إجراءات التحقيق الخاصة بالجرائم السيبيرانية

د/ بومحراث ليندة، أستاذ محاضر أ
جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة

إجراءات التحقيق الخاصة بالجرائم السيبيرانية
Cybercrime investigative procedures

الملخص:

تعتبر الجرائم السبيرانية نوع مستحدث من الجرائم يختلف عن الجرائم التقليدية تبعا لخصوصية التقنيات التي يتم من خلالها والبيئة التي يتم فيها، الأمر الذي استدعى مواكبة النصوص التشريعية لهذه الخصوصية ومن ثم إيجاد حلول للإشكالات القانونية التي طرحتها هذه الجرائم وقد عالجت هذه الورقة البحثية واحدا من أهم هذه الإشكالات ومفاده: ما هي إجراءات التحقيق التي من شأنها تسهيل الكشف عن الجريمة السيبيرانية وإثباتها؟ وتوصلت إلى أن الطبيعة الخاصة للجريمة السبيرانية وامتدادها عبر الحدود إضافة إلى سرعة تنفيذها وصعوبة اكتشافها تستوجب إجراءات تحقيق خاصة زيادة على الإجراءات العامة المتبعة في الجرائم التقليدية.

الكلمات المفتاحية:

الجريمة السبيرانية – المعاينة الإلكترونية –التفتيش الإلكتروني –المراقبة الإلكترونية –حفظ وإفشاء المعطيات الإلكترونية

Abstract

Cybercrime is a new type of crime that differs from traditional crimes due to the specificity of the technologies through which it is carried out and the environment in which it takes place, which required legislative texts to keep pace with this specificity and thus find the legal issues raised by these crimes. This paper addresses one of most important of these issues, namely: What are the investigative procedures that would facilitate the detection and proof of cybercrime? The paper concludes that the special nature of cybercrime and its extension across borders, in addition to its speed of execution and difficulty of detection, require special procedures in addition to the general procedures followed in traditional crimes.

Keywords:

Cybercrime – Electronic preview - Electronic inspection – Electronic surveillance – Electronic data storage and creation

مقدمة:

إن الثورة المعلوماتية التي شهدها العالم في السنوات الأخيرة، حولته إلى قرية صغيرة تلاشت فيها الحدود الجغرافية والسياسية بين الدول. وعلى قدر ما كان لهذه الثورة من إيجابيات أضحى تجاوزها أو التنازل عنها ضرب من الخيال سواء على مستوى علاقات الأفراد ومعاملاتهم أم على مستوى المعاملات والعلاقات الدولية، كان لها أيضا جملة من السلبيات التي باتت تهدد أمن المجتمعات والدول، ويأتي في مقدمة هذه السلبيات ما يعرف بالجرائم السبيرانية أو الإلكترونية (**cyber crimes**)، التي تعتبر نوع مستحدث من الجرائم يختلف عن الجرائم التقليدية تبعا لخصوصية التقنيات التي تتم من خلالها والبيئة التي تتم فيها، الأمر الذي استدعى مواكبة هذا النوع من الجرائم بنصوص تشريعية تتماشى وخصوصيتها خاصة فيما يتعلق بإجراءات التحقيق والبحث والتحري عنها، وهو ما سيكون موضوع هذه الورقة البحثية، التي ستعالج إشكالا رئيسا مفاده: "ما هي إجراءات التحقيق التي من شأنها تسهيل الكشف عن الجريمة السبيرانية وإثباتها؟"

ويندرج تحت هذا التساؤل الرئيس جملة من التساؤلات الفرعية، يمكن إيجازها في الآتي:

1-ما مفهوم الجريمة السبيرانية؟ ما الفرق بينها وبين الجريمة التقليدية؟

2-فيما تتمثل خصوصية التحقيق في الجريمة السبيرانية؟

3-هل يمكن تطبيق القواعد العامة للتحقيق على الجريمة السبيرانية أم أنه يجب على المشرع استحداث قواعد إجرائية خاصة تتناسب الطبيعة المميزة لهذا النوع من الجرائم؟

وستتم الإجابة عن هذه التساؤلات من خلال بيان مفهوم الجريمة السبيرانية وخصوصية التحقيق فيها (في محور أول)، ثم التطرق إلى تطبيق إجراءات التحقيق العامة والمستحدثة على الجريمة السيبيرانية (وهذا في محور ثان).

المحور الأول: مفهوم الجريمة السيبيرانية وخصوصية التحقيق قيها

أولا: مفهوم الجريمة السبيرانية

لتحديد مفهوم الجريمة السبيرانية ينبغي علينا تعريفها وبيان خصائصها التي تمييزها عن الجريمة التقليدية، ثم بيان تصنيفاتها المختلفة، والمجالات التي تستهدفها.

ا -تعريف الجريمة السبيرانية

1-التعريف الفقهي للجريمة ا السبيرانية:

تعرف الجريمة بوجه عام بأنها: «كل فعل أو نشاط يتم بطريقة غير مشروعة ويقرر له القانون عقوبة أو تدبيرا احترازيا»[1]. بمعنى أنها تشمل كل نشاط مخالف للقوانين الجزائية السارية في الدول[2].

أما الجريمة السبيرانية فقد اختلفت آراء الفقهاء في تعريفها تبعا لاختلافهم في الأسس المعتمدة في التعريف، أهي وسيلة ارتكاب الجريمة، أم توافر معرفة الجاني بتقنية المعلومات، أم هي موضوع الجريمة، أم أنها الجمع بين كل هذه الأسس.

لذلك وجدت عدة تعريفات لهذه الجريمة لعل أهمها أنها: «نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي»[3].

غير أن ما يمكن أن يلاحظ على هذا التعريف هو أنه ربط الجريمة السبيرانية بالحاسب الآلي، وهذا أمر لا يمكن أن يؤخذ على إطلاقه ذلك أن التطورات المتلاحقة في مجال وسائل الاتصال أسفر عن إمكانية استعمال الهواتف النقالة لدخول شبكة المعلومات الدولية "الإنترنت"، ومن ثم فإنها يمكن أيضا أن تكون وسيلة لارتكاب الجريمة السيبيرانية.

---

[1]-طارق الخن: الجرائم المعلوماتية، منشورات الجامعة الإفتراضية السورية، 2018م، ص22.

[2]-عبد الصبور عبد القوي علي المصري: التنظيم القانوني للتجارة الإلكترونية، ط1، الرياض، مكتبة القانون والاقتصاد، 1433هـ-2012م، ص91.

[3]-عبد الفتاح بيومي حجازي: الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، ط1، مصر، دار الكتب القانونية، 2007م، ص13.

كما تم تعريفها بأنها: «الجرائم التي لا تعرف الحدود الجغرافية، والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الإنترنت، وبواسطة شخص على دراية فائقة»[1].

لذلك فإنه من الأفضل استعمال مصطلح وسائل الاتصال الإلكترونية بدل الحاسب الآلي، لأن هذا المصطلح يمكنه أن يستوعب وسائل الاتصال الموجودة في هذا العصر، كما يمكنه استيعاب أي وسيلة اتصال يمكن التوصل إليها لاحقا، وعليه يمكن صياغة التعريف السابق على النحو الآتي: «هي نشاط إجرامي تستخدم فيه وسائل الاتصال الإلكترونية بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي».

إضافة إلى هذا هناك تعريفات أخرى تناولت الجريمة السبيرانية بمعان قريبة من هذا التعريف نذكر منها على سبيل المثال:

-أنها: «مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب»[2].

-أنها: «الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا»[3].

- وعرفتها منظمة التعاون الاقتصادي بأنها: «كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتج عن تقنية المعلوماتية»[4].

2-تعريف الجريمة السبيرانية في التشريع الجزائري:

لم يستعمل المشرع الجزائري مصطلح "الجريمة السبيرانية" وإنما استعمل مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات".

وقد عرف هذا المصطلح في المادة 2/02 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، حيث جاء فيها: «جرائم المساس بأنظمة

---

[1]-منير محمود الجنبيهي: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، د.ط، الإسكندرية، دار الجامعة الجديدة، 2005م، ص13.

[2]-يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والأنترنت، دار العدالة، ط1، القاهرة، 2011م، ص09.

[3]-أسامة أحمد المناعسة، جرائم الحاسب الآلي والأنترنت، دار وائل للنشر، ط1، عمان، 2001م،ص73.

[4]-التعريف مذكور في موقع المنظمة على الرابط: www.ocde.org .

المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية»[1].

من خلال التعريفات المختلفة للجريمة السبيرانية يتضح أنها تتميز عن الجريمة التقليدية من حيث أن الأداة في الجريمة السبيرانية ذات تقنية عالية، كما أن مكان الجريمة لا يتطلب انتقال الجاني إليه انتقالا ماديا، فالجريمة السبيرانية تتم عن بعد باستخدام شبكات الانترنت بين الجاني والمجني عليه، غير أن الجريمتين تتشابهان في أطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة، وضحية قد يكون شخصا طبيعيا أو معنويا[2].

II- تصنيفات الجريمة السيبيرانية[3]

هناك تصنيفات عديدة للجريمة السبيرانية ، تبعا لتعدد المعايير المتبعة في هذه التصنيفات على أنها لا تخرج عن ثلاث تصنيفات أساسية هي الجرائم الواقعة على الأموال، والجرائم الواقعة على الأشخاص، والجرائم الواقعة على أمن الدول، على أنه تندرج تحت كل صنف عدة أنواع على نحو التفصيل الآتي:

1- الجرائم الواقعة على الأموال:

-الجرائم التي تستهدف الأموال باستثناء السرقة: وتشمل أنشطة الاقتحام أو الدخول أو الاتصال غير المرخص به مع نظام الكمبيوتر أو الشبكة، وتخريب البيانات والنظم والممتلكات، وخلق البرمجيات الخبيثة والضارة ونقلها عبر النظم والشبكات، وكذلك استخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص.

---

(1)-قانون رقم 09-04 المؤرخ في 14 شعبان 1430ه الموافق ل 05أوت 2009م المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، ع47

(2)-عبد الله ذيب عبد الله محمود: حماية المستهلك في التعاقد الإلكتروني دراسة مقارنة، مرجع سابق، ص94-95.

(3)-أنظر: مركز البحوث والدراسات لغرفة التجارة الصناعية بالرياض قطاع البحوث ومنتدى الرياض الاقتصادي: الغش التجاري في المجتمع الإلكتروني، ورقة عمل مقدمة إلى الندوة الرابعة لمكافحة الغش التجاري والتقليد في دول مجلس التعاون الخليجي تحت عنوان: "ظاهرة الغش التجاري والتقليد في ظل التطور التقني والتجارب العالمية المعاصرة"، في الفترة 20-21 سبتمبر 2005م.

-جرائم الاحتيال والسرقة: مثل التلاعب بالبيانات والنظم واستخدام الكمبيوتر للحصول على البطاقات المالية للغير واستخدامها دون ترخيص أو حتى تدميرها، الاختلاس عبر الكمبيوتر أو بواسطته، سرقة معلومات أو خدمات الكمبيوتر، قرصنة البرامج، وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر.

-جرائم المقامرة والجرائم الأخرى ضد الأخلاق والتزوير: وتشمل تملك وإدارة وتسهيل مشروعات المقامرة على الإنترنت وغيرها.

2- الجرائم الواقعة على الأشخاص:

-اختراق الأمن الشخصي للأفراد: مثل الاحتيال بانتحال صلاحيات شخص مفوض، الإزعاج، التحرش، التهديد، قرصنة البرمجيات...

-اختراق الحماية الخاصة بالاتصالات وأمن البيانات: مثل الاعتداء على البيانات، والاعتداء على البرمجيات.

-الجرائم التي تستهدف الأشخاص: ومن أبرز أشكالها الجرائم غير الجنسية التي تستهدف الأشخاص، والجرائم الجنسية.

3- الجرائم الواقعة على أمن الدولة: وتشمل هذه الطائفة[1]:

أ-كافة جرائم تعطيل الأعمال الحكومية، وتنفيذ القانون، والإخفاق في الإبلاغ عن جرائم الكمبيوتر، والحصول على معلومات سرية.

ب-والإرهاب الإلكتروني: استفادت المنظمات الإرهابية من التطورات الحديثة لوسائل الاتصال وبصفة خاصة شبكة الإنترنت، حيث أسست مواقع افتراضية لها واتخذتها وسيلة لبث ثقافة الارهاب، كما أنها تتخذها وسيلة لإعلان مسؤوليتها عن الهجمات التي ترتكبها، أو نفي البيانات أو التعليق على أخبار الصادرة من منظمات أو جهات دولية أخري.

[1]-يراجع تفصيل المسألة لدى: يوسف صغير: الجريمة المرتكبة عبر الأنترنت، مرجع سابق، ص55-59، محمد أمين بلبحري: الجريمة الإلكترونية كجريمة منظمة عابرة للحدود، مرجع سابق، ص53،

إضافة إلى ما تقدم فإن الجماعات الارهابية تتخذ الإنترنت وسيلة لتجنيد عناصر ارهابية جديدة وتساعدهم على تنفيذ أعمالهم الاجرامية عبر الوسائط الإلكترونية المختلفة.

جـ-الجريمة المنظمة: استفادت الجريمة المنظمة ليست من تقدم وسائل الاتصال والتكنولوجيات الحديثة، حيث أصبحت غير محدودة لا بقيود الزمان ولا بقيود المكان، وأصبح انتشارها على نطاق واسع وكبير كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة على شبكة الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية بسهولة، فقد اكتشفت هذه الجماعات أن استخدام هذه الشبكة تستطيع أن يؤمن لها فرص جديدة وفوائد وأرباح كبيرة.

د-جرائم التجسس: التجسس يعني الاطلاع على معلومات خاصة بالغير مؤمنة في جهاز آخر وليس مسموحا لغير المخولين بالاطلاع عليها. وقد سهلت شبكة الإنترنت الأعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية والوطنية.

ويصنف التجسس إلى ثلاث أصناف أساسية هي: التجسس العسكري، التجسس السياسي، والتجسس الاقتصادي، كما تستخدم العديد من الدول التجسس عبر وسائل الاتصال الحديثة معتمدة على شبكة الإنترنت، سواء للتجسس على دول أخرى، أم على مواطنيها، كما تستخدمه الشركات للتجسس على الشركات الأخر المنافسة لها.

4-جرائم المساس بالأمن الفكري:

إن الكم الهائل من المعلومات التي يمكن الحصول عليها من عدة مصادر لا يمكن التحكم فيها ومتابعتها أو الإشراف عليها، كل ذلك جعل هذه الشبكة من أهم مقومات المجتمع المعلوماتي التي تؤدي إلى الانحراف الفكري، من خلال تعرض الشخص إلى الكثير من المؤثرات الفكرية التي تستخدم شبكة الإنترنت والحواسيب الآلية، وتهدد الأمن بأبعاده كافة، حيث تتوالى الهجمات الثقافية والحضارية التي قد تزعزع الأمن الفكري والعقدي للشعوب المغلوبة على أمرها، وتنشر عبرها القوى الغالبة فكرها، ولغتها وقيمها وقد ظهر في أدبيات بعض الباحثين من بدايات شبكة

الإنترنت إشارات التحذير من الغزو الفكري المركز الذي سيقبله الجيل العربي المسلم مما يجعله عرضة للهزيمة الفكرية[1].

وعليه يتضح جليا تعدد وتنوع أشكال الجريمة السيبيرانية والتي تزداد وتتنوع تبعا للتطور المتسارع الذي تشهده تقنيات المعلومات والاتصالات المستخدمة في هذا النوع من الجرائم.

III -**القطاعات التي تستهدفها الجريمة السيبيرانية:** بالنظر إلى التصنيفات السابقة للجريمة الإلكترونية يتضح أنها لا تستهدف قطاعا واحدا وإنما تستهدف عددا كبيرا من القطاعات نذكر منها:

1-المؤسسات المالية والاقتصادية: (التجارة الإلكترونية)

2-الأشخاص الطبعيون: (حرمة الحياة الخاصة وسرقة الأموال)

3-المؤسسات العسكرية: (نادرة الوقوع إلا أنها موجودة في الواقع بدليل اختراق موقع البنتاغون الأمريكي وسرقة 29 وثيقة خاصة بالأسلحة النووية من قبل الألماني هيس لأندر).

ثانيا: خصوصية التحقيق في الجريمة السبيرانية

يعرف التحقيق الجنائي بأنه: "مجموعة من الإجراءات التي تباشرها الجهة المكلفة بالتحقيق لدى وقوع الجريمة بغية البحث والتحري والتنقيب عن الأدلة التي تفيد في الكشف عن الحقيقة".

وإن كان هذا الأمر يتسم بالصعوبة في الجريمة التقليدية فإنه يزداد صعوبة في الجريمة السبيرانية انطلاقا من خصوصية هذه الأخيرة من حيث شخص القائم بها (المجرم)، ومن حيث الجريمة في حد ذاتها، ومن حيث الجهة المتضررة وأخيرا من حيث الجهة المكلفة بالتحقيق، وهو ما سنتاوله على نحو التفصيل الآتي:

1-صعوبة التحقيق الجنائي من حيث القائم بها (المجرم): يختلف الجاني في الجريمة السبيرانية عن الجاني في الجريمة التقليدية، وذلك لأنه يتمتع بجملة من الخصائص التي عادة لا تتوفر في الجاني التقليدي والتي يمكن إيجازها في:

[1]-يوسف صغير، الجريمة المرتكبة عبر الأنترنت، المرجع السابق، ص59.

-إن الجاني في الجريمة السبيرانية يتمتع بدرجة عالية من الذكاء والمعرفة، ولا نقصد هنا المستوى الأكاديمي وإنما نقصد مستوى المعرفة بتقنيات تكنولوجيا المعلومات والاتصالات.

-إن الجاني في الجريمة السبيرانية لا يهدف دائما لتحقيق منفعة مادية، بل قد يهدف إلى الانتقام، أو مجرد إثبات قدرته على اختراق نظام معين، لأن في هذا إثبات لقدراته ومهاراته التقنية.

2-صعوبة التحقيق الجنائي في الجريمة السبيرانية من حيث الجريمة في حد ذاتها:

-غياب الدليل المرئي.

-صعوبة الوصول إلى الدليل بسبب وسائل الحماية التقنية التشفير، كلمة السر...

-سهولة محو الدليل أو تخزينه

-ضخامة المعلومات والبيانات الواجب فحصها مع إمكانية خروجها عن النطاق الإقليمي للدولة بسبب البعد الجغرافي بين الجاني والمجني عليه (الضحية).

3- صعوبة التحقيق الجنائي في الجريمة السبيرانية من حيث الجهة المتضررة:

-عدم إدراك خطورة الجريمة السبيرانية من قبل المسؤولين عن المؤسسات.

-تسابق الشركات في تسهيل استخدام البرامج والأجهزة الإلكترونية وملحقاتها الخاصة بالحاسب الآلي وزيادة الإنتاج دون مراعاة الجانب الأمني.

-الإحجام عن الإبلاغ عن الجرائم السبيرانية تفاديا للمساس بسمعة ومصداقية المؤسسات.

-خوف المؤسسات والشركات التجارية العاملة في ميدان الانترنت من حجز الجهات المكلفة بالتحقيق للحواسب الآلية أو تعطيل شبكاتها لفترة طويلة تساهم في تحميلها خسائر مالية أكثر.

4- صعوبة التحقيق الجنائي في الجريمة السبيرانية من حيث الجهة المكلفة بالتحقيق:

-نقص المهارة التقنية المطلوبة في التحقيق الجنائي السيبيراني.

-قلة الخبرة في مجال التحقيق الجنائي السبيراني وقلة إتقان اللغة الإنجليزية والمصطلحات التقنية.

-عدم رصد ميزانية مالية كافية لاستقطاب النخبة المتميزة في المجال المعلوماتي.

المحور الثاني: تطبيق إجراءات التحقيق العامة والمستحدثة على الجريمة السيبيرانية

أولا: تطبيق إجراءات التحقيق العامة على الجريمة السيبيرانية

على الرغم من تعدد إجراءات التحقيق العامة في الجرائم التقليدية، إلا أننا ستقتصر هذه الورقة البحثية على إجراءي المعاينة والتفتيش لأهميتهما، وهو ما سنفصله في الآتي:

1- المعاينة:

لم يحدد المشرع الجزائري المقصود بالمعاينة ولكن قانون الإجراءات الجزائية أشار إلى إجراء المعاينة باعتباره إجراء من إجراءات السلطات التحقيقية بمختلف فئاتها وطوائفها، حيث نصت المادة 79 من الأمر رقم 66- 155 المتضمن ق.إ.ج.ج على أنه: «**يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها....**» [1].

أما على مستوى الفقه، فقد حظيت بتعريفات عديدة منها:

-أنها: «رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة» [2].

أو هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها، فهي الإثبات المادي لحالة الأشياء والأمكنة والأشخاص ذات الصلة بالحادث والوجود المادي للجريمة، وعلى أساس ذلك فهي تصوير واقعي لجميع ما يحتويه مسرح الجريمة لكشف الغموض وكيفية وقوع الجريمة من ناحية، وبالتوصل إلى مقترف الجريمة من ناحية أخرى[3].

---

[1]-فاطمة الزهراء بخي، إجراءات التحقيق في الجريمة الإلكترونية، مرجع سابق، ص85.

[2]-المادة 79 من الأمر رقم 66- 155، مرجع سابق، ص38.

[3]-فؤاد كروم، إجراءات المعاينة التقنية لمسرح الجريمة، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2018م، ص26-27.

وللمعاينة أهمية تختلف حسب طبيعة الجرائم، فدورها في الكشف عن الحقيقة في الجرائم التقليدية يختلف عن الجرائم الإلكترونية، وذلك راجع إلى أن الجرائم التي تقع على نظم المعلومات قد لا يتخلف عن ارتكابها آثار مادية، وأيضا احتمالية أن عدد كبير من الأشخاص قد يتردد على مسرح الجريمة[1]، لذا وجب معرفة مدى صلاحية مسرح الجريمة لإجراء المعاينة، كما يجب معرفة الإجراءات التي تتم بها المعاينة التقنية.

أ- مدى صلاحية مسرح الجريمة للمعاينة:

-**المسرح التقليدي:** هو مسرح الجريمة الذي يقع خارج بيئة الحاسب الآلي ويمكن لرجل الضبط الجنائي العثور فيه على آثار مادية خلفها الجاني، كالأوراق والأقراص المرنة والصلبة وأشرطة تخزين المعلومات والقطع الإلكترونية وأجهزة المودم والبرامج المستخدمة والطابعات وأقراص الليزر والبطاقات المستخدمة ووسائل الحفظ، وأشرطة الحاسب الآلي وكابلاته وشاشة العرض الخاصة به ومفاتيح التشغيل والأسطوانات وغيرها من مكونات الحاسب ذات الطابع المادي المحسوس. وليس هناك صعوبة مادية لتقرير مدى صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل ضباط الشرطة القضائية والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبها إلى شخص معي[2]. فالمعاينة التي تتم على مستوى مسرح الجريمة التقليدي تتسم بالسهولة لوقوعها على عناصر مادية ملموسة.

-**المسرح الافتراضي:** هو المسرح الإلكتروني الذي يقع داخل النظام المعلوماتي أو العالم الافتراضي والذي قام فيه المجرم بجريمته أو قام بها بواسطته، ويصل إليه رجل الضبط الجنائي بطريقة فنية تستلزم الالمام بالتقنية والاتقان لها، ويمكن من خلال هذا المسرح استخلاص الدليل الجنائي الإلكتروني وغيره من الأدلة المعلوماتية التي تثبت وقوع الجريمة ونسبها إلى مرتكبيها

---

[1]-مريم بلغفور، صليحة عتروز، آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص87.

[2]-يراجع تفصيل المسألة لدى: خالد مرزوق سراج العتيبي، الجوانب الإجرائية في الشروع في الجريمة السيبيرانية، مكتبة القانون والاقتصاد، ط1، الرياض، المملكة العربية السعودية، 2014م، ص64.عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، مكتبة الإسكندرية، دط، الإسكندرية، مصر، د.ت، ص226، ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة السيبيرانية، مرجع سابق، ص09.

[1]. وهذا المسرح يتكون من البيانات الرقمية التي تتواجد في ذاكرة الأقراص الصلبة الموجودة داخل الحاسوب[2].

ب-الانتقال إلى مسرح الجريمة وتأمينه: وتتم المعاينة في الجريمة السيبيرانية المرتكبة عبر الإنترنت أو بواسطة الحاسب الآلي كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية، إلا أن الانتقال هناك لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي [3].

ويلتزم المحقق عادة قبل البدء في المعاينة الإلكترونية بجملة من التدابير الفنية والتحفظية التي تساعده في القيام بمهامه على أحسن وجه وهي كالتالي:

-الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد وموقع الأجهزة الإلكترونية وشبكاتها وسائر ملحقاتها والنهايات الطرفية المتصلة بها المتوقع مداهمتها.

-توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة يمكن الاستعانة بها في الفحص، التشغيل، الضبط والتأمين وحفظ المعلومات.

-تأمين التيار الكهربائي بشكل لا يتم التلاعب أو التخريب عن طريق قطع التيار أو تعديل الطاقة الكهربائية.

-التأكد من خلو المحيط الخارجي لمسرح الجريمة السبيرانية من أية مجالات لقوى مغناطيسية أو ممرات اتصالات يمكن أن تتسبب في محو البيانات المسجلة أو إتلاف الآثار الأخرى للجريمة.

-التحفظ على محتويات سلة المهملات ومستندات الادخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.

-إعداد فريق من المتخصصين وأهل الخبرة في مجال تكنولوجيا الإعلام الآلي للاستعانة بهم عند الحاجة[4].

---

[1]-خالد مرزوق سراج العتيبي، الجوانب الإجرائية في الروع في الجريمة السيبيرانية، المرجع السابق، ص64.

[2]-ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة السيبيرانية، المرجع السابق، ص09.

[3]-المرجع نفسه، ص63.

[4]-بشير حماني، خصوصية التحقيق في الجريمة الإلكترونية، مرجع سابق، ص64-65.

فالمعاينة هي أول إجراء للتحقيق في الجريمة السبيرانية، وهي تتعلق بشكل مخصوص بمسرح الجريمة بنوعيه التقليدي والافتراضي ومدى صلاحيته لإجراء المعاينة، ولهذا خصها المشرع بمجموعة من الضوابط والشروط التي على ضباط الشرطة القضائية اتباعها من انتقال لمسرح الجريمة إلى تأمينه والسيطرة عليه.

2- التفتيش:

يعد التفتيش من أخطر الإجراءات التي تقوم بها الضبطية القضائية للبحث عن أدلة تتعلق بجريمة تحقق وقوعها، وذلك وفقا لضوابط نص عليها قانون الإجراءات الجزائية أو نصوص خاصة، وتزيد أهمية هذا الإجراء في مجال الجريمة السبيرانية التي باتت تهدد الحقوق والحريات الخاصة من خلال استخدام الحاسب الآلي وما يحتويه من أدلة مادية أو معنوية.

أ-تعريف التفتيش: تعددت التعريفات الفقهية للتفتيش، وجميعها لا تخرج عن كونه: إجراء من إجراءات التحقيق، يباشر من مختصين عند وقوع جناية أو جنحة للبحث عن أدلة الجريمة متى استلزمت ضرورة التحقيق ذلك، ويباشر في محل له حرمة سواء رضي به من يباشر حياله أم لم يرضى". كما أنه عرف على أنه:" إجراء من إجراءات التحقيق تقوم به سلطة مختصة حددها القانون، يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة[1].

ويقصد بالتفتي في الجريمة السيبيرانية تفتيش النظم المعلوماتية ولو عن بعد من خلال جمع الأدلة المخزنة أو المسجلة بشكل إلكتروني كالملفات والبرامج المخزنة في الحواسيب والمعطيات والاتصالات الإلكترونية سواء كانت معطيات ذات طابع مادي أو معنوي تفيد كدليل إلكتروني في الكشف عن الحقيقة؛ أو هو البحث الدقيق أو الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه سواء كان مسكنا أو شخصا محله جهاز حاسوب أو أنظمة معلوماتية أو شبكة الأنترنت[2].

---

[1]-عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، دار الثقافة، ط1، الأردن، 2010م، ص500-501.

[2]-يوسف مناصرة: الدليل الإلكتروني في القانون الجزائي دراسة مقارنة، ط1، الجزائر، دار الخلدونية، 2021، ص348.

ب- الشروط القانونية للتفتيش في الجرائم الإلكترونية: التفتيش إجراء قانوني ينال من الحرية الشخصية، لذلك حرصت كافة التشريعات على إحاطته بشروط وضمانات أساسية ولعل الغرض من ذلك يتمثل في تحقيق مصلحة المجتمع في القصاص من المجرم وردعه، وضمان حق الفرد وحرياته. ومن هذه الشروط والضمانات التي ينبغي توافرها لإجراء التفتيش ما هو موضوعي، ومنها ما هو شكلي[1].

1-**الشروط الشكلية:** وتتمثل هذه الشروط في:

-الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في البيئة الإلكترونية: يعتبر هذا الإجراء من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم، حيث أن المتهم هو الشخص الذي يستوجب القانون حضوره عند إجراء التفتيش، إذ أن الإجراء المتخذ يمسه هو، غير أنه قد لا يتسنى للمتهم الحضور في حال كان محل التفتيش مسكنه، فمن أجل ذلك أجاز القانون له أن يُنيب عنه غيره ليجري التفتيش في حضوره، وإلا وجب استدعاء شاهدين في بعض الأحوال، كما يحق للمتهم أن يستعين بمحاميه عند إجراء التفتيش، ومن ثم يجوز للمحامي الحضور أيضا، كذلك إذا جرى التفتيش لدى غير المتهم وجب إتاحة الفرصة لحائز المكان في الحضور رعاية لمصالحه، ويخول المشرع للنيابة العامة أيضا حق الحضور أثناء التفتيش الذي يجريه قاضي التحقيق[2]. وهو ما نص عليه المشرع الجزائري في المادة 1/45[3]. إلا أنه استثنى بموجب الفقرة الأخيرة من نفس المادة عدة جرائم من بينتها جرائم المساس بنظم المعالجة الآلية

---

[1]-عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، مرجع سابق، ص511-512.

[2]-عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية أو الاستثنائية، المرجع السابق، ص515- 516.

[3]-التي نصت على أنه: والتي نصت على ما يلي:" **إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له. وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته**"، المادة 45 من الأمر 66- 155، مرجع سابق، ص06.

للمعطيات نظرا لطبيعتها التقنية الخاصة التي تستدعي السرعة في استخلاص الدليل الرقمي قبل فقدانه [1].

2-**موعد إجراء التفتيش في الجرائم الإلكترونية:** اختلفت التشريعات الإجرائية في وضع ميعاد زمني لتفتيش نظم المعلوماتية، فمنها من حظر القيام بهذا الإجراء في أوقات معينة في الليل مثلا، وهنالك من قرنه بوقت معين حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المساكن، وهنالك من تركه على مطلقه يتم في أي ساعة من ساعات الليل والنهار وترك السلطة التقديرية في ذلك للقائم أو للسلطة المكلفة بالتفتيش[2]. والمشرع الجزائري قد تطرق للمسألة في المادة 47 من ق.إ.ج.ج[3].

ب-الشروط الموضوعية: وهي الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاث شروط أساسية هي السبب، المحل، والسلطة المختصة بالقيام بالتفتيش[4]، وفيما يلي تفصيل كل شرط:

1-**سبب التفتيش في البيئة الإلكترونية:** من المستقر عليه في أن السبب في التفتيش هو الذي يحرك السلطة المختصة إلى اصدار قرارها بالتفتيش ومباشرته، أي أنه الواقعة المنشئة للسلطة في التفتيش والتي تخول للمحقق الحق في أن يصدر الأمر بالتفتيش. فالسبب هو وقوع

---

[1]-عبد اللطيف دحية وآخرون، المواجهة الإجرائية لجرائم المعلوماتية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2019م، ص46

[2]-عائشة بوخبزة، الحماية الجزائية من الجريمة السيبيرانية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، وهران، الجزائر، 2013م، ص194.

[3]-حيث نصت على أنه: «-عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص. -عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن قاضي التحقيق أن يقوم بأية عملية أو حجر ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضابط الشرطة القضائية المختصين للقيام بذلك» المادة 47 /3-4 من الأمر 66- 155 المعدلة بالقانون رقم 06- 22 المؤرخ في ديسمبر 2006م المتضمن قانون الإجراءات الجزائية، ج.ر، ع84، ص06.

[4]-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، المرجع السابق، ص99.

الجريمة جناية أو جنحة، وتوافر أمارات قوية وقرائن على وجود دليل يفيد في كشف الجريمة لدى المتهم أو غيره وهذا السبب لا ينشأ إلا بعد وقوع الجريمة، واتجاه قرائن الاتهام ضد شخص، أو وجود أمارات قوية ضد آخر على حيازته ما يفيد في كشف الحقيقة. فلا يجوز إجراؤه قانونا إلا إذا كان هناك احتمال للعثور على دليل من ورائه، وهذا الأمر متروك لتقدير السلطات القائمة به، وتراقبها المحكمة في سلامة الاستدلال. فإذا ثبت أن سلطات التحقيق قد باشرت إجراء التفتيش دون احتمال فائدة مرجوة من ورائه، فإنها تكون متعسفة في ذلك[1].

2- محل التفتيش: يشترط كذلك لصحة ومشروعية التفتيش في الجريمة السبيرانية أن ينصب على محل بحيث يشترط أن يكون محددا أو قابلا للتحديد ويكون مشروعا يرد على محل جائز قانونا. كالمكونات المادية والمعنوية للكمبيوتر وملحقاته وبرامجه، الهاتف الذكي وشبكات الاتصال عن بعد[2].

والمحل في الجرائم الإلكترونية لا يكون قائما بذاته، بل يكون إما مقترنا بمكان معين كمسكن المتهم أو بشخص معين (مالك أو حائز) كما هو الشأن في الحاسب المحمول أو الهاتف النقال، لذا قبل مباشرة التفتيش يجب مراعاة طبيعة المكان الذي تتواجد فيه الوسائل الإلكترونية المراد تفتيشها وكذا الضمانات القانونية المحاطة به، ويشترط في محل التفتيش أن يكون معينا تعينا نافيا للجهالة للمحافظة على حرمات وحريات الأفراد، إذ لا يمكن تفتيش كل الحواسيب المتواجدة في شركة ما أو الهواتف النقالة الخاصة لكل أفراد العائلة مثلا، كما نشير إلى استثناء بعض الأشخاص والأماكن من التفتيش مثل أشخاص ومساكن وسيارات أعضاء السلك الدبلوماسي وأعضاء المجالس النيابية، ومكاتب المحامين لتمتعه بالحصانة، وعليه فأي تفتيش لها يعد منافيا للقانون ومآله البطلان[3].

3-السلطة المختصة بالقيام بالتفتيش: انطلاقا من أن إذن التفتيش الذي يصدر من غير الجهة المختصة يعتبر باطلا كان من الضروري تحديد الجهة المختصة بالتفتيش في الجرائم السيبيرانية، وبالرجوع إلى التشريع الجزائري، نجد المشرع حدد هذه الجهة بموجب نص المادة 5

---

[1]-عبد الله ماجد العكايلة، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، مرجع سابق، ص512- 513.

[2]- لامية وعلي، كاهنة سعودي، إجراءات المكافحة الجريمة الإلكترونية، مرجع سابق، ص 82.

[3]- جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص36.

من القانون 09-04 حيث جاء فيها: «يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية ، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول بغرض التفتيش ولو عن بعد إلى: أ-منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها. ب-منظومة تخزين معلوماتية.» [1].

ومن ثم يمكننا القول أن المشرع جعل السلطة القضائية هي السلطة المختصة أصلا بالتفتيش في الجرائم السيبيرانية، إلا أنه منحها الحق في أن تأمر أطرافا أخرى بالقيام بالتفتيش نظرا لما تتميز به هذه الجرائم من خصوصية تستدعي تدخل أطراف لها دراية وخبرة بالأنظمة المعلوماتية حفاظا على المعطيات محل التفتيش وحماية لها من أي تصرف يؤدي إلى إتلافها[2].

ثانيا: تطبيق إجراءات التحقيق المستحدثة على الجريمة السبيرانية

سنقتصر في هذه الورقة البحثية على إجراءين أساسيين:

ا-المراقبة الإلكترونية:

استحدث المشرع الجزائري و بموجب المادة الثالثة 03 من القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها إجراء المراقبة الإلكترونية حينما أجاز تبعا لمستلزمات التحريات أو التحقيقات القضائية الجارية في إطار هذا النوع من الجرائم، اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها، فجاء نص المادة كما يلي:" **مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميعها وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية**"[3].

---

[1]-القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[2]-يراجع: رضا هميسي: تفتيش المنظومات المعلوماتية في التشريع الجزائري، مقال منشور بمجلة العلوم القانونية والسياسية، ع5، جوان 2012.

[3]-المادة 03 من القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

وقد عرف الفقه إجراء المراقبة الإلكترونية على أنه مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر[1]. في حين لم يتطرق المشرع الجزائري إلى تحديد المقصود بالمراقبة الالكترونية، بل اكتفى بتعريف الاتصالات الإلكترونية فقط، كون المراقبة الإلكترونية تتمثل في مراقبة شبكة الاتصالات.

فالمراقبة الإلكترونية إذا هي إجراء يقوم به خبير في مجال المراقبة باستعمال تقنية المعلومات لمراقبة وتتبع كل ما يقوم به شخص مشتبه فيه من إرسال واستقبال لمكالمات أو تسجيلات صوتية أو كتابات أو صور ومعلومات باستعمال وسيلة من وسائل تكنولوجيات الإعلام والاتصال في إحدى الجرائم المنصوص عليها في القانون.

ومن ثم يمكن القول أن المراقبة الإلكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، بحيث يقوم بها المراقب الإلكتروني والذي يتمثل في ضابط من ضباط الشرطة القضائية ذي كفاءة تقنية عالية، وباستخدام برامج إلكترونية[2].

1- **مضمون المراقبة الإلكترونية** : لم يتطرق المشرع الجزائري إلى تحديد المقصود بمراقبة الاتصالات الإلكترونية مكتف في ذلك بتحديد مفهوم الاتصالات الإلكترونية فحسب، ففي منظوره المراقبة الإلكترونية هي عملية تتم على الاتصالات الإلكترونية، وفي حالات حددها القانون[3].

وقد أحاط المشرع هذا الإجراء باعتباره وسيلة إجرائية في مجال الجريمة السيبيرانية بمجموعة من الحالات التي تستدعي اللجوء للمراقبة الإلكترونية للاتصالات، حددها بموجب

---

[1]–بشير حماني: خصوصية التحقيق في الجريمة الالكترونية، مرجع سابق، ص73- 74.

[2]–عبد المطلب طاهري: الإثبات الجنائي بالأدلة الرقمية، مرجع سابق، ص23- 24.

[3]–حيث جاء في نص المادة 05 من المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015م الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:" الاتصالات الإلكترونية هي كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال. المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015م الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.، ع53.

المادة 4 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ويمكن حصر هذه الحالات في الآتي[1]:

– للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

– في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

– لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

2- شروط المراقبة الإلكترونية والآثار المترتبة عنها:

أ- شروط المراقبة الإلكترونية

المراقبة الإلكترونية وباعتبارها وسيلة إجرائية في مجال الجريمة السيبيرانية، قيدها المشرع الجزائري بمجموعة من الشروط تم استنتاجها مما ورد من أحكام في المادة 4 من القانون 09-04 وتتمثل في:

-أن يتم تنفيذ هذا الإجراء تحت سلطة القضاء

-الحصول على الإذن من الهيئات المختصة بذلك.

-أن تكون هناك ضرورة تتطلب هذا الإجراء.

-توفر عناصر نجاح العملية وذلك عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري أو التحقيق دون اللجوء إلى المراقبة الإلكترونية.

ب- الآثار المترتبة على عملية المراقبة الإلكترونية: تترتب عن المراقبة السرية للاتصالات عموما ومن ضمنها الاتصالات الإلكترونية، تسجيل محتوى تلك الاتصالات وتخزينها على وسائط مادية قابلة للنقل، بغية استخدامها فيما بعد لإثبات الجريمة الواقعة، ولكن تختلف نوعية التسجيل هنا بحسب ما إذا كانت المحادثة الإلكترونية المراقبة هي عبارة عن اتصال

[1]–المادة 04 من القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق..

صوتي فقط، أو اتصال صوتي مرئي، ففي الأول يكون التسجيل صوتي فقط، في حين أنه يكون في الثاني تسجيل صوتي مرئي، وما ينبغي الإشارة إليه أن المراقبة السرية الإلكترونية للاتصالات الإلكترونية، ومن ضمنها المحادثات الهاتفية لا يمكن اعتبارها نوعا من أنواع التفتيش، وذلك لأن المراقبة الإلكترونية ترد على البيانات الإلكترونية المتحركة والتي تتجسد هنا بالاتصالات الإلكترونية حال إجرائها دون تلك التي انتهت وخزنت، في حين التفتيش يرد فقط على البيانات الإلكترونية الساكنة أو المخزنة والتي تتجسد هنا بالاتصالات الإلكترونية التي تمت وخزنت[1].

II-الحفظ والإفشاء العاجلان للمعطيات الإلكترونية :

حفظ وإفشاء المعطيات الإلكترونية يعد أحد الإجراءات المستحدثة للكشف عن الجرائم السيبيرانية، وقد نص عليه المشرع الجزائري في نص المادة 10 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]، حيث يتم هذا الإجراء من قبل مقدمي خدمات الإنترنت، من خلال قيامهم بالحفظ عن طريق الحيازة بالأرشيف بهدف حماية المعطيات التي سبق وجودها في شكل مخزن مما يحول دون تلفها أو تجريدها من صفتها أو تغييرها عن حالتها الأصلية، وتقديمها إلى جهات التحقيق فور طلبها.

[1]-نادية غرباوي، أساليب البحث والتحري في الجرائم المعلوماتية، مرجع سابق، ص82- 83.

[2]-القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

الخاتمة:

خلصت هذه الورقة البحثية إلى جملة من النتائج يمكن إجمالها في الآتي:

1-من الصعب ضبط تعريف دقيق للجريمة السبيرانية على الرغم من المحاولات الفقهية والتشريعية وذلك لارتباط هذه الجريمة بمنظومة معلوماتية سريعة التطور.

2-يواجه التحقيق الجنائي في الجريمة السبيرانية جملة من الصعوبات والعوائق منها ما يتعلق بالجاني ومنها ما يتعلق بخصوصية الجريمة في حد ذاتها ومنها ما يعلق بالجهة المتضررة والجهة القائمة بالتحقيق.

3-الطبيعة الخاصة للجريمة السبيرانية وامتدادها عبر الحدود إضافة إلى سرعة تنفيذها وصعوبة اكتشافها في كثير من الحالات يستوجب اتباع إجراءات تحقيق خاصة زيادة على الإجراءات العامة المتبعة في الجرائم التقليدية.

4-تتمثل أهم الإجراءات العامة التي يمكن تطبيقها على الجرائم السبيرانية في المعاينة والتفتيش الإلكتروني، أما أهم الإجراءات المستحدثة فتتمثل في المراقبة الإلكترونية إضافة إلى الحفظ والافشاء العاجلين للمعطيات الإلكترونية

التوصيات:

خلصت الورقة البحثية إلى جملة من التوصيات أهمها:

1-ضرورة تكوين المكلفين بالتحقيق في الجرائم السبيرانية تكوينا تقنيا يتماشى مع سرعة تطور المنظومة المعلوماتية، مع ضرورة اتقانهم للغة الإنجليزية التي تعتبر اللغة الأولى في مجال تكنولوجيا المعلومات والاتصالات.

2-التوجه نحو القاضي المتخصص ومن ثم تكوين قضاة متخصصين في مجال المعلوماتية حتى يتسنى لهم التعامل مع الجرائم السبيرانية وتقدير الأدلة الرقمية.

3-توعية المجتمع بخطر الجرائم السبيرانية وضرورة الإبلاغ عنها.

4-العمل على اقتناء أحدث برامج تأمين المعاملات والاتصالات الإلكترونية ومواكبة التطور في هذا المجال تفاديا أولا بأول تفاديا للهاكرز.