوعات الجامعية، الإسكندرية، 2015.
- 2- المراجع القانونية الخاصة.
- الدكتور احمد خليفة الملط.
الجرائم المعلوماتية، دراسة مقارنة، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.
 - القاضي أسامة أحمد المناعسة والقاضي جلال محمد الزعبي.
جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2014.
 - المحامي أمير فرج يوسف.
الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2008.
 - الدكتور جميل عبد الباقي الصغير.
الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002.
 - الدكتور حسن ظاهر داود.
جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000.

- **الدكتور حسين بن سعيد الغافري.**
السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009.
- **حنان ربحان مبارك المضحكي.**
الجرائم المعلوماتية، دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014.
- **المحامي خالد عياد الحلبي.**
إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011.
- **الدكتور خالد ممدوح إبراهيم.**
فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2010.
- **الدكتور سامي جلال فقي حسين.**
التفتيش في الجرائم المعلوماتية، دراسة مقارنة، دار الكتب القانونية و دار شتات للنشر والبرمجيات، مصر، 2011.
- **الدكتور سليمان بن مهجع العنزي.**
وسائل التحقيق في جرائم نظم المعلومات، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003.
- **الدكتور سعيد عبد اللطيف حسن.**
إثبات جرائم الكمبيوتر والجرائم الإلكترونية المرتكبة عبر شبكة الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.
- **الدكتور طارق إبراهيم الدسوقي عطية.**
الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

- **الدكتور طارق عفيفي صادق احمد.**
الجرائم الإلكترونية، جرائم الهاتف المحمول، دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015.
- **الدكتور عادل عزام سقف الحيط.**
جرائم الدم والقدح والتحقير، المرتكبة عبر الوسائط الإلكترونية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2015.
- **الدكتور عبد العال الديربي والأستاذ محمد صادق إسماعيل.**
الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة، مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.
- **الدكتور عبد الفتاح بيومي حجازي.**
- مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية و دار شتات للنشر والبرمجيات، مصر، 2007.
 - الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، الطبعة الأولى، بدون ناشر، 2009.
- **الدكتور علي جبار الحسيناوي.**
جرائم الحاسوب والإنترنت، الطبعة العربية، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009.
- **الدكتور علي حسن الطوالبة.**
- التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، عالم الكتب الحديث، اربد، الأردن، 2004.
 - الجرائم الإلكترونية، الطبعة الأولى، جامعة العلوم التطبيقية، مملكة البحرين، 2008.

- علي عدنان الفيل. إجراءات التحري، وجمع الأدلة، والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، 2012.
- المحامي عماد محمد سلامة. الحماية القانونية، لبرامج الحاسب الآلي، ومشكلة قرصنة البرامج، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، 2005.
- الدكتور عمر محمد أبو بكر بن يونس.
 - الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، الطبعة الأولى العربية، دار النهضة العربية، القاهرة، 2004.
 - الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب، وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 2006/2005.
- الدكتور كامل عفيفي عفيفي. جرائم الكمبيوتر، وحقوق المؤلف، والمصنفات الفنية، ودور الشرطة والقانون، دراسة مقارنة، بدون ناشر، 2000.
- الدكتور محمد الأمين البشري. التحقيق في الجرائم المستحدثة، الطبعة الأولى، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
- الدكتور محمد الشناوي. جرائم النصب المستحدثة، الإنترنت وبطاقة الائتمان والدعاية التجارية الكاذبة، دار الكتب القانونية، المحلة الكبرى، مصر، 2008.
- الدكتور محمد حمادة مرهج الهيتي. جرائم الحاسوب، دراسة تحليلية، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، 2006.

- **الدكتور محمد فتحي محمد أنور عزت.**
تفتيش شبكة الإنترنت، لضبط جرائم الإعتداء على الآداب العامة والشرف والإعتبارات التي تقع بواسطتها، دراسة مقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.
- **الدكتور محمود احمد طه.**
المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، دراسة مقارنة، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2016/2017.
- **الدكتور محمود محمد محمود جابر.**
الأحكام الإجرائية للجرائم الناشئة عن إستخدام الهواتف النقالة، جرائم نظم الإتصالات والمعلومات، دراسة مقارنة، في التشريع المصري والفرنسي والأمريكي، والإتفاقيات الدولية والإقليمية، الكتاب الثاني، المكتب الجامعي الحديث، الإسكندرية، 2017/2018.
- **الدكتور مدحت رمضان.**
جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000.
- **الدكتور مصطفى محمد موسى.**
التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009.
- **الدكتور ممدوح عبد الحميد عبد المطلب.**
البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2006.
- **نبيلة هبة هروال.**
الجوانب الإجرائية لجرائم الإنترنت، في مرحلة جمع الإستدلالات، دراسة مقارنة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.
- **الدكتور هشام محمد فريد رستم.**
الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 1994.

- الدكتور هلاي عبد اللاه احمد.
- تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، الطبعة الثانية، بدون ناشر، 2008.
- إتفاقية بودابست لمكافحة جرائم المعلوماتية، معلقا عليها، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011.
- المواجهة الجنائية لجرائم المعلوماتية، في النظامين المصري والبحريني، على ضوء إتفاقية بودابست، الطبعة الثانية، دار النهضة العربية، القاهرة، 2013.
- جرائم الحاسب والإنترنت، بين التجريم الجنائي واليات المواجهة، دار النهضة العربية، القاهرة، 2015.

ثالثاً : الإتفاقيات.

- ميثاق الأمم المتحدة الصادر عن الجمعية العامة للأمم المتحدة، بتاريخ 1945/6/26.
- الإتفاقية الأوروبية لحقوق الإنسان الصادرة عن مجلس أوروبا، بتاريخ 1950/11/4، روما.
- القانون الأساسي للمنظمة الدولية للشرطة الجنائية (الإنتربول) الصادر بتاريخ 1956/6/13، فينا.
- إتفاقية فينا للعلاقات الدبلوماسية الصادرة بتاريخ 1961/4/18، فينا.
- العهد الدولي الخاص بالحقوق المدنية والسياسية الصادرة عن الجمعية العامة للأمم المتحدة، بتاريخ 1966/12/16.
- إتفاقية الرياض للتعاون القضائي الصادرة عن جامعة الدول العربية، بتاريخ 1983/4/6، الرياض، المملكة العربية السعودية،
- إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية الصادرة عن الجمعية العامة للأمم المتحدة، بتاريخ 2000/11/15.
- الإتفاقية الأوروبية لمكافحة الجرائم السيبرانية الصادرة عن الاتحاد الأوروبي، بتاريخ 2001/11/23، بودابست، المجر.

- القانون الأساسي للمحكمة الجنائية الدولية نظام روما الأساسي للمحكمة الجنائية الدولية، الذي اعتمده مؤتمر الأمم المتحدة المعنى بإنشاء محكمة جنائية دولية بتاريخ 1998/7/17، دخل حيز النفاذ بتاريخ 2002/7/1.
- الإتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية الصادرة عن جامعة الدول العربية، بتاريخ 2010/12/21، دخلت حيز النفاذ بتاريخ 2013/10/5.
- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية، بتاريخ 2010/12/21، بالقاهرة، دخلت حيز النفاذ، بتاريخ 2014/2/7.

رابعاً : الإعلانات والتوصيات الدولية.

- الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة، بتاريخ 1948/12/10.
- إعلان القاهرة، حول حقوق الإنسان في الإسلام الصادر عن منظمة المؤتمر الإسلامي، بتاريخ 1990/8/5، القاهرة، مصر.
- توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات حول القواعد الإجرائية في بيئة جرائم الكمبيوتر، الشق الإجرائي، المنعقد بتاريخ 4 إلى 9/10/1994، في ريو دي جانيرو، البرازيل.
- توصيات المؤتمر الثاني للرابطة الدولية للقانون الجنائي حول الجرائم الرقمية، المنعقد في عام 2000، في أمستردام، هولندا.

خامساً : الأبحاث والمقالات والمحاضرات.

- الدكتور محمد الأمين البشري. التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في كلية الشريعة والقانون، من 1 إلى 3 /5 /2000، الطبعة الثالثة، المجلد الثالث، جامعة الإمارات العربية المتحدة.

- **الدكتور محمد الصاعدي.**
جرائم الإنترنت، وجهود المملكة العربية السعودية في مكافحتها، بحث مقدم إلى ندوة مكافحة الجريمة عبر الإنترنت على المستوى العربي، المنعقد في شهر ابريل/2008، شرم الشيخ، مصر.
- **الدكتور عبد الحكيم بوزيوجة.**
موقف المشرع الجزائري من الجريمة المعلوماتية، بحث مقدم للمؤتمر العلمي الحادي عشر، المنعقد من تاريخ 5 إلى 7 /5/2015، كلية الحقوق، جامعة جرش، الأردن.
- **الدكتور علال فالي.**
حجية الأدلة الرقمية أمام القاضي الجزائري، بحث مقدم للمؤتمر العلمي الحادي عشر، المنعقد من تاريخ 5 إلى 7 /5/2015، كلية الحقوق، جامعة جرش، الأردن.
- **الدكتور عبد اللطيف محمود ربايعة.**
الجرائم الإلكترونية، التجريم والملاحقة والإثبات، بحث مقدم إلى المؤتمر الأول للجرائم الإلكترونية، المنعقد في جامعة النجاح الوطنية، بتاريخ 17/4/2016، نابلس، فلسطين.
- **الدكتور علي عبد القادر القهوجي.**
الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في كلية الشريعة والقانون، من 1 إلى 3 /5/2000، الطبعة الثالثة، المجلد الثالث، جامعة الإمارات العربية المتحدة.
- **الدكتور علي محمود علي حمودة.**
الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في أكاديمية شرطة دبي، 4/2003، المجلد الأول، الإمارات العربية المتحدة.
- **الدكتور سعيد حماد صالح القبالي.**
الجهود الدولية في مواجهة الجرائم المعلوماتية، بحث مقدم إلى المؤتمر العلمي الحادي عشر، تحت عنوان الجرائم المعلوماتية، 5 إلى 7 /5/2015 جامعة جرش، الأردن.

- الدكتور هشام محمد فريد رستم.

• الجرائم المعلوماتية، أصول التحقيق الجنائي الفني والية التدريب التخصصي للمحققين، مقالة منشورة في مجلة الأمن والقانون، كلية شرطة دبي، العدد الثاني، 1999.

• أصول التحقيق الجنائي الفني، وإقتراح إنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في كلية الشريعة والقانون، من 1 إلى 3 / 2000/5، الطبعة الثالثة، المجلد الثالث، جامعة الإمارات العربية المتحدة.

- محاضرات للخبير البريطاني **Jon Blake**، بعنوان التحقيق في الجرائم الإلكترونية، أعطيت في مقر الهيئة القضائية لقوى الأمن، بتاريخ 24 إلى 25/2/2018، رام الله، فلسطين.

سادساً : المقابلات.

- مقابلة بحثية مع الأستاذة نسرين زينة، رئيسة نيابة مكافحة الجرائم الإلكترونية، أجريت بتاريخ 2018/5/2، الساعة العاشرة صباحاً، في مكتب نيابة مكافحة الجرائم الإلكترونية، مقر النائب العام، رام الله، فلسطين.

- مقابلة بحثية مع المقدم/ سامر الهندي. رئيس وحدة مكافحة الجرائم الإلكترونية، في جهاز الشرطة، أجريت بتاريخ 2018/5/6، الساعة الخامسة والنصف مساءً، في مكتب وحدة مكافحة الجرائم الإلكترونية، مقر الشرطة، رام الله، فلسطين.

سابعاً : القرارات القضائية.

1-قرارات قضائية دستورية.

-قرار المحكمة الدستورية العليا المصرية، في القضية رقم 5، س 4 قضائية، الصادر بتاريخ، 1984/2/2، أحكام المحكمة الدستورية العليا المصرية، ج 3، رقم 13، ص 67.

- قرار المحكمة الدستورية العليا الفلسطينية، في القضية رقم (12)، لسنة (2) قضائية، الصادر بتاريخ 2017/11/19، منشور بالجريدة الرسمية، بتاريخ 2017/11/29، بالعدد (138).

2-قرارات قضائية جزائية.

- نقض جنائي مصري بتاريخ 1957/5/7، أحكام النقض، س 8، ق 130، ص 471.
- نقض جنائي مصري بتاريخ 1957/6/10، أحكام النقض، س 8، ق 173، ص 633.
- نقض جنائي مصري بتاريخ 1961/2/20، أحكام النقض، س 12، رقم 40، ص 233.
- نقض جنائي مصري بتاريخ 1967/11/13، أحكام النقض، س 18، ق 229، ص 1101.
- نقض جنائي مصري بتاريخ 1972/5/22، أحكام النقض، س 23، رقم 177، ص 786.
- نقض جنائي مصري بتاريخ 1972/6/19، أحكام النقض، س 23، ق 209، ص 936.
- نقض جنائي مصري بتاريخ 1976/1/11، أحكام النقض، س 27، ق 9، ص 52.
- نقض جنائي مصري بتاريخ 1976/2/16، أحكام النقض، س 27، ق 45، ص 225.
- نقض جنائي مصري بتاريخ 1979/3/18، أحكام النقض، س 30، رقم 72، ص 351.
- نقض جنائي مصري بتاريخ 1981/11/19، أحكام النقض، س 32، ق 163، ص 944.
- نقض جنائي مصري بتاريخ 1983/10/2، أحكام النقض، س 34، رقم 167، ص 841.
- نقض جنائي مصري بتاريخ 1987/11/11، أحكام النقض، س 38، ق 153، ص 943.
- تمييز جزاء أردني رقم 97/697، مجلة نقابة المحامين الأردنيين، س 1998، ع 3 و4، ص 941.
- تمييز جزاء أردني رقم 99/420، مجلة نقابة المحامين الأردنيين، س 2000، ص 1147.

ثامناً : المواقع الالكترونية.

- موقع ويكيبيديا، الموسوعة الحرة على الإنترنت.

<https://ar.wikipedia.org>