جامعة بيرزيت

كلية الدراسات العليا

برنامج ماجستير القانون

رسالة ماجستير بعنوان

اجراءات الضبط والتفتيش في الجرائم الإلكترونية في النظام القانوني الفلسطيني

Search and seizure Procedures of cybercrimes in the Palestinian legal system

اعداد الطالب: مهدي رضوان

الرقم الجامعي: 1195373

اشراف

د. مصطفى عبد الباقي

شباط 2023

كلية الدراسات العليا

برنامج ماجستير القانون

رسالة ماجستير بعنوان

اجراءات الضبط والتفتيش في الجرائم الإلكترونية في النظام القانوني الفلسطيني

Search and seizure Procedures of cybercrimes in the Palestinian legal system

إعداد الطالب

مهدي صلاح الدين محمود رضوان

الرقم الجامعي: 1195373

إشراف

د. مصطفى عبد الباقي

قدمت هذه الرسالة استكمالاً لمتطلبات درجة الماجستير في القانون من كلية الدراسات العليا

جامعة بيرزيت، فلسطين

2023

كلية الدراسات العليا

برنامج ماجستير القانون

رسالة ماجستير بعنوان

اجراءات الضبط والتفتيش في الجرائم الإلكترونية في النظام القانوني الفلسطيني

Search and seizure Procedures of cybercrimes in the Palestinian legal system

اعداد الطالب

مهدي صلاح الدين محمود رضوان

نوقشت هذه الرسالة وأجيزت بتاريخ (2023/2/25)

أعضاء لجنة المناقشة	التوقيع
د. مصطفى عبد الباقي (مشرفاً ورئيساً) جامعة بيرزيت	.....
د. فايز بكيرات (ممتحناً ومناقشاً داخلياً) جامعة بيرزيت	.....
د. أنور جانم (ممتحناً ومناقشاً خارجياً) جامعة النجاح الوطنية	.....

الشكر والتقدير

أتقدم بجزيل الشكر والامتنان إلى استاذي القدير الدكتور مصطفى عبد الباقي، لتفضله بقبول الإشراف على رسالتي وتقديراً لجهوده وملاحظاته القيمة التي أغنت هذه الرسالة.

كما ويطيب لي أن أتقدم بجزيل الشكر والتقدير إلى أعضاء لجنة المناقشة، الدكتور فايز بكيرات والدكتور أنور جانم على تفضلهم بقبول مناقشة هذه الرسالة

والشكر موصول أيضاً، إلى جميع أساتذتي وكافة الهيئة التدريسية في كلية الحقوق والإدارة العامة في جامعة بيرزيت، الذين كان لهم الأثر الكبير فيما وصلت إليه الآن.

كما وأخص بجزيل الشكر والتقدير إلى رئيس نيابة قلقيلية المحترم الأستاذ أيمن طربية وإلى جميع الأعضاء والعاملين في النيابة العامة الذين ساعدوني بالوصول إلى هذا النتاج القانوني المثمر.

فلهم مني كل التقدير والاحترام

الباحث

إهداء

إلى من أبصرت بها طريق حياتي واستمدت منها قوتي واعتزازي، إلى ينبوع العطاء المتنافي ... إلى معلمتي الأولى والأخيرة

أمي الغالية

إلى من علمني أن الدنيا جِدٌ وكفاح وأن وسلاحها العلم ... إلى الذي لم يبخل علي بأي شيء

أبي العزيز

إلى السند والعون أخي الطبيب محمود

إلى رمز العطاء أختي الطبيبة سنابل

إلى بذرة الفؤاد وأمل الغد اخوتي الصغار

عبد الرحيم وإبراهيم

الى شهداء فلسطين الابرار، الى من روت دماؤهم أرض فلسطين،، رحمهم الله

الى الاسرى الابطال الذين ضحوا بحريتهم من أجل فلسطين،، فكَ الله قيدهم

المحتويات

الملخص

تأتي هذه الرسالة في إطار فهم القواعد الإجرائية لعملية التفتيش والضبط القضائي في الجرائم الإلكترونية في النظام القانوني الفلسطيني، إضافة إلى دراسة قواعد الاتفاقيات الدولية التي تنظم الجريمة الإلكترونية ومنها الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) والاتفاقية العربية لمكافحة الجريمة الإلكترونية. ومن أجل توضيح موضوع التفتيش والضبط القضائي في الجرائم المعلوماتية قام الباحث بتقسيم هذه الرسالة إلى ثلاثة فصول يدرس كل منها على حدة. ففي الفصل التمهيدي يدرس الباحث ماهية التفتيش القضائي في الجرائم الإلكترونية ومن ثم تعريف التفتيش في الجرائم الإلكترونية وبيان مدى صلاحية نظم الحاسوب والانترنت للتفيش الجنائي.

وفي الفصل الأول وبعد توضيح التفتيش الجنائي في الجرائم الإلكترونية سوف يدرس الباحث الدليل الالكتروني في مجال الاثبات الجنائي، والذي يتمثل بتعريف الدليل الالكتروني في مجال الاثبات الجنائي وتوضيح أنواع وأشكال الدليل الالكتروني، ومن ثم دراسة خصائص هذه الأدلة، إضافة إلى دراسة مسرح الجريمة الإلكترونية، عن طريق توضيح دور المحقق الجنائي في معاينة مسرح الجريمة الإلكترونية واستخلاص الدليل الالكتروني عن طريق الأدوات المخصصة في جمع الأدلة الإلكترونية، ثم ضبطها وتحريزها.

وفي الفصل الثاني من هذه الرسالة يوضح الباحث القواعد العامة في ضبط وتفتيش نظم الحاسوب في النظام القانوني الفلسطيني، والتي تتمثل بتوضيح السلطات المختصة في عملية التفتيش والتحقيق في الجرائم الإلكترونية وصلاحيتها، ودراسة الصعوبات التي تواجه عملية التحقيق في الجرائم الإلكترونية، والضمانات القانونية للمتهم أثناء عملية التفتيش والتحقيق في الجرائم الإلكترونية، إضافة إلى دراسة التنظيم القانوني والضمانات الخاصة للمتهم عند عملية ضبط المراسلات واعتراض المكالمات.

Abstract

This thesis comes within the framework of understanding the procedural rules of search and seizure of cybercrime in the Palestinian legal system, in addition to studying the rules of international conventions that regulate cybercrime, including the Convention on Cybercrime, Budapest, November 23, 2001. In addition to the Arab Convention against Cybercrime 2010/21/12, so, in order to clarify the matter of search and seizure of cybercrime, the researcher decided to divide this thesis into three chapters, which will study each of them separately. In the introductory chapter of this thesis, the researcher studies the nature of judicial inspection in cybercrime, and indicates the validity of computer and Internet systems for inspection as they consist of material and moral elements.

In the first chapter, after clarifying the criminal inspection in cybercrime, the researcher will study the digital evidence as a type of digital evidence, which is represented by defining the digital evidence. In addition to clarifying the types and forms of digital evidence and then studying the characteristics of this evidence, the researcher will also study the cybercrime scene by clarifying the role of the criminal investigator in examining the cybercrime scene and extracting the digital evidence from the cybercrime scene, then seizing it.

In the second chapter of this thesis, the researcher clarifies the general rules for searching and seizing computer systems in the Palestinian legal system, which are represented by clarifying the competent authorities in the process of searching and seizing cybercrime and their validity. The researcher also highlights the importance of studying the difficulties facing the investigation process of cybercrime. The researcher will study the legal guarantees of the accused during the process of inspection and investigation of cybercrime, in addition to studying the legal regulations and special guarantees for the accused during the process of adjusting correspondence and intercepting calls.

مقدمة

تبتدئ الدعوى الجزائية بمرحلة التحقيق الابتدائي وتنتهي بمرحلة التحقيق النهائي وصدور الحكم إما بالإدانة أو بالبراءة. ومن إجراءات التحقيق الابتدائي التي تقوم بها النيابة العامة التفتيش، وهو أحد الاعمال التي تقوم بها النيابة العامة أو تنتدب الضابطة القضائية للقيام به. ويعتبر التفتيش من الإجراءات الخطيرة الذي تلجأ له النيابة العامة من اجل الكشف عن الحقيقة، فهو يمس حريات الأشخاص، فقد نصت المادة (17) من القانون الأساسي المعدل بان للمساكن حرمة، فلا تجوز مراقبتها أو دخولها أو تفتيشها إلا بأمر قضائي مسبب ووفقاً لأحكام القانون؛ وعليه فقد حرص المشرع الجزائي على تنظيم اعمال التفتيش وأحاطه بالعديد من الضمانات التي تكفل حرية المتهم وتكفل عدم المساس بحرمة المساكن، وقد نص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 في المواد 39-52 على إجراءات التفتيش والضوابط الواجب اتباعها والضمانات القانونية للمتهم في حال التفتيش. وكون إجراءات التفتيش من الموضوعات الخطيرة فقد عالجها قانون الإجراءات الجزائية في فصل منفصل وأورد احكامها بالتفصيل. ونعيش الآن عصر التطور التكنولوجي وانتشار الجرائم الإلكترونية، حيث أصبح الانترنت جزءاً لا يمكن أن ينفصل عن حياتنا اليومية وأصبحت الهواتف الذكية وأجهزة الكمبيوتر المحمول تدخل في صلب حياتنا اليومية وتطور مفهوم الجريمة ليمتد إلى تلك الجرائم التي ترتكب عبر الأجهزة الإلكترونية وشبكة الانترنت بغض النظر عن انواعها، وهي ما تسمى بالجريمة الإلكترونية، وأصبحت اغلب دول العالم تضع نصوصا تشريعية لتنظم إجراءات التحقيق والتقاضي في مثل هذا النوع من الجرائم، وعليه فإن التفتيش لم يعد يقتصر فقط على البحث عن ادلة مادية تربط المتهم بالجريمة، كالبحث عن سلاح الجريمة وانما امتد التفتيش ليشمل تفتيش الأجهزة الإلكترونية بمختلف أنواعها كأجهزة الكمبيوتر المحمولة والهواتف الذكية، إضافة إلى أوعية التخزين الرقمي كالأقراص المدمجة والاقراص الصلبة. ويختلف التفتيش في الجرائم الإلكترونية عن غيره من الجرائم العادية كون

الضابطة القضائية في هذه الحالة تقوم بالدخول والولوج إلى ملفات رقمية مختلفة المصدر، وهذا النوع من التفتيش يكون غالبا بحاجة إلى إمكانيات تفوق تلك الإمكانيات اللازمة للتفتيش التقليدي داخل منزل المتهم؛ فهذه الادلة الرقمية بحاجة إلى آلية تعامل تختلف عنها في الجرائم التقليدية. كما أن سرعة التخلص من الأدلة الرقمية في الجرائم الإلكترونية وإمكانية نسخها أكثر من مرة استدعت أن يكون هناك خبرات ومؤهلات خاصة فيمن يتعامل معها، وعليه فإن أفراد الضابطة القضائية من المفترض أن يكون لديهم العلم الكافي والخبرة الكافية من اجل القيام بعملية التفتيش والضبط في الجرائم الإلكترونية. وهذا ما اتجهت إليه اغلب دول العالم فأنشأت جهاز شرطة خاص للجرائم الإلكترونية بمختلف مسمياته هدفه مباشرة إجراءات التحقيق في الجرائم الإلكترونية وملاحقة المتهمين وضبط الأدلة الإلكترونية والتعامل معها بحذر تام. وفي فلسطين تم انشاء قسم التحقيق في الجرائم الإلكترونية في كل من الشرطة والأمن الوقائي والمخابرات العامة، كما تم انشاء نيابة متخصصة لمكافحة الجرائم الإلكترونية في مكتب النائب العام بناء على قرار صادر عن عطوفة النائب العام بتاريخ 2016/3/20، وتعمل هذه النيابة تحت اشراف النائب العام مباشرة، وتم تكليف رئيس نيابة يتولى شأنها يعاونه عدد من وكلاء ومعاوني النيابة العامة إضافة إلى كادر اداري يساندهم في المهمة، وفي تلك الفترة لم يكن هناك اطار قانوني خاص ينظم الجرائم الإلكترونية إلى حين صدور القرار بقانون رقم (16) لسنة 2017 والذي تم الغاؤه بموجب القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية والذي عُدل بقرار بقانون رقم (28) لسنة 2020م والقرار بقانون رقم (38) لسنة 2021 واستقر الاطار القانوني بعد ذلك للجرائم الالكتروني على ما ورد أعلاه.

إشكالية الدراسة

تعتبر اعمال التفتيش والضبط القضائي احد اهم اعمال التحقيق التي تقوم بها النيابة العامة فهي تمس حقوق وحريات المتهم وعليه اتجه المشرع إلى تنظيم قانوني لإجراءات التفتيش والضبط القضائي ووضع العديد من الضمانات القانونية امام إجراءات التفتيش والضبط القضائي، فقد نصت المادة (1/39) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م بأن دخول المنازل وتفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها ويجب ان تكون المذكرة مسببة، ولكن لم يعد التفتيش القضائي يقتصر على تفتيش منزل المتهم واغراضه الشخصية فقد امتد ليشمل أجهزة الحاسوب والنظم الإلكترونية في حال كان هناك جريمة الكترونية مرتكبة عن طريق وسيلة الكترونية، وعليه فقد اصبحت الأمور اكثر تعقيدا ودقة.

تتمحور إشكالية البحث حول توضيح إجراءات التفتيش والضبط في الجرائم الإلكترونية التي تتمثل بالصعوبة والدقة أثناء عملية جمع الأدلة الإلكترونية وضبطها، والتي تتميز بطبيعة خاصة عن غيرها من الأدلة في الجرائم التقليدية، نظراً لسرعة اتلاف هذا النوع من الأدلة وتعلقها ببيانات معنوية، فاتجهت اغلب الدول إلى اصدار قوانين تنظم الجريمة الإلكترونية وفي فلسطين فقد نصت المادة (52) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته "على حق النيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة. وبالمقارنة فيما ورد بنصوص القرار بقانون الخاصة بالتفتيش والضبط بالجرائم الإلكترونية وما ورد في المواد 39–52 المتعقلة بالتفتيش في قانون الإجراءات الجزائية الفلسطيني نلاحظ ان المادة سابقة الذكر في القرار بقانون بشأن الجرائم الإلكترونية تركت الباب مفتوحاً امام العديد من التساؤلات.

أسئلة الدراسة

1- تحدث قانون الإجراءات الجزائية الفلسطيني في المادة (39) منه على وجوب ان يكون التفتيش بمذكرة، على العكس لم يتطرق القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في المادة (52) إلى وجوب ان يكون التفتيش متبوعاً بمذكرة قانونية، وعليه ما هي الضمانات القانونية للمتهم في عملية التفتيش والتحقيق الجنائي في الجرائم الإلكترونية؟

2- كما لم يتطرق القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته إلى حدود التفتيش والضبط التي نص عليها قانون الإجراءات الجزائية في المادة (50) حيث لا يجوز التفتيش إلا عن الأشياء الخاصة بالجريمة الجاري التحقيق بشأنها، وعليه ما هي حدود التفتيش في البيانات المخزنة على الذاكرة الرقمية وماذا لو ظهرت اثناء عملية التفتيش الالكتروني بيانات يعد تخزينها في حد ذاته جريمة يعاقب عليها القانون.

3- كيف عالجت المادة (2) من القرار بقانون الاختصاص القضائي الدولي، للجريمة الإلكترونية وما هو موقف الاتفاقيات الدولية منها.

4- إلى أي مدى اتاحت للدول التعاون فيما بينها في حالة الجرائم العابرة للحدود؟ إضافة إلى دراسة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي تنظم مكافحة الجرائم الإلكترونية في الدول العربية.

5- مدى جواز اجبار المتهم على فتح الفضاء الالكتروني الخاص به أو البوح عن كلمة السر لحسابه على مواقع التواصل الاجتماعي أو بريده الالكتروني تعارض ذلك مع مبدأ عدم جواز اجبار المتهم على تقديم دليل يدينه.

أهمية الدراسة

تنبثق أهمية الدراسة في التفتيش القضائي عندما يتعلق بالجرائم الإلكترونية ففي هذه الحالة تصبح الأمور أكثر تعقيدا لدى النيابة العامة والضابطة القضائية فما زالت الجرائم الإلكترونية حديثة النشأة مقارنة بغيرها من الجرائم؛ وعليه من المهم معالجة إجراءات التحقيق والضبط القضائي التي تحيط بارتكاب الجريمة الإلكترونية، إضافة إلى التطور السريع الذي يلحق بهذا النوع من الجرائم وظهور نوع جديد من هذه الجرائم في فترة وجيزة وهذا يشكل حاجة إلى إعادة ترميم المنظومة القانونية من وقت لآخر لكي تتناسب مع التطور العصري.

أهداف الدراسة

في هذه الدراسة يهدف الباحث إلى توضيح العديد من الأمور أهمها:

1- تسليط الضوء على الجوانب الإجرائية التي تتعلق في عملية التفتيش في الجرائم الإلكترونية كونها أحد مراحل التحقيق الابتدائي.

2- بيان الطبيعة الخاصة للدليل الالكتروني وما يميزه على باقي الأدلة في الجرائم العادية والتي لا تدخل في حيز الفضاء الالكتروني.

3- بيان إمكانية إعمال النصوص الواردة في قانون الإجراءات الجزائية على الجرائم الإلكترونية.

4- تعزيز المعرفة لدى الجهات المختصة عن الطبيعة الخاصة للدليل الالكتروني وإمكانية التعامل معه بصورة مناسبة تضمن عدم اتلافه او ضياعه.

منهجية الدراسة

اعتمد الباحث المنهج الوصفي التحليلي فسوف يقوم الباحث باستقراء النصوص القانونية ذات العلاقة بإجراءات التفتيش بشكل عام في قانون الإجراءات الجزائية رقم (3) لسنة 2001 الساري في فلسطين ومن ثم استقراء نصوص القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته ودراسة مدى توافقها مع ما ورد في قانون الإجراءات الجزائية، وكذلك التعرف على أساليب التحقيق والضبط القضائي في الجرائم الإلكترونية ومدى توافقها مع ما ورد في قانون الإجراءات الجزائية الفلسطيني ومقارنتها بما ورد في نصوص الاتفاقية الأوروبية لمكافحة جرائم تقنية المعلومات (بودابست) 2001 /11/23.

مراجعة موجزة للأدبيات السابقة

- د. مصطفى محمد موسى التحقيق الجنائي في الجرائم الإلكترونية، القاهرة، مصر، 2009

تعتبر هذه الدراسة احدى الدراسات المعمقة في إجراءات التحقيق في الجرائم الإلكترونية فقد تناول الدكتور مصطفى محمد موسى العديد من الجوانب المتعقلة بالتحقيق في الجرائم الإلكترونية بدأً من التقنية الإلكترونية وشبكاتها وامتد لدراسة قواعد وإجراءات التفتيش في الجرائم الإلكترونية ودراسة المحقق الجنائي في الجرائم الإلكترونية، وقد تحدث بشكل مفصل عن تدوين محاضر التحقيق الجنائي وتحريز الدليل الالكتروني في الجرائم الإلكترونية، واختتم دراسته في ذكر تطبيقات للتحقيق الجنائي في الجرائم الإلكترونية في مصر.

تتفق هذه الدراسة مع دراستنا في تناولها لعملية التحقيق الجنائي في الجرائم الإلكترونية وعملية ضبط الأدلة الرقمية وتحريزها، ولكن ما جد في درستنا تناولها لموضوع التحقيق الجنائي في الجرائم الإلكترونية بشكل مخصص في فلسطين، كما ان التطور السريع في التقنية الإلكترونية وشباكتها وظهور خطوط الانترنت

فائقة السرعة أدى إلى امتداد الدليل الالكتروني إلى خارج حدود الدول ولتصبح الجريمة الإلكترونية جريمة عابرة للقارات.

– طاهر محمود أبو القاسم، الجرائم المعلوماتية صعوبات وسائل التحقيق فيها وكيفية مواجهتها، جامعة الدول العربية، 2019

في هذه الدراسة تناول الباحث كشف المعوقات بأشكالها المختلفة والتي تحدث خللاً في إجراءات التحقيق الجنائي بالجرائم الإلكترونية وتؤثر سلباً عليها وهذا يؤدي بشكل حتمي إلى افلات الجناة من العقاب وقد قسم هذه الصعوبات إلى قسمين فالقسم الأول هي الصعوبات التي تتعلق بالجريمة نفسها كاختلاف خصائص الجريمة الإلكترونية عن الجريمة العادية، اما القسم الثاني من الصعوبات فهي التي تتعلق بالجهاز الأمني بحد ذاته او الضابطة القضائية ومنها قلة الخبرة لدى الأجهزة الأمنية في موضوع الجرائم الإلكترونية او عدم توفر المعدات اللازمة من اجل إتمام عملية التحقيق، وفي الختام تطرق الباحث إلى إيضاح دور المنظمات والمؤسسات الدولية بالتعاون فيما بينها من اجل مكافحة الجريمة الإلكترونية حيث ان هذه الجرائم تتميز بانها لا تتقيد بحدود جغرافية.

تتفق هذه الدراسة مع بحثنا في تناولها الطبيعة الخاصة للدليل الالكتروني وتأثيرها على عملية التحقيق الجنائي في الجرائم الإلكترونية بالإضافة إلى تعزيز المعرفة لدى الضابطة القضائية بخصوص التعامل مع الأدلة الرقمية لسرعة فقدانها او تلفها، وكذلك ضرورة التعاون الدولي من اجل مكافحة الجريمة الإلكترونية، وما يجد في دراستنا الحالية هو تخصيص الباحث لدراسة الضوابط والضمانات القانونية للمتهم في عملية التفتيش والضبط القضائي للجرائم الإلكترونية، إضافة إلى مدى قدرة النيابة على اجبار المتهم على تقديم رموز من اجل الوصول إلى دليل يدينه ومدى تعارضها مع مبدأ (عدم جواز اجبار المتهم على تقديم دليل يدينه).

– عائشة مصطفى، حجية الدليل الالكتروني في مجال الاثبات الجنائي، جامعة الإسكندرية 2010

تناولت الباحثة في هذه الدراسة العديد من الجوانب التي تتعلق بالدليل الالكتروني، فقد طرحت عدة أسئلة تتعلق بالدليل الالكتروني كان أهمها، كيف يمكن استخراج الدليل الالكتروني وهل تكفي القواعد الإجرائية المقررة للجرائم التقليدية لكي تسري على الجرائم الإلكترونية أم ان هناك إجراءات أكثر دقة وخصوصية من اجل البحث عن الأدلة في الجرائم الإلكترونية؟ وأكدت الباحثة في نتائج دراستها على ضرورة التعاون الدولي لمواجهة الجرائم الإلكترونية وضرورة ان يكون هناك اتفاقيات تنص على تبادل المعلومات والخبرات في المسائل المتعقلة بالجريمة الإلكترونية، إضافة إلى أهمية دراسة اتفاقية بودابست لمواجهة الجريمة الإلكترونية وإمكانية الانضمام لها.

تتفق هذه الدراسة مع بحثنا في تناولها لحجية الدليل الالكتروني في مجال الاثبات الجنائي ومدى قدرة القواعد الإجرائية المقررة في الجرائم التقليدية في سريانها على الجرائم الإلكترونية مقارنة بإجراءات خاصة تتبع منهج اكثر دقة واكثر خصوصية في استخراج الدليل الالكتروني، وما يجد في دراستنا الحالية ويميزه عن الدراسة السابقة هو الخوض في تفاصيل اكثر دقة تتعلق بالدليل الالكتروني كمدى قدرة الضابطة القضائية عن البحث والتحري عن الدليل الالكتروني وما هو مدى سرعة افراد الضابطة القضائي في عملية البحث والتحري عن الدليل الالكتروني كون هذا الدليل يتمتع بصفات خاصة عن الدليل في الجرائم العادية، كسرعة التخلص من الدليل الالكتروني، إضافة إلى دراسة مدى الخبرة التي يجب ان تتوافر في الضابطة القضائية من اجل إتمام عملية الضبط الجنائي في الدليل الالكتروني دون أي فرصة لتلف هذا الدليل او فقدانه.

تقسيم الدراسة

من اجل تحقيق الهدف من هذه الدراسة والاجابة على التساؤلات المطروحة امامنا فقد رأى الباحث ان يقوم بتقسيم هذه الرسالة إلى عدة فصول:

في الفصل التمهيدي سوف يقوم الباحث بدراسة **ماهية التفتيش الجنائي في الجرائم الإلكترونية** وذلك في عدة مواضيع تتمثل فيما يلي، المبحث الأول تعريف التفتيش الجنائي والطبيعة القانونية له، المبحث الثاني مدى صلاحية نظم الحاسوب والانترنت للتفتيش الجنائي.

في الفصل الاول من هذه الدراسة فسوف يدرس الباحث **الدليل الالكتروني في مجال الاثبات الجنائي** وذلك في ثلاثة مباحث، في المبحث الأول تعريف بالدليل الرقمي في مجال الاثبات الجنائي، والمبحث الثاني: الطبيعة القانونية للدليل الرقمي، والمبحث الثالث مسرح الجريمة الالكتروني وأدوات الاثبات في الجرائم الإلكترونية.

في الفصل الثاني من هذه الدراسة سوف يدرس الباحث **القواعد العامة في ضبط وتفتيش نظم الحاسوب في النظام القانوني الفلسطيني** وذلك في عدة مواضيع تتمثل فيما يلي، المبحث الأول السلطات المختصة بالتفتيش والتحقيق في الجرائم الإلكترونية وصلاحيتها، المبحث الثاني الصعوبات التي تواجه عملية التحقيق في الجرائم الإلكترونية، المبحث الثالث الضمانات القانونية للمتهم في عملية التفتيش والتحقيق الجنائي في الجرائم الإلكترونية.

الفصل التمهيدي

ماهية التفتيش القضائي في الجرائم الإلكترونية

يعتبر التفتيش أحد أهم إجراءات التحقيق في الجريمة حيث يؤدي إلى كشف ملابسات وظروف الجريمة، وكون الجرائم الإلكترونية من الجرائم التي تخفي خلف وقوعها العديد من الملابسات والظروف الغامضة فقد خصص الباحث هذا الفصل التمهيدي من أجل دراسة التفتيش القضائي في الجرائم الإلكترونية وذلك في مبحثين منفصلين، ففي المبحث الأول سوف يدرس الباحث تعريف التفتيش القضائي وأحكامه في القانون، وفي المبحث الثاني سوف يدرس مدى صلاحية نظم الحاسوب والانترنت للتفتيش القضائي.

المبحث الأول

تعريف التفتيش القضائي واحكامه في القانون

يعتبر التفتيش خروجاً عن القاعدة العامة حيث أن للمساكن حرمة فقد أجاز المشرع للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي القيام بإجراءات التفتيش وفقاً لضوابط محددة، ولأن التفتيش اجراء ينطوي على المساس بحرية الأشخاص او انتهاك لحرية المساكن والحرية الشخصية التي نصت عليها المواثيق الدولية والتشريعات الوطنية[1]، فقد حدد المشرع لعملية التفتيش شروطاً وقيوداً لا يجب أن تخرج عملية التفتيش عن إطارها؛ إلا في حالات استثنائية أخرى أجازها القانون، وفي إطار دراسة التفتيش في الجرائم الإلكترونية لا بد من تعريف التفتيش القضائي وتوضيح احكامه وعليه سوف يقسم الباحث هذا المبحث إلى مطلبين في المطلب الأول سوف يدرس تعريف التفتيش القضائي وفي المطلب الثاني سوف يدرس التفتيش القضائي في الجرائم الإلكترونية.

[1] محمد سعيد نمور (شرح أصول الإجراءات الجزائية) (دار الثقافة للنشر، عمان، 2005) ص 352

المطلب الأول: تعريف التفتيش

التفتيش يعتبر أحد أهم وأخطر الإجراءات التي تمر بها مراحل الدعوى الجزائية، وهو من أخطر الصلاحيات الممنوحة لسلطات التحقيق لما له من انتهاك للخصوصية والحرمات وعليه لا بد من توضيح المفهوم اللغوي والقانوني للتفتيش، وعليه وسوف نقسم هذا المطلب إلى فرعين في الفرع الأول سوف نتحدث عن التعريف الفقهي والقضائي للتفتيش وفي الفرع الثاني عن الاحكام العامة القانونية للتفتيش.

الفرع الأول: تعريف التفتيش في القضاء والفقه

سوف يتطرق الباحث إلى التعريف اللغوي للتفتيش، والتعريف الفقهي له، والتعريف القضائي كلاً على حدته.

أولاً: التعريف اللغوي للتفيش

التفتيش لفظاً: هو من مصدر فتش ويعني البحث لاستخراج ما يكون قد خفي، أي فتَّش الحقيبةَ فَحَصَها، تفقّدها، بحث فيها بدقّة، وفتَّش عن الكتاب بحث عنه، سأل عنه واستقصاه وفتَّش في الكتاب أي بحث فيه[2].

ثانياً: التعريف الاصطلاحي للتفتيش

يعرف التفتيش اصطلاحاً على أنه "البحث عن الحقيقة في مستودع السر، وهو اجراء من إجراءات التحقيق الابتدائي تملكه سلطة التحقيق، فيخضع بذلك لسائر الخصائص التي تحكم هذه الإجراءات والهدف منه هو كشف الحقيقة بشأن ارتكاب الجريمة ومدى ثبوتها"[3].

---

[2] معجم المعاني الجامع

[3] محمد سعيد نمور **(مرجع سابق)** ص 352

ثالثاً: التعريف الفقهي للتفتيش

ويُعرفه جانب من الفقه أيضاً "بأنه إجراء من إجراءات التحقيق التي تقوم به سلطة حددها القانون، ويتم بالبحث في مستودع السر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة وتمثل مستودع السر في شخص المتهم أو في المكان الذي يعمل به أو يقيم فيه".[4]

ولقد ورد في قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 "دخول المنازل وتفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها، بناء على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو لوجود قرائن قوية على انه يجوز أشياء تتعلق بالجريمة".[5]

رابعاً: التعريف القضائي للتفتيش

وقد ورد في حكم لمحكمة النقض المصرية بأن التفتيش هو ذلك الاجراء الذي رخص الشارع فيه بالتعرض لحرمة ما، بسبب جريمة وقعت أو ترجح وقوعها وذلك تغليباً للمصلحة العامة على مصالح الافراد الخاصة، واحتمال الوصول إلى دليل مادي يفيد في كشف الحقيقة.[6]

وعليه يرى الباحث أن أغلب التعريفات اعتبرت التفتيش بمثابة رخصة منحها القانون لسلطات التحقيق من أجل البحث في مستودع سر المتهم بهدف كشف الحقيقة والعثور على الأدلة من أجل عرضها على المحكمة صاحبت الاختصاص، كما أن الأصل حرمة المساكن ولذلك فإن التفتيش يعتبر اعتداء على حرية

---

[4] محمد طوالبة: **التفتيش الجنائي على نظم الحاسوب والانترنت دراسة مقارنة** (رسالة دكتوراه منشورة)، جامعة عمان العربية، عمان، 2003 ص 9

[5] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (1/39)

[6] عبد الحميد الشورابي، **ضمانات المتهم في مرحلة التحقيق الجنائي**، منشأة المعارف للنشر والتوزيع، الإسكندرية، 1996، ص 350

الحياة الشخصية للمتهم وعليه لا بد أن يكون هناك العديد من الضمانات والاحكام التي تحيط عملية التفتيش وهذا ما سوف نوضحه.

الفرع الثاني: الاحكام العامة للتفتيش

ان اهم ما يمكن دراسته في التفتيش القضائي هو الضمانات القانونية للمتهم اثناء عملية التفتيش وتنظيم محضر التفتيش والجزاء القانوني المترتب في حال عدم مراعاة الاحكام الواردة في قانون أصول الاجراءات الجزائية بخصوص التفتيش وهو البطلان.

أولاً: تنظيم محضر التفتيش وضمانات المتهم اثناء عملية التفتيش

لقد تطرق المشرع الجزائي في فلسطين إلى تنظيم محضر التفتيش فقد نصت المادة (2/50) من قانون الإجراءات الجزائية على ضبط جميع الأشياء التي يعثر عليها أثناء إجراء التفتيش والمتعلقة بالجريمة وتحرز وتحفظ وتثبت في محضر التفتيش ويتم احالتها إلى الجهات المختصة.[7] كما نصت كذلك الفقرة الرابعة على انه يحرر محضر التفتيش من قبل القائم عليه، ويذكر فيه الأشياء التي يتم ضبطها ومكان تواجدها ويوقع من قبل القائم على إجراءات التفتيش.

وحسب ما ورد في إجراءات التفتيش يجب ان يتمتع التفتيش بالعديد من الضمانات القانونية وهي كالتالي:

1- يكون التفتيش بموجب مذكرة صادرة عن النيابة العامة دون غيرها، الا انه يجوز بناء على نص المادة (48) دخول المنازل دون مذكرة في وذلك في حالة طلب المساعدة من الداخل أو وجود حريق أو الغرق، أو إذا كان هناك جريمة متلبس بها أو في حالة تعقب شخص يجب القبض عليه، أو شخص فر من مكان أوقف فيه بوجه مشروع.[8]

---

[7] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (2/50)

[8] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (48)

2- أن يكون التفتيش بناء على اتهام موجه للشخص المقيم في المنزل بارتكاب جناية او جنحة[9]

3- يجب أن تكون مذكرة التفتيش مسببة.[10]

4- يجب أن تحرر مذكرة التفتيش باسم واحد أو أكثر من مأموري الضبط القضائي، فلا يجوز لغير ما ورد اسمه في المذكرة القيام بأعمال التفتيش.[11]

5- يجب تحديد مدة سريان مذكرة التفتيش بالتاريخ والساعة.[12]

6- يجب أن يكون التفتيش نهاراً ولا يجوز التفتيش ليلاً الا إذا كان هناك تلبس بالجريمة أو أن ظروف الاستعجال تستوجب ذلك.[13]

7- يجب التفتيش بحضور المتهم أو حائز المنزل وإذا تعذر حضوره يجري التفتيش بحضور شاهدين من جيرانه او اقاربه.[14]

8- لا يجوز التفتيش الا عن الأشياء الخاصة بالجريمة وإذا ظهر عرضاً اثناء التفتيش أشياء تعد حيازتها جريمة جاز لمأمور الضبط القضائي ضبطها.[15]

ثانياً: بطلان إجراءات التفتيش

يعرف الدكتور محمد نجم البطلان بانه "عدم ترتب الأثر القانوني الذي نصت عليه القاعدة الإجرائية، لان العمل الاجرائي لم يستكمل شروط صحته أو شكله أو صيغته أو الكيفية المنصوص عليها، فيصبح الاجراء وما يترتب عليه من إجراءات لا قيمة لها قانونياً.[16]

---

[9] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (1/39)

[10] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (2/39)

[11] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (3/39)

[12] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (6/40)

[13] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (41)

[14] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (43)

[15] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (50)

[16] محمد صبحي نجم: **أصول المحاكمات الجزائية**، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2000، ص381

وتنص المادة (474) من قانون الإجراءات الجزائية الفلسطيني (يعتبر الإجراء باطلاً إذا نص القانون صراحة على بطلانه أو إذا شابه عيب أدى إلى عدم تحقيق الغاية منه)، فالبطلان هو جزاء قانوني يترتب في حال عدم مراعاة الاحكام الواردة في القانون.

وقد نص قانون الإجراءات الجزائية الفلسطيني على البطلان في حال عدم مراعاة أي حكم من أحكام الفصل الواردة فيه قواعد التفتيش المنصوص عليها.[17]

يقسم الدفع بالبطلان إلى نوعين بطلان مطلق وبطلان نسبي، فالأول يتعلق بالنظام العام والآداب العامة ويجوز اثارته من قبل أي من الخصوم وفي أية مرحلة من مراحل الدعوى[18]، على النقيض من ذلك فأن البطلان النسبي لا يتعلق بالنظام العام والآداب ولا يجوز اثارته الا لمن شرع لمصلحته ما لم يكن قد تنازل عنه صراحة او ضمناً.[19]

ويترتب على بطلان الاجراء الذي يتعلق بالتفتيش، بموجب حكم صادر عن المحكمة، بطلان ما يترتب على هذا الاجراء من أدلة، ففي حالة حكم المحكمة ببطلان التفتيش، أصبحت الأدلة التي تم ضبطها باطلة أيضاً ولا يجوز الاستناد إلى هذه الأدلة في ادانة المتهم.[20]

لا يؤثر البطلان على بطلان الإجراءات السابقة عليه، أو الإجراءات اللاحقة له إذا لم تكن مبنية عليه.[21] وإذا كان الاجراء باطلاً في جزء وحده فأن هذا الجزء وحده الذي يبطل ويبقى الجزء الاخر نافذاً.

---

[17] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (52)

[18] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (475)

[19] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (476)

[20] مصطفى عبد الباقي: **شرح قانون الإجراءات الجزائية رقم (3) لسنة 2003 (دراسة مقارنة)**، جامعة بيرزيت، كلية الحقوق والإدارة العامة، وحدة البحث العلمي للنشر، بيرزيت، فلسطين، ص 256

[21] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (477)

فإذا كان الاجراء باطلاً جزئيا بطل الدليل المستمد من تلك الجزئية فقط، وكذلك فأن بطلان الاجراء لا يؤثر على الإجراءات السابقة عليه إذ تبقى هذه الإجراءات صحيحة ومنتجة لكافة اثارها القانونية، كما أن بطلان الإجراءات لا يمتد ليشمل الإجراءات اللاحقة له إذا لم تكن مبنية عليه فاذا كان الاجراء اللاحق بالتفتيش الباطل هو اعتراف المتهم فأن الاعتراف يعتبر باطلاً ايضاً وذلك في حالة كونه تابعاً للتفتيش وناجماً عنه، أما اذا كان هذا الاعتراف ليس له أي صلة بإجراءات التفتيش يبقى هذا الاعتراف مرتباً لكافة اثاره القانونية.[22]

ويرى الباحث أن البطلان يعتبر الجزاء القانوني المترتب عند عدم إتباع النصوص القانونية الإجرائية، وعليه ينعدم الأثر القانوني للإجراء، ويترتب على ذلك بطلان الدليل المستمد من إجراء التفتيش، وبناء على ذلك لا بد من مأمور الضبط القضائي المختص عند القيام بعملية التفتيش والبحث عن الأدلة إتباع الإجراءات القانونية المنصوص عليها في قانون الإجراءات الجزائية الفلسطيني والقرار بقانون بشأن الجرائم الإلكترونية وإلا أصبح هذا الدليل معرض لجزاء البطلان، وعليه سوف يدرس الباحث في المطلب القادم تعريف التفتيش القضائي في الجرائم الإلكترونية.

المطلب الثاني: التفتيش القضائي في الجرائم الإلكترونية

مع التطور التكنولوجي الواسع الذي جعل التكنولوجيا تدخل في جميع نواحي الحياة أدى ذلك إلى نشوء نوع جديد من الجرائم يسمى بالجرائم الإلكترونية واتسع نطاق الضابطة القضائية في التفتيش إلى تفتيش الأجهزة الإلكترونية والبيانات المخزنة على كافة طرق التخزين المعلوماتي من اجل الوصول إلى الحقيقة، واتسع نطاق الدليل الجنائي ليمتد إلى ما يسمى بالدليل الرقمي ومن هنا سوف يتحدث الباحث في هذا المطلب عن الجريمة الإلكترونية وتوضيح اقسامها ومن ثم تعريف التفتيش في الجرائم الإلكترونية.

---

[22] مصطفى عبد الباقي: **مرجع سابق**، ص 256

الفرع الأول: ماهية الجريمة الإلكترونية واقسامها

اتجه بعض الفقه إلى تعريف الجريمة الإلكترونية مستنداً إلى وسيلة ارتكابها فقد عرفها الفقيه تايدمان بأنها (كل اشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب).[23] والاتجاه الثاني يعتمد على وسيلة ارتكاب الجريمة ومحلها، فقد عرف كل من الفقيه جاك بولوجنا وروبرت لند كويست الجريمة الإلكترونية بأنها (الجريمة التي يُستخدم الحاسوب كوسيلة أو أداة لارتكابها أو يمثل اجراء ذلك، أو جريمة يكون الحاسوب نفسه ضحيتها)، وقد عرفها قاموس اوكسفورد على أنها (الجرائم التي ترتكب بواسطة الانترنت)[24]، وعرفت منظمة الأمم المتحدة الجريمة الإلكترونية في مؤتمرها العاشر لمنع الجريمة الذي عقد في فيينا في عام 2000م على أنها (أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكباها في بيئة الكترونية).[25] والمجرم الالكتروني هو ذلك الشخص الذي لديه مهارات تقنية او دراية بالتكتيك المستخدم في نظام الحاسب الالي والقادر على استخدام هذا التكتيك لاختراق الكود السري لتغيير المعلومات او لتقليد البرامج او التحويل من الحسابات عن طريق استخدام الحاسوب نفسه.[26]

وبعد توضيح مفهوم الجريمة الإلكترونية لا بد لنا من توضيح أصناف الجريمة الإلكترونية، فالجريمة الإلكترونية لها مفهوم عام وهو ما ذكرناه سابقا، فهناك العديد من التصنيفات للجريمة الإلكترونية فبعض الباحثين قسموها إلى خمسة اقسام والبعض الاخر إلى أربعة أقسام.[27] وقد اعتمد القرار بقانون بشأن الجرائم

---

[23] علي حسن طوالبة: **الجرائم الالكترونية**، البحرين، جامعة العلوم التطبيقية، كلية الحقوق، 2008 ص 74

[24] Mustafa Abdelbaqi (Ph.D.), **Enacting cybercrime legislation in an endeavour to counter cybercrime in Palestine**, Global Journal of Comparative Law 5 (pp.226-261),2016, p. 228

[25] رشاد خالد عمر: **المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية: دراسة تحليلية مقارنة**، المكتب الجامعي الحديث، الإسكندرية مصر، 2007، ص 25

[26] مصطفى محمد موسى: **التحقيق الجنائي في الجرائم الالكترونية**، ط1، دار الكتب القانونية، القاهرة، مصر، 2009، ص 143

[27] Mustafa Abdelbaqi (Ph. D), **Ibid**. p. 236.

الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في فلسطين وكذلك اتفاقية بودابست إلى تصنيف الجريمة الإلكترونية لأربعة طوائف وهذا ما سوف يعتمده الباحث.[28]

أولاً: الجرائم التي تمس خصوصية وسلامة وتوافر بيانات الحاسوب

وتتمثل هذه الجرائم في الاعتداء على خصوصية البيانات أو الاعتداء على أو سلامة هذه البيانات وتوفرها، كجريمة النفاذ غير المشروع والاعتراض غير المشروع والتدخل في البيانات حيث نظمها القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في نص المادة (4)، والتدخل في النظام وإساءة استخدام الحاسوب،[29] والتي نظمها القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في فلسطين وذلك في نصوص المواد (5-9) من ذات القرار، كما وردت هذه الجرائم في الفصل الأول من الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) في المواد (2-6)، ووردت ايضاً في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المواد (6-9).

ثانياً: الجرائم ذات صلة بالحاسوب

وتتمثل هذه الجرائم في ثلاثة اشكال وهي التزوير المرتبط بالكمبيوتر حسب نص المادة (11) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، والاحتيال المرتبط بالكمبيوتر وسرقة الهوية حسب نص المادة (14) من ذات القرار، كما وردت هذه الجرائم في الفصل الثاني من الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) في المادتين (7) و (8)، ووردت ايضاً في الاتفاقية العربية لمكافحة جرائم تنقية المعلومات في المادتين (10) و (11).

[28] التقرير التفسيري لاتفاقية بودابست المواد (2-10)

[29] Dr. Marco Gercke, **Understanding cybercrime: phenomena, challenges and legal response**, ITU, 2014, p. 17

ثالثاً: جرائم ذات صلة بالمحتوى

وتتثمل هذه الفئة من الجرائم بالمحتوى الذي يعتبر غير قانوني، بما في ذلك المواد الإباحية لأشخاص قاصرين حيث نظمها القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في نص المادة (16)، والمواد المعادية للأجانب أو الإهانات المتعلقة بالرموز الدينية وذلك في نص المادة (24) من ذات القرار.[30] كما وردت هذه الجرائم في الفصل الثالث من الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) في المادة (8)، ووردت ايضاً في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المواد (12-14).

رابعاً: الجرائم المتعقلة بحقوق النشر والتأليف والحقوق الأخرى ذات الصلة

ومنها الاعتداء على حقوق الملكية الفكرية، وتتمثل في الاعتداء على حقوق التأليف وبراءة الاختراع والعلامات التجارية حيث نظمها القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في فلسطين في نص المادة (20).[31] كما وردت هذه الجرائم في الفصل الرابع من الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) في المادة (10)، ووردت ايضاً في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة (17).

ومن الواضح أعلاه أن الجريمة الإلكترونية تعتبر كباقي الجرائم حيث تتكون من عدة أركان، تتمثل في ركن مادي وهو الفعل فمثلاً قيام الجاني بالدخول إلى أنظمة الحاسوب والعبث بها في جريمة الاختراق، إضافة إلى النتيجة والعلاقة السببية فيجب أن يكون هناك علاقة الفعل والنتيجة التي حصلت، إضافة الركن المعنوي والذي يتمثل في نية الجاني بارتكاب هذا الفعل واحداث أثر معين يمس في سلامة امن المعلومات

[30] Dr. Marco Gercke, **Ibid**, p. 22
[31] Mustafa Abdelbaqi (Ph. D), **Ibid**. p. 258

او خصوصية الافراد إضافة إلى الركن القانوني وهو وجود قانون يجرم هذا الفعل وتعتبر الجريمة الإلكترونية في هذه الحالة جريمة مكتملة الأركان، وردعها يكون من اختصاص السلطة القضائية.

الفرع الثاني: التفتيش القضائي والضبط في الجرائم الإلكترونية

يعرف التحقيق الجنائي في الجرائم الإلكترونية على أنه عمل قانوني يقوم به مأمور الضبط القضائي المختص بتفويض من النيابة العامة لضبط الجرائم الإلكترونية الرقمية من فاعل ودليل الكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل.[32]

ومن وجهة نظر الباحث يمكن تعريف التفتيش في الجرائم الإلكترونية بأنه ذلك الاجراء الذي تقوم به النيابة العامة أو الضابطة القضائية بتفتيش أجهزة الحاسوب الرقمي وشبكة المعلومات وذلك بحثاً عن ادلة تدين ارتكاب الفعل الجرمي المسند إلى المتهم. أما الضبط فيعني العثور على أدلة في الجريمة والتي يباشر التحقيق بشأنها والتحفظ عليها، فالضبط هو الغاية من التفتيش والنتيجة المباشرة والمستهدفة له.

ومن هنا يرى الباحث انه لا يجوز الخلط بين التفتيش والضبط فالتفتيش هو البحث في مستودع سر المتهم من اجل العثور على ادلة تفيد ارتكاب الجرم المنشود او تدين المتهم، وكما ذكرنا سابقاً فأنه تكون وفقاً لإجراءات قانونية وشروط قانونية اختلالها يؤدي إلى بطلان التفتيش، اما الضبط هو النتيجة المترتبة على عملية التفتيش والتي تتثمل في تحريز الدليل والتحفظ عليه من اجل مباشرة التحقيق في الجريمة، وسوف يقوم الباحث بتوضيح الدليل الرقمي بشكل مفصل وإجراءات ضبطه وكيفية تحريزه فيما بعد.

---

[32] مصطفى محمد موسى: **مرجع سابق**، ص 166

المبحث الثاني

مدى صلاحية نظم الحاسوب والانترنت للتفتيش

من اجل دراسة مدى صلاحية نظم الحاسوب والانترنت للتفتيش الجنائي لا بد من دراسة ماهية نظم الحاسوب والانترنت وذلك من خلال توضيح مصطلح الحاسوب وبيان الكيانات التي يتكون منها، ومن هذا المنطلق خصص الباحث المطلب الأول لدراسة عناصر الحاسوب التي تكون محلاً للتفيش والمطلب الثاني عن مدى خضوع مكونات الحاسوب المعنوية والمادية للتفتيش.

المطلب الأول: عناصر الحاسوب محل التفتيش

من اجل توضيح العناصر التي يتشكل منها الحاسوب وتكون محلاً للتفتيش القضائي في الجرائم الإلكترونية لا بد من تعريف الحاسوب، وعليه فتعني عبارة الحاسب الالي ذلك الجهاز الذي يقبل، يعالج، يخزن، يسترجع أو ينتج بيانات محوسبة.[33]

ويعرف ايضاً على انه جهاز الكتروني يتكون من مجموعة من الأجهزة أو الوحدات التي تعمل بصورة متكاملة مع بعضها بعضاً بهدف تشغيل مجموعة البيانات الداخلة طبقاً لبرنامج محدد تم وضعه مسبقاً للحصول على نتائج معينة.[34]

وقد عرفت الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) منظومة الكمبيوتر بأنها " أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها، أو أكثر وفقاً لبرنامج، بالمعالجة الآلية للبيانات.[35]

---

[33] محمد الأمين البشري: **التحقيق في جرائم الحاسب الآلي والانترنت**، جامعة نايف العربية للعلوم الأمنية، المجلة العربية للدارسات الأمنية، مج 15، عدد 30، ص ص.317-380، ص 322

[34] محمد طوالبة: **مرجع سابق**، ص 16

[35] التقرير التفسيري لاتفاقية بودابست، المادة (1)

وعليه يتكون الحاسوب من مكونات مادية (Hardware) وهي مجموعة من الوحدات التي تتصل مع بعضها بعضاً بشكل يجعلها تعمل كنظام متكامل مثل لوحة المفاتيح والشاشة وغيرها.[36] ومكونات معنوية (Software) وهي البيانات المخزنة على ذاكرة الحاسوب، وسوف ندرس كل مها على حدة في فرعين، الفرع الأول نخصصه لدراسة المكونات المادية للحاسوب والفرع الثاني لدراسة المكونات المعنوية للحاسوب.

الفرع الأول: المكونات المادية للحاسوب الالي وعناصرها

تعرف المكونات المادية للحاسب الآلي بأنها الأجزاء الملموسة أو المادية لجهاز الحاسوب،[37] بمعنى آخر هو جهاز الحاسب نفسه، وهو عبارة عن مجموعة من الدوائر الإلكترونية مع بعض القطع الملحقة والتي تكون موجودة في صندوق مع بعض الأجهزة الأساسية التي تستخدمها مثل الشاشة ولوحة المفاتيح والفأرة.[38]

وتقسم المكونات المادية للحاسوب من حيث الوظيفة إلى عدة اقسام (وحدة المعالجة المركزية، وحدات الادخال، وحدات الإخراج، وحدة التخزين الرئيسة، وحدة التخزين الثانوية).[39]

اولاً: وحدات المعالجة المركزية (Central Processing Unit)

وينصب دور هذه الوحدة على تلقي الأوامر عن طريق أجزاء الادخال ثم معالجتها واخراجها بالكيفية التي يرغبها مشغل الجهاز، حتى لو كان الفاعل مجرماً معلوماتياً، فجهاز الحاسوب يتعامل مع معلومة أو بيان بصرف النظر عن الشخص الذي يتولى تشغيل الجهاز أو يطلب البيان.[40]

---

[36] خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، دار الثقافة للنشر، عمان، الأردن، ص 158

[37] Thomas Holt, Adam Bossler, Kathryn Seigfried-Spellar, **Cybercrime and Digital Forensics an Introduction**, Second Edition, published by Routledge, NYC, USA 2018, p. 509

[38] ثوار ثابت عارف، **اساسيات تكنولوجيا الحاسب**، ط1، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2005، ص 24

[39] عطا الله احمد الحسبان، **نظم المعلومات المحاسبية**، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2013، ص 4

[40] عبد الفتاح بيوم حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، ط1، دار الفكر الجامعي، الإسكندرية، مصر 2006، ص 62

ويرى الباحث ان وحدة المعالجة المركزية تمثل العقل المدبر لاي نظام تكنولوجي او محوسب فهي التي تقوم بمعالجة البيانات وقراءتها وتحليل الشيفرة الخاصة بها ومن اجل ان تقوم بعملها بصورة صحيحة يجب ان يحتوي جهاز الحاسوب على وحدات تخزين عشوائية ورئيسة.

ثانياً: وحدة التخزين الرئيسة أو العشوائية (Random Access Memory)

تستخدم هذه الذاكرة لتخزين البرامج والبيانات الواقعة تحت عملية المعالجة، ويعني ذلك ان محتويات هذه الذاكرة متغيرة طيلة فترة الاستخدام وذلك بناء على العمليات المحوسبة التي يقوم بها المستخدم، وتفقد هذه الذاكرة محتوياتها عند اقفال الجهاز عن جهاز الحاسوب، ولذلك على القائم بعملية تفتيش جهاز الحاسب الآلي ان ينتبه إلى هذه المسألة كي لا يفقد الملفات والمعلومات الموجودة على هذه الذاكرة.[41]

ثالثاً: وحدة التخزين الثانوية (Secondary storage unit)

وهي تلك التي تستخدم من اجل تخزين البيانات والاوامر عندما لا تستخدم في عملية المعالجة المركزية، ومنها القرص الصلب (Hard disk) والذي يخزن البيانات والملفات المحوسبة بشكل دائم ولا تفقد هذه الوحدة الملفات المخزنة عليها عند اقفال الجهاز الا انها بحاجة إلى خصوصية محددة في حالة ضبطها وهذا ما سوف نوضحه في ضبط الأدلة الإلكترونية لاحقاً.

رابعاً: وحدات الادخال (Input units)

وهي تلك الوحدات التي تعمل على تحويل البيانات إلى شكل الكتروني مناسب بحيث يمكن ان يتعامل الحاسوب معها ومن هذه الوسائل لوحة المفاتيح والفأرة ومشغل الاقراص والماسح الضوئي ومسجل الصوتيات وشاشة اللمس.[42]

---

[41] محمد طوالبة، **مرجع سابق** ص 19

[42] عطا الله احمد الحسبان، **مرجع سابق** ص 7

خامساً: وحدات الإخراج (Output device)

وظيفة هذه الوحدات استقبال البيانات وتمريرها إلى المستخدم بالصيغة المناسبة ومن اهم هذه الوحدات (الشاشة، الطابعة، مشغل الأقراص، وسائل الإخراج الصوتية وغيرها).[43] إن وسائل الإخراج هذه تلعب دوراً مهماً بحيث تشكل جزأ لا يتجزأ من المنظومة الحاسوبية وفي نظر الباحث تشكل هذه الوسائل المخرجات النهائية في حال ارتكاب جريمة الكترونية، فمثلا في جريمة تزوير الأموال تستخدم الشاشات الدقيقة والمعالجات فائقة السرعة من اجل تصميم نموذج عملة مثلاً، وتستخدم الطابعات المتخصصة لطابعة مثل هذه التصميمات.

الفرع الثاني: المكونات المعنوية للحاسوب الالي

هي مجموعة من الأوامر والتعليمات التي تعد بواسطة المبرمجين لعمل توافق بين المستخدم والحاسوب، سواء كانت على شكل نظام تشغيل أو برمجيات جاهزة.[44]وتعرف أيضاً على أنها برامج تتضمن تعليمات محددة تؤدي جهاز الحاسوب للقيام بمهام معينة.[45]

وقد عرف القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته البيانات والمعلومات الإلكترونية بأنها "كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو توريده أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات، وغيرها".[46]

---

[43] عطا الله احمد الحسبان **مرجع سابق**، ص 8

[44] محمود الهواس، حيدر البرزنجي: **تكنولوجيا وأنظمة المعلومات في المنظمات المعاصرة**، دار الكتب والوثائق الوطنية، بغداد، العراق، 2014، ص 122

[45] Thomas Holt, Adam Bossler, Kathryn Seigfried-Spellar, **Ibid**, p. 509

[46] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (1)

وقد عرفت الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) بيانات الحاسوب بأنها " أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الحاسوب، بما في ذلك برنامج مناسب يساعد نظام الحاسوب في أداء وظيفة معينة.[47]

وبناءً على ما ورد أعلاه من تعريفات للكيانات المعنوية يرى الباحث بأن الكيانات المعنوية للحاسوب الالي يمكن تقسيمها إلى قسمين رئيسين (برامج النظام الأساسية، البرامج الجاهزة أو التطبيقية).

أولاً: برامج النظام

هي برامج مرتبطة بنظام التشغيل وتمثل مجموعة من برامج الحاسوب التي تدير موارد الحاسوب وتسيطر على وحدة المعالجة المركزية ومعداتها الملحقة بها، وتعمل برامج النظام كجهة وسيطة بين البرامج التطبيقية الأخرى والأجهزة المادية للحاسوب.[48]

ومن أمثلتها نظام التشغيل ويندوز (Windows) أو نظام التشغيل الماك (Mac OS) أو نظام التشغيل لِينُكس (Linux)، وتأتي هذه الأنظمة محملة على الحاسوب وتعتبر هذه الأنظمة جزأً لا يتجزأ منه.

ثانياً: برامج التطبيقات

تطورت هذه البرامج بعد تطور الحواسيب وتنوعها إذ تتميز بسهولة استخدامها فضلاً عن انتشارها في جميع مستويات المعرفة الإنسانية، وازداد الطلب على هذه البرمجيات في الآونة الأخيرة، وظهرت شركات خاصة بإنتاج البرمجيات الجاهزة والمصممة لإنجاز تطبيقات متنوعة ومختلفة حسب الاتجاه والتخصص، ويمكن

---

[47] التقرير التفسيري لاتفاقية بودابست المادة (1)

[48] عطا الله احمد الحسبان، **مرجع سابق**، ص 8

تخزين هذه البرامج في الحاسوب على شكل ملفات قابلة للتنفيذ والتشغيل.[49] ومن امثلتها برامج (Microsoft office).

ويكمن الفرق بين برنامج التطبيقات وبرامج النظام بأن نظام التشغيل (Windows) مثلا هو نظام يعمل كواجهة بين المستخدم والأجهزة ويسيطر على جميع العلميات داخل وحدة المعالجة المركزية على عكس برنامج التطبيق (Microsoft office) والذي يقوم بأداء مهمة محددة فقط تتمثل في طباعة النصوص وتخزينها.[50] ولا شك بأن هذه البرامج بمختلف أنواعها هي بحاجة إلى الحماية القانونية كونها تمس مباشرة بحياة الأشخاص او أنشطة المؤسسات حفاظاً على سرية ما يتم تداوله من معلومات بواسطة هذه البرامج.

المطلب الثاني: مدى صلاحية المكونات المادية والمعنوية للتفتيش

كون التفتيش هو البحث عن المكونات المادية المتعلقة بالجريمة المرتكبة والتي تفيد كشف الحقيقة فانه يجب لمعرفة مدى انطباق هذا المفهوم على نظم الحاسوب والبيانات المحوسبة أن نفرق بين التفتيش الذي يقع على المكونات المادية للحاسوب وبين التفتيش الذي يتم البحث فيه داخل وسائل التقنيات الحديثة والبيانات المحسوبة، فالأول يتم البحث عن جهاز الكمبيوتر ذاته وهو الكيان المادي فلا توجد صعوبة عند معاينة القائمين على التفتيش لمسرح الجريمة الواقعة على المكونات المادية للحاسوب[51]. أما بالنسبة للحالة للثانية وهي البحث عن المكونات المعنوية والتفتيش داخل أنظمة الحاسوب المعنوية فقد انقسم الفقه في هذه الحالة إلى قسمين منهم من اعتبر ان الكيانات المعنوية للحاسوب لا تصلح لان تكون محلا للتفيش

---

[49] محمود الهواس، حيدر البرزنجي: **مرجع سابق**، ص 135

[50] (مرجع الكتروني) (https://ar.strephonsays.com/difference-between-operating-system-and-application-software) تاريخ اخر زيارة (10/12/2022)

[51] خالد الحلبي، **مرجع سابق، ص** 158

الجنائي ومنهم من قال بأنها تعتبر مثلها مثل أي كيان مادي ملموس يصلح للتفيش الجنائي وسوف ندرس ذلك في فرعين.

الفرع الأول: مدى صلاحية المكونات المادية للحاسوب للتفيش

يكون التفتيش في هذه الحالة على معدات الحاسب الالي وملحقاته مثل الكابلات وشاشة العرض الخاصة به، مفاتيح التشغيل والطابعات وغيرها.[52] ولا يوجد صعوبة عند معاينة مسرح الجريمة وذلك لان مسرح الجريمة يحتوي على الأدلة المادية، والتي تدل دلالة واضحة على وقوع الجريمة ونسبتها إلى شخص معين.[53]

وعليه اتجهت اغلب التشريعات المقارنة إلى إمكانية تفتيش المكونات المادية دون أي إشكالية ولا بد من أن نستعرض بعضها إضافة لموقف المشرع الفلسطيني.

وقد اتجه القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته على تفتيش الأجهزة والأدوات التي لها علاقة بالجريمة وضبطها فقد نص في المادة (52) "إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها".[54]

---

[52] عبد الفتاح بيوم حجازي، **مرجع سابق**، ص 194

[53] خالد الحلبي، **مرجع سابق، ص** 159

[54] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته المادة (3/52)

وكذلك فأن الاتفاقية الأوروبية للجريمة الإلكترونية (بودابست) اتجهت بأن تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير بغية تمكين سلطاتها المختصة من البحث عن أي دعامة تخزين يمكن ان تكون بيانات الكمبيوتر مخزنة داخلها.[55]

ويرى الباحث استناداً إلى النص القانوني أعلاه أن المشرع الفلسطيني اتجه إلى جواز تفتيش المكونات المادية للحاسوب الآلي وضبط الأدوات والوسائل التقنية التي لها صلة بالجريمة الإلكترونية. وهذا ما أتجه اليه المشرع الأردني،[56] والمشرع المصري[57].

الفرع الثاني: مدى صلاحية المكونات المعنوية للحاسوب للتفيش

إن كون المكونات المادية للحاسوب محل اتفاق فقهي بجوازيه تفتيشها، فإن الخلاف قد ظهر فيما يتعلق بالمكونات والأدلة المعنوية التي يحتويها الحاسب الآلي، فقد انقسم الفقه في هذه المسألة إلى تيارين رئيسين من المهم أن نبينها، فقد اتجه التيار الأول بعدم جواز اخضاع المكونات المعنوية للحاسوب إلى التفتيش القضائي بينما اتجه التيار الاخر إلى إمكانية اخضعاها للتفيش القضائي وسوف نعرض كل منها على حدة إضافة إلى موقف التشريع الفلسطيني من هذه الاتجاهات.[58]

---

[55] التقرير التفسيري لاتفاقية بودابست لمكافحة الجريمة الالكترونية المادة (1/19/ب)

[56] اتجه المشرع الأردني في تفتيش المكونات المادية للحاسوب الى ذات الاتجاه التي اتجه اليه المشرع الفلسطيني، فقد نصت المادة (13) من قانون الجرائم الالكترونية على انه" ... يجوز لموظف الضابطة العدلية بعد حصوله على موافقة المدعي العام أو المحكمة المختصة الدخول إلى أي مكان تشير الدلائل إلى استخدامه في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج...".

[57] كذلك حذا المشرع المصري الى إمكانية تفتيش المكونات المادية للحاسوب فقد نص قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على انه لجهات الضبط القضائي أن تصدر امراً بسحب أي دعامة أو حاسب تكون الأدلة الالكترونية موجودة فيها.

[58] احمد أسامة كامل، **التفتيش في الجرائم الالكترونية في التشريع الفلسطيني: دراسة تحليلية مقارنة بالتشريع العماني**، مجلة جيل الأبحاث القانونية المعمقة، عدد 28، 2018، ص ص. 11-38، ص 21

أولاً: الاتجاه الرافض بجواز تفتيش المكونات المعنوية للحاسوب

ذهب أنصار هذا الاتجاه للقول بعدم صلاحية اجراء التفتيش والضبط على برامج وبيانات الحاسب الآلي باعتباره وسيلة للإثبات المادي يهدف لضبط ادلة مادية تتعلق بالجريمة وتفيد كشف الحقيقة، وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسوب الآلي.[59] فهناك من يرى انه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم لا ينطبق على بيانات الحاسب الآلي غير المحوسبة والمحوسبة.[60]

ومن أنصار هذا الاتجاه جانب من الفقه الفرنسي الذي يرى أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تعد شيئاً مادياً بالمعنى المصطلح، وعليه يرى هذا الجانب من الفقه ضرورة أن يضاف للغاية التقليدية للتفيش عبارة البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب.[61]

ثانياً: الاتجاه المؤيد بجواز تفتيش المكونات المعنوية للحاسوب

يرى أنصار هذا الاتجاه بأن المعلومات التي لا تعد شيئاً مادياً وإنما هي ذات طبيعية معنوية، أي مجرد ذبذبات ونبضات الكترونية أو إشارات أو موجات كهرومغناطيسية، إلا أنها قابلة للتخزين في أوعية ووسائط مادية، كالأقراص والاشرطة الممغنطة، بالتالي فهي ليست شيئاً معنوياً بل هي أشياء مادية محسوسة لها وجود ملموس في العالم الخارجي، لذلك يصح أن يرد عليها التفتيش والضبط.[62]

---

[59] احمد براك: **الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية تأصيلية مقارنة**، ط1، دار الشروق، رام الله، 2019، ص 346

[60] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 379

[61] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 380

[62] احمد براك، **مرجع سابق**، ص 365

إن اغلب التشريعات الحديثة اتجهت إلى التأكيد على هذا الاتجاه بحيث أصبحت مكونات الحاسوب المعنوية محلاً للتفتيش والضبط القضائي، ففي الولايات المتحدة مثلاً جرى تعديل القاعدة رقم (34) وهي من القواعد الخاصة بالإجراءات الجنائية عام 1970 لتصبح تنص على السماح بإمكانية تفتيش الكمبيوتر والكشف عن الوسائط الإلكترونية بما في ذلك البريد الالكتروني والبريد الصوتي.[63]

ثالثاً: موقف المشرع الفلسطيني والقوانين المقارنة

وقد نص القرار بقانون بشأن الجرائم الإلكترونية في فلسطين على تفتيش مكونات الحاسب المعنوية فقد أجاز لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات.[64]

وكذلك اتجه المشرع الأردني ذات الاتجاه الذي اتجه اليه المشرع الفلسطيني في تفتيش المكونات المعنوية للحاسوب.[65] وكذلك المشرع المصري في قانون مكافحة جرائم تقنية المعلومات.[66]

وكذلك فأن الاتفاقية الأوروبية للجريمة الإلكترونية (بودابست) اتجهت بأن تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير بغية تمكين سلطاتها المختصة من البحث عن او النفاذ إلى أي نظام كمبيوتر أو أي جزء منه وبيانات الكمبيوتر المخزنة فيه.[67]

---

[63] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 380

[64] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (4/32)

[65] فقد نص قانون الجرائم الالكترونية على انه" ... يجوز لموظف الضابطة العدلية بعد حصوله على موافقة المدعي العام أو المحكمة المختصة الدخول إلى أي مكان تشير الدلائل إلى استخدامه في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم...".

[66] قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، المادة (6) ""لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمرًا مسببًا، لمأموري الضبط القضائي المختصين... ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها في أي مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه".

[67] التقرير التفسيري لاتفاقية بودابست لمكافحة الجريمة الالكترونية، المادة (1/19/أ)

الفصل الأول

الدليل الالكتروني في مجال الاثبات الجنائي

بعد أن قام الباحث بتوضيح ماهية الجريمة الإلكترونية والعناصر المعنوية والمادية التي يتشكل منها الحاسوب، وعليه يتسنى له دراسة الدليل الالكتروني في مجال الاثبات الجنائي، وقد رأى الباحث تقسيم هذا الفصل إلى ثلاثة مباحث من المهم لنا أن نتناولها، في المبحث الأول سوف يدرس الباحث ماهية الدليل الالكتروني في مجال الاثبات الجنائي وخصائصه، ومن ثم سوف يتطرق في المبحث الثاني إلى بيان الطبيعة القانونية للدليل الالكتروني، وأخيراً في المبحث الثالث سوف يدرس الباحث مسرح الجريمة الالكتروني وأدوات الاثبات في الجرائم الإلكترونية.

المبحث الأول

ماهية الدليل الالكتروني في مجال الاثبات الجنائي وخصائصه

تعتبر الأدلة الجنائية بمثابة الوسيلة التي تعتمد عليها النيابة العامة والضابطة القضائية في الاثبات الجنائي من أجل التوصل إلى الحقيقة وتحقيق العدالة في المجتمع، ويعرف الدليل الجنائي على أنه معنى يدرك من مضمون واقعة تؤدي إلى ثبوت البراءة أو ثبوت الإدانة، ويتم ذلك باستخدام الأسلوب العقلي وإعمال المنطق في وزن وتقدير تلك الواقعة، ليصبح المعنى المستمد منها أكثر دقة في الدلالة على الإدانة أو البراءة[68]. ونتيجة التطور السريع لتكنولوجيا المعلومات فقد ظهرت طائفة جديدة من الأدلة، وقد قسم الباحث هذا المبحث إلى مطلبين في المطلب الأول سوف يقوم بتعريف الدليل الرقمي وفي المطلب الثاني يقوم ببيان خصائص الدليل الرقمي في مجال الاثبات الجنائي.

---

[68] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 85

المطلب الأول: تعريف الدليل الالكتروني في مجال الاثبات الجنائي

اعتبر الفقه الجنائي الأدلة الجنائية الرقمية بأنها تلك التي تشتمل على جميع البيانات الإلكترونية أو الرقمية التي يمكن أن تثبت وجود ووقوع الجريمة، أو تُوجد علاقة بين الجريمة المرتكبة والجاني أو تُوجد علاقة بين الجريمة والضحية، ويقصد بالبيانات الرقمية مجموعة الأرقام التي تمثل المعلومات الرقمية المختلفة وذلك على شكل رسومات ونصوص مكتوبة أو الصوت أو الصورة.[69] وقد عرف القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته البيانات والمعلومات الإلكترونية بأنها كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو توريده أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات وغيرها.[70]

ويعرف الدليل الالكتروني ايضاً بأنه الدليل الذي يجد أساساً له في العالم الافتراضي ويقود إلى الجريمة، فهو كل بيانات يمكن اعدادها أو تخزينها بشكل الكتروني بحيث تمكن الحاسوب من انجاز مهمة ما".[71]

وقد عرفته المنظمة العالمية لدليل الكمبيوتر (IOCE) في أكتوبر 2001 بأنه المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية والتي يمكن اعتمادها في المحكمة.[72]

وجاء في تعريف الدليل الرقمي بأنه الدليل المأخوذ من أجهزة الكمبيوتر على شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجيا وهي مكون رقمي

---

[69] رشيد بن فريحة، **التحري الجنائي في مسرح الجريمة المعلوماتية**، مجلة جامعة القدس المفتوحة للبحوث والمعلومات الاجتماعية، عدد 42، ص ص. 52-6-،2017، ص 54

[70] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (1)

[71] خالد عياد الحلبي، **مرجع سابق**، ص 229

[72] مصطفى ممد موسى، التحقيق في الجرائم الالكترونية، **مرجع سابق**، ص 213

لتقديم معلومات في اشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الاشكال والرسوم وذلك من أجل اعتماده أمام أجهزة انفاذ القانون.[73]

وعليه يرى الباحث أن الدليل الالكتروني يتشكل من مجموعة من البيانات والمعلومات الرقمية والتي يمكن تخزينها أو قراءتها أو معالجتها باستخدام أنظمة الحاسوب المختلفة ومن المهم في هذه الحالة توضيح ما هو المقصود بالبيانات التي نصت عليها التعريفات السابقة وأشكال الدليل الرقمي.

ومن أجل التعرف على الدليل الرقمي لا بد من توضيح أنواع وأشكال الدليل الرقمي حيث تكمن أهمية ذلك في بيان الهيئة التي يكون عليها الدليل الرقمي ومن هذا المنطلق يمكن ذلك الباحث من الحكم على القيمة القانونية للدليل الرقمي فيما بعد.[74]

الفرع الأول: أنوع الدليل الالكتروني من حيث الاثبات

تقسم الأدلة الرقمية من حيث الاثبات الجنائي إلى قسمين رئيسيين (أدلة مرتبطة بوظائف الجهاز الرقمي وهي الأدلة التي اعدت لتكون وسيلة اثبات، وأدلة مرتبطة بسلوك المجرم وهي التي لم تعد لتكون وسيلة اثبات)[75].

اولاً: أدلة مرتبطة بوظائف الجهاز الرقمي

وهو ذلك النوع من الأدلة التي تكون في الغالب اعدت لتكون وسيلة اثبات ويمكن اجمال هذا النوع من الأدلة فيما يلي:

---

[73] توفيق خشاشنة، **مسرح الجريمة ومعاينته عبر شبكة المعلومات الدولية**، دار الثقافة للنشر والتوزيع، ط1، 2020، عمان، الأردن، ص 278

[74] توفيق خشاشنة، **مرجع سابق**، ص 286

[75] مسعود بن حميدي المعمري، **الدليل الالكتروني لأثبات الجريمة الالكترونية**، مجلة كلية القانون الكويتية العالمية، مجلد 6 ملحق، ص ص. 189–253، 2018، ص 202

1- السجلات والبيانات التي تم انشائها بواسطة الآلة تلقائياً، حيث تعتبر هذه البيانات من مخرجات الالة نفسها والتي لم يساهم الانسان في انشائها مباشرة مثل ملفات الدخول التي يتم حفظ جميع التغيرات التي تحصل في قاعدة البيانات (log files) أو ملفات تعريف الارتباط الخاصة بالمتصفحات.[76]

2- السجلات التي تم حفظ جزء منها بالإدخال وجزء تم انشاؤه بواسطة الحاسوب، ومن امثلتها رسائل البريد الالكتروني حيث يقوم الشخص بكتابة محتوى الرسالة الإلكترونية ويقوم الحاسوب بإكمال بعض البيانات مثل توقيت الارسال والاستلام وحفظها في البريد المرسل.[77] وكذلك ايضاً لو قام شخص بإدخال بيانات معينة مثلاً وطلب من الحاسوب معالجة البيانات.

ثانياً: أدلة مرتبطة بسلوك المجرم

وهذا النوع من الأدلة نشأ دون إرادة الشخص الجاني وغالباً ما يكون هذا الدليل الالكتروني بسهو الجاني وذلك عن طريق أثر يتركه الجاني في الجهاز الرقمي يدل على ارتكابه للجريمة المقصودة، فهناك العديد من العمليات التي يقوم بها الفاعل أثناء ارتكابه للجريمة المعلوماتية واستخدام الأجهزة الرقمية يمكن تحليلها والتوصل إلى سلوكيات الفاعل عن طريقا، ويسمى ايضاً هذا النوع من الأدلة بالآثار المعلوماتية الرقمية والتي يتركها المستخدم بسبب تسجيل الرسائل التي يرسلها أو يستقبلها، وفي الغالب هذا النوع من الأدلة لم تُعد لتكون وسيلة اثبات.[78]

فهذا الدليل الالكتروني في الأصل لم يعد من أجل الحفظ من قبل الشخص المستخدم لشبكة الحاسوب، أو الجهاز المستخدم من قبل الفاعل، فالفاعل في الجريمة المعلوماتية لم يخطط مسبقاً لترك الأثر، الا أن أجهزة الحاسوب تقوم بحفظ هذا النوع من الأدلة من تلقاء نفسها، وعليه فإن كافة العمليات التي تم إجراؤها

---

[76] توفيق خشاشنة، **مرجع سابق**، ص 287

[77] مسعود بن حميدي، **مرجع سابق**، ص 202

[78] توفيق خشاشنة، **مرجع سابق**، 288

من قبل المستخدم على جهاز الحاسوب يمكن ضبطها كأدلة من قبل المختصين أو بواسطة التقيات والبرامج اللازمة لذلك عند الحاجة لذلك.[79]

ثالثاً: التمييز بين الأدلة المرتبطة بوظائف الجهاز الرقمي والأدلة المرتبطة بسلوك المجرم

إن الطبيعة الخاصة لهذه الأنواع من الأدلة أظهرت حاجة للتميز بينها فيما يلي:

1- إن الأدلة المرتبطة بسلوك المجرم تعتبر أهم من الأدلة المرتبطة بوظائف الجهاز الرقمي والسبب في ذلك أن المعلومات والبيانات الرقمية التي تربط بين الجريمة الإلكترونية ومرتكبها لم تعد اصلاً لان تكون أثراً لمن صدر عنه الفعل.[80]

2- إن الأدلة المرتبطة بوظائف الجهاز الرقمي تتميز بسهولة الحصول عليها، لأنها اعدت اصلاً لتكون أدلة اثبات على الوقائع التي تتضمنها، أما الأدلة المرتبطة بسلوك المجرم فيتم الحصول عليها بإتباع الأساليب التقنية الخاصة.[81]

3- الأدلة المرتبطة بوظائف الجهاز الرقمي نسبة ضياعها قليلة مقارنة بالأدلة المرتبطة بسلوك المجرم؛ وذلك كون هذه الأدلة اعدت بذاتها لتكون وسيلة اثبات، على العكس من ذلك فإن الادلة المرتبطة بسلوك المجرم غير معدة للحفظ أساساً فهي معرضة للفقدان أو الاندثار لأبسط الأسباب.[82]

ومن منطلق التمييز بين هذين النوعين من الأدلة والطبيعة الخاصة بكل نوع تنعكس على قيمته الاثباتية، فمثلاً هذه الادلة ليست على درجة واحدة من القوة والقبول أمام المحاكم الامريكية.[83]

---

[79] مسعود بن حميدي، **مرجع سابق**، 203ص

[80] توفيق خشاشنة، **مرجع سابق**، ص 288

[81] مسعود بن حميدي، **مرجع سابق**، 203

[82] توفيق خشاشنة، **مرجع سابق**، 288

[83] عائشة بن قارة مصطفى، **حجية الدليل الالكتروني في مجال الاثبات الجنائي**، دار الجامعة الجديدة، ط1، الإسكندرية، مصر، 2010، ص 76

وعليه، يرى الباحث أن هذا التقسيم للأدلة الإلكترونية له أهمية كونه يساعد النيابة العامة والضابطة القضائية في اتخاذ الإجراءات والتدابير اللازمة عند التعامل مع هذه الأدلة بناء على خصائص وميزات كل منها، ويقلل من فرصة فقدان الدليل الالكتروني أثناء عملية التفتيش، فمن المهم التعامل مع هذه الأدلة بناء على الطبيعة الخاصة لكل منها وسوف يوضح الباحث ذلك لاحقاً ان شاء الله.

الفرع الثاني: أشكال الدليل الالكتروني

تتخذ الأدلة الإلكترونية عدة أشكال، وتقسم إلى قسمين الأدلة المادية التي لها قيمتها في الاثبات الجنائي الالكتروني وهي تتميز بطبيعة خاصة، إلى جانب تعلقها بالجرائم الإلكترونية بشكل رئيسي، والقسم الاخر من الأدلة هي الأدلة الرقمية التي لها قيمتها في مجال الاثبات الجنائي الالكتروني.

أولاً: ادلة مادية لها قيمتها في الاثبات الجنائي بالجرائم الإلكترونية

1- الأوراق: يحتفظ جهاز الحاسوب الالي بكم هائل من الأوراق والمستندات والتي قد يقوم الجاني بطباعتها، وتكون هذه الاوراق لها قيمة مهمة في الاثبات الجنائي الالكتروني لاحتوائها على بيانات رقمية أراد الجاني طباعتها للتأكد من تنسيق المستند.[84]

2- الأقراص الصلبة الأقراص المرنة: يعرف القرص الصلب بأنه وحدة التخزين الرئيسية في الحاسوب، فهو ثابت ومستديم داخل الحاسوب، اما عن القرص المرن فهو وسيط لتخزين البيانات يتألف من قطعة دائرية رفيعة مرنة ويكون منفصلا عن الحاسوب ويتم إدخاله واخراجه حسب الحاجة. وتعتبر الأقراص من أهم الأدلة الإلكترونية كونها تحتوي على البيانات والملفات وكلمات المرور والتقارير وخطط ارتكاب الجريمة.[85]

---

[84] بيومي حجازي، **مرجع سابق**، ص 60

[85] مسعود بن فريحة، **مرجع سابق**، ص 55

3- أجهزة المودم: تستخدم في نقل البيانات والمعلومات وتستخدم بعض هذه الأجهزة كجهاز رد على المكالمات الهاتفية مما يجعلها دليل محتمل بالغ الأهمية.[86]

4- الكروت والبطاقات الممغنطة: وهي عادة ما تكون ذات طبيعة خاصة وبحاجة إلى تقنية خاصة من أجل التعامل معها كالبطاقات البنكية والتي يمكن من خلالها رصد جميع تحركات الجاني المالية.

5- ملحقات الحاسوب: ومنها الفأرة ولوحة المفاتيح والشاشة وذواكر التخزين (الفلاشات) والتي يمكن ضبطها واعتبارها من الأدلة الإلكترونية.

ثانياً: الأدلة الرقمية التي لها قيمتها في الاثبات الجنائي

تتمثل الأدلة الرقمية بالبيانات والمعلومات المخزنة على ذاكرة الحاسوب وهي تلك النبضات الكهرومغناطيسية، وهي معلومات تعتبر ذات قيمة لقضية جنائية يتم تخزينها على الحاسوب أو تناقلها بشكل رقمي، وتكون على ثلاثة أشكال رئيسية (الصور الرقمية، التسجيلات الصوتية، النصوص المكتوبة).[87]

1- الصور الرقمية: وهي تعد البديل الرقمي عن الصور الفوتوغرافية وهي أحد اهم عناصر المعرفة البشرية والصور الرقمية تتميز عن الصور الفوتوغرافية بأنها تتولد من خلال الكمبيوتر وتتميز بسهولة الوصول اليها ونسخها والتعامل معها.[88]

2- التسجيلات الصوتية: هي التي تم ضبطها وتخزينها بواسطة الحاسوب إضافة إلى ملفات الوسائط المتعددة مثل التسجيلات المرئية.[89]

---

[86] مسعود بن فريحة، **مرجع سابق**، 55

[87] Debra Shinder, Ed Tittel, **Scene of the Cybercrime Computer Forensics Handbook**, Syngress Publishing, 1st Edition, 2002, P.550

[88] توفيق خشاشنة، **مرجع سابق**، ص 289

[89] توفيق خشاشنة، **مرجع سابق**، ص 289

وقد نص القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في المادة (22) حيث جرم نشر أخبار أو صور أو تسجيلات صوتية أو مرئية تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة.[90]

3- النصوص المكتوبة: وهي تلك النصوص المكتوبة بواسطة الجهاز الرقمي وتشمل رسائل البريد الالكتروني ورسائل الهاتف المحمول وجميع الرسائل التي تدخل ضمن الشبكة الإلكترونية، ولا تشبه أدلة الحاسوب أدلة المستندات الأخرى والتي تكون عادة على الورق، فالنصوص الرقمية يمكن نسخها بسهولة أو تغيرها أو حتى التخلص منها.[91]

ومن أمثلة ذلك تجريم القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، في المادة (24) لنشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد عرض أي كلمات مكتوبة أو سلوكيات من شأنها أن تؤدي إلى إثارة الكراهية العنصرية أو الدينية أو التمييز العنصري.[92]

المطلب الثاني: خصائص الدليل الالكتروني في مجال الاثبات الجنائي

إن أدلة الاثبات في جرائم الحاسوب والانترنت تختلف عن أدلة الاثبات في الجرائم العادية، لان الجرائم الإلكترونية تتم في بيئة غير مادية وعبر نظام الحاسوب وشبكة الانترنت، وعليه يمكن للجاني أن يقوم بالعبث في البيانات والبرامج وذلك في وقت قياسي قد يكون جزءاً من الثانية. وهذا ما يجعل الدليل الإلكتروني يختلف في بعض خصائصه عن الدليل الجنائي في الجرائم التقليدية وسوف نوضح في هذا المطلب بعض الأسس العلمية المهمة في الأدلة الجنائية الإلكترونية والتي ترتكز عليها الطبيعة القانونية

---

[90] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (22)

[91] Debra Shinder, Ed Tittel, **Ibid**, 551

[92] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (22)

للدليل الالكتروني. في البداية سوف نقوم بالإجابة على سؤال مهم وهو ما الذي جعل الدليل الرقمي يتخذ خصائص تميزه عن غيره من الادلة وذلك في الفرع الأول بعنوان موقع الدليل الرقمي من تقسيمات الأدلة الجنائية بصفة عامة وفي الفرع الثاني سوف نقوم بتوضيح خصائص الدليل الالكتروني بشكل مفصل.

الفرع الأول: موقع الدليل الالكتروني من تقسيمات الأدلة الجنائية بصفة عامة

منذ البداية كان هناك العديد من المحاولات لوضع تقسيمات للأدلة الجنائية، فمنهم من قسم الأدلة من حيث وظيفتها (أدلة اتهام، أدلة نفي، أدلة حكم) ومنهم من قسم الأدلة من حيث قيمتها في الاثبات (دليل كامل، دليل ضعيف، دليل غير كافي)، ومنهم من قسم الأدلة من حيث صلتها بالواقع (أدلة مباشرة كالشاهد، وأدلة غير مباشرة كالقرائن)، ومنهم من قسمها من حيث الجهة التي يقدم لها (ادلة قضائية وأدلة غير قضائية).[93] إن ما يهمنا في هذا المجال هو تقسيم الدليل من حيث نسبته إلى مصدره فهو أساس المقارنة ما بين الدليل الجنائي التقليدي والدليل الالكتروني حيث تتمثل في التقسيمات الأربعة (الأدلة القانونية، الأدلة الفنية، الأدلة القولية، الأدلة المادة).[94]

أولاً: الأدلة القانونية

وهي تلك الأدلة التي حددها المشرع وعين قوة كل منها، بحيث لا يكون الاثبات الا بها وهذا هو الأصل في المواد المدنية، على العكس من ذلك في المسائل الجنائية فإن تلك الأدلة غير محصورة، والقاضي حر في تكوين قناعته من أي دليل موجود امامه.

---

[93] عائشة بن قارة مصطفى، **مرجع سابق**، ص66

[94] توفيق خشاشنة، **مرجع سابق**، ص 285

ثانياً: الدليل الفني

وهي الأدلة التي تنبعث من رأي الخبير، والخبرة هي أحد إجراءات التحقيق التي يعهد القاضي بها إلى شخص يختص بمهمة محددة، وتتعلق بواقعة معينة، يستلزم بحثها من أجل ابداء الرأي الفني أو العلمي، ولا يتوافر حتى لدى المثقف العادي ولا يستطيع القاضي الوصول اليه وحده.[95]

ثالثاً: الدليل القولي

وهو الذي يكون مصدره أشخاص أدركوا وقائع ومعلومات بإحدى حواسهم ومن شأنها أن تفيد في كشف الحقيقة، وأشهر هذه الأدلة الشهادة واعتراف المتهم.

رابعاً: الدليل المادي

هو الدليل الناتج عن عناصر مادية ناطقة بنفسها وتؤثر في قناعة القاضي وتشكل أحد الأدلة الرئيسية في كشف الجريمة وقد حظي الدليل المادي باهتمام القضاء والفقه.

ويبقى السؤال المطروح أمامنا هو أين موقع الأدلة الإلكترونية من بين هذه الأنواع العديدة فهل تعتبر الأدلة الإلكترونية أدلة مادية كونها ناتجة عن عناصر مادية ملموسة وتستخدم العلم لاستخلاصها، أم تعتبر من الأدلة الفنية كونها بحاجة إلى معايير علمية محددة؛ انقسم الفقه في هذه المسألة إلى قسمين:

الاتجاه الأول: يرى أنصار هذا الاتجاه بكل بساطة أن الدليل الالكتروني ما هو الا دليل مادي ملموس؛ ويبني هذا الاتجاه رأيه على إمكانية استخلاص الدليل الالكتروني من الواقع عن طريق البرامج العلمية

[95] آمال يوسف حسن، **الأدلة العلمية الحديثة ودورها في الاثبات الجنائي**، جامعة الشرق الأوسط، رسالة ماجستير منشورة، 2012 ص 117

الحديثة وعن طريق الطابعات وغيرها، ويقترب في تشكيله من الأدلة العلمية الأخرى كبصمة الاصبع والبصمة الوراثية.[96]

الاتجاه الثاني: يرى أن الدليل الالكتروني يتمتع بخصائص مميزة عن الأدلة السابقة، على الرغم من وجود الطابع الفني والمادي في الدليل الالكتروني الا أنه دليل قائم بذاته وليس من الصحيح نسبته إلى أي من تلك الأدلة.[97] ومن هذا المنطلق قامت الولايات المتحدة الامريكية بإنشاء المنظمة الدولية لأدلة الحاسوب في عام 1995 ومهمتها تزويد وكالات انفاذ القانون الدولية بمعلومات تتعلق بالتحقيق الرقمي في الجرائم الإلكترونية.[98]

إن هذه الخصائص المذكورة أعلاه سبغت على الدليل الالكتروني طابع متميز، وجعلت هذا الدليل يتميز عن غيره من الأدلة الجنائية التقليدية من حيث أدلة الاثبات ومن هذا المنطلق وجب علينا من أجل بيان الدليل الالكتروني في مجال الاثبات الجنائي توضيح خصائص الدليل الالكتروني بشكل مستقل ومفصل.

الفرع الثاني: خصائص الدليل الإلكتروني

يتميز الدليل الالكتروني عن غيره من باقي الأدلة ببعض الخصائص والتي سوف نجملها فيما يلي:

أولاً: الدليل الالكتروني دليل علمي

إن أحد أهم ما يميز الدليل الالكتروني بأنه يعتبر دليل علمي فهو يتكون من مجموعة البيانات والمعلومات ذات الهيئة الإلكترونية غير الملموسة، ومن هذا المنطلق يتطلب إدراك هذه البيانات والمعلومات الاستعانة بالأجهزة والمعدات اللازمة لذلك، والتي تتشكل من أدوات الحاسوب الالي والبرامج والأنظمة الحاسوبية؛

---

[96] توفيق خشاشنة، **مرجع سابق**، ص 286

[97] عائشة بن قارة مصطفى، **مرجع سابق**، ص 69

[98] (https://uia.org/s/or/en/1100029648) اخر زيارة بتاريخ (2021/12/30)

فبدونها لا يمكن إدراك الدليل الالكتروني وتحليله وفهمه واستخلاصه إلى الواقع.[99] وما ينطبق على الدليل العلمي ينطبق ايضاً على الدليل الالكتروني، فيخضع الدليل العلمي لقاعدة لزوم تجاوبه مع الحقيقة كاملة اذ يستبعد تعارضه مع القواعد العلمية السليمة وبذات الاتجاه فأن للدليل الالكتروني ذات الطبيعة حيث لا يجوز أن يخرج عن ما توصل اليه العلم الرقمي.[100]

ثانياً: الدليل الالكتروني دليل تقني

ويقصد بذلك أن الدليل الالكتروني يستوحى من البيئة الرقمية وتتمثل في العالم الافتراضي الالكتروني ويتكون هذا العالم الواسع من أجهزة وخوادم ومضيفات وشبكات الكترونية، فالدليل الالكتروني ليس كالدليل التقليدي فالتقنية لا تنتج سلاح يستدل به على الجاني، وانما تنتج نبضات الكترونية رقمية تتسم بسعتها العالية وإمكانية انتقالها من مكان لآخر بسرعة خيالية عبر الشبكات الإلكترونية.[101]

ثالثاً: الدليل الالكتروني يصعب التخلص منه

هي أحد أهم خصائص الدليل الالكتروني التي تميزه عن غيره من الأدلة، بالرغم من سهولة التلاعب بالبيانات الرقمية، الا أنه يمكن استرجاعها بعد محوها أو إصلاحها في حال اتلافها وكذلك إعادة الحال لما كان عليه قبل التعديل عليها أو التلاعب بها.

فلا يخفى علينا أنه عندما يشطب ملف من جهاز الحاسب الالي يبقى موجوداً على القرص الصلب، وباستخدام برمجيات من الطبيعة الرقمية ذاتها يمكن بمقتضى هذه البرمجيات استرداد كافة الملفات التي تم الغاؤها أو ازالتها من الحاسوب وأحد هذه البرمجيات هو برنامج (X Tree Pro gold) وهو برنامج يمكن

---

[99] توفيق خشاشنة، **مرجع سابق** 283

[100] عائشة بن قارة مصطفى، **مرجع سابق**، ص 62

[101] مسعود بن حميدي المعمري، **مرجع سابق**، ص 198

المحقق من الحصول على الملفات في أي مكان على الشبكة أو القرص الصلب.[102] كما يمكن البرنامج من إظهار ملفات النظام والملفات المخفية على القرص الصلب.[103] وكذلك وجميع هذا البرامج تعمل من أجل إظهار الحقيقة في حال حاول المتهم اخفائها داخل القرص الصلب أو الشبكة الإلكترونية.

رابعاً: الدليل الالكتروني قابل للنسخ

يمكن استخراج نسخ من الأدلة الجنائية الرقمية تكون مطابقة للأصل ولها نفس القيمة العلمية والحجية الثبوتية وهذه الخاصية لا تتوفر في أنواع الأدلة الأخرى.[104]

وتعتبر خاصية نسخ الدليل الالكتروني أحد الخصائص الفريدة في الدليل الالكتروني فهي تمكن المحقق الجنائي بعمل نسخة طبق الأصل عن الدليل الرقمي حيث تساعده في الإبقاء على النسخة الاصلية من هذا الدليل والاحتفاظ بها كما هي، في حين أن المحقق الجنائي يستطيع عمل أكثر من نسخة طبق الأصل عن الدليل الالكتروني وهذا يعجل في عملية التحقيق في الجرائم الإلكترونية، حيث يقوم بإعطاء نسخة عن الدليل لأكثر من محقق في نفس القضية من أجل دراستها والتوصل إلى نتيجة محددة.[105]

ويرى الباحث ان هذه الخاصية هي أحد الخصائص التي تميز الدليل الالكتروني عن غيره من الأدلة وينفرد بها؛ فهذه الخاصية تساعد افراد الضابطة القضائية والنيابة العامة للحفاظ على الدليل الالكتروني من الفقدان أو التغير أو التلف، ومن هذا المنطلق ايضاً يشترط على النيابة العامة أو الضابطة القضائية أن تتأكد أن النسخ المأخوذة من الأدلة الرقمية لم تتغير أو تتعدل بعد مقارنتها بالأصل.

---

[102] طاهر محمود أبو القاسم، **الجرائم المعلوماتية صعوبات وسائل التحقيق فيها وكيفية مواجهتها**، المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2019، ص 130

[103] Franklin Clark, Ken Diliberto, **Investigating Computer Crime**, CRC Press, Florida, 1996, P. 71

[104] بهنوس امال، **الدليل الرقمي في الإجراءات الجنائية**، المجلة الاكاديمية للبحث القانوني، مجلد 16، عدد 2، 2017، ص 178

[105] Richard Watson and Stephen Pearson, **Digital Triage Forensics: Processing the Digital Crime Scene**, Syngress, 2010, P.65

خامساً: الدليل الالكتروني دليل عابر للحدود

في أغلب الأحيان لا يمكن أن يتواجد الدليل الالكتروني في حيز محدد، كما هو شأن الأدلة التقليدية وقد يتواجد الدليل الالكتروني في أكثر من مكان وفي وقت واحد، سواء كان داخل حدود الدولة أو خارجها؛ ويرجع السبب في ذلك إلى ارتباط هذا الدليل بالبيئة الافتراضية والتي من الممكن أن تتعدى حدود الدولة الجغرافية، فشبكة الانترنت لا تعرف حدوداً لتبادل المعلومات والبيانات بين سكان العالم فيمكن ذلك الجاني من نقل الدليل الالكتروني من دولة لأخرى بكل سهولة.[106]

كما هذه الخاصية في الدليل الالكتروني جعلت من الدول بأن تقوم بتنظيم اتفاقيات فيما بينها من أجل تجنب الجريمة الإلكترونية ومن أجل تنظيم ملاحقة مرتكبي هذه الجرائم العابرة للحدود ومنها الاتفاقية الأوروبية للجريمة الإلكترونية (بودابست) والتي تتكون من (64) طرفاً وتتيح للدول خارج الاتحاد الأوربي للانضمام لها وتعتبر المغرب إحدى الدول العربية المنضمة إلى اتفاقية بودابست، إضافة إلى انضمام دولة الاحتلال كطرف في هذه الاتفاقية.[107]

ويرى الباحث أن الدليل الالكتروني يختلف في تكوينه عن باقي الأدلة في الجرائم التقليدية كما في شكله ومضمونه عن الدليل في الجريمة التقليدية، إضافة إلى أن الدليل الرقمي يتمتع بالعديد من الخصائص والميزات التي لا تتوفر في غيره من الأدلة، فهو دليل علمي تقني يصعب التخلص منه وقابل للنسخ وعابر للحدود لا يتوقف في وجوده على حدود جغرافية لدولة ما، وهذا ما جعل الدول تقوم بتنظيم الاتفاقيات الثنائية والجماعية من أجل مكافحة الجريمة الإلكترونية على نطاق واسع، وكل هذا يقودنا إلى أهمية دراسة الطبيعة الخاصة للأدلة الرقمية في المبحث القادم.

---

[106] مصطفى إبراهيم العربي، **دور الدليل الرقمي في الاثبات الجنائي**، مجلة البحوث القانونية، مجلد 4، عدد 1، 67–107، 2016، ص 75

[107] الموقع الرسمي لمجلس اروبا (https://www.coe.int/en/web/cybercrime/the-budapest-convention) تاريخ الزيارة (12/20/2021)

المبحث الثاني

الطبيعة القانونية للدليل الالكتروني

بعد أن عرف الباحث الدليل الالكتروني ودرس خصائصه التي تميزه على غيره من الأدلة التقليدية؛ وتوصل إلى أن الدليل الالكتروني يختلف في خصائصه وأشكاله عن الدليل التقليدي وهو دليل قائم بذاته، ومن هذا المنطلق برزت الاهمية في توضيح الطبيعة القانونية للدليل الالكتروني. إن القيمة القانونية للدليل الالكتروني تكتسب من مشروعية هذا الدليل وحجيته في الاثبات أمام القضاء الجنائي، وعليه فإن الباحث سوف يقسم هذا المبحث إلى مطلبين، في المطلب الأول سوف يدرس مشروعية الدليل الالكتروني، وفي المطلب الثاني سوف يدرس حجية الدليل الالكتروني في مجال الاثبات أمام القضاء الجنائي.

المطلب الأول: مشروعية الدليل الالكتروني

يشترط في الدليل الجنائي لكي يتم قبوله في المحكمة والاعتماد عليه كدليل إثبات يساعد في كشف الحقيقة؛ أن يكون مشروعاً من حيث وجوده، ومشروعاً من حيث الحصول عليه، فمشروعية الوجود تقتضي إجازة القانون للقاضي الاستناد على الدليل الجنائي في تسبيب الحكم القضائي في الدعوى الجزائية، أما مشروعية الحصول على الدليل الجنائي تقتضي الحصول عليه باتباع الإجراءات التي ينص عليها قانون الإجراءات الجزائية المطبق داخل الدولة.[108] ومن هنا سوف يقوم الباحث بدراسة فرعين رئيسيين، الأول هو مشروعية وجود الدليل الالكتروني المستمد من التفتيش، والفرع الثاني، مشروعية الحصول على الدليل الالكتروني الناشئ عن التفتيش.

[108] وهيبة لعوارم، **مشروعية الدليل الالكتروني الناتج عن التفتيش الجنائي**، مجلة القانون والفقه، العدد 20، 99–113، 2014، ص 100

الفرع الأول: مشروعية وجود الدليل الالكتروني المستمد من التفتيش

يقصد بمشروعية وجود الدليل الالكتروني أن يكون الدليل معترفاً به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إلى هذا الدليل من أجل تكوين عقيدته للحكم بالإدانة، ومن هنا فأن النظم القانونية تختلف في موقفها من الأدلة التي تقبل كأساس للحكم بالإدانة بحسب الاتجاه الذي تتبناه، فهنالك اتجاهان رئيسان، الاتجاه الأول هو نظام الأدلة القانونية والاتجاه الثاني هو نظام الاثبات الحر.[109]

أولاً: نظام الأدلة القانونية

في ظل هذا النظام يحدد المشرع الأدلة التي يجوز للقاضي اتباعها والاخذ بها عند بناء حكمه في الدعوى، وتكون إرادة القاضي بمرتبة أدنى من إرادة المشرع، كما أن إرادة المشرع هي التي تحدد القوة القانونية للأدلة، فعندما تتوافر الشروط والعناصر التي وضعها المشرع بالدليل الجنائي يكون للقاضي الحكم بالاستناد اليها[110]. وبذلك يكون القاضي ملزماً بأن يبني قناعته ويؤسس حكمه بصرف النظر عن اقتناعه الشخصي، ومن هنا لا سبيل للاستناد إلى أي دليل ما لم ينص القانون صراحة على هذا الدليل ضمن أدلة الاثبات ولذلك يسمى هذا النظام بنظام الاثبات المقيد.[111]

وينتمي هذا النظام للدول ذات النظم الانجلو سكسونية ومنها المملكة المتحدة البريطانية والولايات المتحدة الامريكية وكندا، وعليه فإن هذه الدول لا تقبل أي دليل جنائي دون أن يكون هذا الدليل قد نظمه المشرع مسبقاً واجاز استخدامه والاستناد له. ومن هذا المنطلق فأن النظم التي تتبنى هذا النظام في الاثبات لا

---

[109] خالد عياد الحلبي، **مرجع سابق**، ص 237

[110] مسعود بن حميد المعمري **مرجع سابق**، ص 204

[111] خالد عياد الحلبي، **مرجع سابق**، 249

يمكن في ظلها الاعتراف بالدليل الرقمي بأي قيمة اثباتية ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الاثبات ومهما توافرت فيه شروط اليقين لا يجوز للقاضي الاستناد اليه لتكوين عقيدته.[112]

وقد أصدرت بريطانيا قانون إساءة استخدام الحاسوب في عام 1990م، ولم يتناول الأدلة الناتجة عن الحاسوب وذلك لوجود قانون البوليس والاثبات الجنائي لسنة 1984م، والذي حوى تنظيما محددا لمسألة الاثبات قبول مخرجات الحاسوب والانترنت كأدلة اثبات في المواد الجنائية، وفي الولايات المتحدة الامريكية تناولت بعض القوانين حجية الأدلة الإلكترونية ومن ذلك ما نص عليه قانون الحاسوب لسنة 1984م، الصادر في ولاية (أيوا)، أن مخرجات الحاسوب تكون مقبولة بوصفها أدلة اثبات بالنسبة للبرامج والبيانات المخزنة، وكذلك أتاح قانون الاثبات الصادر في ولاية كاليفورنيا نسخ المخرجات من البيانات الحاسوب واستخدامها كأدلة إثبات.[113]

ويرى الباحث أن تقييد سلطة القاضي قد يؤدي إلى ظهور العديد من المشاكل القانونية فالأدلة الإلكترونية بطبيعتها لا يمكن أن يخضع القاضي لقيود بشأنها، ففي بعض الأحيان قد يحتاج الامر لسلطة القاضي التقديرية للاقتناع بالأدلة الموجودة امامه.

ثانياً: نظام الاثبات الحر

وفقاً لهذا النظام فإن القاضي الجنائي يتمتع بحرية مطلقة في شأن اثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للاستناد لها في تكوين قناعته، وله أن يبني قناعته على أي دليل أمامه وإن لم يكن منصوصاً عليه ويسود مبدأ حرية الاثبات في الدول التي تأخذ بالنظام اللاتيني.[114]

---

[112] وهيبة لعوارم، مرجع **سابق**، ص 101

[113] وهيبة لعوارم، **مرجع سابق**، ص101

[114] خالد عياد الحلبي، **مرجع سابق**، ص 237

ولا تثور إشكالية مشروعية الدليل الالكتروني من حيث وجوده في ظل نظام الاثبات الحر، فالقاضي يجوز له الاخذ بأي دليل ومنها الأدلة الإلكترونية، فالأصل في هذه الحالة مشروعية وجود الدليل ويبقى اقتناع القاضي بالدليل المعروض عليه سواء بقبول هذا الدليل أو رفضه.[115]

إلا أن حرية الاختيار والتقدير للقاضي وفق قناعته لا يعني أنها مطلقة، فلا يجوز للقاضي أن يدخل تخميناته وتصوراته الشخصية ضمن ادلة الاثبات الجنائي التي يبني عليها حكمه.[116]

وقد تم الاخذ بنظام الاثبات الحر في عدد من الدول على المستوى العربي والعالمي، حيث جاء في القانون الفرنسي على أن تثبت الجرائم بجميع طرق الاثبات ويحكم القاضي تبعاً لاقتناعه الخالص وقد اخذت كل من مصر والأردن بمبدأ حرية الاثبات.[117]

وفي فلسطين فقد اخذ المشرع بمبدأ حرية الاثبات[118]. فوسائل الاثبات لم يرد عليها حصر، كما لم يحدد المشرع وزن أي منها، إنما يتاح للخصوم إقامة الدليل بطرق الاثبات كافة طالما كانت مشروعة، وعليه يعود تقدير مدى قبولها وتأثيرها في الاثبات إلى القاضي، فالقانون لم يقيد القاضي الجزائي بأدلة معينة خوله بصفة مطلقة أن يكون عقيدته من أي دليل يقدم له في الدعوى.[119]

وبناءً على ما ورد أعلاه فإن مشروعية وجود الدليل الالكتروني لا تشكل أي إشكالية في النظام القانوني الفلسطيني، وبالرغم من ذلك فقد صدر القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته والذي عالج موضوع الأدلة المتحصلة من تكنولوجيا المعلومات فقد

---

[115] مسعود بين حميد المعمري، **مرجع سابق**، ص 105

[116] مسعود بن حميد المعمري، **مرجع سابق**، ص 205

[117] توفيق خشاشنة، **مرجع سابق**، ص 298

[118] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م ، المادة (1/6) " تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات، إلا إذا نص القانون على طريقة معينة للإثبات"

[119] مصطفى عبد الباقي، شرح قانون الإجراءات الجزائية الفلسطيني، **مرجع سابق**، ص 386

نصت المادة (57) على أنه "يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات"، حتى أن اغلب الدول التي تأخذ بنظام الأدلة القانونية شرعت العديد من القواعد والتي تتيح مشروعية وجود الدليل الالكتروني وذلك تماشياً مع تطور الجريمة في المجتمع.

الفرع الثاني: مشروعية الحصول على الدليل الالكتروني

يشترط لقبول الدليل الجنائي كدليل اثبات أن يتم الحصول على هذا الدليل بطريقة مشروعة، ويقصد في هذه الحالة أن تكون الجهة المختصة بجمع الأدلة الإلكترونية التزمت بالشروط التي نص عليها القانون صراحة، وإلا يعد الدليل باطلاً، إذ أن مشروعية الدليل تتطلب صدقه في مضمونه وأنه تم الحصول على هذا الدليل الالكتروني بطريقة مشروعة تدل على الأمانة والنزاهة، واذا خالفت إجراءات جمع الأدلة الإلكترونية القواعد الإجرائية التي تنظم كيفية الحصول عليها، فأنها تكون باطلة ولا تصلح لان تكون أدلة تبنى عليها الإدانة في المواد الجنائية إذن أنه يجب أولاً الحصول على الدليل بصورة مشروعة، وثانياً يجب أن تكون الأدلة الإلكترونية قاطعة يقينية.[120]

أولاً: الحصول على الدليل الالكتروني بصورة مشروعة

ويقصد بالحصول على الدليل بصورة مشروعة، بأن تكون الأدلة المتحصلة في الجرائم الإلكترونية تتفق فيها إجراءات الحصول على البيانات والمعلومات أو مخرجات الوسائل الإلكترونية بما جاء في القواعد القانونية والأنظمة الثابتة، وينص مبدأ الشرعية الاجرائية بأنه (لا إجراء في الدعوى إلا بنص في القانون).

ولابد من صدور إذن رسمي من السلطة المختصة بالتحقيق وإجراء المعاينة والتفتيش في مسرح الجريمة الإلكترونية بحثاً عن الدليل الرقمي، وفي هذه الحالة وعملاً بمبدأ الشرعية القانونية (لا جريمة ولا عقوبة إلا

[120] وهيبة لعوارم، **مرجع سابق**، ص 104

بنص) فلا يجوز للمشرع اصدار إذن بتفتيش الأجهزة الإلكترونية إلا في حالة كون المشرع قد نص على الجرائم التي تشكل اعتداء على الحقوق والحريات ضمن نصوص التجريم العقابية.[121]

وبالرجوع إلى قانون الإجراءات الجزائية، ولكي تكون عملية الحصول على الدليل الجنائي صحيحة فيجب، مراعاة قواعد جمع الأدلة المنصوص عليها في قانون الإجراءات الجزائية الفلسطيني ومراعاة القواعد المنصوص عليها في القرار بقانون بشأن الجرائم الإلكترونية، وتتمثل شرعية الحصول على الدليل الجنائي الالكتروني أيضاً مراعاة إجراءات التفتيش المنصوص عليها في قانون الإجراءات الجزائية، وصفة القائم بالتفتيش أو الجهة المخولة بالقيام بعملية التفتيش ونطاق التفتيش، فبطلان إجراءات التفتيش يفقد الدليل الالكتروني شرعيته وبهذا نصبح أمام دليل باطل لا يجوز الاعتداد به أمام المحكمة المختصة في إدانة المتهم.

ثانياً: يجب أن تكون الأدلة الإلكترونية قاطعة يقينية

والمقصود بأن تكون الأدلة الإلكترونية قاطعة يقينية، بأنه يجب أن تكون الأدلة المتحصلة من الأجهزة الرقمية مقتربة من واقع الجريمة الحاصلة قدر الإمكان، وابتعاد هذه الأدلة عن الشكوك والتخمينات، ويتم التوصل إلى اليقينية في الأدلة الرقمية من خلال ما يعرف بمختلف اشكال الرقمية التي تتوفر عن طريق الوصول المباشر، أو من خلال عرض لمخرجات المعالجة بواسطة الحاسوب على الشاشة أو على الأقراص الممغنطة، وفي هذه الحالة يكون باستطاعة القاضي أن يحكم بالقضية المقدمة أمامه وأن يعمل على تحديد قوتها الاستدلالية ومدى ارتباط الجريمة بشخص معين.[122]

---

[121] توفيق خشاشنة، **مرجع سابق**، ص 302

[122] توفيق خشاشنة، **مرجع سابق**، ص 304

وإذا كان القاضي يستطيع الوصول إلى اليقين بالأدلة التقليدية عن طريق المعرفة الحسية التي تدركها الحواس، أو المعرفة العقلية التي يقوم بها القاضي والتي تتمثل بالتحليل والاستنتاج، فإن الجزم بوقوع الجريمة الإلكترونية ونسبتها إلى المتهم تتطلب نوعاً جديداً من المعرفة وهي المعرفة العلمية للقاضي بالأمور المعلوماتية، لاسيما أن القاضي الجنائي يلعب دوراً ايجابياً في عملية الاثبات، ومن هذا المنطلق فقد يؤدي الجهل في بعض الأحيان إلى التشكيك في قيمة الدليل الالكتروني ومن ثم يقضي القاضي بالبراءة.[123]

ثالثاً: قابلية الدليل الالكتروني للمناقشة

لا يجوز للقاضي أن يؤسس قناعته الا على العناصر الاثباتية التي طرحت في جلسة المحاكمة وخضعت لحرية مناقشة أطراف الدعوى، فقد نصت المادة (207) من قانون الإجراءات الجزائية الفلسطيني "لا يبنى الحكم إلا على الأدلة التي قدمت أثناء المحاكمة والتي تمت مناقشتها في الجلسة بصورة علنية، أمام الخصوم".[124]

وبناء على ذلك فإن كل دليل يتم الحصول عليه من خلال البيئة الإلكترونية يجب أن يعرض في الجلسة، وليس من خلال ملف الدعوى في التحقيق الابتدائي فقط، ولكن بصفة مباشرة أمام القاضي وهذه الاحكام يتم تطبيقها على كافة مخرجات الأجهزة الإلكترونية، حتى شهود الجرائم الإلكترونية الذين يتم سماعهم في التحقيق الابتدائي يجب أن يعيدوا اقوالهم مرة أخرى من جديد أمام المحكمة، إضافة إلى خبراء الأنظمة المعلوماتية يجب أن يمثلوا بشكل شخصي أمام المحكمة من أجل مناقشتهم والعمل على إيضاح التقارير التي خلصوا اليها من أجل اظهار الحقيقة.[125]

---

[123] عائشة قارة بن مصطفى، **مرجع سابق**، ص 279

[124] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (207)

[125] توفيق خشاشنة، **مرجع سابق**، ص 307

ومن هنا يرى الباحث أهمية توفر شرطي المشروعية أعلاه في الدليل الرقمي من حيث الحصول عليه ومن حيث وجوده. ان توفر هذه الشروط تسهل على القاضي مهمته في اظهار الحقيقة كما أن توفرها في الأدلة الرقمية أيضاً يساعد الضابطة القضائية والنيابة العامة في التعامل مع هذه الأدلة بصورة تخلو من أي نقص في الإجراءات المتبعة والذي قد يسبب في بعض الأحيان إلى بطلان هذا الدليل.

المطلب الثاني: حجية الدليل الالكتروني في الاثبات أمام القضاء الجنائي

إن مجرد الحصول على الدليل الرقمي وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، اذ إن الطبيعة الفنية الخاصة بالدليل الرقمي تمكن العبث بمضمون هذا الدليل على نحو يؤدي إلى تحريف الحقيقة، دون أن يكون بمقدور المتخصص إدراك ذلك العبث. إضافة إلى ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق من اجل اظهار الحقيقية تبدو عالية في حالة الأدلة الفنية والإلكترونية؛ ومن هذا المنطلق تثور فكرة الشك في مصداقية الدليل الالكتروني كدليل من أدلة الاثبات الجنائي.[126] ومن أجل توضيح حجية الدليل الجنائي فقد رأى الباحث في هذا المطلب دراسة فرعين مهمين، الفرع الاول يدرس تقييم الدليل الالكتروني من حيث السلامة الفنية للإجراءات المتبعة للحصول عليه والفرع الثاني يدرس تقييم الدليل الالكتروني من حيث سلامته من العبث.

الفرع الأول: تقييم الدليل الالكتروني من حيث السلامة الفنية للإجراءات المتبعة للحصول عليه

كما ذكرنا سابقاً فإن الحصول على الدليل الالكتروني يجب أن يكون مشروعاً من أجل اعتماده أمام القاضي، وبالرغم من مشروعية الدليل الالكتروني والحصول عليه بالطرق القانونية السليمة، الا أنه من المهم أيضاً اتباع الإجراءات الفنية الصحيحة من أجل الحصول على الدليل الالكتروني، وبالرغم من أن نسبة الخطأ الفني في الحصول على الدليل الالكتروني نادرة، إلا أنها تبقى ممكنة، ويرجع الخطأ في

---

[126] طارق الجملي، **الدليل الرقمي في الاثبات الجنائي، مجلة الحقوق**، المجلد 12، عدد 1، ص ص. 40–73، البحرين، 2015، ص 66

الحصول على الدليل الالكتروني أساساً إلى الخطأ في استخلاص الدليل الالكتروني أو الخطأ في استخدام الاداة المناسبة في الحصول عليه.[127]

وعليه، ومن أجل التأكد من سلامة الحصول على الدليل الالكتروني يجب اتباع بعض الإجراءات الفنية من قبل الضابطة القضائية للتأكد من سلامة الأدلة المعروضة أمام القضاء، ولذا فإنه يمكن في هذا الشأن اعتماد ما يعرف باختبارات داو برت (Daubert Standard)[128]، كوسيلة للتأكد من سلامة الإجراءات المتعبة في الحصول على الدليل الرقمي، ومن هنا سوف نعرض إحدى الخطوات المستخدمة في للتأكد سلامة الدليل الرقمي.[129]

أولاً: اخضاع الأدوات المستخدمة لعدة تجارب لتأكد من دقتها وسلامتها

تخضع الأدوات المستخدمة في تحصيل الدليل الالكتروني إلى عدة اختبارات يعتبر أولها اختبار السلبيات الزائفة (False negative)، ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل الالكتروني لاختبار يبين مدى قدرة هذه الأداة على عرض كافة البيانات المتعقلة بالدليل الالكتروني دون اغفال أحد البيانات المهمة، وفي الجانب الاخر تخضع الأداة المستخدمة في الحصول عل الدليل الالكتروني إلى اختبار الإيجابيات الزائفة (False positive)؛ ويقصد بهذا الاختبار ما يكون مفاده التأكد بأن الأداة المستخدمة في جمع الدليل الالكتروني لا تعرض بيانات إضافية جديدة.[130]

---

[127] بهونس امال، **مرجع سابق**، ص 185

[128] اختبارات داو بورت أو ما يعرف بمصطلح (Daubert Standard) " يعتبر معيار داو برت قاعدة أدلة في القانون الفدرالي في الولايات المتحدة الأمريكية فيما يتعلق بمقبولية شهادة الخبراء الفنيين، حيث يجوز لاي طرف رفع اقتراح الى المحكمة لاستبعاد تقديم أدلة غير مؤهلة إلى هيئة المحلفين"

[129] طارق الجملي، **مرجع سابق**، ص 69

[130] خالد الحلبي، **مرجع سابق**، ص 250-251

ويرى الباحث أن كل من اختبار السلبيات الزائفة والايجابيات الزائفة يشكلان طريقة مهمة من أجل الكشف عن مدى تعلق البيانات الموجودة على الحاسوب أو الشبكة الإلكترونية بالجريمة المرتكبة حينها، حيث أن الطبيعة الخاصة للدليل الالكتروني لا تحتمل أن يكون هناك خلل في الأدوات المستخدمة في عملية الحصول على الأدلة الإلكترونية فالزيادة أو النقصان من الممكن أن تؤدي إلى عرقلة تحقيق العدالة في بعض الأحيان وخصوصاً في الجرائم الإلكترونية.

ثانياً: الاعتماد على أداوت اثبتت الدراسات العلمية كفاءتها في الحصول على الدليل الالكتروني

تبين الدراسات العلمية في مجال تقنية المعلومات العديد من الطرق السليمة التي يجب اتباعها في الحصول على الدليل الالكتروني، وفي المقابل فأن الدراسات العلمية أوضحت العديد من الأدوات المشكوك في كفاءتها، مما يسهم في التأكد من مصداقية هذه الأدوات والتأكد من مصداقية المخرجات المستمدة من تلك الأدوات، وتتيح الدراسات لسلطات التحقيق والضابطة القضائية التأكد من مدى فعالية هذه الأدوات ومدى قدرتها على اظهار الحقيقة.[131]

وفي هذه الحالة من المهم أن تقوم الضابطة القضائية بالاعتماد على الأدوات المستخدمة في جمع الأدلة الإلكترونية والتي اثبتت الدراسات العلمية كفاءتها، فعملية استخلاص الدليل الالكتروني بحاجة إلى دقة متناهية، وتتمثل هذه العملية في استخدام البرامج الموثوقة في عملية التفتيش، وأحد هذه البرامج الموثوقة ما أطلقته شركة مايكروسوفت العالمية لاسترجاع الملفات المحذوفة (Windows File Recovery).[132]

---

[131] خالد عياد الحلبي، **مرجع سابق**، ص 251

[132] برنامج استرجاع الملفات لمايكروسوفت (Windows File Recovery) " هو أداة مساعدة لبرنامج موجه الأوامر من مايكروسفت لاستعادة الملفات المحذوفة" انظر (https://www.microsoft.com/en-us/p/windows-file-recovery/9n26s50ln705#activetab=pivot:relateditemtab) تاريخ اخر زيارة (1/29/2022)

انظر ايضاً (https://en.wikipedia.org/wiki/Windows_File_Recovery) تاريخ اخر زيارة (1/29/2022)

ومن هنا يرى الباحث أن عملية تقييم الدليل الالكتروني من حيث السلامة الفنية للإجراءات المتبعة للحصول عليه، لها أهمية كبيرة في صحة الدليل. وبالرغم من تطور الأدلة الإلكترونية إلا أن هناك العديد من الطرق التي تصلح للتأكد من سلامة الإجراءات الفنية للحصول على الدليل الالكتروني بدءاً باختبارات داو بيرت وانتهاءً بالبرمجيات والتقنيات الحديثة، فكل هذه الطرق تؤدي إلى نتيجة واحدة الا وهي التأكد من السلامة الفنية للإجراءات المتبعة للحصول على الدليل الالكتروني.

الفرع الثاني: تقييم الدليل الالكتروني من حيث سلامته من العبث

إن الدليل الالكتروني من الممكن أن يخضع للعبث[133] للخروج به على نحو يخالف الحقيقة، ومن ثم يقدم هذا الدليل ليعبر عن واقعة مخالفة للواقعة التي صنع الدليل الالكتروني من أجل اثباتها، وهذا العبث في الدليل الالكتروني لا يستطيع الشخص غير المتخصص إدراكه، وعلى هذا النحو فإن سائر الأدلة الإلكترونية التي تقدم للقضاء أصبح من السهل تعديلها أو العبث بها بحيث يظهر هذا الدليل بنسخة اصلية في تعبيره عن الحقيقة.[134]

ويجرم القرار بقانون بشأن الجرائم الإلكترونية في فلسطين العبث بالأدلة المعلوماتية فقد نصت المادة (67) "كل من أقدم على العبث بأدلة قضائية معلوماتية أو أقدم على إتلافها أو إخفائها أو التعديل فيها أو محوها، يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار

133

Evidence tampering" refers to situations whereby a person alters, falsifies, or conceals evidence with the intent " to interfere with an investigation process. This is alternatively known as spoliation of evidence in a civil case. Evidence tampering could have serious consequences for a case and impact its final verdict. The issue with digital evidence tampering is that one cannot know for sure whether tampering has occurred, since perpetrators can make minor unnoticeable changes that are enough to impact a verdict. Constantly comparing digital evidence with copies to identify tampering may not be practically possible as this requires a lot of resources such as additional .security infrastructure and personnel

(مرجع الكتروني (https://blog.vidizmo.com/tamper-detection-how-it-works-to-keep-digital-evidence-safe) تاريخ اخر زيارة (2022/1/30)

134 خالد عياد الحلبي، **مرجع سابق**، ص 247

أردني، أو ما يعادلها بالعملة المتداولة قانوناً. وهناك العديد من الطرق التي تستخدم في كشف التلاعب بالأدلة الإلكترونية، والتي سوف نجمل بعضها فيما يلي:

أولاً: التحليل التناظري

يلعب علم الحاسوب دوراً مهماً في عملية تقديم المعلومات الفنية التي تساهم في فهم مضمون وشكل الدليل الالكتروني، ويمكن الاستعانة بهذه العلوم المحوسبة في كشف مدى التلاعب الذي جرى على الأدلة الإلكترونية. وتبدو فكرة التحليل التناظري الالكتروني احدى الوسائل المهمة في الكشف عن مصداقية الدليل الالكتروني ومدة التلاعب بهذا الدليل، ومن خلال هذه الفكرة يتم مقارنة الدليل الالكتروني المقدم للقضاء ويمكن معرفة مدى حصول عبث في النسخة المستخرجة أم لا.

ثانياً: استخدام أدوات وبرامج خاصة

قد يتم اللجوء في بعض الأحيان إلى الأدوات والبرامج الخاصة في كشف تحريف الأدلة الإلكترونية. وتختلف هذه البرامج والأدوات باختلاف الوظيفة المحددة لها، فبعض هذه البرامج مخصص لكشف التحريف في الصور والفيديوهات ومنها برنامج (vidizmo)[135]. وبعبارات بسيطة، يقوم النظام بتقييم ملف الأدلة الرقمي لأي تغييرات للتأكد من أن الملف هو نفسه الملف الأصلي الذي تم تحميله. وبالنسبة للأدلة الرقمية

[135] VIDIZMO's Digital Evidence Management portal caters to this challenge by allowing you to run a tamper detection check on your digital evidence in a few clicks.
How does VIDIZMO's work
In simple terms, the system assesses the digital evidence file for any changes to ensure the file is the same as the one originally uploaded. For digital evidences that do not match their original state, the system shows them as tampered evidence when a check is run .
When any file is initially uploaded on VIDIZMO Digital Evidence Management portal, a miniature identifier called a "hash" value is created for that file which is stored in the database for future comparisons. The hash value is created using the data of the file. Therefore, this hash value is unique to the file and changes even if the contents of the file are modified to the slightest extent .
To put things into perspective, every video file is essentially a series of binary codes. If we have video file A with its binary code "01110110", it will create a hash value that is unique to this "01110110" binary code. A modification in the file would lead to creation of a new binary code (for example, "11110110"), which in turn would generate a different hash value. This difference makes it possible to detect tampering.
Visit site (https://blog.vidizmo.com/tamper-detection-how-it-works-to-keep-digital-evidence-safe).

التي لا تتطابق مع حالتها الأصلية، يعرض النظام إذا كان الدليل قد تم التلاعب به عند إجراء الفحص أم لا.[136]

وخلاصة القول أنه في حال توافر الشروط العامة لما يمثل أساساً للثقة في هذا الدليل، فانه من غير المعقول أن يعيد القاضي تقييم هذا الدليل، فالدليل الالكتروني بوصفه دليلاً علمياً فإن دلالته قاطعة بشأن الواقعة المستشهد به عنها، فاذا سلمنا بإمكانية التشكيك في سلامة الدليل بسبب قابليته للعبث أو نسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنها برأي حاسم، إن لم يقطع به أهل الاختصاص.[137]

ومن الجدير بالذكر عدم الخلط بين الشك الذي يشوب الدليل الالكتروني بسبب إمكانية العبث فيه أو لوجود خطأ في الحصول عليه، وبين القيمة الاقناعية له، فالحالة الأولى لا يملك القاضي الفصل بها لأنها مسألة فنية تعود لأهل الاختصاص والقول فيها قول أهل الخبرة، فإن سلم الدليل الالكتروني من العبث والخطأ، فأنه في هذه الحالة لا يكون للقاضي سوى قبول هذا الدليل ولا يمكن التشكيك في حجيته الاثباتية لكونه وبحكم طبيعته الفنية يمثل إخباراً صادقاً عن الواقع، ما لم يثبت عدم صلة الدليل بالجريمة المراد اثباتها.[138]

---

[136] مرجع الكتروني (https://blog.vidizmo.com/tamper-detection-how-it-works-to-keep-digital-evidence-safe) تاريخ اخر زيارة (2022/1/30)

[137] طارق الجملي، **مرجع سابق**، ص 70

[138] خالد عياد الحلبي، **مرجع سابق**، ص 252

المبحث الثالث

مسرح الجريمة الالكتروني وأدوات الاثبات في الجرائم الإلكترونية

يعتبر مسرح الجريمة هو المفتاح لحل لغز أي جريمة وهو الوسيلة الأولى والهامة لبداية التعامل مع القضية الجنائية. ومسرح الجريمة الإلكترونية يمكن أن يكون مسرحاً تقليدياً يقع خارج بيئة الحاسوب الالي كالأقراص الصلبة واشرطة التخزين وغيرها من المكونات المادية، ومسرحاً معلوماتياً يتكون من البيانات والمعلومات محل الجريمة. ويعرف مسرح الجريمة الإلكترونية بأنه مسرح الجريمة الذي يقع داخل النظام المعلوماتي أو العالم الافتراضي والذي قام فيه المجرم بجريمته أو قام بهذه الجريمة بواسطته، ويصل اليه رجال الضبط الجنائي بطريقة فنية تستلزم الالمام بالتقنية والاتقان، ويمكن من خلال هذا المسرح استخلاص الدليل الالكتروني.[139] وفي هذا المبحث سوف ندرس مطلبين اساسيين المطلب الأول معاينة مسرح الجريمة الالكتروني، والمطلب الثاني استخلاص الدليل الالكتروني من مسرح الجريمة.

المطلب الأول: معاينة مسرح الجريمة الالكتروني

إن المعاينة لمسرح الجريمة اجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الاثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة.[140]وأوجب قانون الإجراءات الجزائية الفلسطيني على الضابطة القضائية اجراء معاينة لمسرح الجريمة في حال وقوع التلبس.[141]

---

[139] خالد العتيبي، **الجوانب الإجرائية في الشروع في الجرائم المعلوماتية: دراسة مقارنة**، (ط1، مكتبة القانون والاقتصاد للنشر والتوزيع، الرياض، المملكة العربية السعودية، 2014) ص 64

[140]د خالد ممدوح إبراهيم، **الاثبات الالكتروني في المواد الجنائية والمدنية**، (دار الفكر الجامعي الإسكندرية، مصر، 2020) ص 90

[141] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (27) من "يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فورا إلى مكان الجريمة، ويعاين الآثار المادية لها ويتحفظ عليها، ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، ويسمع أقوال من كان حاضرا أو من يمكن الحصول منه على إيضاحات في شان الجريمة ومرتكبيها، ويجب عليه أن يخطر النيابة العامة فورا بانتقاله، ويجب على عضو النيابة المختص بمجرد إخطاره بجناية متلبس بها الانتقال فورا إلى مكان الجريمة.

ويقصد بمعاينة مسرح الجريمة الإلكترونية، معاينة الاثار التي يرتكبها مستخدم الشبكة المعلوماتية أو الانترنت وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات والبيانات التي تم معالجتها خلال الكمبيوتر والشبكة العالمية.[142] وسوف يتحدث الباحث في هذا المبحث في موضوعين مهمان، دور المحقق الجنائي في القيام بالمعاينة الإلكترونية، ومدى إمكانية تتبع مرتكبي الجرائم المعلوماتية والتنظيم القانوني له في فلسطين.

الفرع الأول: دور المحقق الجنائي في القيام بالمعاينة الإلكترونية

تتم المعاينة في الجرائم الإلكترونية على مرحلتين، أولها بالانتقال المادي للمحقق الجنائي في الواقع المادي، بحيث تكون الجريمة واقعة على المكونات المادية للنظام المعلوماتي أو بواسطته مع ظهور الأدلة واثار الجريمة على المكونات المادية، ففي هذه الحالة لا يوجد صعوبة من اجراء المعاينة فمسرح الجريمة صالح للمعاينة بما يتضمنه من الآثار المادية، أما في حالة المعاينة في المسرح الافتراضي ففي هذه الحالة تقوم الضابطة القضائية بالانتقال عبر هذا العالم عن طريق الحاسوب الآلي المكتبي، أو من خلال مكتب خبراء هيئة الاتصالات وتقنية المعلومات.[143]

أولاً: الانتقال المادي للمحقق الجنائي

في هذه المرحلة على موظف الضابطة القضائية أن ينتقل فوراً إلى مكان ارتكاب الجريمة الإلكترونية للمعاينة والقيام بجمع التحريات اللازمة والمحافظة على الآثار والأدلة الإلكترونية للجريمة قبل ضياع هذه الأدلة واختفائها، ولضبط كل ما يمكن أن يؤدي إلى اظهار الحقيقة واثبات حالة الأماكن والأشخاص وكل

---

[142] خالد إبراهيم، **مرجع سابق**، ص 103

[143] خالد العتيبي، **مرجع سابق**، ص 64

ما يفيد في كشف الحقيقة.[144]ويجب على مأمور الضبط القضائي قبل الانتقال إلى مسرح الجريمة أن يقوم باتخاذ بعض الإجراءات تتمثل فيما يلي:

1- توفير معلومات مسبقة عن مكان وقوع الجريمة ونوع وعدد الأجهزة المتوقع مداهمتها لتحديد إمكانية التعامل معها فنياً، إضافة إلى اعداد خريطة للموقع الذي تتم الاغارة عليه.[145]

2- ضرورة الحصول على الاحتياجات اللازمة من الأدوات والبرامج للاستعانة بها من أجل الفحص والتشغيل عن طريق خبراء متخصصين.[146]

3- تأمين التيار الكهربائي بحيث لا يتم التلاعب بالبيانات أو تخريبها عن طريق قطع التيار أو تعديل الطاقة الكهربائية.[147]

ثانياً: الانتقال الالكتروني للمحقق الجنائي

تتم المعاينة بالانتقال إلى محل الواقعة الاجرامية كقاعدة إجرائية مقررة في هذا الشأن إلا أنه في إطار الجرائم الإلكترونية فأن الانتقال يعد من الموضوعات المستحدثة ويجب أن تكون عبر العالم الافتراضي، أي الانتقال إلى الفضاء الالكتروني (Cyber space).[148]

وقد نصت المادة (4/52) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته على صلاحية وكيل النيابة أو مأمور الضبط القضائي أو أهل الخبرة بالنفاذ المباشر إلى أي وسيلة من وسائل تكنولوجيا المعلومات واجراء التفتيش فيها. والمعاينة في الجرائم الإلكترونية لها أشكال مختلفة، والتي تختلف حسب طبيعة أو نوع الجريمة المرتكبة، وهناك وسائل مختلفة

---

[144] توفيق خشاشنة، **مرجع سابق**، ص 88

[145] خالد إبراهيم، **مرجع سابق**، ص 97

[146] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 189

[147] نبيلة هروال، **مرجع سابق**، ص 219

[148] خالد إبراهيم، **مرجع سابق**، ص 96

تستطيع النيابة العامة أو الضابطة القضائية استخدامها في معاينة الجرائم الإلكترونية، فمثلاً هناك وسيلة تصوير شاشة الحاسوب، والتي قد تكون عن طريق برمجة متخصصة في اخذ صورة لما يظهر على شاشة الحاسوب أو استخدام الة تصوير تقليدية ويطلق عليه مصطلح "تجميد شاشة الحاسوب".[149]

ومن المهم أن تتبع النيابة العامة أو الضابطة القضائية المختصة بالتحقيق العديد من الخطوات عند البدء في معاينة مسرح الجريمة المعلوماتية، فعند وجود الحاسوب في حالة تشغيل عدم العبث به وتدوين الحالة التي هو عليها، فلو كان الحاسوب في حالة تشغيل تدون ذلك ولو كان مطفأ موصول بالكهرباء أو غير موصول.[150] وقد أجاز قانون الإجراءات الجزائية الفلسطيني في المادة (58) لوكيل النيابة في جميع إجراءات التحقيق أن يصطحب كاتباً لتدوين المحاضر ويوقعها معه.[151]

ومن المهم أن تقوم النيابة العامة أو الضابطة القضائية بملاحظة الطريقة التي تم بها اعداد النظام والآثار الإلكترونية، وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكة المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام المحدد.[152] وإذا كان الجهاز في حالة تشغيل تقوم النيابة العامة بوضع ورق داخل الجهاز وإعادة الطباعة إضافة إلى تفقد النظام من أي برامج تم استخدامها قبل لحظة الدخول لمسرح الجريمة.[153]

ومن هنا يرى الباحث أن اتباع إجراءات متخصصة في قيام النيابة العامة أو مأموري الضابطة القضائية المتخصصة بمعاينة مسرح الجريمة الإلكترونية يخفف من نسبة فقدان البيانات داخل النظام المعلوماتي والتي من الممكن ان تكون أدلة اثبات امام المحاكم الجنائية والتي تلعب دوراً مهماً في اظهار الحقيقة.

---

[149] توفيق خشاشنة، **مرجع سابق**، ص 86

[150] توفيق خشاشنة، **مرجع**، **سابق**، ص 94

[151] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (58) "يصطحب وكيل النيابة في جميع إجراءات التحقيق كاتبا لتدوين المحاضر ويوقعها معه".

[152] خالد ممدوح، **مرجع سابق**، ص 109

[153] توفيق خشاشنة، **مرجع سابق**، ص 96

الفرع الثاني: المعاينة بتتبع المجرم المعلوماتي الكترونياً

التتبع في الجرائم يشابه اقتفاء الأثر في التقصي الخاص بالجرائم التقليدية والهدف من التتبع في الجرائم الإلكترونية هو الوصول لمرتكب الفعل الاجرامي عن طريق تحديد الجهاز المستخدم في ارتكاب الجريمة وتحديد موقعه حيث لكل كمبيوتر متصل بالأنترنت عنوان خاص به (IP Address) وهذا العنوان يتكون من جزئين، الأول يشمل ارقام الشبكة والثاني يشمل ارقام مقدم الخدمة.[154]

وهناك جانبان رئيسيان للتبع الالكتروني، أولهما الرجوع على مزودي خدمة الانترنت للحصول على الهوية الحقيقة لشخص ما، أو التنصت على المكالمات السلكية واللاسلكية ومن المهم توضيح كيف يمكن تتبع الأشخاص عبر شبكات الانترنت والتنظيم القانوني في فلسطين للرجوع على مزودي الخدمة بمعلومات المشتركين.[155]

أولاً: الرجوع على مزودي الخدمة

جميع معلومات المشتركين تكون مرتبطة بالحساب الخاص بهم لدى مزودي الخدمة باسم الحساب الشخصي الخاص بهم، وحالة الاشتراك ومعلومات الفواتير، إضافة إلى هوية الهواتف الخاصة بهم إضافة إلى برتوكولات الانترنت التي قاموا بزيارتها في الوقت والتاريخ المحددان.[156] ولكن ما مدى الزامية مزود الخدمة بتقديم هذه المعلومات إلى النيابة وسلطات التحقيق.

تنص المادة (1/51) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في فلسطين "يلتزم مزود الخدمة، وفقاً للإجراءات القانونية بتزويد الجهات المختصة

---

[154] إيهاب محمد التاج، **التحقيق وجمع الأدلة في الجرائم المعلوماتية**، مجلة العدل – وزارة العدل، المملكة العربية السعودية المجلد 11، عدد 26، ص ص. 391 – 406، 2009، ص 404

[155] توفيق خشاشنة، **مرجع سابق**، ص 96

[156] **Investigations Involving the Internet and Computer Networks**, u.s department of justice, office of justice program, National Institute of Justice (U.S.), 2007, p. 15

بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة".[157] فالأجهزة الرقمية المتصلة بالأنترنت مع بعضها البعض يكون لكل جهاز منها متصل بالأنترنت عنوناً خاصاً به يعطى هذا العنوان من قبل مزود خدمة الانترنت (ISP)، حيث يمكن استخدام هذا العنوان لتحديد الجهاز المستخدم في الفعل الجرمي ويمكن اعتباره كرقم الهاتف أو الرمز البريدي. [158]

ويختلف بروتوكول الانترنت عن أرقام الهواتف والرموز البريدية التي لا تتغير من حين لآخر بحيث تبقى ثابتة للمشترك، على العكس من ذلك تكون عناوين بروتوكول الانترنت التي تعطى للمستخدم قصيرة المدى تتغير من حين لآخر، ولهذا السبب على المحقق بيان التاريخ والوقت بالتحديد في حال تتبع البروتوكول. ويحتفظ مزود الخدمة بهذه السجلات في حالة الحاجة لها، فبعض مزودي الخدمة يحتفظون بها لمدة (90) يوماً وبعضهم يحتفظ بها لمدة (12) شهر.[159]

أما في فلسطين فقد نص القرار بقانون المنظم لأحكام الجرائم الإلكترونية في المادة (3/51) يلتزم مزود الخدمة، وفقاً للإجراءات القانونية بالاحتفاظ بمعلومات المشترك لمدة لا تقل عن ثلاث سنوات لغايات ما ورد في الفقرة (1) من هذه المادة.[160]

ومن أمثلة ذلك عند وجود شكوى حول رسالة في البريد الالكتروني تحتوي على سب أو تهديد، فهنا يتم فحص البريد الالكتروني للمجني عليه والرسالة الواردة محل الجريمة ومعرفة عنوان الانترنت الخاص بالشخص المرسل (IP)، ومن ثم يتم مخاطبة الشركة التي يتبعها رقم العنوان للحصول على بيانات المستخدم مرسل الرسالة.[161]

---

[157] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (1/51)

[158] توفيق خشاشنة، **مرجع سابق**، ص 96

[159] توفيق خشاشنة، **المرجع السابق**، ص 99

[160] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (2/51)

[161] مسعود بن حميد المعمري، **مرجع سابق**، ص 246

ثانياً: مراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها

إحدى الطرق التي تستخدم في تتبع الجاني في الجرائم الإلكترونية هي مراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها ومراقبة الاتصالات السلكية واللاسلكية التي يجريها المتهم من هاتفه. وتبرز أهمية هذا التتبع بالكشف على بعض الجرائم كجرائم التهديد بجناية أو اسناد أمور خادشه للشرف أو الاعتبار.[162]

وعملية مراقبة المحادثات السلكية واللاسلكية نظمها قانون الإجراءات الجزائية قبل صدور القرار بقانون المتعلق بالجرائم الإلكترونية فقد نصت المادة (51) "يجوز للنائب العام أو أحد مساعديه مراقبة المحادثات السلكية واللاسلكية، وإجراء تسجيلات لأحاديث في مكان خاص بناءً على إذن من قاضي الصلح متى كان لذلك فائدة في إظهار الحقيقة في جناية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سنة.[163]

وقد نظم القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته عملية مراقبة الاتصالات والمحادثات وتسجيلها فقد نص في المادة (54) على أنه "لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها...".[164]

ومن الملاحظ أن كل من قانون الإجراءات الجزائية والقرار بقانون الخاص بالجرائم الإلكترونية اشترط لإتمام عملية المراقبة بوجود اذن من قاضي الصلح وأن تكون الدعوى الجزائية من نوع جناية أو جنحة يعاقب

---

[162] نص المادة (91) من قانون رقم (3) لسنة 1996 بشأن الاتصالات السلكية واللاسلكية ونص المادة (15) قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية

[163] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (51)

[164] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (54) "أنه "لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جدية"

عليها بالحبس أكثر من سنة، وفي القرار بقانون فقد شدد من إجراءات المراقبة فلا يجوز أن تزيد عملية المراقبة عن خمسة عشر يوماً تجدد مرة واحدة فقط ويجب أن تتوافر دلائل جدية.[165]

ويؤكد الباحث على ضرورة اتخاذ الإجراءات الاحترازية الكاملة عند التعامل مع الفضاء الالكتروني، كما أنه يجب على من يقومون بالتعامل مع مسرح الجريمة الإلكترونية واجراء معاينة الأدوات التي ارتكب فيها الفعل الجرمي أن تكون لديهم القدرة الخاصة في التعامل مع هذه الأدوات ومعاينتها، فأي خطأ يقع من الممكن أن يؤدي إلى اتلاف الأدلة الإلكترونية. ومن هذا المنطلق وبعد أن درس الباحث أساليب التعامل مع مسرح الجريمة المعلوماتي فتح لنا المجال لدراسة الدليل الالكتروني وكيفية استخلاصه من مسرح الجريمة المعلوماتية وما هي الأدوات المستخدمة في استخلاص الدليل.

المطلب الثاني: استخلاص الدليل الالكتروني من مسرح الجريمة الإلكترونية

إن عملية جمع الأدلة الإلكترونية من مسرح الجريمة المعلوماتي تتطلب الماماً شديداً من قبل الجهة المختصة بالتحقيق في الجرائم الإلكترونية كون هذه الأدلة ذات طبيعة خاصة تتطلب إجراءات معينة في عملية جمعها وحفظها واستخلاصها. فعندما يرى المحقق الجنائي نفسه أمام أدلة الكترونية منتجة في الدعوى الجزائية ومن الممكن أن تؤدي إلى اظهار الحقيقة، فعليه في هذه الحالة أن يقوم بعملية ضبط هذا الدليل الالكتروني وتحريزه من أجل عرضه على القضاء. وسوف يدرس الباحث في هذا المطلب فرعين مهمين في الفرع سوف يتناول أدوات جمع الدليل من مسرح الجريمة الإلكترونية، وفي الفرع الثاني سوف يدرس تحريز الدليل الالكتروني من مسرح الجريمة الإلكترونية.

[165] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (54)

الفرع الأول: أدوات جمع الدليل الالكتروني من مسرح الجريمة الإلكترونية

بالعادة تتواجد الأدلة الرقمية في مخرجات الطابعة والتقارير والرسوم وفي أجهزة الحاسوب وملحقاته وفي الأقراص المرنة والصلبة وأشرطة التخزين على شكل بيانات ومعلومات وتتواجد الأدلة الإلكترونية ايضاً في أجهزة المودم والبرامج وأجهزة التصوير وهذا ما أوضحناه سابقا.[166] ومن أجل جمع واستخراج هذه البيانات لا بد أن يلجأ المحقق الجنائي إلى استخدام بعض الطرق والأدوات والتي يمكن اجمالها فيما يلي:

أولاً: برنامج إذن التفتيش (Computer Scorch Warrant Program)

وهو برنامج قاعدة بيانات، ويسمح برنامج اذن التفتيش بإدخال كل المعلومات المهمة المطلوبة لترقيم الأدلة وتسجيل البيانات منها، ويمكن لهذا البرنامج أن يقوم بإصدار ايصالات باستلام هذه الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو الظروف التي ضبط فيها هذا الدليل، ويساعد هذا البرنامج المتخصصين والنيابة العامة في عملية جمع الدليل الالكتروني وتسهيل عملية الوصول إلى الأدلة الإلكترونية في حال جمعها.[167]

ثانياً: قرص بدء تشغيل الكمبيوتر (Bootable Diskette)

عندما يكون نظام التشغيل الموجود ملفات المعنية بداخله محمي بكلمة مرور ولا تستطيع كل من النيابة العامة أو الضابطة القضائية الولوج إلى الملفات المحددة ففي هذه الحالة من الممكن اللجوء إلى قرص بدء التشغيل والذي يمكّن الجهة المختصة بالتحقيق من تشغيل النظام المحمي بكلمة المرور وضبط الملفات المعنية.[168]

---

[166] خالد إبراهيم، **مرجع سابق**، ص 59

[167] توفيق خشاشنة، **مرجع سابق**، ص 315

[168] خالد ابراهيم، **مرجع سابق**، ص 59

ويجب أن يكون القرص مزود ببرنامج مضاعفة المساحة وهو برنامج يسمح للمستخدم زيادة كمية البيانات التي يمكن تخزينها على الأقراص، وذلك عن طريق ضغط البيانات وإلغاء ضغطها أثناء التنقل بشفافية داخل نظام التشغيل. وتم تصميم هذا البرنامج بشكل أساسي للاستخدام على الأقراص الصلبة ولكنه يدعم ايضاً استخدامه على الأقراص المرنة.[169] ويجب أن يحتوي قرص بدء التشغيل على هذا البرنامج تحسباً إذا قام الجاني بضغط الملفات الموجودة على القرص الصلب ومضاعفة مساحته.

ثالثاً: تقنيات النسخ (Imaging techniques)

تسمح تقنيات النسخ للمستخدم بنسخ محتويات القرص الصلب إلى قرص صلب آخر او وحدة تخزين خارجية. وتعمل هذه البرامج على تأمين الملفات المنقولة بحيث لا يمكن نسخها مرة أخرى من داخل القرص الصلب.[170] ويعد برنامج (encase forensic)[171] أكثر البرامج تكلفة في عملية جمع الأدلة الإلكترونية إذ تستخدمه الجهات الأمنية من شرطة ومخابرات ومباحث، وذلك من أجل البحث والتنقيب في جهاز الحاسوب.[172] وتقوم آلية هذا البرنامج على عمل مسح شامل للقرص الصلب وذلك لاستعادة الأدلة من محركات الأقراص الصلبة المضبوطة.[173] وأحد برامج النسخ أيضاً والذي يستخدم في عملية استخلاص وجمع الأدلة الإلكترونية برنامج (Lap link)، وهو برنامج يقوم بنسخ الملفات من الحاسوب الخاص بالمتهم

---

[169] مرجع الكتروني عن برنامج مضاعفة المساحة (DoubleSpace) " https://en-academic.com/dic.nsf/enwiki/1674981" اخر زيارة بتاريخ (2022/2/27)

[170] Michael Cross: **Scene of the Cybercrime**, Second Edition, Syngress Publishing, USA, 2008, P. 640

[171] **(EnCase)**: is the shared technology within a suite of digital investigations products by Guidance Software (acquired by OpenText in 2017). The software comes in several products designed for forensic, cyber security, security analytics, and e-discovery use. Encase is traditionally used in forensics to recover evidence from seized hard drives. Encase allows the investigator to conduct in depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information.

[172] توفيق خشاشنة، مرجع سابق، ص 316

[173] مرجع الكتروني، الموقع الرسمي للشركة المنتجة للبرنامج (https://blogs.opentext.com/announcing-opentext-security-protection-cloud-ce-21-1/) تاريخ اخر زيارة (2022/3/1)

ونقلها إلى قرص آخر سواء على طريقة التوازي أو على طريقة التوالي ويعد أحد البرامج المفيدة للحصول على نسخة من حاسوب المتهم قبل تدميرها.[174]

وأجاز القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته عملية نسخ البيانات والمعلومات التي لها علاقة بالجريمة الإلكترونية فقد نص في المادة (3/53)" إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً أو تعذر إجراؤه، تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات.[175] وهذا ما اقرته الاتفاقية الأوروبية (بودابست) لمكافحة الجريمة المعلوماتية من اجراء نسخة من البيانات الحاسوبية والاحتفاظ بها وذلك في ظل تمكين الدول الأطراف من مصادرة البيانات والمعلومات والاحتفاظ بها.[176]

كما نصت أيضاً الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ضبط المعلومات بإن تلتزم الدول الأطراف بتبني الإجراءات الضرورية التي من شأنها تأمين البيانات والمعلومات وعمل نسخة من البيانات والمعلومات والاحتفاظ بها.[177]

وفي صدد هذا الموضوع يرى الباحث أن عملية استخلاص الدليل الرقمي بحاجة إلى برامج متخصصة وقد تكون مكلفة في بعض الأحيان، ومن هذا المنطلق تظهر ضرورة وجود التعاون الدولي المشترك في عملية التحقيق بالجرائم المعلوماتية.

---

[174] خالد إبراهيم، **مرجع سابق**، ص 59

[175] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (3/53)

[176] التقرير التفسيري للاتفاقية المتعلقة بالجريمة الالكترونية بودابست، 2001/11/23، المادة (3/19/ب)

[177] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، 2010/12/21، المادة (1/27/ب)

الفرع الثاني: تحريز الدليل الالكتروني

حرص المشرع الفلسطيني على تحريز وضبط موجودات التفتيش فقد نص في المادة (2/50) من قانون الإجراءات الجزائية الفلسطيني على ما يلي "يتم ضبط جميع الأشياء التي يعثر عليها أثناء إجراء التفتيش والمتعلقة بالجريمة وتحرز وتحفظ وتثبت في محضر التفتيش وتحال إلى الجهات المختصة".[178]

فبعد أن تقوم السلطات المختصة باستخلاص الدليل الالكتروني من النظام الرقمي بإحدى الطرق الموضحة أعلاه، سواء باستخدام البرامج أو الضبط المادي للأقراص ، يأتي دور تحريز الدليل الالكتروني من أجل عرضه على القضاء، وعند قيام الجهة المختصة بتحريز الدليل الالكتروني فيجب عليها مراعاة الاختلافات بين الأدلة المضبوطة، فهناك ما هو معرض للضياع وهناك ما هو غير معرض للضياع كما أنه هناك نوعان من التحفظ على البيانات الرقمية فمنها ما يتم التحفظ عليه داخل الحاسوب المضبوط نفسه ومنها ما يتم التحفظ عليه خارج الجهاز المضبوط.[179]

أولاً: تحريز الأدلة المعرضة للضياع

كما ذكرنا سابقاً أن بعض الأدلة الإلكترونية قد تكون معرضة للفقدان أو الضياع وذلك بسبب الطبيعة المؤقتة لها وكونها ذا طابع معنوي، وقد اجاز القرار بقانون ضبط الأدلة المتحصلة في مسرح الجريمة الإلكترونية من بيانات ومعلومات فقد نصت المادة (2/53) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات "للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة.

---

[178] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001، المادة (2/50)

[179] توفيق خشاشنة، **المرجع السابق**، ص 341

وتشمل هذه الأدلة (تفاصيل إعداد الشبكة، توصيلات الشبكة المفتوحة أو المغلقة، ذاكرة الوصول العشوائي، الملفات المفتوحة وسجلات الدردشة ورسائل البريد الالكتروني وكلمات السر ومفاتيح التشفير. ويتم تحريز هذه الأدلة باستخدام وسائط تخزينية وبرامج محددة، وأمثلة هذه البرامج برنامج (Win3dd) ويقوم هذا البرنامج بعمل نسخة احتياطية لذاكرة الوصول العشوائي (RAM)[180]، وبرنامج (FTK Imager) ويقوم بمعاينة البيانات وعمل نسخة احتياطية عنها وتقييم الدليل الالكتروني إذا كان بحاجة إلى الطب الشرعي الرقمي.[181]

ثانياً: تحريز الأدلة غير المعرضة للضياع

هناك بعض الأدلة الإلكترونية ذات طبيعة مادية قد تكون نسبة فقدانها أو تلفها قليلة مقارنة بالأدلة المعنوية

وقد أجاز القرار بقانون ضبط الأدلة المادية في مسرح الجريمة الإلكترونية فقد نصت المادة (2/52)" إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.[182]

وتشمل هذه الأدلة (الأقراص الصلبة الداخلية والخارجية، الأقراص المدمجة (CD&DVD)، بطاقة الذاكرة، الفلاش ميموري، الكاميرات الرقمية، مشغلات الصوت والصورة، الهواتف الخلوية، أجهزة المودم والطابعات)

---

[180] مرجع الكتروني (https://www.forensicfocus.com/forums/forensic-software/win32dd-new-tool-to-image-ram-on-vista-w2k3/) تاريخ اخر زيارة (2022/4/3)

[181] **FTK® Imager** is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Forensic Toolkit (FTK®) is warranted.

[182] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (2/52)

ويتم تحريز هذه الأدلة، بإستخدام، عبوات التخزين وأكياس مضادة للكهرباء الساكنة، واقراص فارغة وأشرطة أدلة.[183]

ثالثاً: طرق التحفظ على البيانات والمعلومات

وهناك عدة طرق للتحفظ على الأنظمة المعلوماتية، فيمكن التحفظ على هذه المعلومات عن طريق ابقائها داخل النظام أو الحاسوب نفسه وتتم عن طريق حجز الحاسوب الذي يتواجد الدليل الرقمي فيه، أما الطريقة الثانية فيتم التحفظ على البيانات والمعلومات خارج الحاسب الالي وذلك عن طريق استخدام فلاش ميموري أو عن طريق استخدام أقراص صلبة خارجية.[184]وقد أجاز القرار بقانون عملية نسخ البيانات والمعلومات إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً أو تعذر إجراؤه.[185] ومن المهم اتخاذ الإجراءات الضرورية لمنع وصول من ليس له علاقة إلى البيانات المخزنة في حال تعذر التحفظ على البيانات والمعلومات موضوع التفتيش، فقد نصت المادة (4/53) من القرار بقانون "إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات".

وقد اتجهت الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) إلى ذات الاتجاه فقد اشترطت على الدول الأطراف اتخاذ التدابير اللازمة لتمكين سلطاتها من تأمين بيانات الحاسوب ذات صلة بالجريمة وجعلها غير قابلة للنفاذ على نظام الحاسوب الذي تم الولوج اليه أو ازالتها.[186]كذلك اتجهت الاتفاقية العربية لمكافحة الجرائم المعلوماتية ذات الاتجاه فقد اشترطت ايضاً على الدول الأطراف اتخاذ التدابير التي تمنع

---

[183] توفيق خشاشنة، **مرجع سابق**، ص 343

[184] توفيق خشاشنة، **مرجع سابق**، ص 344

[185] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (3/53)

[186] التقرير التفسيري للاتفاقية المتعلقة بالجريمة الالكترونية بودابست، 2001/11/23، المادة (3/19/د)

الوصول إلى البيانات المخزنة أو ازالتها وذلك من أجل ضمان عدم التلاعب بالبيانات المخزنة على الوسط الافتراضي.[187]

ومن هنا وبعد التعرف على مسرح الجريمة المعلوماتية يرى الباحث أهمية مراعاة الظروف التي تحيط به، فهو ذو طبيعة تختلف عن مسرح الجريمة في الجرائم التقليدية. وبذلك لا بد على الدولة أن تمتلك الخبرات الكافية من أجل إتمام التحقيق في الجرائم الإلكترونية، إضافة إلى أن البرامج والأدوات المستخدمة في التحقيق في الجرائم الإلكترونية وكشفها قد تكون في بعض الأحيان مكلفة، وعليه لا بد من وجود تعاون دولي من أجل التخفيف من حدة الأعباء على الدول، وبهذا الصدد تسهيل عملية مكافحة الجرائم الإلكترونية.

[187] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، 2010/12/21، المادة (1/27/د)

الفصل الثاني

القواعد العامة في ضبط وتفتيش نظم الحاسوب في النظام القانوني الفلسطيني

بعد أن قام الباحث بتوضيح التفتيش الجنائي في الجرائم الإلكترونية وتوضيح الدليل الالكتروني وبيان خصائصه والطبيعة القانونية له، إضافة لتوضيح مسرح الجريمة في الجرائم الإلكترونية؛ يفتح ذلك المجال للباحث لدراسة القواعد العامة في ضبط وتفتيش نظم الحاسوب في النظام القانوني الفلسطيني. وقد قسم الباحث هذا الفصل إلى عدة مباحث تتمثل فيما يلي، في المبحث الأول سوف يدرس الباحث السلطات المختصة بالتفتيش والتحقيق في الجرائم الإلكترونية وصلاحيتها، وفي المبحث الثاني سوف يدرس الصعوبات التي تواجه عملية التحقيق في الجرائم الإلكترونية، وفي المبحث الثالث سوف يدرس الضمانات القانونية للمتهم في عملية التفتيش والتحقيق الجنائي في الجرائم الإلكترونية.

المبحث الأول

السلطات المختصة بالتفتيش في الجرائم الإلكترونية وصلاحيتها

يتمثل التحقيق الابتدائي في مدلوله في القانون إلى مجموعة الإجراءات التي تباشرها سلطات التحقيق المختصة للتنقيب عن أدلة الجريمة وجمعها لتحديد مدى كفاية هذه الأدلة إلى إحالة المتهم إلى المحكمة من أجل الحكم إما بإدانة هذا المتهم لاقتناع القاضي بالأدلة المعروضة أمامه من قبل النيابة العامة أو الحكم بالبراءة لعدم كفاية الأدلة أو غيره من الأسباب القانونية. ويعتبر التفتيش اجراء من إجراءات التحقيق كما بين الباحث في الفصل الأول من هذا البحث، وفي هذا المبحث سوف يقوم الباحث بتوضيح شقين رئيسيين في مطلبين المطلب الأول سوف يقوم بتحديد السلطات المختصة بالتفتيش في الجرائم الإلكترونية وفي المطلب الثاني سوف يقوم ببيان نطاق اختصاص هذه السلطات في القانون.

المطلب الأول: تحديد السلطات المختصة بالتفيش في الجرائم الإلكترونية

اختلفت النظم الإجرائية فيما بينها في تحديد السلطة المختصة بالتفتيش وجاء هذا الاختلاف بسبب الأنظمة الجزائية المختلفة حول العالم، وعند الحديث عن الجرائم الإلكترونية فإننا بصدد جرائم بحاجة إلى إمكانيات أكثر من قبل السلطة المختصة بالتفتيش ومن هنا تبرز أهمية تحديد السلطة المختصة للقيام بعملية التفتيش في الجرائم الإلكترونية وعليه سوف يدرس الباحث في هذا المطلب فرعين رئيسيين في الفرع الأول سوف يدرس التفتيش من قبل النيابة العامة بصفتها صاحبة الاخصاص الأصيل والثاني سوف يدرس التفتيش بالإنابة لاحد أفراد الضابطة القضائية.

الفرع الأول: التفتيش من قبل النيابة العامة

الاصل في القانون الفلسطيني أن التفتيش عمل من أعمال التحقيق التي تختص بها النيابة العامة أو الضابطة القضائية، فقد نصت المادة (1/39) من قانون الإجراءات الجزائية الفلسطيني" دخول المنازل وتفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها...لوجود قرائن قوية على أنه يحوز أشياء تتعلق بالجريمة".[188]

كما نص القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في المادة (1/52) " للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة". وعليه فإن الجهات التي تختص بتفتيش الجرائم الإلكترونية في فلسطين هي النيابة العامة أو أحد افراد الضابطة القضائية المنتدبين.[189]

---

[188] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001، المادة (1/39)

[189] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (1/52)

ومن الواضح أعلاه أن النيابة العامة صاحبة الاختصاص الأصيل في عملية التفتيش في الجرائم التقليدية وفقاً لما ورد في قانون الإجراءات الجزائية الفلسطيني، وبصدور القرار بقانون بشأن الجرائم الإلكترونية في فلسطين نلاحظ بإن القرار بقانون قد خطى على خطى قانون الإجراءات الجزائية حيث اعتبر أن النيابة العامة هي صاحبة الاختصاص الأصيل أيضاً بالتفتيش في الجرائم الإلكترونية. وهذا ما حذا عليه كل من المشرع الأردني.[190]والمشرع المصري.[191]

وقد نص القرار بقانون على انشاء جهاز تحقيق خاص بالجرائم الإلكترونية وذلك في نص المادة (3) "تنشأ وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية"، وتتولى النيابة العامة الإشراف القضائي عليها، كل في دائرة اختصاصه.[192]

---

[190] وفي الأردن فقد أجاز قانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1961 وتعديلاته في المادة (33) التفتيش في الجرائم التقليدية قانون الإجراءات الجزائية الأردني رقم (9) لسنة 1961 وتعديلاته "إذا تبين من ماهية الجريمة أن الأوراق والأشياء الموجودة لدى المشتكى عليه يمكن أن تكون مدار استدلال على ارتكابه الجريمة فللمدعي العام أو من ينيبه أن ينتقل حالاً إلى مسكن المشتكى عليه للتفتيش عن الأشياء التي يراها مؤدية إلى إظهار الحقيقة" .وقد أجاز قانون الجرائم الالكترونية الأردني لسنة 2015 التفتيش عن الأدلة في الجرائم الالكترونية في نص المادة (13)" مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على ادن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص

[191] في مصر فتعتبر النيابة العامة صاحبة الاختصاص الأصيل بالتفتيش في الجرائم التقليدية حسب قانون الإجراءات الجنائية رقم 150 لسنة 1950 المعدل بالقانون رقم 189 لسنة 2020. ولقاضي التحقيق ايضاً سلطة التفتيش حسب حالات خاصة اجازها القانون ويتميز قاضي التحقيق عن النيابة العامة بسلطته في تفتيش غير المتهم سواء في شخصه أو في منزله حسب المواد (93-94) من قانون الإجراءات الجنائية المصري، على العكس من النيابة العامة التي لا تمتلك ذلك بمفردها بل يجب عليها لاتخاذ إجراءات التفتيش الحصول على إذن من القاضي الجزائي. وقد نص قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 على تحديد السلطة المختصة بالتحقيق والتفتيش في الجرائم الالكترونية هي ذاتها السلطة المختصة بالتحقيق في قانون الإجراءات الجنائية حسب الأصول.

[192] القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، المادة (3)

وهناك بعض الدول لا تعتبر النيابة العامة صاحبة الاختصاص الأصيل في التفتيش مثل فرنسا فقد اناط الاختصاص الأصيل بالتفتيش لقاضي التحقيق ولا يجوز للنيابة العامة اجراء التفتيش الا في حالة التلبس ومع ذلك يجوز لها ان تطلب من قاضي التحقيق اجراء التفتيش في محل معين.[193]

وفي الدول الفدرالية كالولايات المتحدة الامريكية مثلاً اعتبرت الجرائم الإلكترونية جرائم فدرالية وذلك حسب مدونة القوانين في الولايات المتحدة الامريكية.[194] وتختص مكاتب التحقيق الفدرالي في الولايات المتحدة الامريكية بعملية التحقيق في الجرائم ويكون الاختصاص الأصيل في الولايات المتحدة الامريكية لشرطة انفاذ القانون (federal law enforcement officer) أو محامي الحكومة (attorney).[195]

وقد تم انشاء وكالة تابعة لمكتب التحقيقات الفدرالي إلى جانب المركز الوطني لحماية البنية التحتية مهمتها التنسيق في مكافحة القرصنة المعلوماتية، وهناك وحدة متخصصة تابعة لقسم العدالة الأمريكي مكلفة بمكافحة الاجرام المعلوماتي تتكون من خبراء في تقنيات الحاسوب والانترنت ومن مستشارين قانونيين.[196]

الفرع الثاني: التفتيش من قبل السلطات المنتدبة في الجرائم الإلكترونية

الأصل كما ذكرنا سابقاً في تنفيذ مذكرة التفتيش، أن يباشر تنفيذها من خصه القانون أي النيابة العامة، بصفتها صاحبة اختصاص اصيل وقد أجاز القانون للنيابة العامة أن تنتدب أحد مأموري الضبط القضائي من أجل انجاز مهمة التفتيش من خلال صدور الاذن بالتفتيش.[197]

---

[193] محمد طوالبة، **مرجع سابق**، ص 86

[194] مرجع الكتروني (https://brandonsample.com/federal-cyber-crimes/) تاريخ اخر زيارة (3/15/2022)

[195] مرجع الكتروني (https://www.law.cornell.edu/rules/frcrmp/rule_4) تاريخ اخر زيارة (3/15/2022)

[196] نبيلة هروال، **مرجع سابق**، ص 110

[197] محمد طوالبة، **مرجع سابق**، ص 97

ويقصد بالأذن بالتفتيش "ذلك التفويض الموجه من سلطة التفتيش المختصة إلى أحد مأموري الضبط القضائي متضمناً تخويله إياه اجراء التفتيش الذي تختص به تلك السلطة". ويسري على الاذن بالتفتيش أحكام الندب للتحقيق بوجه عام.[198]

وقد نص قانون الإجراءات الجزائية الفلسطيني في المادة (1/30) أن دخول المنازل وتفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها وكذلك الفقرة الثالثة من ذات المادة "تحرر مذكرة التفتيش باسم واحد أو أكثر من مأموري الضبط القضائي".[199]

وعليه فقد أجاز قانون الإجراءات الجزائية الفلسطيني للنيابة العامة أن تصدر إذن لإحدى الجهات المختصة تندبها للقيام بعملية التفتيش، وقد جاء القرار بقانون بشأن مكافحة الجرائم الإلكترونية في فلسطين ليتوافق مع ما ورد في قانون الإجراءات الجزائية الفلسطيني فقد أجاز للنيابة العامة أن تنتدب أحد مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة.[200]

ويشترط لصحة الندب توفر مجموعة من الشروط أبرز ما يعنينا منها، أن يكون إذن التفتيش محدداً، خصوصاً في محله، والاشياء المراد البحث عنها لضبطها، أو بمعنى اخر، واصفاً بشكل خاص ودقيق الشيء المراد ضبطه كما لو تضمن ذلك الاذن القيام بتحديد القطع الصلبة المكون منها الحاسوب. وتجدر الإشارة إلى أن تحقق هذا الشرط في اذون التفتيش الصادرة بشأن جرائم الحاسب الالي عامة وجرائم الانترنت

---

[198] نبيلة هروال، **مرجع سابق**، ص 243

وقد أخذ القانون الأردني بنظام الجمع بين سلطتي الاتهام والتحقيق ويجعل السلطتين من اختصاص النيابة العامة، وينص على الانابة في المادة (1/48) من قانون أصول المحاكمات الجزائية ويرد في نص المادة ما يلي" يمكن للمدعي العام أثناء قيامه بالوظيفة في الأحوال المبينة في المادتين (42/29) أن يعهد الى أحد موظفي الضابطة العدلية". أما قانون الإجراءات الجنائية المصري فقد نص في المادة (200) من ذات القانون بأنه يجوز لكل من أعضاء النيابة العامة في حالة اجراء التحقيق بنفسه تكليف أي مأمور من مأموري الضبط ببعض الاعمال التي من اختصاصه.

[200] القرار بقانون رقم (10) لسنة 2018 بشأن مكافحة الجرائم الالكترونية، المادة (52)

خاصة أمر صعب جداً؛ كونها تتطلب من مصدر الإذن أو منفذه اموراً فنية تتجاوز ثقافته العامة ومعارفه للأشياء التي ينبغي ضبطها.[201]

كما أن التفتيش عن البيانات المخزنة آلياً يتطلب القيام بعملية الولوج إلى الأنظمة المعلوماتية التي تحويها لضبط ما يعد صالحاً من هذه البيانات كدليل أو قرينة لارتكاب جريمة ما، وهذا الامر يتطلب مسبقاً، معرفة معقولة من قبل الشخص القائم بالتفتيش بكيفية التعامل مع هذه البرامج وملفات البيانات المخزنة بجهاز الحاسوب وكذلك التعامل مع كلمات السر والمرور اللازمين للدخول إلى النظام المعني تفتيشه.[202]

وعليه ففي مجال تفتيش نظم الحاسوب والانترنت يشترط أن يكون عضو الضابطة العدلية المناب في عملية التحقيق ذو خبرة ودراية فنية في تفتيش نظم الحاسوب والانترنت وذلك حتى يستطيع أن يتعامل عملياً وبصورة سليمة وصحيحة مع مخرجات الحاسوب والانترنت ومع أقراص الحاسوب والاشرطة الممغنطة وذلك من أجل الحفاظ على سلامة الأدلة المتحصلة من الجريمة المعلوماتية.[203]

ويرى جانب من الفقه الجنائي أن مأموري الضبط القضائي القائمين على التفتيش والضبط عليهم اتخاذ إجراءات محددة ومعينة في سبيل تنفيذ مهمتهم في جرائم الحاسب الآلي، وفريق التفتيش والضبط المعني هو جزء من الفريق الذي يتولى معاينة مسرح الجريمة وتفتيش وضبط ما فيه، سواء كان ذلك من خلال مأموري الضبط القضائي أو من خلال سلطة التحقيق المختصة، حسب ما إن كنا بصدد جمع حالات استدلالات أو بمناسبة التحقيق الابتدائي.[204]

---

[201] نبيلة هروال، **مرجع، سابق**، ص 243

[202] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 197

[203] محمد الطوالبة، **مرجع سابق**، ص 104

[204] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 203

وقد اعتبر القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية موظفو الوزارة المعينون من قبل الوزير من مأموري الضابطة القضائية المختصة بالتفتيش عن الجرائم الإلكترونية حيث نص في المادة (54) " تتولى الوزارة وفقاً لاختصاصها تقديم الدعم والمساعدة الفنية لجهات إنفاذ القانون، ويعتبر موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ أحكام هذا القرار بقانون؛ وقد الغي نص المادة بالقرار بقانون رقم (38) لسنة 2021م المعدل للقرار بقانون رقم (10) لسنة 2018.[205]

ومن هذا المنطلق فيرى الباحث أن السلطات المختصة تفتيش أنظمة الحاسوب في فلسطين تتمثل بالنيابة العامة كصاحبة اختصاص اصيل أو مأموري الضبط القضائي كجهة منتدبة، ويشترط للجهة القائمة على عملية التفتيش أن تكون ذو دراية وخبرة بالأدلة الإلكترونية المراد التفتيش عنها كون هذه الأدلة بحاجة إلى دقة أكثر وخصوصية بالتعامل تختلف عن غيرها من باقي الأدلة.

المطلب الثاني: نطاق اختصاص السلطات المختصة بالتفتيش

يجب أن تمارس السلطة المختصة عملية التفتيش في الجرائم الإلكترونية وغيرها من الجرائم داخل حدود اختصاصها، ومعنى ذلك يشترط أن تمارس السلطات صلاحياتها داخل دائرة الاختصاص المكاني، وسوف نتحدث في هذا المبحث عن حدود اختصاصات سلطات التفتيش في الجرائم الإلكترونية سواء أكان التفتيش من قبل النيابة العامة نفسها أو عن طريق انتداب أحد افراد الضابطة القضائية المختصة كما وضحنا سابقا، ولكن من المعتاد عليه أن أجهزة الحاسوب في بعض الأحيان قد تكون مرتبطة بعضها ببعض عن طريق دائرة داخلية تنتمي إلى ذات الشركة أو البنك أو المدرسة أو المؤسسة وذلك عن طريق شبكة محلية (Local area network) أو عن طريق شبكة الانترنت العالمية أو عن طريق شبكة واسعة النطاق (Wide area network) ويمكن أن تمتد إلى داخل النطاق الإقليمي أو خارجه، وعليه فإن تفتيش جهاز

[205] قرار بقانون رقم (38) لسنة 2021م بتعديل قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته، المادة (26) " تلغى المادة (54) من القانون الأصلي"

معين يستتبع بالضرورة الدخول إلى جهاز آخر ينتمي إلى شخص آخر في مكان مختلف فيقوم رجال الضبط القضائي في هذه الحالة باستخدام برامج معينة ابتداء من الجهاز محل التفتيش إلى جهاز ثاني وربما ثالث.[206]

وعليه سوف يجيب الباحث في هذا المطلب على أحد أهم أسئلة البحث وهي مدى قدرة سلطة التحقيق بالوصول إلى حاسوب أو بيانات ذات نهاية طرفية وبمعنى آخر هل يمتد إذن التفتيش الصادر من مأمور الضبط القضائي إلى أجهزة الحاسوب المرتبطة بجهاز الحاسوب محل الاذن سواء داخل الدولة أو خارجها.[207] وسوف نقسم المطلب لفرعين رئيسيين، الفرع الأول سوف ندرس ارتباط حاسوب المتهم بنهاية طرفية داخل إقليم الدولة والفرع الثاني: ارتباط حاسوب المتهم بنهاية طرفية خارج إقليم الدولة.

الفرع الأول: ارتباط حاسوب المتهم بنهاية طرفية داخل إقليم الدولة

إن تفتيش المكان المملوك للمتهم أو غيره من الأشخاص المشاركين في الجريمة لا تثير أي صعوبة واشكالية لأنها محددة مسبقا وذلك في قانون الإجراءات الجزائية فقد نصت المادة (39) على أن دخول المنازل وتفتيشها عمل من أعمال التحقيق وتختص به النيابة العامة أو الضابطة القضائية. كما أنه لا يجوز دخول المنازل وتفتيشها من السلطات المختصة دون مذكرة إلا في حالات استثنائية أجازها القانون وذلك في نص المادة (48) من قانون الإجراءات الجزائية، ولكن ما يدق ناقوس الخطر عندما يتعلق الامر بتفتيش نظم الحاسوب الالي، فقد يكون الحاسوب مرتبط بنهاية طرفية مع حاسوب آخر أو شبكة إنترنت خارجية متواجدة في مكان آخر داخل إقليم الدولة نفسها فهل يجوز امتداد التفتيش لها أم لا؟.[208]

---

[206] مصطفى علي خلف، **التفتيش وفقاً لأحكام القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات**، المركز القومي للبحوث الاجتماعية والجنائية، المجلة الجنائية القومية، المجلد 63، العدد 3، ص ص. 1 – 73، 2020م، ص 8

[207] مصطفى علي خلف، **مرجع سابق**، ص 9

[208] أحمد حسنية، **مرجع سابق**، ص 24

وفي هذه الحالة يرى جانب من الفقه جواز امتداد التفتيش لها طالما أن ذلك يفيد في نهاية المطاف إلى أدلة وآثار قد تقود السلطة المختصة بالتفتيش إلى اثبات الجريمة[209]، وإن كان ذلك مشروط فيه أن يكون هناك احتمال وجود أدلة تتعلق بالجريمة محل الاتهام ويفيد ضبطها وتفتيشها في اظهار الحقيقة، ومع ضرورة استيفاء ضوابط التفتيش في هذه الأمكنة التي تتواجد فيها الحواسيب المحتوية على المعلومات فوجود الحاسوب في مكان سكن يوجب أن تراعي سلطة التحقيق ضوابط تفتيش المنازل مثلا.[210]

ويرى البعض بأنه لا بد من وجود قيود على عملية الدخول والتفتيش إلى البيانات والمعلومات التي تمتد إلى نهاية طرفية، كون أن امتداد التفتيش لنهاية طرفية يمنح سلطة التحقيق مبرراً للدخول والتفتيش في العديد من الأماكن التي قد تبين عندها أن المعلومات المتوفرة على الحاسوب محل التفتيش مرتبطة بمعلومات أخرى على حواسيب أخرى في أماكن غير المكان الموجود فيه الحاسوب المراد تفتيشه، مع العلم أن الأجهزة الذكية اليوم تعمل بنظام المزامنة التي تربط بين جهازين أو أكثر من خلال تبادل المعلومات التلقائي فتكون رسائل البريد الإلكتروني موجودة على أكثر من جهاز في آن واحد دون أن يكون لتلك الحواسيب الأخرى أي علاقة بالجريمة التي يتم التفتيش بشأنها. وفي هذه الحالة فقد وضعت بعض الدول قيوداً على تفتيش الأجهزة المرتبطة بنهاية طرفية داخل الدولة.[211]

وفي فلسطين فقد أجازت نصوص القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته أن يمتد التفتيش إلى البيانات والمعلومات الموجودة على حاسوب آلي في موقع آخر، فعند الرجوع إلى نص المادة (2/53) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم

---

[209] من أمثلة ذلك الفقه الألماني حيث أنه في حال كون حاسوب المتهم مرتبط بنهاية طرفية موجودة في مكان آخر داخل الدولة نفسها، يمكن أن يمتد التفتيش الى سجلات البيانات التي تكون في موقع آخر استناداً الى مقتضيات القسم (103) من قانون الإجراءات الجنائية الألماني، وفي هولندا ايضاً قد نص القانون على جواز امتداد التفتيش الى نظم المعلومات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة وذلك بمراعاة بعض القيود – عبد الفتاح بيومي حجازي، مرجع سابق، ص 380

[210] احمد حسينة، **مرجع سابق**، ص 24

[211] أحمد حسينة، **مرجع سابق**، ص 25

الاتصالات وتكنولوجيا المعلومات نرى أنه قد نص على أن "للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة".

وبالرجوع إلى نصوص القرار بقانون أعلاه نلاحظ أن المشرع الفلسطيني قد حسم الخلاف بشأن منح سلطة التحقيق أو الضبط القضائي صلاحية واسعة في الولوج إلى ملفات وأنظمة محسوبة موجودة في غير موقع ارتكاب الجريمة؛ فقد أوجب في نص المادة (53) أن يتوافر لدى سلطات الضبط القضائي إذن من النيابة من أجل الوصول إلى ملفات وبيانات ذات نهاية طرفية داخل إقليم الدولة نفسها.[212]

أما بخصوص ما ورد في اتفاقية بودابست فقد عالجت الاتفاقية موضوع صلاحيات سلطة الضبط القضائي بالوصول إلى ملفات على حاسوب ذو نهاية طرفية، ففي المادة (19) من الفصل الرابع أجازت لسلطات الضبط القضائي القائمة بعملية تفتيش الحاسوب في الدول الأطراف، والموجود الحاسوب محل التفتيش في دائرة اختصاصها، أن تمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يمكن الدخول لها من الكمبيوتر الأصلي محل التفتيش.[213]

وقد جاءت نصوص الاتفاقية العربية لمكافحة الجرائم المعلوماتية بنصوص تتوافق مع الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية، وأجازت للدول الأطراف تفتيش أجهزة الحاسوب المرتبطة بنهاية طرفية فقد نصت المادة (2/26)" تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1/أ) اذا كان هناك

---

[212] أحمد حسينة، **مرجع سابق**، ص 25

[213] التقرير التفسيري للاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية المادة (2/19) "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان أنه في حال إنجاز سلطاتها لعلميات البحث أو النفاذ إلى نظام كومبيوتر أو إلى جزء منه، وفقاً للفقرة (١/أ) وتوفر أسس لديها للاعتقاد بأن البيانات المطلوبة مخزنة داخل نظام كومبيوتر آخر أو على جزء منه على أراضي الدولة الطرف، وأنه يمكن النفاذ إلى تلك البيانات أو أنها متاحة قانونياً على النظام الأصلي، ينبغي أن تتمكن السلطات من تعجيل توسيع نطاق البحث أو النفاذ إلى النظام الآخر.

اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانوناً أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.[214]

الفرع الثاني: ارتباط حاسوب المتهم بنهاية طرفية خارج إقليم الدولة

يظهر أثناء عملية القيام بتفتيش نظام المعلومات باتصال الجهاز محل التفتيش بأجهزة خارج إقليم الدولة، كما لو تعلق الامر بشركة رئيسية أو فروعها في الخارج، حيث ترتبط تلك الأجهزة بقاعدة بيانات موجودة في الخارج.[215] ومن المتصور طبقاً لهذه الفروض قيام مرتكبي الجرائم المعلوماتية بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصالات البصرية بهدف القيام بعرقلة سلطات الضبط القضائي.[216]

ظهر إشكال مهم في عالم الجريمة الإلكترونية وهو مدى جواز امتداد إذن التفتيش ليشمل حواسيب أو أنظمة خارج نطاق الدولة. وهذا السؤال المطروح هنا قد أبرز الاختلافات في المواقف التشريعية والنظم القانونية، وكون الجريمة الإلكترونية جريمة عابرة للحدود فلا بد من توضيح كيف يمكن للسلطات المختصة أن تتعامل مع الجريمة الإلكترونية عند ظهور أدلة مرتبطة بنهاية طرفية خارج إقليم الدولة.

---

[214] الاتفاقية العربية لمكافحة الجريمة المعلوماتية المادة (2/26)

وفي القانون المصري فعند الرجوع الى نص المادة (1/6) من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات نرى أن المادة سمحت بتتبع البيانات والمعلومات في أي مكان أو نظام أو حاسب تكون موجودة فيه. "لجهة التحقيق المختصة بحسب الأحوال... ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه". وقد أنقسم رأي الفقهاء في تفسير نص المادة الى ثلاثة أراء الرأي الأول أقر بامتداد التفتيش للنظام التقني المتصل بالنظام محل الاذن واستندوا الى طبيعة الأدلة الالكترونية الخاصة إذ يمكن العثور عليها مخبأة داخل نظام معلوماتي آخر لم يتم الحصول على إذن بتفتيشه، أما الرأي الثاني فيرى بعدم جواز امتداد التفتيش الى خارج النظام المعلوماتي محل الاذن، ووقف الرأي الثالث موقف وسط بين الاثنين حيث يرى جواز تفتيش الأجهزة المرتبطة بالحاسوب محل التفتيش ولكن يجب مراعاة بعض القواعد والضوابط

[215] مصطفى علي خلف، **مرجع سابق**، ص 19

[216] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 382

أولاً: الاختصاص الدولي القضائي

قد عالج المشرع الفلسطيني مثل هذه الحالة في القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، عندما أكد بموجب المادة (2) أن أحكام هذا القرار تطبق على الجرائم الواردة فيه سواء تم ارتكابها كليا أو جزئياً داخل فلسطين أو خارجها، وسواء كان الفاعل اصلياً أو شريكاُ مع اشتراط أن تكون هذه الجرائم معاقب عليها خارج فلسطين، مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ، وقد أحال القرار بقانون مبادئ الاختصاص الدولي إلى قانون العقوبات النافذ. وقد أخذ المشرع بشرط الازدواجية والذي ويقصد به "أن يكون الفعل المطلوب التسليم بشأنه معاقباً عنه في قوانين كلتا الدولتين الطالبة للتسليم والمطلوب منها ذلك، وإذا لم يتحقق هذا الشرط بالنسبة للدول التي تتمس به فإنه يرفض التسليم لعدم توافر شرط من شروطه في التجريم.[217]

ويبقى السؤال المطروح ماذا لو كانت الجريمة معاقب عليها في فلسطين ولم يكن معاقب عليها في الدولة الموجود فيها المتهم؛ ففي هذه الحالة لا يجوز إعمال مبدأ الازدواجية في التجريم، فقد رفض القضاء التسليم في قرارات عديدة لعدم توفر شرط الازدواجية في التجريم، إذ جاء في قرار المحكمة العليا الامريكية عام 1903م "المبدأ العام في القانون الدولي، يقضي بأنه في كل حالات تسليم المجرمين فإن الفعل الذي طلب من أجله يجب أن يكون جريمة في قوانين كلتا الدولتين.[218]

وأضاف القرار بقانون في الفقرة الثانية من ذات المادة الحالات التي تطبق فيها أحكام القرار السابق عندما تتعلق بجرائم الكترونية ارتكبت خارج فلسطين[219]، وما ورد في المادة (2/3) بأن تتولى المحاكم النظامية

---

[217] وسيم الأحمد، أصول تسليم المجرمين في ضوء الاتفاقيات الدولية والتشريعات الداخلية، دار غيداء للنشر والتوزيع، عمان، الأردن، 2020، ص 25

[218] وسيم الأحمد، **مرجع سابق**، ص 25

[219] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (2/2) "يجوز ملاحقة كل من يرتكب خارج فلسطين، إحدى الجرائم المنصوص عليها في هذا القرار بقانون في إحدى الحالات الآتية: أ. إذا ارتكبت من مواطن فلسطيني. ب. إذا

والنيابية العامة وفقاً لاختصاصهما بالنظر في الدعاوى التي تكون موضوعها أحد الأفعال المجرمة بموجب هذا القانون، وهذا ما يمكن وصفه بأنه موقف محمود للمشرع الفلسطيني لأنه يحسم الجدل ويضع حلاً لإشكالية قانونية تثيرها هذه النوعية من الأفعال.[220]

ثانياً: التعاون مع الشرطة الدولية (الانتربول)

تعتبر فلسطين دولة عضو في المنظمة الدولية للشرطة الجنائية (الانتربول) منذ عام 2017م وهي منظمة حكومية دولية تظم 195 دولة عضواً، مهمتها أن مساعدة أجهزة الشرطة في جميع هذه الدول من أجل تبادل البيانات المتعلقة بالجرائم والمجرمين والوصول إليها، وتقديم الدعم الفني والميداني بمختلف أشكاله.[221]

وبالتعاون الوثيق مع البلدان الأعضاء والقطاع الخاص والفرق الوطنية تقوم منظمة الشرطة الدولية (الانتربول) للتصدي للعديد من الجرائم الإلكترونية، حيث قامت الشرطة الدولية بعملية يطلق عليها (Goldfish Alpha) والتي كشفت عن أكثر من 20 ألف موجه انترنت مقرصن، إضافة إلى كشف العديد من البرمجيات الخبيثة في مواقع التجارة الإلكترونية والتي تستهدف سرقة تفاصيل بطاقات الدفع والمعلومات الشخصية.[222]

وقد نص القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في المادة (1/62) بأن تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق بقصد الإسراع في تبادل المعلومات، وذلك

ارتكبت ضد أطراف أو مصالح فلسطينية. ج. إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد بالأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية.

[220] احمد حسينة، **مرجع سابق**، ص 26

[221] الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الانتربول) (https://www.interpol.int/ar/3/3)

[222] الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الانتربول)
(https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations)

من أجل تفادي ارتكاب الجرائم المعلوماتية والمساعدة في التحقيق بها.[223] وكفلت الفقرة الثانية من ذات المادة على سرية المعاملات بين الدول والمنظمات الدولية بحيث يتوقف التعاون المشار اليه في حال أخلت الدول أو المنظمات الدولية بالتزاماتها بالسرية.[224] وعليه فإن ارتباط حاسوب المتهم بنهاية طرفية خارج حدود الدولة قد يمتد في بعض الأحيان إلى تطبيق قواعد الاختصاص المكاني المنصوص عليها في القرار بقانون، إضافة لعملية التعاون الدولي ضمن الاتفاقيات الدولية المنظمة لموضوع الجرائم الإلكترونية تحت نطاق التعاون الدولي.

وقد أطلق المجلس الأوروبي على تفتيش النظام إذا كان موجوداً في دولة أخرى اسم الاختراق المباشر أو التفتيش عبر الحدود، وقد أصدر المجلس توصيات في هذا الشأن اجازت هذه التوصيات أن يمتد التفتيش التقني لأجهزة الحاسوب إلى الشبكة المتصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة.[225]

ثالثاً: دور الاتفاقيات الدولية عند ظهور أدلة مرتبطة بنهاية طرفية خارج إقليم الدولة

أجازت الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) الوصول إلى البيانات ذات نهاية طرفية في خارج حدود الدولة، فقد نصت المادة (32) "يجوز لدولة طرف دون ترخيص من دولة طرف أخرى أن تنفذ إلى بيانات الكمبيوتر المخزنة والمتاحة للعموم بغض النظر عن مكان تواجد البيانات جغرافياً، أو النفاذ إلى بيانات كومبيوتر مُخزنة موجودة لدى دولة طرف أخرى أو تلقيها، من خلال نظام كومبيوتر داخل

---

[223] القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية المادة (1/62) "تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات، بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال، وتفادي ارتكابها، والمساعدة على التحقيق فيها، وتتبع مرتكبيها"

[224] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (2/62) " يتوقف التعاون المشار إليه في الفقرة السابقة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعينة بهذا القرار بقانون.

[225] مصطفى علي خلف، **مرجع سابق**، ص 19 " نصت التوصيات رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات في مادتها الثالثة على أنه (لسلطة التحقيق عند تفتيش المعلومات وفقاً لضوابط معينة أن تقوم بمد مجال تفتيش الكمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة ما دامت مرتبطة بشبكة واحدة وأن تضبط البيانات الموجودة فيها ما دام أنه من الضروري التدخل الفوري للقيام بذلك)

أقاليمها، في حال حصول تلك الدولة الطرف على الموافقة القانونية والطوعية للشخص الذي يتوفر على السلطة القانونية للكشف عن البيانات لتلك الدولة الطرف عبر نظام الكومبيوتر المذكور".[226]

ومن هذا المنطلق فقد عالجت الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) حالة ارتباط جهاز المتهم بنهاية طرفية خارج حدود الدولة حيث أن الاتفاقية لم تتوسع في تفسير هذه الحالة وانما توجب في نصوصها ان تتوقف عملية التفتيش في البيانات الخاصة على الموافقة الطوعية للشخص الذي تتوافر البيانات والمعلومات محل التفتيش معه. ونصت المادة (40) من الاتفاقية العربية لمكافحة الجريمة المعلوماتية "يجوز لاي دولة طرف، وبدون الحصول على تفويض من دولة أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات".[227] أما بخصوص المعلومات والبيانات غر مفتوحة المصدر فيجوز لها أن تصل أو تستقبلها من خلال تقنية المعلومات في اقليمها وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانوني للكشف عن تلك المعلومات.[228]

وعليه فإن قيام ما يقارب 22 دولة عربية بالتوقيع على الاتفاقية العربية لمكافحة الجريمة المعلوماتية من ضمنها 7 دول صادقت عليها ومنها فلسطين حيث صادقت عليها في عام 2012 ومصر والمملكة الأردنية الهاشمية؛ يفتح ذلك المجال أمام هذه الدولة بالتعاون الدولي في عملية التحقيق والتفتيش في الجرائم الإلكترونية وفي حال كانت البيانات المراد ضبطها تقع ضمن أحد الدول المصدقة عليها.[229]

---

[226] الاتفاقية الأوروبية لمكافحة الجريمة الالكتروني (بودابست) المادة (32)

[227] الاتفاقية العربية لمكافحة الجريمة المعلوماتية، المادة (1/40)

[228] الاتفاقية العربية لمكافحة الجريمة المعلوماتية، المادة (1/40)

[229] الاتفاقية العربية لمكافحة الجريمة المعلوماتية (قائمة الدول العربية الموقعة والمصدقة على الاتفاقية العربية لمكافحة الجريمة المعلوماتية)
وفي مصر نصت المادة (4) من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات على أن تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية الثنائية المصدق عليها؛ وعليه فقد جعل المشرع المصري امتداد التفتيش داخل نظام معلوماتي يوجد في مكان آخر خارج الدولة مسألة تخضع للاتفاقيات الدولية والمعاهدات ونظام المعاملة بالمثل ما بين المنح والمنع

المبحث الثاني

الصعوبات التي تواجه عملية التفتيش في الجرائم الإلكترونية

إن التحقيق في الجرائم الإلكترونية كما ذكرنا سابقاً بحاجة إلى مراعاة بعض الضوابط والقيود ويختلف في طبيعته كونه ذا طبيعة فنية، ومن المهم أن تكون السلطة المختصة بممارسة عملية التحقيق في الجرائم الإلكترونية تتمتع بخلفية واضحة عن الخصوصية التي تحتاجها الجريمة الإلكترونية وتميزها عن غيرها من الجرائم، وكون الجريمة الإلكترونية ذات طبيعة فنية؛ فقد تواجه السلطات المختصة بالتحقيق البعض من الصعوبات، وخصوصاً في حال أن الدليل الإلكتروني يتمتع بالطبيعة الفنية، وقد قام الباحث بصدد بتقسيم هذا المبحث إلى مطلبين رئيسيين في المطلب الأول سوف يدرس ماهية الصعوبات الفنية التي تواجه الضابطة القضائية وفي المطلب الثاني سوف يدرس آلية الاستعانة بالخبراء الفنيين من أجل مواجهة الصعوبات الفنية.

المطلب الأول: الصعوبات الفنية التي تواجه الضابطة القضائية في التفتيش بالجرائم الإلكترونية

يمكن تحديد الصعوبات التي تواجه الضابطة القضائية في الجرائم الإلكترونية عن طريق تحديد الطبيعة الخاصة للجرائم الإلكترونية والتي تحدثنا عنها سابقا، فكما ذكرنا سابقا أن الجريمة الإلكترونية تتمتع بالطابع الفني، وكون إجراءات التحقيق العملية والفنية والنفسية يتوقف استخدامها على ظروف كل جريمة على حدة مع مراعاة الخصوصية التي تتسم بها الجريمة الإلكترونية.[230]

ومن هذا المنطلق تنتج بعض الصعوبات التي تتعلق بالجريمة الإلكترونية نفسها والبعض الآخر يتعلق بالدليل الرقمي كونه يتمتع بطابع فني يجعله يختلف عن غيره من الأدلة. وقد شرحنا سابقاً عن الدليل الالكتروني باعتباره أحد أدلة الاثبات الجنائي، ومن هنا فقد رأى الباحث أن يقوم بتقسيم الصعوبات التي

---

[230] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 108

تواجه الضابطة القضائية إلى قسمين، القسم الأول يتمثل في توضيح الصعوبات التي تتعلق بالجريمة الإلكترونية نفسها في الفرع الأول، والقسم الثاني يتمثل في توضيح الصعوبات التي تتعلق بالدليل الالكتروني في الفرع الثاني.

الفرع الأول: الصعوبات التي تتعلق بالجريمة الإلكترونية

هناك العديد من الصعوبات التي تواجه سلطات التحقيق بحيث يكون سبب هذه الصعوبات الطبيعة الخاصة بالجريمة الإلكترونية ذاتها، ومن هذه الصعوبات الصعوبة التي تكون بسبب الجهات المتضررة وسببها الإحجام عن الإبلاغ عن الجريمة المعلوماتية وفقدان الاثار التقليدية للجريمة وصعوبة تحديد الجاني.

أولاً: صعوبات مصدرها الإحجام عن الإبلاغ

تظل الجريمة الإلكترونية مستترة ما لم يتم الإبلاغ عنها من قبل المتضررين، ومن ثم يتم تحريك الدعوى الجنائية حسب القانون السائد، والصعوبة التي تواجه أجهزة الامن والمحققين الجنائيين هي أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالطرق العادية كما هو الحال في الجرائم التقليدية وذلك لصعوبة اكتشاف مثل هذا النوع من الجرائم من قبل الأشخاص العاديين أو حتى الشركات والمؤسسات، أو لأن هذه الجهات تحاول درء الأثر السلبي للإبلاغ عن الجريمة فلا تبلغ عن الجرائم التي ارتكبت ضدها.[231]

وتتعمد أغلب الشركات والأشخاص التستر على الجريمة الإلكترونية وعدم الإبلاغ عنها للجهات المختصة غالباً في جرائم الابتزاز، وهذا يؤدي إلى عدم التعاون مع السلطات المختصة في مكافحة الجرائم المعلوماتية، كما أن كثير من الجهات التي تتعرض أنظمتها المعلوماتية للاعتداء، وتتعمد هذه الجهات إلى عدم الكشف

[231] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 109

والتبليغ عن ذلك لدى السلطات المختصة تجنباً للأضرار بسمعتها أو خوفاً من الكشف عن أسلوب ارتكاب الجريمة مما يؤدي إلى تكرار وقوعها من أطراف أخرى.[232]

وفي الولايات المتحدة الامريكية مثلاً طالب البعض بأن تتضمن القوانين المتعلقة بجرائم الحاسوب والمعلومات نصوصاً تلزم موظفي الجهة المجني عليها أياً كانت بضرورة الإبلاغ عما يصل إلى علمهم من الجرائم التي تتعلق بهذا المجال، وتقرير جزاء على الاخلال بهذا الالتزام؛ وكان ذلك من أجل تفعيل عملية الإبلاغ عن الجريمة المعلوماتية وتسهيل كشفها.[233]

ثانياً: فقدان الآثار التقليدية للجريمة

إذا كان من السهل على جهات التحري والتحقيق أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع أو سماع الشهود، فإن الامر يختلف في الجرائم الإلكترونية، وبصدد ذلك فأن الجرائم هذه لا تصل إلى علم السلطات المعنية بطريقة اعتيادية كباقي الجرائم التقليدية؛ كون هذه الجرائم لا تخلف اثاراً مادية، وكل هذا يعود إلى طبيعة الجريمة المرتكبة والوسيلة التي ارتكبت بها هذه الجريمة، ويرجع السبب أيضاً إلى فقدان الآثار التقليدية للجريمة الإلكترونية. وقد لاحظ جانب من الفقه أن هناك بعض العمليات التي يتم ادخال بياناتها مباشرة إلى جهاز الحاسوب دون أن يتوقف هذا الادخال على وجود وثائق ومستندات يتم النقل منها.[234]

وعليه فلو كان البرنامج المراد ارتكاب الجريمة الإلكترونية بصدده معداً ومخزناً على جهاز الحاسوب ويتوفر أمام الشخص الذي يتعامل به عدة خيارات، وليس له سوى أن ينقر أو يضغط على الخيار الذي يريده

---

[232] عماد بلغيث، **صعوبات التحقيق في الجرائم الالكترونية**، مجلة الرسالة للدراسات البحوث الإنسانية، مجلد 6، عدد 3، ص ص. 70 – 83، منشور في جامعة محمد بوضياف، الجزائر،2021، ص 81

[233] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 116

[234] بثينة حبيباتني، **معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية**، العدد 50، الصفحات 85–97، 2018، ص 87

فتكتمل حلقة الامر المطلوب تنفيذه، كما في المعاملات المالية في البنوك أو الشركات والمؤسسات التجارية الكبرى حيث يتم رصد البيانات المخزنة أو حسابات العملاء ونقلها من لآخر حسب الأوامر التي يتم اعطاءها لجهاز الحاسوب ويمكن في الفروض السابقة ارتكاب بعض أنواع الجرائم كالاختلاس أو التزوير وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسوب؛ وتكون النتيجة مخرجات على هوى مستعمل الجهاز الذي أدخل البيانات أو عدل بها دون استخدام وثائق أو مستندات ورقية، وبالتالي تفقد الجريمة آثارها التقليدية.[235]

ثالثاً: صعوبة تحديد الجاني في الجرائم الإلكترونية

إن صعوبة تحديد الجاني في الجرائم الإلكترونية تعتبر من أكثر الصعوبات التي تواجهها السلطات المختصة في مكافحة الجريمة الإلكترونية؛ حيث أن المجرم المعلوماتي يعمل بذكاء للقيام بإخفاء هويته للحيلولة دون تعقبه وكشف هويته وذلك حتى تظل أعماله الاجرامية بعيدة كل البعد عن السلطات المعنية بمكافحة الجرائم الإلكترونية.[236]

كما أن القدرة الكبيرة من الذكاء والتفوق التي يتميز بها المتورطون في الجرائم المعلوماتية تجعلهم يباشرون إجرامهم بدقة متناهية خشية افتضاح امرهم وضبطهم، إذ غالباً ما يقوم المجرم المعلوماتي بعمل سياج أمنى على افعاله غير المشروعة قبل ارتكابها، كي لا يقع تحت طائلة العقاب.[237]إضافة إلى أن المجرم المعلوماتي يتملك خبرة عالية وقدرة تجعل المحقق الجنائي يعاني من صعوبة بتحديد مكانه وذلك عن طريف استخدام تقنيات البروكسي والشبكات الخاصة الافتراضية (VPN).[238]

---

[235] جاسر خلف، **صعوبات الدليل الجنائي في الجرائم المعلوماتية**، مجلة القانون للدراسات والبحوث القانونية، العدد 12، العراق، 2016، ص 10

[236] عماد بلغيث، **مرجع سابق**، ص 81

[237] بثينة حبيباتني، **مرجع سابق**، ص 88

[238] Graeme Edwards, **Cybercrime Investigators Handbook**, 2019, P. 86

ويرى الباحث أن الصعوبات التي تتعلق بالجريمة الإلكترونية تؤدي إلى عرقلة تنفيذ العدالة في بعض الأحيان، كما أن الذكاء المعلوماتي الذي يتمتع به المجرم يزيد من صعوبة اكتشاف الجريمة، إضافة إلى الآثار التي تنتج عن الجريمة نفسها كجرائم الابتزاز الالكتروني، مما لها من أثر واضح على سمعة الأشخاص، تزيد من فرصة التستر على الجريمة المعلوماتية.

الفرع الثاني: الصعوبات التي تتعلق بالدليل الالكتروني

القسم الثاني من الصعوبات التي تواجه سلطات التحري والاستدلال في الجرائم الإلكترونية هي الصعوبات التي تتعلق بالدليل الالكتروني نفسه، فسبق أن قام الباحث بتوضيح الدليل الالكتروني بكافة التفاصيل الخاصة به والطبيعة الخاصة به، وعليه يتوجب علينا بيان الصعوبات التي تواجه الدليل سلطات الاستدلال في التعامل مع الدليل الالكتروني وتتمثل بعض هذه الصعوبات في صعوبة الحصول على الدليل الالكتروني في بعض الأحيان وضخامة البيانات المتعين فحصها إضافة إلى عدم محدودية شبكة الانترنت.

أولاً: صعوبة الحصول على الدليل الرقمي

تكمن الصعوبة في الحصول على الدليل الالكتروني في بعض الأحيان إلى لجوء الفاعلين إلى استخدام تقنيات التشفير أو استخدام كلمات السر؛ وذلك من أجل حماية النشاطات التي يقومون بها على جهاز الحاسوب ويقوم الفاعلون ايضاً بالاستعانة بالبرامج والتطبيقات التي تعمل على طمس هويتهم اثناء ارتكاب الجرائم الإلكترونية.[239] وفي أغلب الأحيان تكون البيانات المخزنة على الحاسوب والمتعقلة بالمتهم مشفرة على الرغم من أن الحاسوب بحد ذاته يكون متاح أمام العلن، فقد يقوم المتهم بتشفير مجلد محدد فقط أو قسم محدد داخل القرص الصلب مع بقاء النظام مفتوحاً أمام المستخدم دون تشفير.[240]

---

[239] عماد، بلغيث، **مرجع سابق**، ص 79

[240] Mohamed Chawki, Ashraf Darwish, Mohammad Khan, Sapna Tyagi Cybercrime, **Digital Forensics and Jurisdiction**, Studies in Computational Intelligence Volume 593, Polish Academy of Sciences, Warsaw, Poland, Springer, 2016, P. 21

وعلى الرغم من قيام الجهات ذات الأنظمة المعلوماتية بحماية نظمها عن طريق الترميز والتشفير وغيرها من طرق الحماية الإلكترونية، فإن قراصنة الحاسوب والعاملين في ذات المؤسسات يمكن لهم القيام باختراق هذه الأنظمة ومن ثم يقومون بكسر نظام الحماية ويجعلونه نظام عديم الجدوى، ولاسيما لو كان أحد الفاعلين هو عامل من داخل المؤسسة نفسها وذلك بغرض الدخول إلى المعلومات السرية أو تغيير الأرقام والبيانات، كما أن الأمور لا تقف عند هذا الحد فقط بل يقوم هؤلاء الأشخاص بفرض تدابير أمنية لمنع التفتيش المتوقع بحثاً عن أدلة من الممكن أن تدينهم وذلك باستخدام كلمات سر أو رموز تشفير خاصة.[241]

ومن الأمثلة التي لجأ فيها الجاني إلى أسلوب التشفير لإعاقة سلطات التحقيق، ما حصل في الولايات المتحدة الامريكية سنة 1996، اذ كان المشتبه به مشغلا للوحة إعلانات (BBS)، وبعد الوصول إلى جهاز الحاسوب الشخصي الذي يستخدمه لإدارة اللوحة وبعد أخذ نسخة احتياطية من القرص الصلب لم يتمكنوا من العثور على كلمة المرور الخاصة بالمشتبه به لأنها كانت مشفرة.[242]

ثانياً: ضخامة البيانات المتعين فحصها

إن إحدى الصعوبات الكبيرة التي تواجه سلطات الاستدلال والتحري في الجرائم الإلكترونية كمية البيانات والمعلومات الضخمة والتي تكون بحاجة إلى فحص ودراسة من أجل أن يستخلص منها دليل الجريمة الإلكترونية، ففضلاً عن ضرورة توفر الخبرة الفنية في مجال الحاسوب الآلي والمعلوماتية لدى رجال الضابطة القضائية، يتعين عليهم القيام بفحص هذا الكم الهائل من البيانات والمعلومات المخزنة على جهاز الحاسوب أو على الأقراص الصلبة والمرنة.[243]

---

[241] بيومي فؤاد حجازي، **مرجع سابق**، ص 90

[242] حورية المتوكل، **تحديات الحصول على الدليل الالكتروني**، مجلة القانون والاعمال، العدد 65، ص ص. 110–120، المغرب، 2016، ص 113

[243] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 184

ويسلك المحقق لمواجهة هذه الصعوبة أحد المسلكين، إما بحجز هذه البيانات الإلكترونية والمعلومات بقدر يفوق قدرته البشرية على مراجعتها أو يقوم بالتغاضي عن كل هذه البيانات على أمل في الحصول على الاعتراف من المتهم بالجريمة المعلوماتية.[244] لذلك يمكن القول أن ضخامة هذه البيانات والمعلومات، تعد عائقاً أمام سلطات الاستدلال في التحقيق في الجرائم الإلكترونية، ذلك أن طباعة كل ما هو موجود على الدعامات الممغنطة لحاسب متوسط العمر مثلاً، يتطلب آلاف من الصفحات في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئاً مفيداً للتحقيق في الجريمة الإلكترونية.[245]

كما تمثل ضخامة البيانات أحد التحديات الرئيسية أمام الطب الشرعي الرقمي (Digital Forensics) فيمكن أن تستغرق عملية التحليل الجنائي وقتاً أطول وأن تتطلب مواردا أكثر من الموارد المتاحة لدى سلطات التحقيق؛ فيؤدي ذلك إلى إبطاء عملية التحقيق الجنائي في بعض الأحيان.[246]

ثالثاً: لا محدودية شبكة الانترنت

من الصعوبات التي تواجه سلطات الاستدلال في الجرائم الإلكترونية هو لا محدودية شبكة الانترنت فهي ليست مملوكة لأحد، ولا تعترف بالحدود الجغرافية للدول، وبالتالي لا يوجد لهذه الشبكة جهاز رقابي عليها ولا يوجد سلطات مركزية تتحكم فيها، فالإنترنت ما هو إلا ظاهرة دولية تنعدم مركزيتها وتتساوى امامه الدول الكبيرة والصغيرة ويؤدي ذلك إلى خلق صعوبة كبيرة أمام الجهات التي تقوم بتعقب أدلة الاثبات عبر هذه الشبكة.[247]

---

[244] بثينة حبيباتني، **مرجع سابق**، ص 89

[245] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 184

[246] André Årnes, **Digital Forensics,** Norwegian University of Technology and Science (NTNU), first edition published by John Wiley & Sons Ltd, 2018, P.313

[247] بثينة حبيباتني، **مرجع سابق**، ص 89

كما أن انتشار تكنولوجيا الانترنت فائق السرعة (ADSL)، والذي لم يسلم هو الاخر من يد المجرمين، إذ استخدموه لتنفيذ مخططاتهم الاجرامية وذلك عن طريق قيامهم بالاشتراك إلى جانب أشخاص اخرين في جهاز واحد عن طريق موزع خطوط واحد؛ ويؤدي ذلك إلى صعوبة التوصل لهم، فضلا عن ظهور تقنية الانترنت اللاسلكي، والذي سهل من جانب اخر قيام المجرمين وقراصنة الانترنت من التنقل إلى عدة أماكن في يوم واحد وصعوبة الوصول لهم وتحديد موقعهم.[248]

وعليه فيرى الباحث أن هناك العديد من الصعوبات التي تواجه سلطات التحقيق في الجرائم الإلكترونية يكون بعضها بسبب الطبيعة الخاصة بالجرائم الإلكترونية نفسها والبعض الاخر بسبب طبيعة الدليل الالكتروني الرقمية والتي بحاجة لدقة أكثر بالتعامل مقارنة بالأدلة التقليدية ، كما أن قدرات الأشخاص العاديين في بعض الأحيان قد لا تستوعب القيام بالبحث في الأدلة الرقمية وذلك لدقة المعطيات المراد البحث بها أو لضخامة البيانات والمعلومات، وعليه تظهر حاجة سلطات التحقيق إلى ندب خبراء فنيين من أجل مواجهة الصعوبات المترتبة أثناء عملية التحقيق في الجرائم الإلكترونية.

المطلب الثاني: الاستعانة بالخبراء الفنيين من أجل مواجهة صعوبات التفتيش في الجرائم الإلكترونية

قد تواجه سلطات التحقيق وجمع الاستدلالات في الجريمة الإلكترونية في بعض الأحيان صعوبات في عملية استخلاص الدليل الإلكتروني أو تحليله أو في حالة التفتيش والتنقيب عنه، وذلك نظراً للطبيعة الفنية الخاصة التي تتمتع بها للأدلة الإلكترونية؛ لذلك ظهرت الحاجة للاستعانة بالخبراء الفنيين في مواجهة هذه الصعوبات التي تطرأ أثناء عملية التحقيق في الجرائم الإلكترونية، ويعتبر الخبير بشكل عام ذلك الشخص الذي يعلم بأمر من الأمور ويمتلك خبرة علمية وفنية في حقل من حقول المعرفة.[249] فالخبرة ليست دليلا

---

[248] نبيلة هروال، **مرجع سابق**، ص 170

[249] مصطفى عبد الباقي، **مرجع سابق**، ص 410

مستقلاً بل هي تقييم مادي للدليل، حيث تلجأ المحكمة لها من أجل كشف الحقيقة.[250] وبشكل عام، يتمثل واجب الخبراء تقديم الحقيقة الموضوعية وغير المتحيزة من المسألة المعروضة على المحكمة وليس من دورهم أن يدافعوا عن جانب واحد.[251] ومن هذا المنطلق فقد رأى الباحث أن يقوم بتقسيم هذا المطلب لفرعين رئيسيين، في الفرع الأول سوف يدرس القواعد القانونية والفنية التي تحكم عمل الخبراء الفنيين في الجرائم الإلكترونية وفي الفرع الثاني سوف يدرس أساليب عمل الخبراء الفنيين في الجرائم الإلكترونية.

الفرع الأول: القواعد القانونية والفنية التي تحكم عمل الخبراء الفنيين في الجرائم الإلكترونية

من أجل دراسة القواعد القانونية التي تحكم عمل الخبراء الفنيين لا بد لنا في البداية أن نقوم بتوضيح تعريف الخبير الفني من الناحية العلمية والقانونية؛ وعليه يعرف الخبير الالكتروني الرقمي بأنه الشخص الذي تعمق في دراسة عمل من الأعمال الإلكترونية وتخصص في أدائه فترة زمنية طويلة مما أكسبه خبرة عملية بحيث أصبح ملماً بتفصيلاته، مما جعله ذلك يتفوق على الشخص العادي وقادر على إبداء الرأي الرقمي في الأمور المتصلة بهذا العمل.[252]

نظم قانون الإجراءات الجزائية الفلسطيني ندب الخبراء، فقد ورد في الفصل الثاني من الباب الأول تحت عنوان التحقيق، كما تطرق للخبرة في موضوع البينات التي تستند لها المحكمة في حكمها، وهذا يعني أن ندب الخبراء هو من إجراءات التحقيق الابتدائي التي تتخذه سلطات التحقيق، ويلجأ القاضي للخبرة في مرحلة المحاكمة لتفسير واقعة غامضة يحتاج فك شيفرتها اللجوء إلى أهل العلم في مجال ذات العلاقة،

---

[250] بيومي فؤاد حجازي، **مرجع سابق**، ص 321

[251] Eoghan Casey, **Digital Evidence and Computer Crime**, Third Edition Forensic Science, Computers, and the Internet, Published by Elsevier, 2011, P. 51

[252] مصطفى محمد موسى، **مرجع سابق**، ص 221

ويجوز للنيابة العامة أن تقوم بانتداب الخبير، أو ينتدب الخبير من المحكمة نفسها أو بناء على طلب أحد الخصوم في الدعوى.[253]

وقد نص القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته في المادة (4/53) "لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات"، ومن الملاحظ أن القرار بقانون ايضاً أجاز الاستعانة بالخبراء الفنيين في حالة تعذر النيابة العامة ومأموري الضبط القضائي من النفاذ إلى البيانات والمعلومات الموجودة على جهاز الحاسوب أو أحد أقراص التخزين.

وقد أجاز قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 الاستعانة بالخبراء الفنيين ونظم عملية الاستعانة بالخبراء وذلك من نص المادة (10) حيث نص على انشاء سجلان لقيد الخبراء الفنيين والتقنيين داخل الجهاز القومي لنظم الاتصالات وتطبق على عملهم القواعد والاحكام الخاصة بقواعد تنظيم الخبرة أمام الجهات القضائية.[254] أما في الأردن فلم يتطرق قانون الجرائم الإلكترونية رقم 27 لسنة 2015 لتنظيم عمل الخبراء، وهذا لا يعني عدم إمكانية اللجوء إلى الخبرة بل يمكن الرجوع إلى قواعد قانون أصول المحاكمات الجزائية الاردني، حيث تطرق إلى الخبرة بشكل في صريح في المواد (39-41).

وفي الولايات المتحدة الامريكية فقد نصت القاعدة (702) من قواعد الاثبات الفدرالية إلى إمكانية اللجوء إلى شهادة الخبير الفني فهم الحقيقة واستيضاح الأدلة العلمية في المحكمة، وينطبق ذلك على الأدلة الرقمية باعتبارها أدلة علمية خاضعة للتقييم أو التحليل.[255]

---

[253] مصطفى عبد الباقي شرح قانون الإجراءات الجزائية الفلسطيني، **مرجع سابق**، ص 411

[254] قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 المصري، المادة (10)

[255] Larry Daniel and Lars Daniel, **Digital Forensics for Legal Professionals Understanding Digital Evidence from the Warrant to the Courtroom**, Syngress, 2012, P. 68

وعليه فقد ترك المشرع للمحقق الجنائي في الجرائم بصفة عامة وفي الجرائم الإلكترونية بصفة خاصة الحرية الكاملة للاستعانة بالخبير من أجل إيضاح مسألة قد يستعصي فهمها، وخاصة أن الحواسيب الإلكترونية الرقمية والشبكات المتعددة تنتمي إلى تخصصات علمية وفنية دقيقة ومتطورة ومتلاحقة لدرجة يصعب حتى على المتخصص تتبعها، وخاصة أنه في هذا الزمان لا يوجد خبير لديه معرفة متعمقة في جميع أنواع التقنية الإلكترونية والشبكات الرقمية كون الجريمة الإلكترونية واسعة المجال كذلك في نفس الحال فلا يوجد خبير قادر على التعامل مع كافة أنواع الجرائم التي تقع عبر الحاسوب وشبكاته أو تقع عليه.[256]

يجب أن يتوافر لدى خبراء الحاسوب المنتدبين للتحقيق في الجرائم الإلكترونية القدرة والامكانية العلمية والفنية في المسألة موضوع الخبرة ولا يكفي في ذلك فقط حصول الخبير على الشهادات العلمية في صلب تخصصه، بل يجب مراعاة الخبرة العلمية، كون هذه الخبرة هي التي تحقق الكفاءة في عمل الخبير الفني.[257]

وتجدر الإشارة إلى أن بعض الفقه، يرى أنه لا يشترط في الخبير المنتدب أن يكون متخرجاً من جامعات ومعاهد متخصصة في علوم الحاسوب والانترنت بل يكفي اكتساب المهارة في استعمال الحاسوب ووسائل تكنولوجيا المعلومات الحديثة، وبالتالي التعامل مع تقنية المعلومات بطريقة عملية وسلسة، إلا أنه بالرغم من واقعية الامر السابق، الا أن ذلك يتعارض مع الواقع القانوني حيث أن الخبير الفني في نهاية عمله يجب أن يقدم تقريراً متكاملاً لعناصره الشكلية والموضوعية وبالتالي لا يمكن لشخص لديه فقط داريه أن يعد هذا التقرير.[258]

---

[256] مصطفى محمد موسى، **مرجع سابق**، ص 224

[257] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 330

[258] توفيق خشاشنة، **مرجع سابق**، ص 328

ويتشكل الخبراء الفنيين من المبرمجين وهم المتخصصون في كتابة أوامر البرمجة سواء كانت برامج النظام أو التطبيقات، إضافة إلى المحلل الذي يقوم بتحليل خطوات العمل وتجميع البيانات، ومهندسو الصيانة والاتصالات المسؤولون عن صيانة التقنيات الإلكترونية، ومشغل الحاسب الالي وشبكاته الذي لديه خبرة في قواعد كتابة البرامج وتشغيل الجهاز، واخيراً مدير النظام المعلوماتي الذي يختص بالإدارة في النظم المعلوماتية.[259]

ويقوم كل خبير اعلاه بتحرير تقرير ليتضمن خلاصة ما توصل اليه من نتائج، وبعد الانتهاء من فحص الدليل الالكتروني يعمل بعدها على تقديم التقرير الكتابي خلال المدة الزمنية المحددة له من قبل القاضي ولا يحق له التأخير دون وجود سبب مقنع، ويخضع هذا التقرير شأنه شأن باقي وسائل الاثبات لتقدير القاضي، فهذا التقرير يعتبر غير ملزم للقاضي حيث يحق له الاخذ بهذا التقرير أو استبعاده بناءً على قناعته الشخصية.[260]

الفرع الثاني: أساليب عمل الخبراء الفنيين في الجرائم الإلكترونية

من أجل أن يقوم الخبير الفني بإتمام عمله في عملية الكشف عن الدليل الرقمي في الجرائم الإلكترونية لا بد له من استخدام بعض الوسائل والأساليب الفنية التي تمكنه من القيام بهذا العمل بصورة صحيحيه، فخبير تحليل الخطوط مثلا يستخدم اجهزة معينة ونمط تحقيق معين لاكتشاف جريمة التزوير، وكذلك الخبير في الجرائم الإلكترونية الذي يستخدم أساليب خاصه به من أجل اكتشاف وقوع الجريمة أو تحليل الدليل المعروض أمامه وتشمل هذه الأساليب قيامه بحصر المواقع وتجميعها باستخدام بروتوكول الانترنت، واستخدام برامج التتبع وكشف الاختراق، وبيان المسائل الفنية التي يصعب على سلطات التحقيق تحليلها.

---

[259] مصطفى محمد موسى، **مرجع سابق**، ص 223

[260] توفيق خشاشنة، **مرجع سابق**، ص 329

أولاً: حصر المواقع وتجميعها

في الجرائم المرتكبة عن طريق الشبكة المعلوماتية يقوم الخبير بحصر وتجميع المواقع التي تشكل في حد ذاتها جريمة كمواقع التهديد والنصب والاحتيال، أو جرائم نسخ وبث صور فاضحة وغيرها، ومن ثم القيام بعملية تحليل رقمي لهذه المواقع وتحديد عناصر حركتها للتوصل إلى بروتوكول الانترنت (IP) الذي ينسب إلى جهاز الحاسوب الذي صدرت عنه هذه المواقع.[261]

وتوجد أكثر من طريقة يمكن من خلالها معرفة العنوان الخاص بجهاز الكمبيوتر في حالة الاتصال المباشر منها على سبيل المثال ما يستخدم في حالة العمل على نظام التشغيل ويندوز حيث يتم كتابة الامر (WINPCFG) في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP) مع الملاحظة أن عنوان الانترنت من الممكن أن يتغير مع كل اتصال بشبكة الانترنت.[262]

ثانياً: التحفظ على الأدلة الرقمية من بروتوكولات النقل والشبكات

يقوم الخبير في هذه الحالة برصد ومعاينة مواقع الانترنت أو المعلومات التي تشير إلى ارتكاب الجريمة والتي تكون في مظهر مختلف كجريمة القذف التي حصلت في غرفة الدردشة مثلا، ففي هذه الحالة يقوم الخبير باللجوء إلى ذاكرة الخادم الذي يتولى ربط غرفة الدردشة المعنية عبر العالم الرقمي، وبذلك يمكن للخبير تحديد موضوع السب والقذف وتحديد التاريخ الذي حصلت فيه الجريمة، أما في الجرائم التي تتم عن طريق النشر يقوم الخبير التقني باستخدام برمجيات مساعدة للتوصل قاعدة بيانات الموقع.[263]

ومن أمثلة ذلك استخدام موقع خرائط جوجل في حل العديد من قضايا القتل عن طريق سجلات البحث التي يستخدمها المتهمين في البحث عن مواقع من أجل التخلص من جثة الضحية، حيث طبق هذا العمل

---

[261] توفيق خشاشنة، **مرجع سابق**، ص 333

[262] مختار تابري، **الخبرة في الجريمة المعلوماتية**، مجلة الحوار المتوسطي، مجلد 11، عدد 3، الجزائر 2020، ص 393

[263] توفيق خشاشنة، **مرجع سابق**، ص 335

في محاكمة سكوت بيترسون في مقتل لاسي بيترسون عندما قدمت النيابة العامة خرائط جوجل التي تم استخرجها من حاسوب سكوت بيترسون حيث كان يستخدمها من أجل العثور على موقع معين للتخلص من الجثة.[264]

ثالثاً: استخدام برامج التتبع وكشف الاختراق

تقوم هذا البرامج بالتعرف على محاولات الاختراق ويتم تقديم بيان إلى المستخدم الذي تم اختراق جهازه، حيث يحتوي هذا البيان في مضمونه على اسم الحدث وتاريخ حدوثه والعنوان الذي تمت من خلاله عملية الاختراق واسم الشركة المزودة للأنترنت، إضافة إلى نظام كشف الاختراق حيث تتولى هذه الفئة مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الشبكة.[265]

ويطلق على برامج كشف الاختراق مصطلح (Intrusion Detection Systems) ومن أمثلتها برنامج (SolarWinds Security Event Manage) حيث يعمل هذا البرنامج على كشف التهديدات التي من الممكن أن تؤثر على نظام المعلوماتي، إضافة إلى تحليل المعطيات داخل النظام المعلوماتي وتفسير سجلات الاحداث التي تم إنشاؤها بواسطة برامج أخرى داخل الشبكة أو النظام المعلوماتي.[266]

رابعاً: بيان المسائل الفنية التي تفوق خبرات السلطات المختصة

هناك العديد من المسائل التي تفوق خبرات الضابطة القضائية والنيابة العامة والتي يتطلب استيضاحها اللجوء إلى الخبير الفني، فتلجأ الجهات المختصة إلى الخبير الفني من أجل عزل النظام المعلوماتي دون تلف الأدلة أو تدميرها، ونقل الأدلة الرقمية إلى وحدات التخزين الخارجية دون اتلافها، إضافة إلى اخراج

---

[264] Larry Daniel and Lars Daniel, **Ibid**, P.215

[265] مختار تابري، **مرجع سابق**، ص 394

[266] Jean Dahj, **Mastering Cyber Intelligence**, Packt Publishing Ltd, Birmingham, UK ,2022, P. 173

الأدلة الرقمية في وسيلة ورقية تتيح للقاضي أن يقوم بقراءتها وفهمها مع إثبات أن الموجود على السطور هو مطابق تماماً للبيانات المسجلة على الحاسوب أو النظام أو الشبكة.[267]

كما يعمل الخبير الفني أيضاً على اصلاح الدليل الرقمي وإعادة تجميعه من مكونات الكمبيوتر المادية في حال فقدانه أو محاولة العبث به، وجمع الاثار المعلوماتية التي تتبدل خلال الشبكة، وأحد المسائل المهمة ايضاً التي يقوم الخبير الفني ببيانها في المحكمة هي التأكد من أن الدليل المعروض امامه لم يتم العبث به أو تعديله وذلك باستخدام الخوارزميات المحوسبة.[268]

ويحتاج الخبير إلى بعض الإمكانيات الرقمية التي تتيح له معالجة الأدلة واكتشاف المعلومات التي يتضمنها الدليل الالكتروني، وتتمثل في الأجهزة والبرمجيات والأنظمة، ومن الأجهزة التي يحتاج لها الخبير جهاز الحاسوب المحمول مزود ببطاقة شبكة الانترنت ووصلات خارجية للربط مع أي شبكة متوفرة، ومجموعة فارغة من أقراص التخزين، أما بخصوص البرمجيات فيحتاج الخبير إلى برامج الضغط وفك الضغط، وبرامج معالجة الصور وبرامج التشفير وفك التشفير مثل برنامج (PGP)، وبرامج استعادة الملفات المحذوفة إضافة إلى العديد من البرمجيات المختلفة التي يمكن أن يستعين بها الخبير من أجل إتمام عمله.[269]

وبعد أن يقوم الخبير بأعمال الخبرة يجب عليه أن يقدم تقريره للمحكمة المختصة ويشترط في هذا التقرير أن يكون مسبباً وموقعاً من الخبير في كل صفحة منه.[270] ويجب أن يقوم الخبير الفني بحلف اليمين بأن يقوم بأعماله بنزاهة وصدق.[271]ويجوز للخصوم رد الخبير إذا وجدت أسباب جدية لذلك بطلب يقدم إلى وكيل النيابة، ويتعين أن يكون الطلب مسبباَ.[272]

---

[267] مصطفى محمد موسى، **مرجع سابق**، ص 225

[268] مختار تابري، **مرجع سابق**، ص 392

[269] مصطفى محمد موسى، **مرجع سابق**، ص 227

[270] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 المادة (69)

[271] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 المادة (68)

[272] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 المادة (71)

المبحث الثالث

الضمانات القانونية للمتهم في عملية التفتيش الجنائي في الجرائم الإلكترونية

يعد التفتيش أحد إجراءات التحقيق الابتدائي الذي يقصد به الاطلاع على حرمة خاصة وذلك للبحث عما يفيد عملية التحقيق، ويعتبر التفتيش أحد الإجراءات التي تمس حرية المتهم في شخصه ومسكنه ومراسلاته، ولما كان اجراء التفتيش يمس حقوق الافراد سواء في حرياتهم الشخصية أو مساكنهم أو مراسلاتهم، فينبغي أن يقدر هذا المساس بقدره ولا يتعدى الغرض الذي ابتغي منه؛ وهو كشف الحقيقة ومن هنا جاءت التشريعات لتضع العديد من الضمانات للمتهم عند تقرير مثل هذا الاجراء.[273] وفي دراستنا هذه فإن التفتيش في الجرائم الإلكترونية يختلف من الناحية الفنية عن غيره من الجرائم؛ وبهذا الصدد فقد قرر الباحث تقسيم هذا المبحث إلى مطلبين رئيسيين الأول يدرس ضمانات المتهم أثناء عملية التفتيش في الجرائم الإلكترونية والمطلب الثاني حدود وضوابط اجراء التفتيش في الجرائم الإلكترونية.

المطلب الأول: ضمانات المتهم أثناء عملية التفتيش في الجرائم الإلكترونية

يعد التفتيش في الأجهزة الإلكترونية من أخطر المراحل التي تتخذ في مسرح الجريمة الإلكترونية إزاء ارتكاب هذه الجريمة، وذلك كون محل التفتيش هو جهاز حاسوب أو أنظمة بيانات ومعلومات معينة.[274] وهناك العديد من الضمانات القانونية التي وضعها المشرع أثناء القيام بعملية التفتيش، فلا يجوز التفتيش ما لم تكن هناك جريمة وقعت وبناء على اتهام موجه للشخص المراد تفتيشه أو تفتيش منزله.[275] ويجب أن يكون هناك فائدة يحتمل الوصول اليها بأجراء التفتيش، ويجب أن يكون التفتيش ضمن النطاق الزماني الذي اتاحه المشرع في قانون الإجراءات الجزائية.

---

[273] خالد الحامدي، **حقوق وضمانات المتهم في مرحلة ما قبل المحاكمة**، دار النهضة العربية، القاهرة، مصر، 2019 ص 119

[274] توفيق خشاشنة، **مرجع سابق**، ص 140

[275] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (1/39)

ولا تقل الضمانات القانونية في التفتيش عن الأدلة الإلكترونية شأنً غيرها من الجرائم، بل والعكس فإن عملية التفتيش في الجرائم الإلكترونية تحتاج إلى ضمانات أكثر من غيرها من الجرائم، كون الدليل في الجرائم الإلكترونية يتمتع بالطبيعة الفنية، وسوف يدرس الباحث في هذا المطلب فرعين رئيسيين، في الفرع الأول سوف يقوم الباحث بتوضيح التفتيش في الجرائم الإلكترونية بناء على مذكرة ومن ثم يدرس الباحث في الفرع الثاني مدى انطباق حالات التلبس على الجرائم المعلوماتية.

الفرع الأول: التفتيش في الجرائم الإلكترونية بناء على مذكرة

نصت المادة (1/52) من القرار بقانون بشأن الجرائم الإلكترونية "أن للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة".[276] يثور لدينا هنا تساؤل عن مدى الزامية النيابة العامة بأذن التفتيش في الجرائم الإلكترونية؛ من الواضح أن عملية التفتيش في الجرائم الإلكترونية لا تتم دون إذن تفتيش، فقد نصت الفقرة الثانية من ذات المادة "يجب أن يكون أمر التفتيش مسبباً ومحدداً".[277] وعليه لا يمكن القول أن المادة سابقة الذكر أعلاه نفت ذكر إذن التفتيش من نصوصها واتاحت للنيابة التفتيش في الجرائم الإلكترونية دون الحاجة إلى إذن تفتيش.[278]

وقد أشار الدكتور أحمد براك في شرح قانون الجرائم الإلكترونية في النظام القانوني الفلسطيني " التفتيش يتطلب إذن يجيز تفتيش أنظمة الحاسب، وأما التفتيش دون إذن أو الحصول على بيانات من جهات ليست محلاً للاشتباه لتعلقها بالمشتبه به، فإنها مسألة تثير الكثير من المعارضة خاصة في ظل ما تقرر من قواعد تحمي الخصوصية وتحمي حقوق الافراد وتوجب مشروعية الدليل وسلامة مصدره، أو تبطل كل

---

[276] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (1/32)

[277] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (2/32)

اجراء يتم خلافاً للقواعد الأصولية المتعقلة بالتفتيش والضبط المنصوص عليها في القانون وهي مسائل ينفد من خلالها الجناة عند عدم إجازة القانون هذا المسلك الاستثنائي، وعلى نحو يجعلنا متمسكين بضرورة عدم اللجوء إلى هذا السلوك، حتى لو أتاح النظام القانوني المعني ذلك، لان المشروعية الإجرائية توجب تحقيق أقصى ضمانات للمتهم تتفق ومقتضيات قرينة البراءة مما يتطلب الإصرار على وجوب استصدار مذكرات تفتيش".[279]

ويجب أن يكون أمر التفتيش سابق الذكر مسبباً ومحدداً، ويقصد هنا بتحديد أمر التفتيش في ظل الجرائم الإلكترونية، عندما يكون المحقق يعلم ابتداءً عن وجود الأدلة المتصلة بجريمة ما ضمن أحد أنظمة الحاسب الالي أو الشبكات، فإن مذكرة التفتيش يتعين أن تكون واضحة في تحديد النظام محل التفتيش، أما إذا كان النظام أو مكان وجود الدليل غير معروف في نطاق المكان محل التفتيش. فيتعين أن تجيء عبارات مذكرة التفتيش عامة ما أمكن حتى لا يكون نصها قيداً على نطاق التفتيش والضبط، والعمومية هنا لا تعني عدم وجوب بيان السبب ومبرر التفتيش ولا تعني تجاوز الاجراء بذاته للقواعد القانونية المقررة لحماية الافراد، خاصة الذين ليس لهم صلة مباشرة بالمشتبه به أو سلوكه.[280]

اما بخصوص تجديد مذكرة التفتيش فقد أجاز القرار بقانون بشأن الجرائم الإلكترونية ذلك وفقا للفقرة الثانية من المادة (52)، ومن الملاحظ أن المشرع الفلسطيني قد توسع في إعطاء صلاحيات التفتيش للضابطة القضائية في الجرائم الإلكترونية عندما أجاز لسلطات التحقيق تجديد مذكرة التفتيش أكثر من مرة ما دامت مبررات هذا الاجراء قائمة.[281] فالمشرع لم يحدد مضمون هذه المبررات أو يضع حد أقصى لذلك وبالتالي

---

[279] احمد براك، **مرجع سابق**، 388

[280] احمد براك، **مرجع سابق**، 389

[281] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (2/32)

ترك أمر تقدير هذه المبررات لسلطة التحقيق وهو ما قد يترتب عليه انتهاكات خطيرة لحقوق وحريات الافراد في عملية التفتيش.[282]

إن مذكرة التفتيش تعتبر شرطاً لصحة اجراء من إجراءات جمع الاستدلال في الجريمة المعلوماتية كغيرها من الجرائم، كما أنها تعتبر ضمانة قانونية للمتهم من أجل الحفاظ على حرمة المسكن وحرمة الأشخاص والمراسلات، ورجوعاً إلى قانون الإجراءات الجزائية الفلسطيني، فقد نص بشكل صريح في المادة (52) من الفصل الرابع المتعلق بقواعد التفتيش "يترتب البطلان على عدم مراعاة أي حكم من أحكام هذا الفصل"، وعليه فإن عدم توافر مذكرة التفتيش في الجرائم كافة يرتب البطلان على الاجراء، ولا يجوز للمحكمة الاخذ بأي دليل ضد المتهم إذا كانت النيابة العامة قد حصلت عليه بطريقة لا تتوافق مع نصوص القانون.

وعليه يرى الباحث أن مذكرة التفتيش تعتبر أحد شروط صحة إجراء التفتيش في الجرائم الإلكترونية، والتفتيش في الجرائم الإلكترونية أساسه قانون الإجراءات الجزائية، لذلك فإنه يخضع لشروط صحة التفتيش ذاتها مع مراعاة بعض قواعد التفتيش الخاصة للتعامل مع الدليل الرقمي وهذا ما نصت عليه المادة (5/52) "يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية"، وذلك من أجل التقليل من فرصة تلف الدليل أو الطعن بمشروعيته كدليل أمام المحاكم الجنائية.

الفرع الثاني: مدى انطباق حالات التلبس على الجرائم المعلوماتية

يقصد بالتلبس في الجرائم التقارب الزمني بين وقوع الجريمة وكشفها[283]، وقد حدد قانون الإجراءات الجزائية الفلسطيني حالات التلبس في المادة (26) "حال ارتكاب الجريمة أو عقب ارتكابها ببرهة وجيزة، إذا تبع المجني عليه مرتكبها أو تبعته العامة بصخب أو صياح، إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملا

---

[282] أحمد حسنية، **مرجع سابق**، ص 29

[283] مصطفى عبد الباقي، **شرح قانون الإجراءات الجزائية الفلسطيني**، **مرجع سابق**، ص 185

آلات أو أسلحة أو أمتعة أو أوراقا أو أشياء أخرى يستدل منها على انه فاعل أو شريك فيها، وإذا وجدت به في هذا الوقت آثار أو علامات تفيد ذلك". ولكن ما مدى انطباق حالات التلبس على الجرائم الإلكترونية وهل يمكن تطبيقها في الامر الواقع، سوف يقوم الباحث للإجابة على هذا السؤال بشرح كل حالة على حدة.

أولاً: مشاهدة الجريمة حال ارتكاب الجريمة

تعتبر هذه الحالة هي حالة التلبس الحقيقية الوحيدة، فيما تعتبر بقية الحالات صورة من صور التلبس الحكمي أو الاعتباري، والتلبس الحقيقي يعني مشاهدة مأمور الضبط القضائي بأحدي حواسه الجاني يقارف فعتله، أو أحد العناصر المكونة للركن المادي للجريمة.[284]

ويمكن تطبيق هذه الحالة على الجرائم الإلكترونية في حالة أن يشاهد مأمور الضبط القضائي مثلاً وهو يتفقد أحد مقاهي الانترنت شخصاً يقوم بمتابعة أحد المواقع الإباحية عبر الشبكة، ويقوم بطباعتها على الطابعة، وفي هذه الحالة تعتبر حالة تلبس بجريمة الكترونية، وفي الغالب تكون الحاسة التي يعاين بها هي حاسة النظر، وعلى هذا الأساس ينعقد لموظف الضابطة العدلية في مثل هذه الحالة بعض الاختصاصات الاستثنائية التي هي في الأصل اختصاص سلطة التحقيق كالقبض على المتهم الحاضر وتفتيشه والتحفظ على الملفات الموجودة معه.[285]

ثانياً: مشاهدة الجريمة عقب ارتكابها ببرهة وجيزة

إن مشاهدة الجريمة لا تعني بالضرورة مشاهدة أفعال التنفيذ المكونة للركن المادي لها، وانما يكفي لتوافر حالة التلبس وجود مظاهر خارجية تنبئ بذاتها عن وقوع الجريمة، فمشاهدة الجريمة عقب ارتكابها ببرهة

---

[284] مصطفى عبد الباقي، **شرح قانون الإجراءات الجزائية الفلسطيني، مرجع سابق**، ص 186

[285] توفيق خشاشنة، **مرجع سابق**، ص 230

وجيزة أفضل مثال وتطبيق لوجود مظاهر خارجية تنبئ بذاتها عن ارتكاب الجريمة كأن يتلقى مأمور الضبط القضائي خبر وقوع جريمة القتل، وانتقاله على الفور ومشاهدة جثة المجني عليه لا تزال تنزف أثر الطعنات مثلاً.[286]

ومن الأمثلة التطبيقية على هذه الحالة قيام أحد الموظفين باستخدام الحاسوب الخاص بعمله سرا والمرتبط بالأنترنت، وذلك لتخزين ملفات تحتوي على صور مخلة بالآداب العامة على القرص الصلب، حيث حصل عليها عن طريق تحميلها عن الانترنت، واستطاع تخزين ما يقارب ألف صورة على القرص الصلب المثبت بجهازه، ففي هذه الحالة فإن مجرد علم موظف الضابطة القضائية ومشاهدة الصورة المخلة بالآداب تقوم حالة من حالات التلبس.[287]

ولا يلزم في هذا الفرض أن يكون الفعل قد وقع علناً أو أن يكون قد خلف اثاراً مادية، وانما يلزم في جميع الأحوال أن يكون الفارق الزمني قصيراً بين لحظتي ارتكاب الجريمة واكتشافها. ويتضح هذا القيد الزماني من الظرف الذي اجازه القانون أي عقب ارتكاب الجريمة.[288]

ثالثاً: الجريمة التي يقبض على فاعلها بناء على صراخ الناس

تقوم حالة التلبس في هذه الحالة عندما يتبع المجني عليه أو العامة مرتكب الجريمة مع صراخ وصخب، ويرى بعض الفقه أنه يكفي في هذا الفرض أن يصيح المجني عليه أو العامة مع الإشارة إلى شخص المتهم

---

[286] رضا الملاح، **الموجز في الضبطية القضائية والتحقيق الابتدائي**، ط1، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، ص 46

[287] توفيق خشاشنة، **مرجع سابق**، ص 232

[288] رضا الملاح، **مرجع سابق**، ص 47

حتى لو لم يتبعوه أو يعدون خلفه، أي يكفي ان يتبعوه بصراخهم وليس بأجسامهم وهنا قضت محكمة النقض المصرية ذلك.[289]

وقد يكون التتبع في الجرائم الإلكترونية في شكل مطاردة تقليدية، كأن يرسل المتهم للمجني عليه رسالة الكترونية تتضمن عبارات السب والقذف فيراه أمامه فيتبعه بالصياح والصراخ للقبض عليه، وقد تكون هذه المطاردة على شكل مطاردة الكترونية كأن يكون لدى المجني عليه معرفة عالية وقدرة في التعامل مع الأجهزة التقنية والمقدرة الفنية لتتبع الجاني ومحاولة معرفته والتوصل اليه من خلال رقم الهاتف الخاص به.[290]

رابعاً: مشاهدة أدلة الجريمة

هذه الحالة تعتبر من حالات التلبس الحكمي، حيث لا يشاهد مأمور الضبط القضائي الجريمة ترتكب وإنما يشاهد فاعلها بعد ارتكاب الجريمة بوقت قصير حاملاً أشياء يستدل منها على أنه فاعل الجريمة أو شريكاً فيها.[291]

ويمكن أن تنطبق هذه الحالة على الجرائم الإلكترونية فمثلاً أن يتم ضبط أحد الأشخاص وهو خارج من أحد مقاهي الانترنت وبحوزته اشرطة أو اقرص صلبة تحتوي على صور مخلة بالآداب العامة، وكان قد أخذها من أحد المواقع خلال وجوده في مقهى الانترنت الذي كان يهم بمغادرته، عندما تبين لمأمور الضبط القضائي أن الموقع ما زال مفتوحاً ولم يتم اغلاقه أو استعماله من أشخاص آخرين، ومثال آخر ايضاً

---

[289] نقض جنائي، جلسة 1951/22، مج س2، 537، رقم 202 "ليس في القانون ما يمنع المحكمة في حدود سلطتها التقديرية من الاستدلال بحالة التلبس على المتهم ما دامت بينت أنه شوهد وهو يجري من محل الحادثة بعد حصولها مباشرة والأهالي يصيحون خلفه أنه القاتل، وهو يعدو أمامهم حتى ضبط على مسافة 150 متراً من مكان الحادثة"

[290] توفيق، خشاشنة، **مرجع سابق**، ص 234

[291] مصطفى عبد الباقي، **شرح قانون الإجراءات الجزائية الفلسطيني**، **مرجع سابق**، ص 187

عندما يعثر مأمور الضابطة القضائية على الهاتف الخاص بالجاني أو الحاسوب الخاص به، وعليه رسائل تحمل التهديد وذلك في مكان قريب من المجني عليه.[292]

ومن هنا يرى الباحث أن التلبس في الجرائم الإلكترونية غير محال؛ فبناء على الأمثلة التي قام بتوضيحها الباحث يكمن أن تنطبق حالات التلبس الوارد في القانون على الجرائم الإلكترونية، وقد تختلف الظروف بناء على طريقة ارتكاب الجريمة واستخدام تقنية المعلومات اللازمة لتنفيذ الفعل الجرمي، وعليه يجب على النيابة العامة أو الضابطة القضائية المختصة مراعاة خصوصية هذه الأدوات عند ضبطها في حالة التلبس.

المطلب الثاني: حدود وضوابط اجراء عملية التفتيش في الجرائم الإلكترونية

عندما تقوم النيابة العامة بإصدار أمر التفتيش في الجرائم الإلكترونية تبدأ عملية التفتيش باختصاص أحد مأموري الضابطة القضائية أو النيابة العامة ومن هنا لا تقتصر الإجراءات القانونية في عملية التفتيش في استصدار أمر التفتيش فقط وإنما لا بد من مراعاة ما نصت عليه قواعد الإجراءات الجزائية أثناء القيام بعملية التفتيش، وقد نص قانون الإجراءات الجزائية الفلسطيني على حدود التفتيش وضبط الأشياء في المادة (50) والتي تتمثل في التفتيش عن الأشياء الخاصة بالجريمة فقط، وضبطها وتحريزها والتحفظ عليها في محضر التفتيش، كما وأنه في حال ظهر أوراق مختومة اثناء التفتيش فلا يجوز لمأمور الضبط القضائي أن يفضها.[293] جميع ما ذكر يعتبر من حدود وضوابط التفتيش في قانون الإجراءات الجزائية الفلسطيني ولكن ما مدى تطبيقها على الحالة المتعلقة بالجرائم الإلكترونية وسوف ندرس في هذا المطلب فرعين الأول التفتيش عن الأشياء الخاصة بالجريمة الإلكترونية فقط، والثاني الضبط والتحفظ في الجرائم الإلكترونية.

---

[292] توفيق خشاشنة، **مرجع سابق**، ص 235

[293] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، المادة (50)

الفرع الأول: التفتيش عن الأشياء الخاصة بالجريمة الإلكترونية فقط

تنص المادة (1/50) "لا يجوز التفتيش إلا عن الأشياء الخاصة بالجريمة الجاري التحقيق بشأنها ومع ذلك إذا ظهر عرضا أثناء التفتيش وجود أشياء تعد حيازتها في ذاتها جريمة، أو تفيد بكشف الحقيقة في جريمة أخرى، جاز لمأمور الضبط القضائي ضبطها". وظهور الدليل بشكل عرضي يفيد أن منهجية مأمور الضبط القضائي في البحث عن الدليل تتسم بالمعقولية، فمثلاً لا يعقل أن يتم التفتيش عن سلاح غير مرخص في مغلف رسائل أو يبحث عن سيارة مسروقة في خزانة.[294]

واستقر قضاء محكمة النقض المصرية على أنه إذا ظهر أثناء التفتيش الصحيح وجود أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة في جريمة أخرى جاز لمأمور الضبط القضائي أن يضبطها بشرط أن تظهر عرضاً أثناء التفتيش ودون سعى يستهدف البحث عنها وكل ذلك لضمان عدم تعسف رجل الضبط القضائي في صلاحية التفتيش.[295]

ويواجه مأمور الضبط القضائي العديد من العقبات عندما يتعلق أمر التفتيش بالأجهزة الإلكترونية الحديثة، ويرجع سبب ذلك إلى الطبيعة الخاصة لهذه الأجهزة التي تحتوي على عدد كبير من الملفات، بالإضافة إلى أن أسماء هذه الملفات لا تدل بالضرورة على ما تحتويها، وفي قانون الإجراءات الجزائية الأمريكي

---

[294] مصطفى عبد الباقي، **شرح قانون الإجراءات الجزائية الفلسطيني مرجع سابق**، ص 252

[295] الحكم رقم 6959 لسنة 80 محكمة النقض المصرية "لما كان ذلك , وكان من المقرر أنه لا يضير العدالة إفلات مجرم من العقاب بقدر ما يضيرها الافتئات على حريات الناس والقبض عليهم بدون وجه حق , وكان من المقرر أيضاً أن التلبس حالة تلازم الجريمة ذاتها لا شخص مرتكبها , والتي لا يوفرها مجرد ما يبدو على الشخص من مظاهر الحيرة والارتباك مهما بلغا ولا يمكن اعتباره دلائل كافية على وجود اتهام يبرر القبض عليه وتفتيشه , وكان مؤدى نص المادة (50) من قانون الإجراءات الجنائية ولازمها أنها لم تجز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات بشأنها أو حصول التحقيق بشأنها وأنه إذا ظهر أثناء تفتيش صحيح وجود أشياء تعد حيازتها جريمة أو تفيد فى كشف الحقيقة فى جريمة أخرى جاز لمأمور الضبط القضائي أن يضبطها بشرط أن تظهر عرضاً أثناء التفتيش ودون سعى يستهدف البحث عنها , وكل ذلك لضمان عدم تعسف رجل الضبط القضائي فى تنفيذ كل تفتيش صحيح يجريه والالتزام بحدود التفتيش وعدم مجاوزة الغرض منه , ولا يسوغ أو يجوز أن يكون التفتيش الإداري الذى اعتنقه الحكم المطعون فيه عصياً على تلك الضوابط يأبى الخضوع إليها وإلا جاز تعسف رجل الضبط القضائي في تنفيذ التفتيش الإداري المنوه عنه وهو ما يأبها المشرع وأحكام الدستور لما فيه من الافتئات على حريات الناس والقبض عليهم وتفتيشهم بدون وجه حق .

أضاف شرط التحديد بأن تكون مذكرة التفتيش مؤسسة ومبينة على أسباب معقولة ومتضمناً وصفا استراتيجياً للتفتيش.[296]

وفي حكم لمحكمة النقض المصرية قضت برد الطعن موضوعاً والمرفوع من النيابة على حكم محكمة الموضوع والقاضي باعتبار التفتيش المتحصل منه صور ومقاطع صوتية ومرئية على هواتف وحواسيب المتهمين باطل كون تفتيشيها لا يتعلق بموضوع الجريمة وهو البحث عن أسلحة وذخائر ومعدات وأن التفتيش داخلها من أجل البحث عن ملفات تدين المتهمين يعد تفتيش باطل في القانون كونه لا يتعلق بالجريمة محل التفتيش.[297]

وفي حكم صادر عن محكمة صلح جزاء شرق عمان قضت المحكمة ببراءة المتهم من تهمة عرض فعل منافي للحياء العام وذلك لبطلان إجراءات التفتيش حيث أن مأمور الضبط القضائي تجاوز صلاحيته أثناء البحث داخل هاتف المتهم عن أدلة لإدانة المتهم في بتهمة إعداد وإعطاء المصدقة الكاذبة وقاموا بتفتيش

---

[296] توفيق خشاشنة، **مرجع سابق**، ص 240

[297] الحكم رقم 28337 لسنة 85 محكمة النقض المصرية "لما كان ذلك ، وكان المستفاد من نص المادة (50) من قانون الإجراءات وما استقر عليه قضاء هذه المحكمة –محكمة النقض –أنه لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها ، وأنه إذا ظهر أثناء تفتيش صحيح وجود أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة في جريمة أخرى جاز لمأمور الضبط القضائي أن يضبطها بشرط أن تظهر عرضا أثناء التفتيش ودون سعي يستهدف البحث عنها ، وكان الحكم المطعون فيه قد أسس قضاءه على أن العثور على الكتب والمطبوعات والصور والمقاطع الصوتية والمرئية على هواتف وحواسيب المتهمين كان نتيجة سعي رجل الضبط القضائي في البحث عن جريمة لم تشملها الأذون ، ولم يكن ظهورها عرضا أثناء تفتيش صحيح في حدود غرضه ، وكان تقدير القصد من التفتيش أمر تستقل به محكمة الموضوع ولها أن تستشفه من ظروف الدعوى وقرائن الأحوال فيها دون معقب ، فإن ما تثيره الطاعنة في طعنها هو لا يعدو أن يكون جدلا موضوعيا في تقدير أدلة الدعوى .ولما كان الحكم المطعون فيه قد قضى ببراءة المطعون ضدهم لبطلان تفتيش مساكنهم لتجاوز القائمين به حدود أذون النيابة الصادرة إليهم ، وكانت الفقرة الثانية من المادة 30من قانون العقوبات قد أوجبت الحكم بمصادرة الأشياء المضبوطة في جميع الأحوال إذا كانت هذه الأشياء تعد حيازتها جريمة في ذاته ولو لم تكن تلك الأشياء ملكا للمتهم ، فإن الحكم المطعون فيه إذ قضى بمصادرة أجهزة الحاسب الآلي والهواتف والمطبوعات والكتب المضبوطة لترويج محتواها لأفكار الجماعة المنشأة على خلاف أحكام القانون يكون قد طبق صحيح القانون .لما كان ما تقدم، فإن الطعن يكون على غير أساس متعينا رفضه موضوعا.

محتويات هاتف المشتكى عليه والعبث في رسائله الخاصة مما يشكل في هذه الحالة تعدي على الحياة الخاصة.[298]

وفي الولايات المتحدة الامريكية قضت المحكمة في قضية المدعو (كاري)[299]، بتوسع ضابط التفتيش في عملية التفتيش، عندما كان يبحث عن رسائل ومستندات على حاسوب المتهم تخص جريمة حيازة المخدرات فوجد، أثناء البحث صورة إباحية لقاصر، واستمر في البحث عن باقي الصور، بالرغم من أن مذكرة التفتيش الصادرة تتعلق بأدلة تخص جريمة حيازة المخدرات، وخلصت المحكمة في قضية كاري أن المحقق بمجرد أن شاهد محتوى أول ملف (JPG) الزمه القانون بأغلاقه والتقدم بطلب للحصول على إذن منفصل للبحث عن المواد الإباحية لأشخاص قاصرين قبل الشروع في فتح مزيد من الصور والملفات، ولم يقم الضابط بهذا الاجراء فأبطلت المحكمة جميع الأدلة المتعقلة بحيازة مواد إباحية لأشخاص قاصرين.[300]

---

[298] الحكم رقم 2888 لسنة 2022 صلح جزاء شرق عمان، (أما فيما يتعلق بجرم عرض فعل منافي للحياء فتجد المحكمة وبالرجوع إلى البينات المقدمة في هذه الدعوى والمتمثلة بملف القضية التحقيقية والمتضمن ضبط تفتيش هاتف بتاريخ 2022/03/03 حيث جاء فيه "...." وبناء على المعلومات الواردة بحق المدني عامل المياومة رقم 2/157 محمد رافع احمد من مرتب إدارة الصيانة/ مشاغل عمان العاصمة الوسط.. بمعلومات مفادها قيامه بتزوير رسالة نصية متضمنة انه مصاب بفيروس كورونا. وبعد أخذ موافقة مدعي عام شرطة شمال عمان المقدم أمجد الحنيطي حيث جرى ضبط المدني المذكور وضبط هاتف نوع (ايفون لون اسود) وبداخله شريحة اتصال.. ورسالة واحدة على تطبيق الماسنجر واردة من المدعو (ALI MAZEN) تتضمن.." إذ تجد المحكمة أن نص المادة 48 من قانون أصول المحاكمات الجزائية قد أعطت الصلاحية للمدعي العام أثناء قيامه بالوظيفة الرسمية أن يعهد إلى أحد موظفي الضابطة العدلية كل حسب تخصصه بقسم من الأعمال الداخلة في وظائفه ومنها تفتيش الأشخاص أو المساكن أو المتعلقات الشخصية إذا رأى ضرورة لذلك عدا استجواب المشتكى عليه، كما نصت المادة 87 من ذات القانون على أنه لا يجوز التفتيش إلا عن الأشياء التي جرى التفتيش لأجلها، وبالرجوع إلى وقائع هذه الشكوى فقد تم ضبط هاتف المشتكى عليه بناء على معلومات تفيد بقيامه بتزوير رسالة تتضمن انه مصاب بفيروس كورونا وحيث وجد منظمي الضبط الرسالة التي تثبت صحة المعلومات الواردة إليهم إلا أنهم تجاوزوا المهمة الموكلة إليهم وقاموا بتفتيش محتويات هاتف المشتكى عليه – أي أنهم تجاوزا صلاحية الأذن الممنوح لهم– مما يشكل والحالة هذه تعدي على الحياة الخاصة، وعليه ونظراً لخلو ملف القضية التحقيقية من أذن التفتيش الممنوح للضابطة العدلية فيكون البطلان قد أصاب كافة الإجراءات اللاحقة له من ضبط المشاهدة، الأمر الذي يتوجب معه إعلان عدم مسؤولية المشتكى عليه عن هذا الجرم.

لذا وتأسيساً على ما تقدم تقرر المحكمة ما يلي – عملاً بأحكام المادة 178 من قانون أُصول المحاكمات الجزائية إعلان عدم مسؤولية المشتكى عليه محمد رافع احمد السرحان عن جرم عرض فعل منافي للحياء العام خلافاً لأحكام المادة 306 من قانون العقوبات – لتجاوز منظمي الضبط الصلاحية الممنوحة لهم.

[299] United States v. Carey, 172 F.3d 1268, 1270 (10th Cir. 1999)

[300] Donald Resseguie, **Computer Searches and Seizure**, 48 Clev. St. L. Rev. 185 (2000) P.9

ويحق لمأمور الضبط القضائي ضبط وتحريز دليل تم العثور عليه عن طريق الصدفة أي أن مأمور الضبط القضائي مخول بضبط الدليل الذي يعثر عليه دون أن يكون هذا الدليل مستهدفاً للبحث خلال البحث والتفتيش، فمثلاً لو صدرت مذكرة تفتيش وبحث عن أدلة جريمة نشر فايروسات وأثناء التفتيش في حاسوب المتهم وجد بالصدفة ملفات مواد اباحية للقاصرين، فإن ضبط مأمور الضبط القضائي لها يعتبر صحيحاً رغم أم التهمة الموجهة له كانت نشر فايروسات وليس حيازة هذه المواد والصور.[301]

وتعرف هذه النظرية في الولايات المتحدة بما يسمى بنظرية (Plain view) حيث يجوز لشرطة التحقيق ضبط الأدلة حتى لو لم تكن تتعلق بموضوع التحقيق في حالة اكتشاف هذا الدليل عن طريق الصدفة أثناء القيام بعملية التفتيش القضائي.[302]

ويشترط قانون الولايات المتحدة الامريكية عند تطبيق هذا المبدأ أن يكون جهاز الحاسوب في حالة التشغيل ويكون الدليل ظاهر على شاشة الجهاز، فلم تطبق هذه النظرية عندما تكون الملفات مغلقة داخل القرص الصلب.[303]

ويرى الباحث أن عملية تفتيش الملفات الموجودة في النظام المعلوماتي المحدد يجب أن تستهدف الملفات موضوع الجريمة، فمثلا لو كانت الجريمة حيازة صور اباحية لأشخاص قاصرين يجب على مأمور الضبط القضائي أن يقوم بالتفتيش بهدف الكشف عن هذه الصور، فلو وجد مأمور الضبط القضائي صوراً تتعلق بمستندات رسمية تم تزيروها يجوز في هذه الحالة لمأمور الضبط القضائي أن يتحفظ على هذه الصور

---

[301] مصطفى عبد الباقي، **التحقيق في الجريمة الالكترونية وإثباتها في فلسطين: دراسة مقارنة**، مجلة دراسات: علوم الشريعة والقانون، مج. 45، ع. 4، ملحق 2، صفحات 284– 299، 2018، ص 291

[302] Carl J. Franklin, **The Investigator's Guide to Computer Crime**, Charles C Thomas Publisher LTD, Spring afield Illinois, USA, 2006, P. 208

[303] Donald Resseguie, **Ibid** P.9

وفقا لنص المادة (1/50) من قانون الإجراءات الجزائية الفلسطيني، حيث تعد حيازة هذه الصور جريمة بحد ذاتها تنفصل عن جريمة حيازة صور اباحية لأشخاص قاصرين.

وقد انقسم الفقه في مسألة إذن التفتيش إلى رأيين فمنهم من اعتبر جهاز الحاسوب صندوقاً مقفلاً واحداً، وبالتالي لا يشترط صدور إذن قضائي مستقل لكل ملف على حدة، وهناك رأي آخر اعتبر أن كل ملف بحاجة إلى إذن قضائي مستقل، ويرجع هذا الرأي إلى أن الحاسوب يحتوي على الكثير من الملفات التي تتعلق بحياة الأشخاص فامتداد اذن التفتيش لملفات أخرى يؤدي إلى اعتداء مأمور الضبط القضائي على الحياة الخاصة للأفراد، ومن جهة أخرى فإن هذا يؤكد مبدأ أنه لا يجوز التفتيش الا عن الأشياء الخاصة بالجريمة وتطبيقاً لذلك فأنه لا ينبغي تفتيش كل الملفات بإذن واحد، ولكن لمأمور الضبط القضائي أن يصادف ملفات تشكل جريمة عرضية فعليه يجوز له التحفظ عليها وضبطها.[304]

ويفترض من مأمور الضبط القضائي أثناء اجراء عملية التفتيش أن يحاول قدر المستطاع المحافظة على أسرار المتهم، فإذا كان يبحث عن برامج على ذاكرة الحاسوب الرئيسية فيجب عليه أن لا يقوم بفتح الملفات الخاصة بأسرار المتهم والاطلاع عليها، إلا أذا كانت تتعلق بالجريمة المعلوماتية المرتكبة، ولا يجوز أيضاً لمأمور الضبط القضائي أن يكشف عما اطلع عليه أو صادفه أثناء اجراء التفتيش سواء داخل ملفات الحاسوب أو خارج نطاق بيانات الحاسوب، فإن فعل ذلك يكون عرضة لجريمة افشاء اسرار المهنة المنصوص عليها في المادة (355) من قانون العقوبات رقم (16) لسنة 1960م.[305]

في بعض الأحيان أثناء القيام بعملية التفتيش يكون الجهاز محل التفتيش مزود بنظام حماية أو كلمة مرور فلا يمكن ذلك الضابطة القضائية من إتمام عملية التفتيش داخل النظام المعلوماتي، فهل يمكن للضابطة

---

[304] توفيق خشاشنة، **مرجع سابق**، 241

[305] علي الطوالبة، **التفتيش الجنائي على نظم الحاسوب والانترنت – دراسة مقارنة**، رسالة دكتوراه منشورة، جامعة عمان العربية، عمان، الاردن، 2003، ص 214

القضائية اكراه المتهم أو حمله على فتح النظام المشفر أو تزويدهم بكلمات المرور. يرفض الفقه اجبار المتهم على تقديم المعلومات اللازمة لتسهيل الدخول إلى النظام المعلوماتي والحجة في هذا القول تتجسد في قاعدة معروفة ومستقرة بأنه لا يجوز اجبار المتهم على تقديم دليل يدينه، ففي ظل التشريعات التي تحترم حقوق الانسان وحرياته فباستطاعة المتهم دائماً أن يرفض الإجابة على موضوع الاتهام الموجه له وهو غير ملزم بالكلام ولا يفسر امتناع المتهم عن الكلام بأنه اعتراف منه.[306]

وهذا ما أخذ به المشرع الفلسطيني فقد نص قانون الإجراءات الجزائية في المادة (1/97) " للمتهم الحق في الصمت وعدم الإجابة على الأسئلة الموجهة إليه"، وكذلك المادة (217) "للمتهم الحق في الصمت، ولا يفسر صمته وامتناعه عن الإجابة بأنه اعتراف منه".

وفي المقابل فإن كان لا يجوز اجبار الشخص على الادلاء بأقواله ضد نفسه، بيد أن ذلك لا ينبغي أن يكون حائلاً دون اجباره على تقديم المعلومات يقتضيها ولوج النظام المعلوماتي للسلطات المختصة متى كانت هذه المعلومات بحوزته قياساً على اجبار الشخص تسليم مفتاح الخزنة الذي بحوزته، ففي فرنسا يرى جانب من الفقه في ظل غياب النص التشريعي بأن الشاهد يكون مكلف بالكشف عن كلمات السر التي يعرفها وشفرات التشغيل ما عدا حالات المحافظة على سر المهنة.[307] إلا أن ما ينطبق على الشاهد لا يجوز اسقاطه على المتهم أثناء عملية التحقيق.

وعليه يرى الباحث أن التفتيش عن الأشياء الخاصة بالجريمة الإلكترونية فقط يعتبر أحد أهم حدود وضوابط إجراء عملية التفتيش في الجرائم الإلكترونية إلى جانب وجود إذن التفتيش الصادر عن السلطة المختصة،

---

[306] أحمد براك، **مرجع سابق**، 369

[307] أحمد براك، **مرجع سابق**، ص 371

وعليه على مأمور الضبط القضائي المختص ألا يتعسف في استخدام سلطته أثناء التفتيش وإلا اعتبر ذلك مخالفاً للقانون ويوجب المسؤولية.

الفرع الثاني: ضمانات المتهم عند عملية ضبط المراسلات واعتراض المكالمات

تعد المحادثات الشخصية والمراسلات العادية والإلكترونية من عناصر الحق في الحياة الخاصة، فسرية حديث المرء مع غيره تعد من الأمور التي ترتبط في كيان الشخص، وفي هذه الأحاديث والاتصالات يثق المتحدث بها بشخص المتحدث اليه، فيتحدث معه دون خوف أو حرج من سماع الاخرين معتقداً أنه في مأمن من استراق السمع أو التجسس عليه. [308] وقد جرمت المادة (7) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته اعتراض أو تسجيل أو تنصت الأشخاص على مراسلات الغير دون وجه حق.[309]

والمقصود بالمراسلات المكتوبة في هذا الصدد كافة الرسائل التي تكون مكتوبة سواء كانت مرسلة بطريق البريد أو بواسطة بريد مضمون كالبريد الالكتروني أو بريد عادي وتشمل البرقيات، في حين أن المحادثات السلكية أو اللاسلكية فهي تعتبر من قبيل الرسائل الشفوية ولكن حتى لو تعلق الامر بالرسائل الشفوية أو الكتابية مهما كانت وسيلتها فهي محل حماية في القانون.[310]

أجازت الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) اتخاذ تدابير تشريعية للدول الأطراف من أجل اعتراض بيانات المحتوى في المادة (21) وكذلك الاتفاقية العربية لمكافحة الجريمة المعلوماتية في المادة (29). وفي صدد دراسة النصوص القانونية التي تنظم الجرائم الإلكترونية في فلسطين منها

---

[308] علي الطوالبة، **مرجع سابق**، ص 218

[309] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (7) " كل من التقط ما هو مرسل عن طريق الشبكة أو إحدى وسائل تكنولوجيا المعلومات أو سجله أو اعترضه أو تنصت عمداً دون وجه حق، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

[310] أحمد حسنية، **مرجع سابق**، ص 18

القرار بقانون رقم (10) لسنة 2018 وتعديلاته نرى أنه أجاز الاعتراض الفوري لمحتوى الاتصالات وذلك في نص المادة (36) وفقاً للقيود التي وضعها المشرع.[311] وتتمثل القيود التي وضعها بضرورة صدور أمر بالمراقبة من السلطة المختصة، والقيام بعملية الاعتراض خلال المدة المحددة بالقانون.

أولاً: يجب أن يصدر أمر بالمراقبة من السلطة المختصة

حتى تكوت مراقبة الاتصالات مشروعة، لا بد من جهات التحقيق عند القيام بها الحصول على إذن من الجهات القضائية المختصة، وإلا اعتبر هذا الاجراء باطلاً لا يصلح كدليل في الاثبات، فما بني على باطل فهو باطل، وليكون الاجراء صحيحاً ويشكل حجية أمام القضاء الجزائي لا بد أن يتم بموجب الإجراءات التي رسمها القانون.[312]

أحد أهم الشروط التي يجب تتوفر في اعتراض محتوى المكالمات وتسجيلها، هي ضرورة صدور أمر بالمراقبة من السلطة المختصة فقد نصت المادة (56) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته "للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له ومدته".

وفي الأردن ينعقد الاختصاص بإصدار الامر بمراقبة المحادثات بكل أنواعها والمرسلات للمدعي العام وله أن ينيب أحد أعضاء الضابطة العدلية الاخرين للقيام بهذا الاجراء، وفي مصر تكون سلطة مراقبة واعتراض

---

[312] فهد سلامة، **مشروعية السلطة التنفيذية بمراقبة الاتصالات الهاتفية**، مجلة العربي للدراسات الإعلامية، العدد 9، الصفحات، 3-11، ص 8

المكالمات بيد قاضي التحقيق.[313] وفي الولايات المتحدة الامريكية يجوز اعتراض الاتصالات الإلكترونية، بما في ذلك اعتراض شبكات الحاسوب، ويشترط الحصول على إذن تفتيش صادر من القاضي المختص.[314]

وفي حكم لمحكمة بداية عمان بصفتها الاستئنافية أيدت قرار محكمة الصلح القاضي بإعلان براءة المتهم من تهمة القدح والتحقير والذم واستبعادها للتسجيل الصوتي كبينة في الدعوى وان هذا التسجيل هو مخالف للقانون لأنه لم يتم بناءً على اذن من المدعي العام المختص وضمن الأصول.[315]

وفي سابقة قضائية لمحكمة النقض الفلسطينية فإن أي تسجيل يتم بواسطة أي جهاز لا يجوز الاعتماد عليه إلا إذا كان بناء على إذن من قاضي الصلح وقد حكمت محكمة النقض ببطلان الدليل وعدم مشروعيته.[316]

---

[313] علي الطوالبة، **مرجع سابق**، 222

[314] علي الفيل، **إجراءات التحقيق الابتدائي في الجرائم المعلوماتية**، مجلة الحقوق – جامعة البحرين، مجلد 8، عدد 17، ص ص. – 439 487، ص 34

[315] الحكم رقم 487 لسنة 2020 محكمة بداية عمان بصفتها الاستئنافية، (وبالرد على سبب الاستئناف وحاصله تخطئة محكمة الدرجة الاولى بإعلان براءة المستأنف ضده عن الجرائم المسندة اليه مخالفة بذلك بينات النيابة ومنها شهادة المشتكي والتسجيل الصوتي المقدم وتقرير الخبرة بهذا الخصوص وبذلك نجد ان قيام محكمة الدرجة الاولى باستبعاد شهادة المشتكي لتناقضها مع ما جاء في لائحة شكواه جاء موافقا للقانون ونؤيدها فيما توصلت ، كذلك فان استبعادها للتسجيل الصوتي كبينة في الدعوى جاء موافقا للقانون وان هذا التسجيل هو مخالف للقانون لأنه لم يتم بناءً على اذن من المدعي العام المختص وضمن الاصول ، وكذلك لا يتبقى اية بينة تربط المستأنف ضده بالجرم المسند اليه ، وحيث توصلت محكمة الدرجة الاولى لذات النتيجة فإننا نقرها فيما توصلت اليه ، ويغدو سبب الاستئناف لا يرد عليه القرار المستأنف

لذا وتأسيسا على كل ما تقدم نقرر وعملا بأحكام المادة 14 من قانون الصلح رد الاستئناف موضوعا وتأييد القرار المستأنف واعادة الاوراق الى مصدرها.

[316] حكم محكمة النقض الفلسطينية رقم 607 لسنة 2019 لنقض الحكم الصادر عن محكمة استئناف رام الله بتاريخ 2019/11/27 في الاستئناف الجزائي رقم 2019/363 "وفي هذا السياق نجد بخصوص ما ابداه الطاعن حول عدم شرعية الادة التي اعتمدتها محكمة الدرجة الاولى ومن بعدها محكمة الاستئناف ومن ذلك نجد بخصوص التسجيل الصوتي السي دي ومحضر التفريغ الصوتي المبرز ن/11 و ن/12 والمنظم من قبل الشاهد الملازم ***** سيما وانه من ضمن الادلة وعناصر الاثبات التي بنت عليها حكمها فالتسجيل الصوتي وما تحصل منه من محضر التفريغ الصوتي تعتبر ادلة غير مشروعة ومخالفة للقانون كونها خالفت نص المادة 35 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية والتي نصت على انه "لقاضي الصلح أن يأذن للنيابة العامة بمراجعة الاتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها" وعليه وفي ضوء النص المذكور فان التسجيل الذي يعول عليه في الحكم هو الذي تقوم به النيابة العامة او من خلالها صاحبة الاختصاص بعد اخذ موافقة قاضي الصلح والا كان التسجيل باطلا فالقاضي الجزائي وان كان حرا في تكوين عقيدته الحكمية من اي عنصر من عناصر الدعوى الا انه مقيد بان لا يكون هذا العنصر مستمد من اجراء باطل وعليه فان التسجيل الصوتي الذي قام به احد المتهمين في الدعوى ولم تراعى فيه احكام المادة 35 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية هو دليل غير مشروع ولا يجوز الاعتماد عليه بالحكم وكان يتوجب على محكمة الاستئناف اسقاطه من عداد البينات لا ان تستند عليه في حكمها وبالتالي يغدو الطعن وارد على القرار المطعون فيه من هذه الجهة للفساد بالاستدلال والقصور من حيث التعليل والتسبيب .

ثانياً: مدة الاعتراض

اتجهت بعض التشريعات إلى وضع قيود زمنية لإجراء عملية اعتراض المراسلات وتسجيل الأصوات، ففي فرنسا مثلاً حدد المشرع الفرنسي المدة القانونية لإجراء اعتراض المكالمات بأربعة أشهر يمكن تجديدها على أن يتم التسجيل وتفريغ التسجيل تحت سلطة قاضي التحقيق ورقابته.[317]

وقد حدد القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات المدة التي يجب أن تتم خلالها عملية اعتراض محتوى الاتصالات في المادة (2/56) (تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة أشهر من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط).[318] كما أكد القرار بقانون في ذات المادة على تنفيذ الاعتراض بالتاريخ الفعلي من المدة المحددة قانونية فقد نص في الفقرة الثالثة من ذات المادة" يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها".[319]

وعليه يرى الباحث أن المشرع الفلسطيني قد وضع قيوداً محددة على عملية اعتراض المكالمات الفورية وتتمثل هذه القيود بصدور إذن من المحكمة المختصة، ولا تتجاوز مدة الاعتراض ثلاثة أشهر تجدد مرة واحدة فقط؛ وهذا موقف محمود فقد اتجهت الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) في المادة (3/21) على أن تتخذ الدول الأطراف التدابير اللازمة للحفاظ على سرية محتوى البيانات والاتصالات التي يتم نقلها عبر مزود الخدمة.

---

[317] عبد الصبور مصري, منال عبد الرحمن، **المحكمة الرقمية والجريمة المعلوماتية: دراسة مقارنة**، ط1، مكتبة القانون والاقتصاد، 2012، ص 342

[318] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (2/56)

[319] القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته، المادة (2/56)

الخاتمة

تناولت هذه الرسالة إجراءات الضبط والتفتيش في الجرائم الإلكترونية في النظام القانوني الفلسطيني، ويعتبر هذا الموضوع من المواضيع المهمة في القرار بقانون بشأن الجرائم الإلكترونية كون الجرائم الإلكترونية تتمثل بطبيعتها الرقمية الخاصة التي تميزها عن غيرها من الجرائم، وتناول الباحث في بداية بحثه تعريف التفتيش القضائي في القانون وبيان الاحكام العامة للتفتيش، واتجه إلى توضيح ماهية الجريمة الإلكترونية والقوانين المنظمة لها في فلسطين، وأوجز تعريف التفتيش القضائي في الجرائم الإلكترونية وفرق بين عملية التفتيش التي تعتبر بمثابة البحث في مستودع سر المتهم وعملية الضبط القضائي والتي تعتبر نتاج عملية التفتيش والتي تتمثل في ضبط الأدلة الرقمية وتحريزها.

وقد تناول الباحث في هذه الرسالة المكونات المادية للحاسوب والمكونات المعنوية وذلك من أجل الخوض في مدى صلاحية هذه المكونات المعنوية والمادية لان تخضع للتفتيش القضائي وفي ذلك بين الباحث بإن المشرع الفلسطيني قد أجاز تفتيش مكونات الحاسوب المادية والمعنوية، ولا بد من مراعاة الجوانب الفنية عند عملية التفتيش في الجرائم الإلكترونية.

وفي صدد عملية التفتيش في الجرائم الإلكترونية تناول الباحث الدليل الالكتروني في مجال الاثبات الجنائي حيث بين الطبيعة الخاصة التي يتشكل منها الدليل الرقمي والذي يتمثل من البيانات الإلكترونية التي يتم اخراجها عن طريق الحاسوب والتي تتمثل في صور أو مستندات أو أفلام رقمية، ويشترط للحصول على هذه البيانات أياً كان شكلها أن تكون هناك مشروعية مستمدة من التفتيش حيث يجيز القاضي الاستناد إلى هذا الدليل من أجل الحكم بالإدانة، كما أنه يجب الحصول على الدليل الرقمي بصورة مشروعة بأتباع اجراءات التفتيش المنصوص عليها في القانون، كما أن الحصول على الدليل الرقمي لا يكفي لاعتماده للإدانة، بل يجب التأكد من سلامة هذا الدليل الرقمي من العبث عن طريق اخضاع الأدوات المستخدمة

في استخراج هذا الدليل للتجارب للتأكد من دقتها وسلامتها إضافة لاستخدام أدوات اثبتت الدراسات العلمية كفاءتها.

وكان لابد للباحث أن يدرس مسرح الجريمة الإلكترونية والذي يقع داخل النظام المعلوماتي أو العالم الافتراضي حيث قام فيه المجرم بجريمته أو بواسطته، فقد أجاز القرار بقانون للجرائم الإلكترونية في فلسطين بمعاينة مسرح الجريمة الرقمي حيث نصت المادة (4/32)، "ويجوز معاينة مسرح الجريمة الإلكترونية بتتبع المجرم المعلوماتي الكترونياً وذلك عن طريق الرجوع على مزودي الخدمة". كما أجاز القرار بقانون في المادة (1/31) مراقبة الاتصالات السلكية واللاسلكية وتسجيلها، وبعد القيام بعملية المعاينة يأتي دور المحقق الجنائي باستخلاص هذا الدليل وتحريزه من مكان العثور عليه، باستخدام العديد من التقنيات والبرامج منها برنامج إذن التفتيش، وبرنامج النسخ، وبرنامج قرص التشغيل، وغيرها من البرامج التي سهلت للسطلة القضائية عملية استخلاص الدليل الرقمي، أما بخصوص التنظيم القانوني لعملية تحريز الأدلة الرقمية في القانون الفلسطيني فقد عالج القرار بقانون في المادة (2/33) آلية تحريز الدليل الالكتروني حيث سمحت للنيابة العامة الضبط والتحفظ على البيانات والمعلومات أو أي وسيلة من وسائل تكنولوجيا معلومات، وجاءت نصوص القرار لتتوافق مع ما ورد في الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية بشأن تحريز الأدلة الإلكترونية وضبطها وذلك في المادة (3/19) التي أجازت للدول الأطراف اتخاذ التدابير اللازمة من أجل تحريز الأدلة الإلكترونية وضبطها من أجل حفظها من الضياع وهذا ما اتجهت له الاتفاقية العربية لمكافحة الجريمة المعلوماتية في المادة (1/27د) والتي اشترطت على الدول الأطراف اتخاذ التدابير التي تمنع الوصول إلى البيانات المخزنة أو ازالتها وذلك من أجل ضمان عدم التلاعب بها.

وقد درس الباحث القواعد العامة في ضبط وتفتيش نظم الحاسوب في النظام القانوني الفلسطيني حيث قام بتحديد السلطات المختصة بالتفتيش والتحقيق في الجرائم الإلكترونية والتي تتمثل في النيابة العامة أو أحد مأموري الضبط القضائي وذلك حسب قواعد الاختصاص في المادة (1/39) من قانون الإجراءات الجزائية الفلسطيني والمادة (1/32) من القرار بقانون بشأن الجرائم الإلكترونية، إضافة إلى تحديد نطاق اختصاص هذه السلطات عند القيام بعملة التفتيش ومدى قدرة سلطة التحقيق في حال كان حاسوب المتهم مرتبط بنهاية طرفية داخل أو خارج إقليم الدولة، كما تناول الباحث الصعوبات التي تواجه سلطات التحقيق والتي تمثلت في الصعوبات الفنية التي تتعلق بالجريمة الإلكترونية وصعوبات تتعلق بالدليل الالكتروني نفسه كونه يختلف عن الدليل في الجرائم التقليدية، وبصدد ذلك تقوم النيابة في بعض الأحيان بانتداب الخبراء الفنيين من أجل التعامل مع هذه الصعوبات حيث أجاز القرار بقانون في المادة (4/32) الاستعانة بأهل الخبرة من أجل النفاذ إلى أي وسيلة من وسائل تكنولوجيا المعلومات.

ويمس التفتيش حقوق الافراد الشخصية وحريات مساكنهم ومراسلاتهم ومن هذا الأساس درس الباحث الضمانات القانونية للمتهم في عملية تفتيش أنظمة الحاسوب حيث أن التفتيش لا يتم الا بمذكرة. وبعد دراسة الواقع العملي في فلسطين فإن التفتيش في الجرائم الإلكترونية يجب أن يتم بمذكرة قانونية، كما أنه لا يجوز التفتيش إلا عن الأشياء الخاصة بالجريمة فقط، إلا أنه يجوز لسلطة الضبط التحفظ على أي ملفات ظهرت اثناء التفتيش تعد حيازتها بحد ذاتها جريمة سواء لم ترتبط بموضوع الجريمة الإلكترونية محل التفتيش، ومن جانب آخر فيجب مراعاة الضمانات القانونية التي نص عليها القرار بقانون أثناء القيام بعملية اعتراض المراسلات التي نص عليها في المادة (36) والتي جاءت لتوافق ما نصت عليه الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية (بودابست) في نص المادة (21) وكذلك الاتفاقية العربية لمكافحة الجريمة المعلوماتية في المادة (29).

وعليه فقد خلصت الرسالة إلى مجموعة من النتائج والتوصيات التي يمكن أن نجملها فيما يلي.

النتائج:

1- أجاز القرار بقانون التفتيش داخل أنظمة المعلومات بقصد الحصول على أدلة تفيد في كشف الحقيقية بالجرائم الإلكترونية، فقد أجاز في نص المادة (4/32) لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات.

2- التفتيش للحصول على الأدلة الإلكترونية في فلسطين يعتبر من اختصاصات النيابة العامة أو الضابطة القضائية التي تنتدبها للقيام بإجراءات التفتيش.

3- التفتيش في الجرائم الإلكترونية لا يتم إلا بمذكرة من الجهات القضائية المختصة ويجب أن يكون أمر التفتيش مسبباً ومحددا، وذلك سنداً لنص المادة (32) من القرار بقانون بشأن الجرائم الإلكترونية.

4- توسع القرار بقانون في إعطاء صلاحيات التفتيش للضابطة القضائية في الجرائم الإلكترونية عندما أجاز للنيابة العامة تجديد مذكرة التفتيش أكثر من مرة ما دام مبررات هذا الاجراء قائمة، ولم يحدد مضمون هذه المبررات أو يضع حداً أقصى لها وترك تقدير هذه المبررات لسلطة التحقيق مما قد يترتب عليه انتهاكات خطيرة لحقوق وحريات الافراد في عملية التفتيش.

5- حسم القرار بقانون الخلاف بشأن منح سلطة التحقيق صلاحية واسعة في الولوج إلى ملفات وأنظمة موجودة في غير موقع ارتكاب الجريمة؛ فقد أوجب في نص المادة (33) أن يتوافر لدى سلطات الضبط القضائي إذن من النيابة من أجل الوصول إلى ملفات وبيانات ذات نهاية طرفية داخل إقليم الدولة نفسها.

6- عالج القرار بقانون حالة ارتباط الملفات بنهاية طرفية خارج إقليم الدولة فقد أكد بموجب المادة (2) أن أحكام هذا القرار تطبق على الجرائم الواردة فيه سواء تم ارتكابها كليا أو جزئياً داخل فلسطين أو خارجها، وشجع القرار بقانون التعاون الدولي في إطار الاتفاقيات الدولية بشأن الجرائم الإلكترونية وذلك في نص المادة (1/42).

7- أجاز القرار بقانون للنيابة العامة أو سلطات الضبط القضائي الاستعانة بالخبراء الفنيين في حال تعذر عليها النفاذ إلى إحدى وسائل تكنولوجيا المعلومات بقصد كشف الحقيقة، وذلك وفقاً لنص المادة (4/32) من ذات القرار.

8- لا يجوز إجبار المتهم أو حمله على فتح النظام المشفر وتزويد سلطات بكلمات المرور. فللمتهم أن يرفض الإجابة على موضوع الاتهام الموجه له وهو غير ملزم بالكلام ولا يفسر امتناعه عن الكلام بأنه اعتراف منه وهذا ما أخذ به المشرع الفلسطيني فقد نص قانون الإجراءات الجزائية في المادة (1/97) " للمتهم الحق في الصمت وعدم الإجابة على الأسئلة الموجهة إليه"، وكذلك المادة (217) "للمتهم الحق في الصمت، ولا يفسر صمته وامتناعه عن الإجابة بأنه اعتراف منه.

9- جاءت نصوص القرار بقانون لتتوافق في مضمونها مع ما جاءت به الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية (بودابست) والاتفاقية العربية لمكافحة الجريمة المعلوماتية وذلك من حيث تفتيش الأنظمة المعلوماتية والتحفظ على الأدلة الرقمية وتحريزها.

التوصيات

1- يوصي الباحث بتعديل الفقرة الأولى من نص المادة (52) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته، لتنص بشكل واضح وصريح على أن يكون إجراء التفتيش في الجرائم الإلكترونية متبوعاً بمذكرة تفتيش قانونية صادرة عن السلطات المختصة وفقاً للقانون، ويخضع لنفس الضمانات القانونية الواردة في قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

2- يوصي الباحث بتعديل الفقرة الثانية من نص المادة (52) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته والتي تنص على تجديد أمر التفتيش، وذلك لتنص بشكل واضح وصريح على تحديد مضمون المبررات القائمة على تجديد أمر التفتيش ووضع حد أقصى لها.

3- مراعاة جميع قواعد التفتيش المنصوص عليها في قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م والمنصوص عليها في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته وذلك من أجل تحقيق سير العدالة وتجنباً لوقوع البطلان.

4- يوصي الباحث الجهات المختصة بضرورة تطبيق مبادئ التعاون الدولي من أجل تبيني مكافحة الجريمة المعلوماتية على الصعيد الدولي وخصوصاً أن هذه الجرائم ترتبط بنهاية طرفية خارج إقليم الدولة.

قائمة المصادر والمراجع

أولاً: المصادر

¤ مصادر أساسية

- معجم المعاني الجامع
- القانون الأساسي الفلسطيني المعدل

¤ القوانين والتشريعات

- **فلسطين**

– قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001

– القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته الساري في فلسطين

– قانون رقم (3) لسنة 1996 بشأن الاتصالات السلكية واللاسلكية الساري في فلسطين

- **الأردن**

– قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015

– قانون أصول المحاكمات الجزائية الأردني لسنة 1961

- **مصر**

– قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018

– قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950

¤ الاتفاقيات الدولية

- الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية (بودابست) لعام 2001
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010

¤ الاحكام القضائية

- **فلسطين**

– الحكم رقم 607 لسنة 2019، محكمة النقض الفلسطينية لنقض الحكم الصادر عن محكمة استئناف رام الله بتاريخ 2019/11/27 في الاستئناف الجزائي رقم 2019/363 "

- **الأردن**

– الحكم رقم 487 لسنة 2020، محكمة بداية عمان بصفتها الاستئنافية

– الحكم رقم 2888 لسنة 2022، محكمة صلح جزاء شرق عمان

- **مصر**

– الحكم رقم 6959 لسنة 80، محكمة النقض المصرية

– الحكم رقم 28337 لسنة 85، محكمة النقض المصرية

– الحكم رقم 1951/22، محكمة النقض المصرية

ثانياً: المراجع

¤ المراجع باللغة العربية

- **الكتب**

- أبو القاسم، طاهر محمود، الجرائم المعلوماتية صعوبات وسائل التحقيق فيها وكيفية مواجهتها، المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2019.
- إبراهيم، خالد ممدوح، الاثبات الالكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي الإسكندرية، مصر، 2020.
- الحامدي، خالد، حقوق وضمانات المتهم في مرحلة ما قبل المحاكمة، دار النهضة العربية ،2009، القاهرة، مصر.
- الحسبان، عطا الله احمد، نظم المعلومات المحاسبية، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2013.
- الحلبي، خالد عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر، عمان، الأردن، 2011.
- الشورابي، عبد الحميد، ضمانات المتهم في مرحلة التحقيق الجنائي، منشأة المعارف للنشر والتوزيع، الإسكندرية، 1996.
- الطوالبة، علي حسن: الجرائم الإلكترونية، البحرين، جامعة العلوم التطبيقية، كلية الحقوق، 2008.
- العتيبي، خالد، الجوانب الإجرائية في الشروع في الجرائم المعلوماتية: دراسة مقارنة، ط1، مكتبة القانون والاقتصاد للنشر والتوزيع، الرياض، المملكة العربية السعودية، 2014.

- الملاح، رضا، الموجز في الضبطية القضائية والتحقيق الابتدائي، ط1، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية.
- الهواس، محمود والبرزنجي، حيدر: تكنولوجيا وأنظمة المعلومات في المنظمات المعاصرة، دار الكتب والوثائق الوطنية، بغداد، العراق، 2014.
- براك احمد: الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية تأصيلية مقارنة، ط1، دار الشروق، رام الله، 2019.
- حجازي، عبد الفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، ط1، دار الفكر الجامعي، الإسكندرية، مصر 2006.
- خشاشنة، توفيق، مسرح الجريمة ومعاينته عبر شبكة المعلومات الدولية، دار الثقافة للنشر والتوزيع، ط1، 2020، عمان، الأردن.
- عارف، ثوار ثابت، اساسيات تكنولوجيا الحاسب، ط1، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2005.
- عبد الباقي، مصطفى: شرح قانون الإجراءات الجزائية رقم (3) لسنة 2003 (دراسة مقارنة)، جامعة بيرزيت، كلية الحقوق والإدارة العامة، وحدة البحث العلمي للنشر، بيرزيت، فلسطين.
- عمر، رشاد خالد: المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية: دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية مصر، 2007.
- مصري، عبد الصبور وعبد الرحمن، منال، المحكمة الرقمية والجريمة المعلوماتية: دراسة مقارنة، ط1، مكتبة القانون والاقتصاد، 2012.
- مصطفى، عائشة بن قارة حجية الدليل الالكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، ط1، الإسكندرية، مصر، 2010.

- موسى، مصطفى محمد: التحقيق الجنائي في الجرائم الإلكترونية، ط1، دار الكتب القانونية، القاهرة، مصر، 2009.
- نجم، محمد صبحي: أصول المحاكمات الجزائية، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2000.
- نمور، محمد سعيد (شرح أصول الإجراءات الجزائية) (دار الثقافة للنشر، عمان، 2005).
- وسيم الأحمد، أصول تسليم المجرمين في ضوء الاتفاقيات الدولية والتشريعات الداخلية، دار غيداء للنشر والتوزيع، عمان، الأردن، 2020

- **الرسائل والأبحاث العلمية**

- آمال، بهنوس، الدليل الرقمي في الإجراءات الجنائية، المجلة الاكاديمية للبحث القانوني، مجلد 16، عدد 2، 2017.
- البشري، محمد الأمين، التحقيق في جرائم الحاسب الآلي والانترنت، جامعة نايف العربية للعلوم الأمنية، المجلة العربية للدارسات الأمنية، مج 15، عدد 30، ص ص. 317-380.
- التاج، إيهاب محمد، التحقيق وجمع الأدلة في الجرائم المعلوماتية، مجلة العدل – وزارة العدل، المملكة العربية السعودية المجلد 11، عدد 26، ص ص. 391 – 406، 2009.
- الجملي، طارق، الدليل الرقمي في الاثبات الجنائي، مجلة الحقوق، المجلد 12، عدد 1، ص ص. 40-73، البحرين، 2015.
- الطوالبة محمد: التفتيش الجنائي على نظم الحاسوب والانترنت دراسة مقارنة رسالة دكتوراه منشورة، جامعة عمان العربية، عمان، 2003.
- العربي، مصطفى إبراهيم، دور الدليل الرقمي في الاثبات الجنائي، مجلة البحوث القانونية، مجلد 4، عدد 1، ص ص. 67-107، 2016.

- العناوسة، معن أحمد، التفتيش في الجرائم الإلكترونية وفقا للتشريعات الجزائية الاردنية: دراسة مقارنة، رسالة ماجستير منشورة على دار المنظومة، جامعة عمان الاهلية، كلية الحقوق، الأردن، 2018.
- الفيل، علي، إجراءات التحقيق الابتدائي في الجرائم المعلوماتية، مجلة الحقوق – جامعة البحرين، مجلد 8، عدد 17، ص ص. 487 – 439.
- المتوكل، حورية، تحديات الحصول على الدليل الالكتروني، مجلة القانون والاعمال، العدد 65، ص ص. 110–120، المغرب، 2016.
- المعمري، مسعود بن حميدي، "الدليل الالكتروني لأثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، مجلد 6 ملحق، ص ص. 189–253، 2018.
- بلغيث، عماد، صعوبات التحقيق في الجرائم الإلكترونية، مجلة الرسالة للدراسات البحوث الإنسانية، مجلد 6، عدد 3، ص ص. 70 – 83، منشور في جامعة محمد بوضياف، الجزائر،2021.
- بن فريحة، رشيد التحري الجنائي في مسرح الجريمة المعلوماتية، مجلة جامعة القدس المفتوحة للبحوث والمعلومات الاجتماعية، عدد 42، 2017.
- تابري، مختار، الخبرة في الجريمة المعلوماتية، مجلة الحوار المتوسطي، مجلد 11، عدد 3، الجزائر 2020.
- حبيباتني، بثينة، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، العدد 50، ص ص. 85–97، 2018.
- حسن، آمال يوسف، الأدلة العلمية الحديثة ودورها في الاثبات الجنائي، جامعة الشرق الأوسط، رسالة ماجستير منشورة، 2012.

- خلف، جاسر، صعوبات الدليل الجنائي في الجرائم المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، العدد 12، العراق، 2016.
- خلف، مصطفى علي، التفتيش وفقاً لأحكام القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، المركز القومي للبحوث الاجتماعية والجنائية، المجلة الجنائية القومية، المجلد 63، العدد 3، ص ص. 1 – 73، 2020.
- سلامة، فهد، مشروعية السلطة التنفيذية بمراقبة الاتصالات الهاتفية، مجلة العربي للدراسات الإعلامية، العدد 9، ص ص. 3-11، 2020
- عبد الباقي، مصطفى، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، كلية الحقوق والإدارة العامة، جامعة بيرزيت، رام الله، فلسطين.
- عبيد، عماد محمود، التفتيش التحقيقي: دراسة مقارنة، معهد الإدارة العامة، دمشق، مجلد 48، عدد 2، ص ص. 233 – 290، 2008م.
- كامل، احمد أسامة، التفتيش في الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية مقارنة بالتشريع العماني، مجلة جيل الأبحاث القانونية المعمقة، عدد 28، ص ص. 11-38، 2018.
- لعوارم، وهيبة، مشروعية الدليل الالكتروني الناتج عن التفتيش الجنائي، مجلة القانون والفقه، العدد 20، ص ص. 99-113، 2014.

- **المراجع الإلكترونية**

- الموقع الرسمي لاتحاد الرابطات الدولية، مقال بعنوان المنظمة الدولية للأدلة الحاسوبية (https://uia.org/s/or/en/1100029648) تاريخ الزيارة (2021/12/30)
- الموقع الرسمي لمجلس اوروبا (https://www.coe.int/en/web/cybercrime/the-budapest-convention) تاريخ الزيارة (12/20/2021)

- الموقع الرسمي لبرنامج مضاعفة المساحة (DoubleSpace)
" https://en-academic.com/dic.nsf/enwiki/1674981" اخر زيارة بتاريخ (2022/2/27)

- المرقع الرسمي لبرنامج استرجاع الملفات لمايكروسوفت (Windows File Recovery)
(https://www.microsoft.com/en-us/p/windows-file-recovery/9n26s50ln705#activetab=pivot:relateditemtab) تاريخ اخر زيارة (1/29/2022)

انظر ايضاً (https://en.wikipedia.org/wiki/Windows_File_Recovery) تاريخ اخر زيارة (1/29/2022)

- الموقع الرسمي لبرنامج كشف الأدلة الرقمية (vidizmo)
(https://blog.vidizmo.com/tamper-detection-how-it-works-to-keep-digital-evidence-safe) تاريخ اخر زيارة (2022/1/30)

- الموقع الرسمي لبرنامج فورنسيك (forensic)
(https://www.forensicfocus.com/forums/forensic-software/win32dd-new-tool-to-image-ram-on-vista-w2k3/) تاريخ اخر زيارة (2022/4/3)

- مرجع الكتروني – الجرائم الإلكترونية الفدرالية
(https://brandonsample.com/federal-cyber-crimes/) تاريخ اخر زيارة (3/15/2022)

- مرجع الكتروني – القانون الفدرالي الأمريكي، القاعدة (4)
(https://www.law.cornell.edu/rules/frcrmp/rule_4) تاريخ اخر زيارة
(3/15/2022)
- الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الانتربول)
(https://www.interpol.int/ar/3/3)

- **المقابلات**

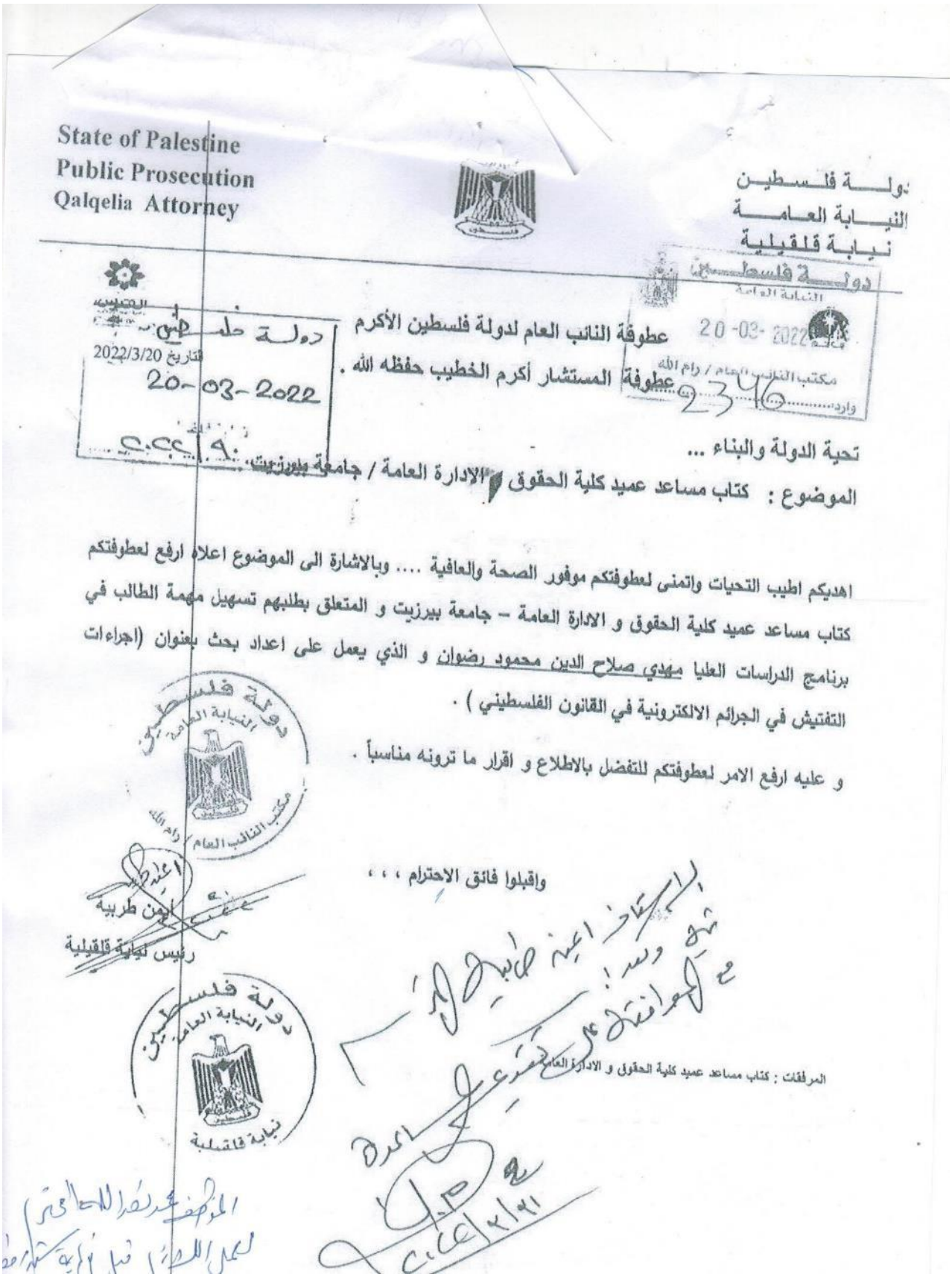
- مقابلة مع، الأستاذ أيمن طربية، رئيس نيابة محافظة قلقيلية، النيابة العامة، فلسطين، 2022/4/26
- مقابلة مع، أ. محمد نصر الله، وحدة الجرائم الإلكترونية في نيابة قلقيلية، فلسطين، 2022/4/26

¤ المراجع باللغة الأجنبية

- Abdelbaqi, Mustafa (Ph.D.). "Enacting cybercrime legislation in an endeavour to counter cybercrime in Palestine", Global Journal of Comparative Law 5 (pp.226-261), 2016.
- Årnes, André. "Digital Forensics", Norwegian University of Technology and Science (NTNU), first edition published by John Wiley & Sons Ltd, 2018.
- Casey, Eoghan. 'Digital Evidence and Computer Crime", Third Edition Forensic Science, Computers, and the Internet, Published by Elsevier, 2011.
- Chawki, Mohamed & Darwish, Ashraf & Khan, Mohammad & Tyagi, Sapna. "Cybercrime Digital Forensics and Jurisdiction", Studies in Computational Intelligence Volume 593, Polish Academy of Sciences, Warsaw, Poland, Springer, 2015.

- Clark, Franklin & Diliberto, Ken. "Investigating Computer Crime", CRC Press, Florida, 1996.
- Cross, Michael. "Scene of the Cybercrime", Second Edition, Syngress Publishing, USA, 2008.
- Dahj, Jean. "Mastering Cyber Intelligence", Packt Publishing Ltd, Birmingham, UK ,2022.
- Daniel, Larry & Daniel, Lars. "Digital Forensics for Legal Professionals Understanding Digital Evidence from the Warrant to the Courtroom", Syngress, 2012.
- Edwards, Graeme. "Cybercrime Investigators Handbook", 2019.
- Franklin, Carl. "The Investigator's Guide to Computer Crime", Charles C Thomas Publisher LTD, Spring afield Illinois, USA, 2006.
- Gercke, Marco. "Understanding cybercrime: phenomena, challenges and legal response", ITU, 2014.
- Holt, Thomas & Bossler, Adam & Spellar, Kathryn. "Cybercrime and Digital Forensics an Introduction", Second Edition, published by Routledge, NYC, USA 2018.
- Investigations Involving the Internet and Computer Networks, U.S department of justice, office of justice program, National Institute of Justice (U.S.), 2007.
- Resseguie, Donald. "Computer Searches and Seizure", 48 +69Clev. St. L. Rev. 185, 2000.
- Shinder, Debra & Tittel, Ed. "Scene of the Cybercrime Computer Forensics", Handbook, Syngress Publishing, 1st Edition, 2002.
- Watson, Richard & Pearson, Stephen. "Digital Triage Forensics: Processing the Digital Crime Scene", Syngress, 2010.

مرفقات



State of Palestine
Public Prosecution
Qalqelia Attorney

دولة فلسطين
النيابة العامة
نيابة قلقيلية

دولة فلسطين
النيابة العامة
20-03-2022
مكتب النائب العام / رام الله
وارد 2346

دولة فلسطين
التاريخ 2022/3/20
20-03-2022

عطوفة النائب العام لدولة فلسطين الأكرم
عطوفة المستشار أكرم الخطيب حفظه الله .

تحية الدولة والبناء ...

الموضوع : كتاب مساعد عميد كلية الحقوق / الادارة العامة / جامعة بيرزيت

اهديكم اطيب التحيات واتمنى لعطوفتكم موفور الصحة والعافية .... وبالاشارة الى الموضوع اعلاه ارفع لعطوفتكم كتاب مساعد عميد كلية الحقوق و الادارة العامة – جامعة بيرزيت و المتعلق بطلبهم تسهيل مهمة الطالب في برنامج الدراسات العليا مهدي صلاح الدين محمود رضوان و الذي يعمل على اعداد بحث بعنوان (اجراءات التفتيش في الجرائم الالكترونية في القانون الفلسطيني) .

و عليه ارفع الامر لعطوفتكم للتفضل بالاطلاع و اقرار ما ترونه مناسباً .

واقبلوا فائق الاحترام ، ، ،

دولة فلسطين
النيابة العامة
مكتب النائب العام / رام الله

أيمن طربية
رئيس نيابة قلقيلية

دولة فلسطين
النيابة العامة
نيابة قلقيلية

المرفقات : كتاب مساعد عميد كلية الحقوق و الادارة العامة

State of Palestine
Public Prosecution
Salfit Prosecution

دولـــــــة فلـسـطيـن
النيـــــابة العـامـــــة
نيـــــابة ســلـــفيـت

التاريخ:2022/2/24

السيد رئيس نيابة قلقيلية المحترم،،

تحية طيبة وبعد،،

الموضوع : إنابة السيد رئيس سلفيت في الملف التحقيقي رقم سفيت
عملا بأحكام المادة 57 من قانون الاجراءات الجزائية رقم 3 لسنة 2001 .

نرسل لكم الانابة في الملف التحقيقي المرقوم أعلاه وموضوعها محاولة اقتطاع جزء من أراضي الدولة لضمها لدولة أجنبية خلافاً لأحكام المادة 1/2 من القرار بقانون رقم 20 لسنة 2014 المعدل للمادة 114 من قانون العقوبات رقم 16 لسنة 1960، بخصوص إصدار مذكرة تفتيش لمنزل المتهم من سكان عزون عتمة قضاء محافظة قلقيلية لغايات ضبط النسخ الأصلية من صورة إخراج القيد وحصر الإرث المرفقة طي الانابة والواردة إلينا بموجب محضر استدلال الامن الوقائي في سلفيت كذلك أية مواد يحظر حيازتها بموجب القانون وتكليف جهاز الأمن الوقائي في قلقيلية لغايات تنفيذ مذكرة التفتيش، ومن ثم موافاتنا بما تم اتخاذه من اجراءات .

مع الاحترام

خليل سلامة
رئيس نيابة سلفيت

دولة فلسطين
النيابة العامة
نيابة سلفيت

المرفقات:

1- صورة عن إخراج القيد.
2- صورة عن حصر الإرث.

ملحق رقم (1) كتاب مساعد عميد كلية الحقوق والإدارة العامة / جامعة بيرزيت

ملحق رقم (2) إنابة في الملف التحقيقي

State of Palestine
Public Prosecution

دولة فلسطين
النيابة العامة

انابة

الاستاذ وكيل/ رئيس نيابة قلقيلية المحترم
تحية طيبة و بعد ،،

انابة في الملف رقم
نيابة سلفيت / تحق

وعملا بأحكام المادة 57 من قانون الإجراءات الجزائية رقم 2001/3 فقد تقرر انابة وكيل نيابة قلقيلية من اجل إصدار مذكرة تفتيش لمنزل المتهم ن سكان عزون عتمة قضاء محافظة قلقيلية لغايات ضبط النسخ الاصلية من صورة بشرى تقيد وحصر الإرث المرفقة طي الانابة والواردة إلينا بموجب محضر استدلال الامن الوقائي في سلفيت كذلك أية مواد يحظر حيازتها بموجب القانون وتكليف جهاز الأمن الوقائي في قلقيلية لغايات تنفيذ مذكرة التفتيش. وذلك بالسرعة الممكنة، و اتخاذ كافة الاجراءات القانونية الممنوحة لكم وفق احكام القانون

وذلك في القضية رقم سلفيت / تحقيـــق

مع الاحترام ،،،

تحريرا في: 2022/02/24

رئيس النيابة
نيابة سلفيت

ملحق رقم (3) انابة من أجل اصدار مذكرة تفتيش

State of Palestine
Preventive Security H.Q
Salfeet Directorate

دولة فلسطين
قيادة الأمن الوقائي
مديرية سلفيت

الأمن الوقائي - سلفيت
صادر
الرقم ٢٠٢٢/٢/١٦٤
التاريخ

سعادة رئيس النيابة العامة في سلفيت .... حفظه الله

تحية الدولة والوطن وبعد ،،

الموضوع : امر نفاذ ودخول الى الاجهزة الالكترونية القضية التحقيقية رقم

يهديكم جهاز الامن الزقائي اطيب التحيات ،بالاشارة الى الموضوع اعلاه وعطفا على كت بكم الوارد الينا بتاريخ ٢٠٢٢/٢/٢١ والمتضمن فحص جهاز ايفون بروماكس لون سكني الخاص بالموقوف / بديا ، نفيدكم بأنه بعد الفحص الاولي من قبل الدائرة الالكترونية تم استخراج ثلاث صور خاصة بقطعه الارض المنوي تسريبها للجانب الاسرائيلي .

* مرفق في طي الكتاب محضر استخراج هذه الصور وجاري العمل على فحص الجهاز بشكل كامل من قبل دائرة الاختصاص وتزويدكم بالنتائج المترتبة على ذلك .

مع فائق الاحترام

مدير مديرية الامن الوقائي/سلفيت
عميد/ سليم زهران

م. ابراهيم محمد احمد
للاطلاع واتخاذ اللازم.

محلق رقم (4) محضر استخراج صور من جهاز رقمي بعد اصدار مذكرة تفتيش في ذات الجريمة

State of Palestine

Public Prosecution

Qalqelia Prosecution

دولـــة فلـــسطيـــن

النيـــابة العـــامـــة

نيابة قلقيلية

25 -10- 2021

al QUDS

السيد مدير الشرطة في محافظة قلقيلية المحترم

العميد/ نهاد ربايعة .. حفظه الله

تحيه الوطن والبناء،،،

الموضوع : أمر نفاذ في القضية التحقيقية رقم (2021/1528) .

بالإشارة إلى الموضوع أعلاه ، للتفضل من حضرتكم بالإيعاز لجهات الاختصاص لديكم "وحدة الجرائم الإلكترونية" للعمل على النفاذ المباشر وتفتيش و تفريغ واسترجاع أي بيانات تخص المخدرات للجهاز المضبوط والمبرز بالحرف ن/ 2 على كافة مواقع التواصل الاجتماعي والاستديو و اية رسائل صوتية او خطية والخاص بالمتهم [redacted] تتعلق بموضوع الدعوى المرقومة اعلاه وتزويدنا بتقرير مفصل بذلك وفق الأصول والقانون.

واقبلوا الاحترام

دولة فلسطين
النيابة العامة
نيابة قلقيلية

أيمن ظريبة
رئيس نيابة قلقيلية

المرفقات :
هاتف من نوع سامسونج لون زهري

* استلمت انا [illegible] مرتب شرطة قلقيلية - فرع المباحث [illegible] جهاز من نوع سامسونج لون زهري وعليه اتحمل كامل المسؤولية

محلق رقم (5) صورة عن أمر نفاذ من أجل تفتيش جهاز رقمي