الجمهورية العربية السورية
جامعة دمشق
كلية الحقوق- قسم القانون الجزائي

فعالية الوسائل التقليدية في إثبات الجريمة المعلوماتية

رسالة مقدمة لنيل درجة الماجستير في القانون الجزائي

إعداد

علي بسام خرما

إشراف

الدكتور عيسى غازي الذيب

المدرس في قسم القانون الجزائي

2024

﴿ يَرْفَعِ ٱللَّهُ ٱلَّذِينَ ءَامَنُوا۟ مِنكُمْ وَٱلَّذِينَ أُوتُوا۟
ٱلْعِلْمَ دَرَجَٰتٍ ۚ وَٱللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ ﴿١١﴾ ﴾

سورة المجادلة

الإهداء

إلى راعي العلم والعلماء في هذا البلد العظيم، ومن لم يبخل بالعطاء في سبيل دفع قاطرة البحث العلمي إلى الأمام.....

السيد الرئيس بشار الأسد أطال الله في عمره

رئيس الجمهورية العربية السورية

القائد العام للجيش والقوات المسلحة

إلى من علّمني كيف أقف بكل ثبات فوق الأرض، قدوتي ومثلي الأعلى في الحياة.....

أبي المبجّل

إلى من اقترن اسمها باسم رب العالمين، ملحمة الحب، وفرحة العمر، ومثال التفاني والعطاء.....

أمي الحنونة

إلى من علمتني أبجدية الحب والشجاعة، رفيقة الكفاح والظروف الصعبة، نبضي وسر حياتي.....

زوجتي الغالية

إلى فلذات الكبد، وفرحة عمري، ومن هنّ نعمة من الله في حياتي.....

بناتي

إلى من شاركوني السراء والضراء، مثال العطاء والكبرياء والتضحية.....

أشقائي

إلى من تطيب الأوقات بصحبتهم، ويصبح لكل شيء معنى أعمق.....

أصدقائي

شكر وتقدير

لا يسعني بعد إتمام هذا البحث إلا أن أحمد الله تعالى وأشكره على فضله ومنّته الواسعة، ومنحه إياي القوة والصبر لإنجاز هذا البحث.

كما أتقدّم بالشكر والتقدير الكبير إلى **الدكتور عيسى غازي الذيب** ، المدرس في قسم القانون الجزائي في كلية الحقوق–جامعة دمشق، والذي شرفني بقبوله الإشراف على هذا البحث، فلم يدّخر جهداً ولا وقتاً في نصحي وإرشادي، وتزويدي بملاحظاته القيّمة ودعمه اللامحدود لإنجاز هذا البحث، فله كل الشكر والامتنان والتقدير...

كما أتوجه بجزيل الشكر والتقدير إلى لجنة الحكم على هذا البحث.

وأتوجّه أيضاً بأسمى آيات التقدير والعرفان إلى **عمادة كلية الحقوق وجميع أعضاء الهيئة التدريسية في كلية الحقوق في جامعة دمشق،** فلهم جميعاً جزيل الشكر والعرفان وجزاهم الله عني كل خير.

الفهرس

العنوان	رقم
المقدمة	1
الفصل الأول **مدى كفاية الوسائل التقليدية في إثبات الجريمة المعلوماتية**	**8**
المبحث الأول: الطبيعة الخاصة لإثبات الجريمة المعلوماتية بالوسائل التقليدية	**9**
المطلب الأول: مفهوم الجرائم المعلوماتية	10
الفرع الأول: تعريف الجرائم المعلوماتية	10
الفرع الثاني: أنواع الجرائم المعلوماتية	13
المطلب الثاني: معوقات إثبات الجرائم المعلوماتية بالوسائل التقليدية	15
الفرع الأول: الأسباب العائدة إلى خصائص الجرائم المعلوماتية	15
الفرع الثاني: الأسباب العائدة إلى الطبيعة الخاصة للجريمة المعلوماتية	19
الفرع الثالث: الأسباب المتعلقة بالمجرم المعلوماتي	21
المبحث الثاني: قدرة الوسائل التقليدية في إثبات الجريمة المعلوماتية	**23**
المطلب الأول: الصعوبات التي تواجه الحصول على الدليل الإلكتروني بوسائل الإثبات التقليدية	23
الفرع الأول: صعوبات متعلقة بالجريمة المعلوماتية	24
الفرع الثاني: صعوبات متعلقة بالدليل الإلكتروني	35
الفرع الثالث: صعوبات متعلقة بأسباب متعددة	39
المطلب الثاني: عدم قدرة الوسائل التقليدية في إثبات الجريمة المعلوماتية	42
الفرع الأول: الخبرة	43

الفرع الثاني: المعاينة	45
الفرع الثالث: التفتيش	51
الفرع الرابع: الضبط	77
الفصل الثاني **إثبات الجريمة المعلوماتية بالوسائل المستحدثة**	**86**
المبحث الأول: الوسائل المستحدثة في إثبات الجريمة المعلوماتية	**88**
المطلب الأول: الوسائل المادية الحديثة	88
الفرع الأول: استخدام بروتوكول **IP/TCP:**	89
الفرع الثاني: استخدام معلومات الكوكيز **. Cookies**	90
الفرع الثالث: استخدام معلومات البروكسي**.: Proxy**	90
الفرع الرابع: استخدام برامج التتبع وكشف الاختراق.	91
المطلب الثاني: الوسائل الإجرائية الحديثة	91
الفرع الأول: الوسائل المتعلقة بالبيانات الساكنة **.**	92
الفرع الثاني: الوسائل المتعلقة بالبيانات المتحركة.	95
المبحث الثاني: فاعلية الوسائل المستحدثة في إثبات الجريمة المعلوماتية وموقف التشريعات منها وضماناتها	**102**
المطلب الأول: أهمية الوسائل المستحدثة في إثبات الجريمة المعلوماتية **.**	102
الفرع الأول: أهمية الوسائل المتعلقة بالبيانات الساكنة في إثبات الجريمة المعلوماتية**.**	103
الفرع الثاني: أهمية الوسائل المتعلقة بالبيانات المتحركة في إثبات الجريمة المعلوماتية.	104
المطلب الثاني: موقف التشريعات من الوسائل المستحدثة وضماناتها.	105

الفرع الأول: موقف التشريعات الجزائية المقارنة.	105
الفرع الثاني: موقف التشريع السوري.	114
الفرع الثالث: ضمانات الوسائل المستحدثة للحفاظ على خصوصية الأفراد.	116
الخاتمة	120
أولاً: النتائج	120
ثانياً: المقترحات	121
المراجع	125

الملخّص

لم يخلف التطور القانوني للتقدم التكنولوجي الذي شهده العالم في منتصف القرن العشرين آثاراً إيجابية فحسب، بل تعدى إلى أبعد من ذلك، فقد استغل ذلك معظم الأشخاص للقيام بمختلف الجرائم، وذلك بالاستعانة بالتقنيات التكنولوجية الحديثة، إذ تمكن المجرمون من تطوير طرق الإجرام على نحو عالٍ من التقنية في البيئة الإلكترونية، فبات من الضروري تطوير وسائل المكافحة، بما يواكب التطور في وسائل الإجرام الإلكتروني، كما أصبح مطلوباً من أجهزة العدالة الجزائية أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجزائي.

ولم يتضمن القانون رقم /20/ لعام 2022 المتعلق بتنظيم التواصل على الشبكة والجريمة المعلوماتية السوري أي تفريد للقواعد الإجرائية المتعلقة بالإثبات، وعلى ضوء ما تقدم فإن إشكالية هذا الموضوع تعد إحدى أهم الإشكالات التي تثيرها الجريمة المعلوماتية على المستوى الإجرائي والمتمثلة في: مدى فعالية وسائل الإثبات التقليدية في إثبات الجريمة المعلوماتية، وإلى أي حد يمكن القول إن وسائل الإثبات التقليدية كافية لإثبات الجريمة المعلوماتية وحدها؟ واتبعنا من أجل دراسة هذا الموضوع المنهج الوصفي لوصف الجريمة المعلوماتية، والمنهج التحليلي لتحليل النصوص القانونية الواردة في قانون الأصول الجزائية السوري، والمنهج المقارن بين التشريع السوري وبعض التشريعات العربية والغربية كلما دعت الضرورة إلى ذلك. وبغرض الإلمام بمختلف جوانب الموضوع، والإجابة على مختلف التساؤلات التي تطرحها الإشكالية اعتمدنا على تقسيم ثنائي للخطّة التّي تتكون من فصلين: الفصل الأول المتعلق ببيان مدى كفاية الوسائل التقليدية في إثبات الجريمة المعلوماتية، والفصل الثاني الذي يبحث في إثبات الجريمة المعلوماتية بالوسائل المستحدثة. وتبين لنا عدم قدرة وكفاية وسائل الإثبات التقليدية في معاينة وتفتيش وضبط إثبات الجرائم المعلوماتية، سواء من الناحيتين القانونية والتقنية، وبيّنا مدى حاجة المشرع إلى أن يستحدث من التشريعات ما يلائم هذا النوع من الجرائم من وسائل مستحدثة، فضلاً عن إنشاء أجهزة فنية متخصصة بالجريمة المعلوماتية يناط بها عملية جمع الأدلة التقنية لهذ الجرائم.

الكلمات المفتاحية: فاعلية – وسائل – إثبات – جرائم – معلوماتية – تقليدية – مستحدثة.

المقدمة

شهدت الوسائل التقنية الحديثة انتشاراً واسعاً في العصر الحالي، فعلى سبيل المثال تغلغلت الحواسيب والإنترنت في جميع جوانب الحياة، بحيث أصبح كثيرٌ من الدول يعتمد عليها في تسيير مرافقه الحيوية كالدفاع والأمن والاقتصاد، كما أن هذه الأخيرة عرفت انتشاراً واسعاً على المستوى الاجتماعي، إذ أصبح معظم الأفراد يلجؤون في تسيير أمورهم إلى استخدام مجموعة من التقنيات الإلكترونية، كالتواصل وتبادل المعارف عبر الإنترنت في شكل أرقام ورموز إلكترونية، ويتم ذلك بمجرد كبسة زر على الحاسوب أو أجهزة الهاتف الجوال الحديثة.

بالإضافة الى ذلك فإن الوسائل العلمية الحديثة ساعدت المجرم في القيام بمختلف الجرائم المعلوماتية، كاختراق الإنترنت وتزييف النقود الإلكترونية وتزوير المستندات الإلكترونية...، بسرعة وبدقة عالية من دون ترك أي أثر للكشف عنها أو معرفة مصدرها، كما أن هذا الاعتداء يمكن أن يكون على مجموعة من المجني عليهم في الوقت نفسه، وفي مختلف أنحاء العالم عن طريق الإنترنت.

وإذا كان البحث في مدى فعالية القواعد الإجرائية التقليدية في ضبط الجريمة المعلوماتية أمراً صعباً، فإن الصعوبة تنطلق من إعطاء مفهوم للجريمة المعلوماتية ذاتها، لذلك يمكننا القول إن الجريمة المعلوماتية بوصفها مظهراً جديداً من مظاهر السلوك الإجرامي لا يمكن تصورها إلا من خلال صورتين، الصورة الأولى إما أن تتجسد في شكل جريمة تقليدية يتم اقترافها بوسائل إلكترونية، والصورة الثانية إما أن تتجسد في شكل استهداف للوسائل المعلوماتية ذاتها، وعلى رأسها قاعدة المعطيات والبيانات أو البرامج المعلوماتية.

وقد أثارت هذه الجريمة بعض التحديات القانونية والعملية أمام الأجهزة المعنية بالبحث عن الجرائم وضبطها، وخصوصاً ما يتعلق بشكل مباشر بإجراءات البحث والتحري التقليدية في بيئة افتراضية لا مكان فيها للأدلة المادية، مما أظهر مدى الحاجة إلى تطوير آليات البحث بما يتلاءم وخصوصيات هذه الجرائم، وجعل مسألة ملاءمة الإجراءات الجزائية في البحث والتحري مع خصوصية الجريمة المعلوماتية تستأثر باهتمام المشرعين في مختلف الدول.

كما أن الجريمة المعلوماتية خلقت عالماً جديداً لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، إذ فقدت الحدود الجغرافية كل آثر لها في بيئة إلكترونية متشعبة العلاقات، الأمر الذي خلق صعوبات وإشكالات قانونية لا تقتصر على ضبط هذه الجرائم وإثباتها فحسب، وإنما أثارت أيضاً تحديات أكثر تعقيداً مرتبطة بتحديد جهة الاختصاص، والقانون واجب التطبيق على هذا الصنف من الجرائم.

- الدراسات السابقة:

استندنا إلى مراجع تناولت بالتحليل مواضيع ذات علاقة بموضوع دراستنا هذه، وفيما يأتي أهم الأطروحات:

- رفاس، حفيظة. (2020)، **دور السياسة الجنائية للمشرع الجزائري في مكافحة جرائم التكنولوجيا الحديثة**، أطروحة دكتوراه تخصص قانون عام، جامعة الدكتور الطاهر مولاي–سعيدة، كلية الحقوق والعلوم السياسية. كان الهدف هو محاولة بيان الأحكام العامة في جريمة تقنية المعلومات الحديثة وملامح إطارها القانوني، ودراسة الأحكام الموضوعية للجرائم الناشئة عن استخدام هذه التقنية، بدءاً من جرائم الاعتداء على حقوق الإنسان في سلامة الجسم والحياة والشرف، ومروراً بالجرائم الجنسية، والإرهاب والتجسس، ودراسة الأحكام الموضوعية لهذه الجرائم من خلال بحث مدى كفاية النصوص الواردة في قانون العقوبات الجزائري وملاءمتها للجرائم الإلكترونية.

- لبيبات، خولة، وعميرات أميرة. (2022)، **الإثبات في الجريمة الإلكترونية**، رسالة ماجستير في القانون الجزائي، جامعة محمد بو ضياف–المسيلة، كلية الحقوق والعلوم السياسية، الجزائر. وتناولت هذه الدراسة بيان الأدلة الحديثة وأهميتها في تحقيق العدالة، وخلصت إلى التوصية باستحداث نص قانوني بخصوص أدلة الإثبات وإضافة الدليل الرقمي، وأن الجرائم الإلكترونية لا يمكن إثباتها بالأدلة التقليدية.

- حمودة، أمجد خليل. (2017)، الوسائل الحديثة لإثبات الجرائم التي ترتكب بواسطة الأجهزة الالكترونية، بحث منشور في **مجلة جامعة الأزهر**–غزة: فلسطين، مج19، عدد خاص بمؤتمر كلية الحقوق الخامس. ناقشت الدراسة عدداً من الجوانب المتعلقة بأدلة الإثبات المستحدثة، وكذلك ما يتعلق بصعوبة الوصول إلى الأدلة، وخلصت إلى أن الأدلة المتعلقة بإثبات الجرائم الإلكترونية ليس من السهل الوصول إليها، أو تحريرها، لأن المجرم الإلكتروني

يتخلص مباشرة من كل الأدلة التي تدينه بعد ارتكاب الجريمة، وبالتالي فإن طبيعة هذه الأدلة لا تعالجها النصوص التشريعية التقليدية.

- إشكالية البحث:

لم يتضمن القانون رقم /20/ لعام 2022 المتعلق بتنظيم التواصل على الشبكة والجريمة المعلوماتية أي تفريد للقواعد الإجرائية المتعلقة بالإثبات، وعلى ضوء ما تقدم فإن إشكالية هذا الموضوع تعد إحدى أهم الإشكالات التي تثيرها الجريمة المعلوماتية على المستوى الإجرائي والمتمثلة في:

مدى فعالية وسائل الإثبات التقليدية في إثبات الجريمة المعلوماتية، وإلى أي حد يمكن القول إن وسائل الإثبات التقليدية كافية لإثبات الجريمة المعلوماتية وحدها؟ ومدى الضرورة للاستعانة بوسائل تقنية لإثبات هذه الجريمة، ومدى إمكانية التوافق بين اللجوء إلى هذه الوسائل التقنية والحفاظ على خصوصية الأشخاص.

- تساؤلات البحث:

يتفرع عن إشكالية بحثنا عدد من التساؤلات الفرعية:

1- ما فعالية الوسائل التقليدية كالتفتيش والمعاينة والضبط في إثبات الجريمة المعلوماتية؟

2- هل الوسائل التقليدية بحاجة إلى تطوير لتتلاءم مع إثبات الجريمة المعلوماتية، لكونها جريمة مستحدثة، ولكون هذه الوسائل وضعت لإثبات الجرائم التقليدية؟

3- ما الوسائل المستحدثة في إثبات الجريمة المعلوماتية؟

4- ما فاعلية الوسائل المستحدثة في إثبات الجريمة المعلوماتية؟

- أهمية البحث:

تظهر أهمية البحث في أنه باستطاعة المجرمين تطوير طرق الإجرام على نحو عالٍ من التقنية في البيئة الإلكترونية، ما يجعل من الضروري تطوير وسائل المكافحة بما يواكب التطور في وسائل الإجرام الإلكتروني، ويتطلب من أجهزة العدالة الجزائية أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجزائي.

وتبرز أهمية الموضوع كذلك من واقع عدم كفاية النظم القانونية التقليدية في إثبات الجريمة المعلوماتية سواء من الناحيتين القانونية والتقنية، ومدى حاجة المشرع إلى أن يستحدث من التشريعات ما يلائم هذا النوع من الجرائم، فضلاً عن إنشاء أجهزة فنية متخصصة بالجريمة المعلوماتية يناط بها عملية جمع الأدلة التقنية لهذه الجرائم.

- مسوغات البحث:

السبب الرئيس الذي دفعنا لاختيار هذا الموضوع هو أنه من الموضوعات المستحدثة التي تعاني نقصاً في الدراسات، كما أن التطرق لهذا الموضوع يسمح لنا بمعرفة مدى مواكبة التطور القانوني للتقدم التكنولوجي الذي شهده العالم في منتصف القرن العشرين لأن هذا التطور لم يخلف آثاراً إيجابية فحسب، بل تعدى إلى أبعد من ذلك، فقد استغل ذلك معظم الأشخاص للقيام بمختلف الجرائم، وذلك بالاستعانة بالتقنيات التكنولوجية الحديثة. وهناك مسوغ آخر يتعلق بالقانون رقم /20/ لعام 2022 الذي لم يتضمن تفريداً للقواعد الإجرائية المتعلقة بإثبات الجريمة المعلوماتية.

- فرضيات البحث:

تتجلى فرضيات البحث فيما يأتي:

أ- الفرضية الرئيسة:

يجب تحديث الوسائل الإجرائية التقليدية في قانون أصول المحاكمات الجزائية السوري من خبرة ومعاينة وتفتيش وضبط، لتستوعب الحصول على الدليل الإلكتروني، وتحديثها على نحو يكفل استجابتها بشكل كاف للحصول على هذا الدليل المستحدث، من غير أن تتعرض حقوق الأفراد وحرياتهم للخطر عند الإثبات به، وضرورة سَنّ القوانين والأنظمة الخاصَّة التي تسدُّ كافَّة ثغرات الحصول على الدليل الإلكتروني، ولا سيما الاهتمام بالوسائل الفنية الحديثة للحصول على الدليل الإلكتروني لكونها تساعد كثيراً في اكتشاف هذا الدليل وحفظه، إذ إن الطرق العلمية والفنية للحصول على الدليل الإلكتروني قد أصبحت هي الأكثر فاعلية للحصول على هذا الدليل.

ب- الفرضيات الفرعية:

1- هنالك اختلاف كبير بين معاينة الجرائم التقليدية التي تتم في العالم المادي، وتلك التي تتم في العالم الافتراضي، إذ يقتضي ذلك السرعة في إجراء هذه المعاينة خشية زوال الدليل الإلكتروني والتخصص الدقيق فيمن يقومون بإجراء هذه المعاينة، فلا ضير من انتقال عضو الضابطة العدلية غير المادي للاطلاع على المعلومات ومعاينتها للحصول على الدليل الإلكتروني، إذ يبقى هذا الدليل مشروعاً، ويجوز الاعتماد عليه بالحكم.

2- إن التفتيش الإلكتروني يرد على كل مكونات الحاسوب، سواء أكانت مادية أم معنوية، وشبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسوب محل التفتيش، ويشمل برامج النظام وبرامج التطبيقات سابقة التجهيز طبقاً لاحتياجات العميل.

3- إن التفتيش المتعلق بمكونات الحاسوب يسهل إجراءه على المكونات المادية، وتأتي سهولة هذا التفتيش لأنه يقع على أشياء مادية منصوص عليها في أغلب القوانين الإجرائية، إذ إنه لا مشكلة في تفتيش الحاسوب، متى كان التفتيش ينصب على المكونات المادية، أي على معدات الحاسوب وشاشة العرض، وفي هذا الفرض تطبق القواعد التقليدية للتفتيش.

4- إن ضبط المكونات المادية للحاسوب والمتمثلة في معدات الحاسوب والإنترنت وكابلات الشاشة وشاشة العرض ومفاتيح تشغيله، يمكن أن يطبق بصددها القواعد التقليدية للضبط ذاتها من دون أدنى صعوبة.

5- عدم كفاية الإجراءات التقليدية للحصول على الدليل الإلكتروني، وضرورة إتباع إجراءات حديثة تتماشى مع طبيعة كل من الدليل الإلكتروني، والجرائم المعلوماتية.

6- إن المراقبة الإلكترونية تُعد اعتداء على حرية الحديث الذي هو حق من الحقوق اللصيقة بالشخصية الإنسانية وتدخلاً في حياته الخاصة، ومن دون خصوصية الحديث يصبح الفرد متردداً وخائفاً من ممارسة حقه والحديث عبر وسائل الاتصال الحديث، وذلك فيه مساس بأهم الحقوق اللصيقة بالإنسان، وتكمن المشكلة في أن المراقبة تكشف أدق أسرار الأشخاص من دون علمهم، وتمتد إلى كشف أسرار كل شخص يتصل بالشخص المراقب. إلا أنه يمكن السماح به في أحوال ضيقة، وأن يكون في نطاق ضيق، لأن إجراء المراقبة الإلكترونية مهم، ويقوم

بدور فعال للحصول على الدليل الإلكتروني، وذلك لعدم كفاية الإجراءات التقليدية للحصول على هذا الدليل والتي لا تتناسب مع طبيعته، ولكن لابد من إحاطة هذا الإجراء بضمانات عدة، ولا سيما تحديد نوع الحديث المراد التقاطه، والجريمة المتعلقة به، والجهة المصرح لها بذلك، وتحديد مدة المراقبة، وكل هذه الضمانات تكفل مشروعية الحصول عل الدليل الإلكتروني.

7- لابد من تطوير النصوص القانونية المتعلقة بالضبط، لتشمل إمكانية ضبط معطيات الحاسوب والبيانات المعالجة إلكترونياً.

8- ضرورة تطوير قواعد الضبط لتتلاءم مع طبيعة البريد الإلكتروني، وتخصيص إجراءات تتصف بالمرونة والسرعة تفوق الإجراءات الخاصة بالبريد العادي لضبط هذا البريد، وذلك نظراً إلى سهولة التخلص من الأدلة الإلكترونية الموجودة فيه.

- هدف البحث:

1- تسليط الضوء على مدى كفاية الوسائل التقليدية في إثبات الجريمة المعلوماتية.

2- معرفة مدى مواكبة القانون للتطور التكنولوجي، وكيفية تعامله مع الأدلة الحديثة، وخاصة الدليل الإلكتروني.

3- تسليط الضوء على تعامل القضاء مع الأدلة الإلكترونية الحديثة، وقوتها الثبوتية، ومدى دور هذه الأدلة في إقناع القاضي الجزائي.

4- الإشارة إلى النقص التشريعي فيما يتعلق بالدليل الإلكتروني.

- حدود البحث:

1- النطاق المكاني: يتمثل النطاق المكاني للبحث في الجمهورية العربية السورية.

2- النطاق الموضوعي: يتمثل النطاق الموضوعي في قانون أصول المحاكمات الجزائية السوري الصادر بالمرسوم التشريعي رقم /112/ لعام 1950، والقانون الخاص بتنظيم التواصل على الشبكة ومكافحة

الجريمة المعلوماتية الصادر بالمرسوم التشريعي رقم /20/ لعام 2022 وبعض التشريعات الجزائية المقارنة.

3- النطاق الزماني: يتمثل النطاق الزماني للبحث في الفترة الزمنية الممتدة بين الربع الأول من العام 2023 حتى الربع الأول من العام 2024.

- منهج البحث:

أمام كل هذه التساؤلات التي تطرحها إشكالية هذا البحث، وبعد أن أعطتنا المقدمة فكرة مبدئية عن موضوع بحثنا، سنتبع أولاً **المنهج الوصفي** لوصف الجريمة المعلوماتية، و**المنهج التحليلي** لتحليل النصوص القانونية الواردة في قانون الأصول الجزائية السوري.

ونلجأ ثانياً وفي كل مرحلة من مراحل الدراسة إلى **المنهج المقارن** بين التشريع السوري وبعض التشريعات العربية والغربية كلما دعت الضرورة إلى ذلك.

- أقسام البحث:

بغرض الإلمام بمختلف جوانب الموضوع، والإجابة على مختلف التساؤلات التي تطرحها الإشكالية اعتمدنا تقسيماً ثنائياً للخطّة التّي تتكون من فصلين متبوعين بخاتمة تبين أهم النتائج التي كشف عنها البحث وفق الآتي:

الفصل الأول

مدى كفاية الوسائل التقليدية في إثبات الجريمة المعلوماتية

المبحث الأول: الطبيعة الخاصة لإثبات الجريمة المعلوماتية بالوسائل التقليدية.

المبحث الثاني: قدرة الوسائل التقليدية لإثبات الجريمة المعلوماتية.

الفصل الثاني

إثبات الجريمة المعلوماتية بالوسائل المستحدثة

المبحث الأول: ماهية الوسائل المستحدثة في إثبات الجريمة المعلوماتية.

المبحث الثاني: فاعلية الوسائل المستحدثة في إثبات الجريمة المعلوماتية وموقف التشريعات منها وضماناتها.

الفصل الأول

مدى كفاية الوسائل التقليدية في إثبات الجريمة المعلوماتية

إن بحث مدى كفاية الوسائل التقليدية في إثبات الجريمة المعلوماتية، يقتضي بيان الطبيعة الخاصة لإثباتها بالوسائل التقليدية، ومن ثم بيان قدرة الوسائل التقليدية في إثبات الجريمة المعلوماتية، وذلك بتقسيم هذا الفصل إلى المبحثين الآتيين:

المبحث الأول: الطبيعة الخاصة لإثبات الجريمة المعلوماتية بالوسائل التقليدية.

المبحث الثاني: قدرة الوسائل التقليدية في إثبات الجريمة المعلوماتية.

المبحث الأول

الطبيعة الخاصة لإثبات الجريمة المعلوماتية بالوسائل التقليدية

إن ظاهرة جرائم الحاسوب والإنترنت، أو جرائم التقنية العالية، أو الجريمة المعلوماتية، أو (السيبركرايم) Crime Cyber أو (جرائم أصحاب الياقات البيضاء Collar White) ، ظاهرة إجرامية مستجدة نسبياً تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن إلى حجم المخاطر وهول الخسائر الناجمة عنها، بحسبانها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، (بيانات ومعلومات وبرامج بكافة أنواعها). فهي جريمة تقنية تنشأ في الخفاء، ويقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسوب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت[1].

وهنالك معوقات عدة تواجه إثبات الجريمة المعلوماتية بالأدلة التقليدية، ولكن قبل التعرض لهذه المعوقات لابد من توضيح مفهوم هذه الجرائم، وبالتالي سنقسم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: مفهوم الجرائم المعلوماتية.

المطلب الثاني: معوقات إثبات الجرائم المعلوماتية بالوسائل التقليدية.

---

[1] عرب، 2002، ص2.

المطلب الأول

مفهوم الجرائم المعلوماتية

إن بحث مفهوم الجرائم المعلوماتية يقتضي تعريف هذه الجرائم، ومن ثم بيان أنواعها، وبالتالي سنقسم هذا المطلب إلى الفرعين الآتيين:

الفرع الأول: تعريف الجرائم المعلوماتية.

الفرع الثاني: أنواع الجرائم المعلوماتية.

الفرع الأول

تعريف الجرائم المعلوماتية

الجرائم المعلوماتية، كما قيل، تقاوم التعريف، ولا مصطلح متفقاً عليه للدلالة عليها، وآية ذلك أن ما قُدّم من كتابات تتناولها شرحاً وتوضيحاً لأساليب ارتكابها وبياناً لأنواعها ووسائل مكافحتها يزخر، حسب تعبير بعض المختصين، " بملايين الكلمات"، التي سطرت في محاولات عدة لصياغة ودحض تعاريفها[1].

ويرى جانب من الفقه أن تعريف الجرائم المعلوماتية يجب أن يكون من الناحية الفنية والقانونية، فالتعريف الفني لها هو أنها " نشاط إجرامي تستخدم فيه تقنية الحاسوب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[2].

أما التعريف من الناحية القانونية فيتطلب تعريف المفردات الضرورية المتعلقة بأركان جرائم الحاسوب الآلي[3].

وهناك تعريفات مختلفة تستند إلى معايير مختلفة، سواء بالنظر إلى وسيلة ارتكابها أو موضوعها، أو حسب توافر المعرفة بتقنية المعلومات، أو استناداً إلى معايير أخرى حسب القائلين بها.

---

[1] R. E. Anderson، 1981، p.260.

[2] حجازي، 2009، ص1.

[3] هلال، 2015م، ص24.

فالتعريفات التي تدخل في حسابها وسيلة ارتكاب الجريمة المعلوماتية تربط تعريفها بالحاسوب، مثل التعريف الذي جاء به الفقيه الألماني "تيدمان" الذي عرفها بأنها: " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"[1]، أو هي " الجرائم التي تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دوراً رئيساً، وذلك حسب تعريف مكتب تقييم التقنية في الولايات المتحدة الأمريكية، أو هي "فعل إجرامي يستخدم الحاسوب في ارتكابه كأداة رئيسة"[2]، أو هي "تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض عمليات فعلية داخل الحاسوب"[3].

وانتُقدت هذه التعريفات لأنها عمومية وواسعة، وتدخل فيها أيضاً الجرائم التقليدية، كما أنها غير منطقية[4].

ويرى الباحث أن هذه التعاريف تقصر هذه الجرائم على التي ترتكب على الحاسوب فقط، مع أنه ترتكب أيضاً بوساطة الإنترنت أيضاً.

أما الذين يعرّفون الجريمة المعلوماتية بالنظر إلى موضوعها، فلا ينظرون إلى الحاسب الآلي بوصفه أداة ارتكاب الجريمة المعلوماتية، بل إن الجريمة تقع على الحاسوب ذاته، وقد تقع داخل نظامه. ومن أمثلة هذه التعريفات أن جريمة الحاسوب " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه"[5].

أما التعريفات المرتبطة بتوافر المعرفة بتقنية المعلومات أو السمات الشخصية للجاني فمنها أن جريمة الحاسوب هي "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطاً بتقنية المعلومات"[6].

---

[1] المخول، 2024م، ص31.
[2] حجازي، 2007.أ، ص 18.
[3] هلال، 2015، ص24.
[4] هلال، 2015، ص24.
[5] حجازي، 2007.أ، ص 18.
[6] حجازي، 2007.أ، ص 19.

ومن هذه التعريفات أيضاً أنها " الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسوب ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها على الجريمة"[1].

كما عرفتها وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث، وتبنتها الوزارة في دليلها لعام 1989، فجاء في التعريف المقترح أنها " أية جريمة لفاعلها معرفة فنية بالحواسيب تمكنه من ارتكابها"[2].

ونرى أن هذه التعريفات قاصرة، لأنها تنطبق على النوع الأول من الجرائم المعلوماتية وهي جرائم الحاسوب، لأنها تقصر وتحصر هذه الجرائم في الجرائم الواقعة على الحاسوب، ولا تنطبق على النوع الثاني منها وهي جرائم الإنترنت.

وعرفت منظمة التعاون الاقتصادي والتنمية (OCDE) الجريمة المعلوماتية في اجتماع باريس عام (1983م) بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرَّح به، يتعلَّق بالمعالجة الآليّة للبيانات أو بنقلها"[3].

لكن هنالك من انتقد هذا التعريف[4] لما فيه من المرونة والسلوك الذي لا يرتب سوى استهجانه أخلاقياً، ذلك أنه لا تلازم دائماً بين الفعل المستهجن أخلاقياً، وذلك المؤثر قانوناً.

وبالتالي، على الرغم من المحاولات الفقهية لوضع تعاريف للجرائم المعلوماتية، إلا أنها جميعها كانت قاصرة ولم تستطع وضع تعريف جامع مانع، وهذا مرده إلى أن هذا النوع من الجرائم معقد وصعب وفي تطور دائم.

---

[1] هلال، 2015، ص24.

[2] هلال، 2015، ص24.

[3] هذا التعريف اقترحه مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية كأساس للنقاش في اجتماع عقد بباريس في عام 1983م، وذلك لبحث الجريمة المرتبطة بالمعلوماتية.

[6] حجازي، 2007.أ، ص 19.

الفرع الثاني

أنواع الجرائم المعلوماتية

للجرائم المعلوماتية أنواع متعددة، وهي جرائم الحاسوب، وجرائم الإنترنت، وجرائم الاتصالات، وأخيراً جرائم باستخدام الحاسوب، وسندرسهما كما يأتي:

أولاً: جرائم الحاسوب:

يُعرف الحاسوب بأنه " آلة تقوم بأداء العمليات الحسابية، واتخاذ القرارات المنطقية على البيانات الرقمية بوسائل إلكترونية، وذلك تحت تحكم البرامج المخزنة فيها"[1].

وجرائم الحاسوب هي النوع الأول من جرائم (Cyber Crime)[2]، وقد عرفها بعض الفقه بأنها " أي سلوك إنساني يشكل فعلاً غير مشروع قانوناً، ويقع على أجهزة الحاسوب، سواء وقع هذا السلوك غير المشروع على Hard Ware أو المكونات المعنوية Soft Ware أو قواعد البيانات الرئيسة Data Base "[3].

كما تُعرف جريمة الحاسوب أو الحاسوب بأنها " نشاط إجرامي تستخدم فيه تقنية الحاسوب بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[4].

كما تُعرف أيضاً بأنها " الاعتداءات التي تستهدف المعلومات والبرامج المخزنة داخل نظم الحاسوب، وتحديداً أنشطة التزوير وسرقة المعطيات، إضافة إلى الدخول غير المصرح به، والذي يتوزع ضمن هذا التقسيم بين دخول غير مصرح به لنظام الحاسوب، ودخول غير مصرح به للشبكات فيتبع لمفهوم جرائم الإنترنت"[5].

ومن أهم أمثلة جرائم الحاسوب نذكر التخريب لمكونات الحاسوب المعنوية، كتعديل أو محو البيانات الرئيسة وغيرها[6].

---

[1] الحلبي، 2011م، ص39.

[2] عبد المطلب، 2006م، ص20.

[3] عبد المطلب، 2006، ص20.

[4] حجازي، 2007.أ، ص 13.

[5] المخول، 2024، ص47.

[6] عبد المطلب، 2006، ص20.

ثانياً: جرائم الإنترنت:

الإنترنت هي الشبكة الدولية للمعلومات، وهي عبارة عن شبكة من أجهزة الحاسوب متصلة بعضها ببعضها الآخر، عن طريق مزود الخدمة (السيرفر) في جميع دول العالم[1].

وتُعرف جرائم الإنترنت بأنها " أي سلوك إنساني يشكل فعلاً غير مشروع قانوناً، وتقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات"[2].

ولا يمكن الآن حصر من يرتكبون جرائم الإنترنت في طبقة أو فئة معينة أو جنس معين، فمرتكب الجريمة قد يكون من البالغين أو الأحداث أو المتعلمين والمثقفين، ومن الفقراء أو الأغنياء، ومن الرجال أو من النساء[3].

ومن أمثلة هذه الجرائم جرائم الدخول غير المشروع إلى مواقع غير مصرح بالدخول إليها، واستخدام عناوين (IP) غير حقيقة أو زائفة للولوج إلى الشبكة العالمية للمعلومات، وكسر البروكسي (Brokcey) أو تقنيات الحماية (Fire Wall) الخاصة بالجهات المتصلة بالشبكة... وغيرها[4].

ثالثاً: جرائم باستخدام الحاسوب:

تسمى الجرائم باستخدام الحاسوب (Computer related Crime)[5]، وهذا النوع من الجرائم المعلوماتية لا يعد استخدام الحاسوب أو الشبكة العالمية للمعلومات أو الإنترنت من طبيعة الفعل الجرمي أو ركناً من أركان الجريمة بمعناها القانوني، مثل الجرائم التي يتم فيها استخدام الحاسوب والإنترنت في عمليات غسل

---

(1) الحلبي، 2011، ص50-51.

(2) عبد المطلب، 2006، ص21.

(3) رمضان، 2000م، ص11.

(4) عبد المطلب، 2006، ص21.

(5) عبد المطلب، 2006، ص21.

الأموال أو نقل المخدرات من مكان إلى آخر وغيرها، فهنا الحاسوب أو الإنترنت هما وسيلة ارتكاب الجاني للجريمة التي يمكن ارتكابها بأي وسيلة أخرى[1].

المطلب الثاني

معوقات إثبات الجرائم المعلوماتية بالوسائل التقليدية

ترجع معوقات إثبات الجرائم المعلوماتية بالأدلة التقليدية إلى أسباب تتعلق بالجرائم المعلوماتية، سواء أكانت متعلقة بخصائص الجرائم المعلوماتية أولاً، أم متعلقة بالطبيعة الخاصة للجريمة المعلوماتية ثانياً، أم لأسباب متعلقة بالمجرم المعلوماتي ثالثاً، وسنعرضها في الفروع الآتية:

الفرع الأول: الأسباب العائدة إلى خصائص الجرائم المعلوماتية.

الفرع الثاني: الأسباب العائدة إلى الطبيعة الخاصة للجريمة المعلوماتية.

الفرع الثالث: الأسباب المتعلقة بالمجرم المعلوماتي.

الفرع الأول

الأسباب العائدة إلى خصائص الجرائم المعلوماتية

إن ارتباط الجرائم المعلوماتية بجهاز الحاسوب والإنترنت أضفى عليها مجموعة من الخصائص المميزة لها عن باقي الجرائم التقليدية[2]، وأهم هذه الخصائص:

---

[1] Brian Carrier. Defining Digital Forensics Examination and Analysis Tools. In Digital Research Workshop II، 2002، Available at:http://www.Dfrws.org/dfrws2002/papars/papars/Brian Carrier.pdf accessed 5April 2024.

[2] هلال، 2015، ص25.

أولاً: عدم تخلف آثار مادية عن الجرائم المعلوماتية:

تتميز الجرائم المعلوماتية بصعوبة متابعتها، إذ إنها في الغالب لا تترك أثراً، فليس هناك أموال وممتلكات مفقودة، وإنما هي أرقام تتغير في السجلات، ومعظم الجرائم المعلوماتية ربما يتم اكتشافها بالمصادفة، وبعد وقت طويل من ارتكابها[1].

فمن أبرز خصائص الجريمة المعلوماتية وقوعها في بيئة معلوماتية، وهذه الخاصية تترتب عليها جمله نتائج تصعّب من مهمة اكتشاف هذه الجرائم، لا بل حتى التحقيق فيها.

وهذا على عكس الجرائم التقليدية، فرجل الشرطة الذي يقوم بجمع التحريات في واقعة سرقة حتى يصل إلى المتهم، ويتم القبض عليه، وتتولى جهات التحقيق استجوابه وإحالته إلى محكمة الموضوع، فكل هذه وقائع خاضعة لسيطرة أجهزة العدالة، والدليل فيها مرئي ومقروء، على عكس الجريمة المعلوماتية التي تتم من دون رؤية لدليل الإدانة، وحتى في حالة وجود الدليل يمكن للجاني طمس الدليل أو محوه، وفي حضور أجهزة العدالة غير المتخصصة، ولذلك فغالبية الجرائم المعلوماتية تكتشف مصادفة وليس بطريق الإبلاغ عنها[2]، لأنها لا تخلف في الغالب أية آثار مادية كتلك التي تخلفها الجرائم التقليدية ، إذ إنها لا تخلف لا سكيناً ولا سلاحاً ولا ظروفاً فارغة لطلقات نارية، ولا بقعاً دموية، أو غير ذلك من الآثار المادية[3].

وليس أدل على ذلك من أن المعاينة في الجريمة المعلوماتية لمسرح الجريمة قد لا تكون مجدية مثل المعاينة لمسرح الجريمة التقليدية[4].

ومن الأمثلة الواقعيَّة على ما تقدَّم ما حصل في دولة الإمارات العربية المتحدة، إذ قام مُشَغِّل حاسوب بتهديد المؤسَّسة التي يعمل لديها حتى تنفذ مجموعة من مطالبه، وذلك بعد أن حذف كافّة البيانات الموجودة على الجهاز الرئيس للمؤسّسة، وقد رفضت المؤسسة الاستجابة لمطالبه، فأقدم على الانتحار، ووجدت المؤسسة صعوبة في استرجاع البيانات التي كانت قد حُذفت.

---

[1] آل ثنيان، 2012م، ص1.

[3] حجازي، 2002، ص 24.

[3] خلف، 2016، ص8.

[4] حجازي، 2007.أ، ص149.

وتتعقد المشكلة عندما يتعلَّق الأمر بمعلومات أو بيانات تم **تخزينها في الخارج** بوساطة شبكة الاتصال عن بُعد، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثًا عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية؛ إذ إن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة، ولمّا كانت أدلة الإثبات المتحصِّلة من التفتيش على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنيّة، ودراية فائقة في هذا المجال؛ فإنَّ نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدِّي إلى ضياع الدليل بل تدميره أحياناً، ويضاف إلى ذلك أنَّ كل المعطيات ليس لها تجسيد دائم على أية دعامة، بمعنى أنها لا توجد مسجلة على أسطوانة صلبة أو مرنة، ولا على أية دعامة مادية منقولة أياً كانت، فقد توجد هذه المعطيات في الذاكرة الحية للحاسوب، ويتم محوها في حالة عدم حفظها أو تسجيلها على أية أسطوانة، وحتى لو كانت المعطيات قد تم تخزينها على دعامة مادية إلا أنّه قد يكون من الصعب الدخول إليها بسبب وجود نظام معلوماتي للحماية، وعلاوة على ذلك قد يتقاعس المجني عليه عن التبليغ عن الجرائم المعلوماتية إلى السلطات المختصة، بالإضافة إلى ما تقدم من صعوبات ومشكلات[1].

ثانياً: الجرائم المعلوماتية جرائم نظيفة:

تتصف الجرائم المعلوماتية بأنها **(جرائم نظيفة)**؛ وذلك لصعوبة اكتشاف دليل ثبوتها؛ فلا أثر فيها لأي عنف أو دماء، وإنما هي مجرد أرقام وبيانات **يتم تغييرها أو محوها من السجلات المخزونة في ذاكرة الحواسيب وليس لها أثر خارجي مادي** [2]، فالجاني لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه[3].

فعلى سبيل المثال، فإن الاحتيال الذي تقوم به جريمة الاحتيال قد تطور كنتيجة لاستخدام التقنية العلمية، وأصبح كثير الوقوع في العمليات الإلكترونية، وبالنظر إلى الطبيعة غير المرئية التي يتم بها فقد يصعب إثباته[4].

---

[1] الطوالبة، 2009م.

[2] بحر، 1999م، ص22.

[3] المخول، 2024، ص 60.

[4] المنشاوي، 2012، ص559.

فالجريمة المعلوماتية لا تترك آثراً، وإن تركت فقد يكون من الصعب تتبعها، فعلى سبيل المثال في جريمة (سرقة البنوك) بطريق الاحتيال المعلوماتي يصعب الإمساك بالمجرمين بسبب السرعة التي تتم بها عملية التحويلات النقدية[1].

ثالثاً– المشكلة التي تواجه أجهزة العدالة الجزائية أن الجرائم المعلوماتية لاتصل إلى علم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية، ولا تخلق آثاراً مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة ، وجثة المجني عليه في القتل ، واختلاس المال من المجني عليه في السرقة وغيرها، ويرجع السبب في فقدان الآثار التقليدية للجريمة المعلوماتية إلى أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسوب من دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها ، كما لو كان البرنامج معداً ومخزناً على جهاز الحاسوب، ويتوافر أمام المتعامل عدة اختيارات، وليس له سوى أن ينقر أو يضغط على الخيار الذي يريد، فتكتمل حلقة الأمر المطلوب تنفيذه ، كما في المعاملات المالية في البنوك أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى، إذ يتم ترصيد الأشياء المخزونة أو حسابات العملاء ، أو نقلها من مكان إلى آخر بطريقة آلية وحسب الأوامر المعطاة إلى جهاز الحاسوب[2].

رابعاً– الجريمة المعلوماتية، تظهر آثارها فيما بعد الجريمة، بل فيما بعد أن يطمس دليلها من المجرم الإلكتروني المتخصص من دون رؤية الدليل ذاته[3].

خامساً– أنها تستعصي على الإثبات بالطرق التقليدية وتستلزم طرقاً خاصة مستحدثة للإثبات، قوامها التعليم والتدريب المتخصص المستمر لعلوم الحاسوب، لذا فإنها تقتضي وجود رجل شرطة معلوماتي، ومحقق معلوماتي، وقاضٍ معلوماتي فضلاً عن الخبير المعلوماتي، حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم، لذا فإن عملية الاستعانة بالخبرة الفنية المتخصصة المؤهلة والمدربة، تصبح حتمية؛ لكشف واشتقاق وتحليل وتفسير

---

[1] حجازي، 2007.أ، ص167–168.

[2] خلف، 2016، ص15.

[3] حجازي، 2007.أ، ص117.

الدليل الجنائي الذي يقدم إلى المحكمة لتقرير البراءة أو الإدانة، فضلاً عن حتمية تدريب رجال الضبط القضائي والمحققين، والقضاة، على نظم وتكنولوجيا المعلومات، وكيفية ضبط وتداول (التعامل) وفهم الأدلة المتخلفة عن هذه الجرائم[1].

سادساً- أن هذا النوع من الجرائم يتسم بالمكر والحيلة والدهاء والغش والاحتيال باستخدام تقنيات معلوماتية عالية الكفاءة أصبحت لسهولة استخدامها وسرعة انتشارها من الوسائل الخطيرة لارتكاب هذه النوعية من الجرائم[2].

لذلك، الجرائم المعلوماتية لا تحدها حدود، وتعدُّ من الجرائم العابرة للحدود، فتثير لذلك تحديات في حقل الاختصاص القضائي والقانون واجب التطبيق[3]، فيمكن عن طريق الحاسوب – أو حتى هاتف نقال–لشخص في الصين أن يرتكب جريمة تزوير أو تزييف أو سرقة معلومات أو نقود، ضد شخص طبيعي أو معنوي في الولايات المتحدة الأمريكية أو العكس[4].

الفرع الثاني

الأسباب العائدة إلى الطبيعة الخاصة للجريمة المعلوماتية

إن الطبيعة الخاصة للجرائم المعلوماتية سوف تنعكس على طبيعة الإثبات الجنائي لهذه الجرائم[5]، وبالتالي تتميز الجريمة المعلوماتية بطبيعة خاصة تجعلها تثير عدداً من المشكلات، وهذا الأمر عقّد إلى درجة كبيرة إثبات الجريمة المعلوماتية، وترجع هذه الصعوبة إلى عدد من الأمور، من أهمها ما يأتي:

1- أن الجريمة المعلوماتية توجد في بيئة لا تعتمد التعاملات فيها- أصلاً- على الوثائق والمستندات المكتوبة، بل على نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بوساطة الحاسوب والبيانات التي يمكن استخدامها كأدلة ضد الفاعل، ويمكن في أقل من ثانية العبث بها أو محوها بالكامل، لذلك فإن

---

[1] فرغلي، و المسماري، 2007م، ص10.

[4] حجازي، 2007.أ، ص 46.

[3] المخول، 2024، ص61.

[4] فرغلي، و المسماري، 2007، ص10.

[5] حجازي، 2007.أ، ص63.

المصادفة وحسن الحظ لهما دور كبير في اكتشافها، وذلك أكثر من الدور الذي تلعبه أساليب التدقيق والرقابة[1]، كما أن المجني عليه له دور في هذه الصعوبة، بسبب دوره السلبي وعدم إبلاغه عن وقوع هذا النوع من الجرائم، فالكثير من الجهات التي تتعرض أنظمتها للانتهاك تعمد إلى عدم الكشف عنها تجنباً لعدم الإضرار بسمعتها، وتكتفي بالإجراءات الإدارية، وفي هذا الخصوص أوصى المؤتمر الدولي الخامس عشر الذي عقد في "ريو دي جانيرو" بالبرازيل من 4-9 /11/ 1994، بضرورة تشجيع المجني عليهم في هذه الجرائم على الإبلاغ عنها فور وقوعها، وهذا بهدف تخفيض الرقم الأسود للجرائم المعلوماتية في الفضاء الافتراضي[2].

2- تختلف الطبيعة القانونية للجرائم المعلوماتية عن الطبيعة القانونية للجرائم العادية، لأن الاعتداء على البيانات والمعلومات والبرامج يختلف أيضاً عن الاعتداء على المكونات المادية المحسوسة التي تخضع للمفهوم التقليدي[3]، ونظراً إلى الطبيعة الخاصة للجرائم المعلوماتية فإن دليل إثباتها يختلف ويتميز عن الدليل الجنائي التقليدي[4].

وبالتالي يمكن القول إن الجريمة المعلوماتية تنشأ عنها عدة معوقات تعوق إثباتها بالأدلة التقليدية، وهذا في إطار الإثبات الجزائي، نظراً إلى الطبيعة الخاصة لهذه الجريمة المستحدثة.

---

[1] حجازي، 2007.أ، ص 92.

[2] مصطفى، 2010م، ص47-49.

[3] الحلبي، 2011، ص54.

[4] عريقات، (د.ت)، ص11.

الفرع الثالث

الأسباب المتعلقة بالمجرم المعلوماتي

استثمر المجرمون معطيات العصر وتطوره العلمي والتقني مستفيدين من التسهيلات التي تقدمها هذه التقنية التي أعطت فرصاً كثيرة لا يستهان بها في استثمارها من قبل ضعاف النفوس ومريدي الإجرام، لما تهيئه من تسهيلات، يمكن لهم بوساطتها التخطيط والتنفيذ لعملهم الإجرامي[1].

والجناة في الجرائم المعلوماتية أي (المجرمين المعلوماتيين) ينتمون إلى المجرمين ذوي الياقات البيضاء، وليس معنى ذلك أنهم أقل خطورة من الناحية الإجرامية عن المجرمين ذوي الياقات الزرقاء، بل يعني أنهم يختلفون عنهم في اتجاهات شخصياتهم، وعلى الرغم من انتمائهم بوجه عام إلى المجرمين ذوي الياقات البيضاء فإنهم طائفة متميزة عنهم تتخصص في جرائم الحاسوب، فهم إما أن يقوموا بالاعتداء على نظام الحاسوب، أو أن يقوموا بالاستعانة بالحاسوب في ارتكاب جرائمهم[2].

وهذا النمط الجديد من الجرائم يتطلب نمطاً جديداً من المجرمين، إذ يمس التغيير الجوانب الشخصية للمجرم، ومستواه الثقافي ودوافعه الإجرامية، مما يجعل مجرم اليوم أكثر خطورة ودهاءً من مجرم الأمس، فهو في سبيل تحقيق أغراضه الإجرامية يلجأ إلى تسخير ثمار العلم إلى أبعد الحدود باستخدام التقنيات العالية والوسائل العلمية المتطورة للتفنن في الجريمة سواء في ارتكابها، أو إخفائها، أو الهروب من مسؤولياتها[3]، ولاسيما أن المجرم المعلوماتي يتسم بأنه "مجرم ذكي" في ذاته، يعكس أعلى درجات المهارة في فنون التعامل مع الحاسوب، ويكفي للتدليل على خطورة هذا الأمر أن بعضهم يتعامل مع هذه النوعية من الجرائم بوصفه يمارس "هواية" لا حرفة[4].

---

[1] المنشاوي، 2012، ص517.

[2] غنام، 2004م، ص628.

[3] مليكة، 2013م، ص4.

[4] حجازي، 2007.أ، ص9.

وقد دعم التقدم العلمي تطور الجريمة، إذ استخدم المجرم كافة التقنيات ولم يترك وسيلة علمية إلا واستعان بها من أجل إنجاح مشروعه الإجرامي[1]، فالجاني يستطيع الجاني أن يرتكب جريمته من دون أن يترك وراءه أثراً خارجياً ملموساً، وإذا كان ثمة دليل على الإدانة فإن الجاني يستطيع تدميره في ثوان معدودة، وخاصة أن المجرم المعلوماتي يتميز بالذكاء وبمهارة تقنية عالية، ومعارف فنية في مجال المعلوماتية وأنظمة وبرامج الحواسيب، ولا سيما أنه على دراية بالأسلوب المستخدم في التشغيل، واللغة المستخدمة في تخزين المعلومات وكيفية استدعائها، بل إنه قد يكون من المختصين في مجال تقنية المعلومات[2].

هذا بالإضافة إلى أن كثيراً من الجرائم المعلوماتية يثير شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية، إذ يقع الفعل الإجرامي عادة من مسافات بعيدة، وذلك باستخدام وحدات طرفية أو اتصال هاتفي يمكن للجاني من خلالها إعطاء تعليمات إلى الحاسب الآلي تمكّنه من اختراق شبكات المعلومات في مناطق أخرى، والنتيجة هي صعوبة الوصول إليه ومعرفته، فقد يكون الجاني في أحد العواصم الأسيوية أو الأوربية ويخترق شبكات المعلومات في الولايات المتحدة أو العكس، كما أنه باستطاعته أن يطمس ويلغي كل ما يدل على جريمته من خطوات[3]. وهكذا فقد استطاع الجناة تطوير طرق الإجرام على هذا النحو من التقنية العالية في بيئة تكنولوجيا المعلومات[4]، وبخصوص ذكاء المجرم الإلكتروني، فإنه يقال عادة إن الإجرام المعلوماتي هو إجرام الأذكياء، وذلك بالمقارنة بالمجرم التقليدي الذي يميل عادة إلى العنف[5].

ويرى الباحث أنه إذا كنا أمام الجرائم المعلوماتية التي هي ظاهرة إجرامية مستجدة تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها وأنماط السلوك الإجرامي المجسدة للركن المادي لكل جريمة من هذه الجرائم، فإن ذلك يستدعي ضرورة تطور طرق إثباتها بحيث يتلاءم مع طبيعتها وخصائصها، وبالتالي نقترح ضرورة تطوير طرق الإثبات كلما تطورت وسائل الإجرام.

---

[1] مليكة، 2013، ص3.

[2] حجازي، 2007.أ، ص46.

[3] حجازي، 2007.أ، ص47.

[4] أحمد، 2004م، ص715.

[5] حجازي، 2007.أ، ص78.

المبحث الثاني

قدرة الوسائل التقليدية في إثبات الجريمة المعلوماتية

تتضمن وسائل الإثبات التقليدية الخبرة والمعاينة والتفتيش والضبط، وهنا سنحاول دراستها وبحث مدى قدرتها في إثبات الجريمة المعلوماتية، ولكن قبل التعرض لمدى قدرة وسائل الإثبات التقليدية كان لابد لنا من عرض الصعوبات التي تواجه الحصول على الدليل الإلكتروني، وبالتالي إثبات الجريمة المعلوماتية في هذه الوسائل.

وبناء على ذلك سنقسم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: الصعوبات التي تواجه الحصول على الدليل الإلكتروني بوسائل الإثبات التقليدية.

المطلب الثاني: عدم قدرة الوسائل التقليدية في إثبات الجريمة المعلوماتية.

المطلب الأول

الصعوبات التي تواجه الحصول على الدليل الإلكتروني بوسائل الإثبات التقليدية

يعد انتشار الأجهزة المحمولة باليد، والمتصلة بشبكات اللاسلكي بمنزلة تطور نوعي كبير في عصر الحاسوب، إلا أن هذا الأمر يعد من أكبر تحديات البحث والتحقيق في الأنشطة الإجرامية في مجال الحاسوب المنتشرة على مستوى العالم، وتتمثل أغلبية هذه الصعوبات في كيفية الحصول على الأدلة من هذه الأجهزة ذات العلاقة بالواقعة محل البحث الجزائي[1].

إذ تواجه الخبير الفني وغيره، صعوبات متعددة ومختلفة، للحصول على هذه الأدلة من أجهزة الحاسوب، أو الشبكات الإلكترونية، فليس من الهين استخراج واستنباط الدليل الإلكتروني، نظراً إلى الطبيعة الخاصة للجريمة المعلوماتية في الدرجة الأولى، وكذلك الدليل الإلكتروني، فهو دليل علمي وفني، وتقني، كما أنه يتميز بسرعة

[1] عبد المطلب، 2006، ص119 – 120.

فقدانه وإتلافه، بالإضافة إلى أن المجرم الذي يقترف هذا النوع من الجرائم، أي الجرائم المعلوماتية، يتميز بالفطنة والذكاء الحادين، ويسعى بكل جهد لعدم ترك أي دليل يقود إليه[1].

لذلك فالصعوبات التي تعترض تحصيل الدليل الإلكتروني كثيرة ومتنوعة، فمن هذه الصعوبات ما يتعلق بالجريمة المعلوماتية، ومنها ما يتعلق بالدليل الإلكتروني نفسه، ومنها أخيراً ما يتعلق بأسباب متعددة، وبالتالي سندرس هذه الصعوبات في الفروع الثلاثة الآتية:

الفرع الأول: صعوبات متعلقة بالجريمة المعلوماتية.

الفرع الثاني: صعوبات متعلقة بالدليل الإلكتروني.

الفرع الثالث: صعوبات متعلقة بأسباب متعددة.

الفرع الأول

صعوبات متعلقة بالجريمة المعلوماتية

تثير الجرائم المعلوماتية، وبصفة خاصة جرائم الإنترنت بعض المشكلات المتعلقة بالإجراءات الجزائية، وخصوصاً في مجال جمع الأدلة، إذ توجد صعوبات عملية تتعلق بالتفتيش على وجه الخصوص[2]، ومن هذه الصعوبات ما هو متعلق أولاً، بخصائص الجريمة المعلوماتية، وثانياً، منها ما هو متعلق بالجاني والمجني عليه، وثالثاً، منها ما هو متعلق بضعف التعاون الدولي في مكافحة هذه الجريمة.

أولاً: صعوبات متعلقة بخصائص الجريمة المعلوماتية:

ترجع الصعوبات المتعلقة بالجريمة المعلوماتية وبخاصة الحصول على الدليل الإلكتروني إلى خصائص الجريمة المعلوماتية، إذ إن ارتباط الجرائم المعلوماتية بجهاز الحاسوب والإنترنت أضفى عليها مجموعة من

---

[1] هلال، 2015، ص69.

[2] رمضان، 2000، ص72.

الخصائص المميزة لها عن باقي الجرائم التقليدية[1]، ومن هذه الخصائص التي تشكل حجر عثرة أمام الحصول على الدليل الإلكتروني ما يأتي:

أ- ازدواجية محل الجريمة المعلوماتية:

بحسبان أن النظام المعلوماتي ليس من طبيعة واحدة فهو يتكون من عناصر مادية وأخرى غير مادية، كان يكون موضوع الجريمة ذا طبيعتين مختلفتين، إحداهما مادية والأخرى غير مادية، كما هو الحال بالنسبة إلى المعلومات، فقد تكون في حالة انتقال، أو موجودة في ذاكرة النظام المعلوماتي، أي إنها في حالة غير مادية، وقد تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة معلوماتية، حتى إن المعلومات بطبيعتها غير المادية أو المادية يمكن أن تخضع لأكثر من نص قانوني، مما يولّد مشكلة تعدد الأوصاف القانونية على المحل نفسه [2].

ب - الجريمة المعلوماتية جريمة عابرة للحدود:

يطلق تعبير "جرائم عابرة للدول" أو جرائم غير وطنية على تلك الجرائم التي تقع بين أكثر من دولة، بمعنى أنها لا تعترف بالحدود الجغرافية للدول، كجرائم تبييض الأموال، والمخدرات وغيرها، وفي عصر الحاسوب، ومع انتشار شبكة الاتصالات العالمية (الإنترنت)، أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة، بحيث يغدو أمر التنقل والاتصال فيما بينها أمراً سهلاً، طالما حدد عنوان المرسل إليه، أو أمكن معرفة كلمة السر، وسواء تم ذلك بطرق مشروعة، أو غير مشروعة. وفي هذه البيئة يمكن أن توصف الجريمة المعلوماتية بأنها جرائم عابرة للدول، إذ غالباً ما يكون الجاني في بلد، والمجني عليه في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه[3].

فقد تقع الجريمة المعلوماتية في كثير من الأحيان في عدة بلدان مختلفة، فيتم الدخول إلى الأجهزة الإلكترونية من بلد معين، ويُتلاعب بالبيانات في بلد آخر، وتسجل البيانات في بلد ثالث، ومن الممكن أن تخزن

---

[1] هلال، 2015، ص25.

[2] هلال، 2015، ص25.

[3] آل ثنيان، 2012، ص23.

الأدلة الإلكترونية في أجهزة موجودة في غير البلد الذي ارتكب فيها الجاني جريمته، فتقع الجريمة بذلك في عدة دول كل دولة لها القانون المختلف عن الأخرى، وهذا ما يشكل تعقيداً أمام الجهات القضائية في تطبيق القانون، وعائقاً في عملية التحقيق والإثبات لهذه الجرائم[1].

فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية، لأن الشبكات تخترق الزمان والمكان، وخاصة بعد ظهور شبكات المعلومات الدولية، أي الإنترنت، إذ إن القائم على النظام المعلوماتي في أي دولة يمكنه أن يحول مبلغاً من المال إلى أي مكان في العالم مضيفاً إليه صفراً أو بعض الأصفار إلى حسابه الخاص، بل يستطيع أي شخص أن يعرف كلمة السر لأي شبكة في العالم ويتصل بها ويغير ما فيها من معلومات[2].

ويترتب على هذه الخاصية أن تزيد الصعوبة في إثبات الجريمة المعلوماتية متى ارتُكبت خارج النطاق المكاني للإقليم، لأنه يصعب في هذه الحالة جمع الدليل الجزائي فيها[3].

وإذا تقرر أن الجرائم المعلوماتية جرائم عابرة للدول تظهر الحاجة الملحة للتعاون الدولي في مجال مكافحة هذه الجرائم وضبط فاعليها[4].

ونظراً إلى صعوبة استخلاص الدليل الإلكتروني في الجريمة المعلوماتية يرى المختصون في جرائم الحاسوب أن هذا الجهاز وما يقع عليه من جرائم معلوماتية، يعد تحدياً هائلاً لرجال الأمن، ذلك أن رجل الأمن غير المتخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادراً على التعامل مع الجريمة المعلوماتية التي تقع بطريقة تقنية عالية[5].

جـ- ضخامة كم البيانات المعلوماتية في الجريمة المعلوماتية:

لعل من الصعوبات الكبيرة التي تواجه رجال الضبط وسلطات التحقيق الجنائي في الجريمة المعلوماتية، كمية المعلومات والبيانات الضخمة التي هي في حاجة إلى فحص ودراسة، كي يستخلصوا منها دليل هذه

---

[1] حمودة، 2017م، ص121.

[2] هلال، 2015، ص25 – 26.

[3] حجازي، 2007.ب، ص31.

[4] آل ثنيان، 2012، ص23.

[5] حجازي، 2007.أ، ص107.

الجريمة، لذلك يمكن القول إن ضخامة هذه البيانات والمعلومات، تعد عائقاً في التحقيق في الجرائم المعلوماتية، ذلك أن طباعة كل ما هو موجود على الدعامات الممغنطة لحاسوب متوسط العمر، يتطلب مئات الآلاف من الصفحات[1]، فحجم البيانات الضخمة التي غالباً ما تستخدم في التحقيق من خلال أنظمة الحاسوب تشكل تحدياً، وهذا راجع إلى أن البحث عن الأدلة اللازمة للإدانة أو البراءة في قدر كبير من البيانات الإلكترونية، صعب جداً ويتطلب جهداً ومهارة عاليين[2]، في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئاً مفيداً للتحقيق، وهذا عكس ضخامة أو وفرة المعلومات في الجرائم التقليدية كالقتل أو السرقة، ذلك أن وفرة المعلومات في مثل هذه الجرائم أمر يساعد العدالة ورجال الضابطة العدلية في استخلاص الدليل الجزائي في هذه الجريمة[3].

ثانياً: صعوبات متعلقة بالجاني والمجني عليه في الجريمة المعلوماتية:

هنالك صعوبات كثيرة ترجع إلى المجرم المعلوماتي تحول دون الحصول على الدليل الإلكتروني، نظراً إلى إخفائه هويته ومحاولة تدميره لهذا الدليل، كما قد يسهم المجني عليه في الجريمة المعلوماتية في الحيلولة دون الحصول إلى هذا الدليل في حال إحجامه عن التبليغ عن الجريمة المعلوماتية التي وقعت عليه، وبناء على ما تقدم سندرس إخفاء المجرمين لهويتهم، ومن ثم تقاعس المجني عليه في الإبلاغ عن الجرائم المعلوماتية، كما يأتي:

أ- إخفاء المجرمين لهويتهم:

من الصعوبات الإضافية التي يمكن أن تعترض العملية الإثباتية في مجال الجرائم المعلوماتية سهولة محو الجاني أو تدميره لأدلة الإدانة في زمن متناه القصر، فضلاً عن سهولة تنصله من مسؤولية هذا العمل بإرجاعه، حسبما تشهد بذلك وقائع عدة سابقة، إلى خطأ في نظام الحاسوب أو الشبكة أو في الأجهزة[4].

فالإغراءات التي تجذب المجرمين نحو الجرائم المعلوماتية هي أنها في الحقيقة جرائم سريعة التنفيذ، إذ غالباً ما يتمثل ركنها المادي في استعمال جهاز الحاسوب، مع إمكانية تنفيذ ذلك عن بُعد، من دون اشتراط

---

[1] حجازي، 2007.أ، ص196.

[2] عبد المطلب، 2006، ص119 - 121.

[3] حجازي، 2007.أ، ص196.

[4] رستم، 2004م، ص429.

الوجود في مسرح الجريمة، وأيضاً ضخامة الفوائد والمكاسب التي يستطيع الجاني تحقيقها في مثل هذه الجرائم، من دون جهد يذكر، ومن دون أن يخاف أن يكتشف أمره، كما أن الجرائم المعلوماتية يمكن عدها إغراء كبيراً للمجرمين، لاستغلال التكنولوجيا الحديثة، بغية اقتراف الجرائم بصورها المتعددة، وخصوصاً عندما يكون الجاني موظفاً في شركة تعتمد الحاسوب في عملها، إذ يكون لديه كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسوب في الشركة، وتحقيق أرباح طائلة والواقع يثبت ذلك[1].

وتبدأ هذه المشكلة عند تعمد المستخدم إخفاء هويته، ويخلق هذا الأمر المزيد من التحديات الأمنية، لأنه حتى عندما لا يبذل المجرمون جهداً في إخفاء هويتهم فإنهم يستطيعون الادعاء بأنهم لم يكونوا مسؤولين عن ذلك، فقد يتخذ المجرمون بعض الإجراءات لإحباط اعتقالهم، وهذا في حال بذلهم لجهد ضئيل لطمس هويتهم على الإنترنت، لكي تظل أنشطتهم مجهولة، ومن هذه الإجراءات مثلاً ما يكون بسيطاً مثل استخدام كومبيوتر في مكتبة عامة، إلا أن هناك عدداً من البرامج والتطبيقات التي تقدم وسائل متباينة لكيفية طمس الهوية على الإنترنت، مما يؤدي إلى تفاقم المشكلة بالنسبة إلى عضو الضابطة العدلية، فهذا الإخفاء يجعل الأمر صعباً على الفاحصين القائمين على تحليل الأدلة التي تم العثور عليها، وتجميعها وإدراجها في مستندات والاحتفاظ بها[2].

كما أن مرتكبي هذه الجرائم لا يتركون في غالب الأحيان آثاراً تدل على ارتكابهم إياها؛ إذْ تكون المعلومات محفوظة تحت رقم أو رمز سري أو مشفرة كليّاً[3]؛ فمن الممكن وضع شيفرة لحماية المعلومات والتقيد بتعليمات مبرمجة لمنع اختراق الحاسوب، وتُعد هذه من الوسائل الفنية لحماية سرية المعلومات في نظم الحواسيب الإلكترونية[4]، والتشفير هو عملية تتمثل في تحويل المعلومات المقروءة إلى إشارات غير مفهومة، لحماية أمن المعلومات ضد أعمال القرصنة ونشر الفيروسات والاعتداء على المعلومات، وبيانات بطاقات الائتمان الممغنطة[5]،

---

[1] آل ثنيان، 2012، ص22 – 23.

[2] عبد المطلب، 2006، ص121.

[3] فتح الله، 2012م، ص26.

(4) Law And Computer Technology: Vol 5، No 2، March 1972، P 45 - 46.

[5] الحلبي، 2011، ص50.

إذْ يصعب الولوج إليها أو معرفتها، وبالتالي إقامة الدليل ضد هؤلاء الجناة[1]. وبالنظر إلى ازدياد انتشار برمجيات التشفير هذه في الدول المتقدمة وما ينجم عنها من مخاطر، فإن بعضها استحدث تشريعات تمّ بموجبها تجريم اللجوء إلى هذه التقنيات من دون ترخيص من الأجهزة المختصة، ومن هذه الدول هولندا، التي سنّت تشريعاً يقضي بوضع ضوابط لعمليات التشفير، ومنها ضرورة الحصول على ترخيص من الجهات المعنية، إلى جانب إيداع مفاتيح التشفير لدى هذه الجهات [2].

وكذلك فعلت فرنسا الشيء ذاته، ومن شأن الإقدام على هذا التشفير بدون ترخيص أن يصبح الفعل جريمة يعاقب عليها القانون، وأيضاً معاقبة الشخص الذي أعد برنامج التشفير بدون ترخيص[3].

ويقترح الباحث ضرورة عدّ الإقدام على التشفير بدون ترخيص جريمة يعاقب عليها القانون، وأيضاً نقترح معاقبة الشخص الذي أعد برنامج التشفير بدون ترخيص.

كما لا بد من خلق وحدات خاصة تكون مهمتها الأساسية مراقبة وتتبع الشبكة عن طريق الإبحار فيها، ومثل هذه المراقبة السابقة قد تعطي نتائج مهمة على مستوى الحد من الجريمة قبل ارتكابها عن طريق الوقاية منها[4].

هذا بالإضافة إلى أن كثيراً من الجرائم المعلوماتية يثير شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية، إذ يقع الفعل الإجرامي عادة من مسافات بعيدة، وذلك باستخدام وحدات طرفية أو اتصال هاتفي يمكن للجاني من خلالها إعطاء تعليمات للحاسب الآلي تمكنه من اختراق شبكات المعلومات في مناطق أخرى والنتيجة هي صعوبة الوصول إليه ومعرفته، فقد يكون الجاني في أحد العواصم الأسيوية أو الأوربية ويخترق شبكات المعلومات في الولايات المتحدة أو العكس، كما أنه باستطاعته أن يطمس ويلغي كل ما يدل على جريمته من خطوات[5].

---

[1] فتح الله، 2012، ص27 – 28.

[2] أرحومة، 2009م، ص4.

[3] بوحويش، 2009 م، ص70.

[4] فتح الله، 2012، ص27 – 28.

[5] حجازي، 2007.أ ، ص47.

وكمثال عن محاولة مرتكبي الجرائم إخفاء جرائمهم أو على الأقل إزالة آثارها، نجد أن التجسس المعلوماتي بنسخ الملفات، من النادر اكتشافه بمعرفة الشركات التي تقع ضحية له، فالتدليس عادة ما يتم خفية عن طريق التلاعب بالقوائم والمعطيات التي يحتويها الجهاز أو البرامج المعلوماتية ذاتها، فالتعديلات التي يقوم بها الجاني في الملفات المعلوماتية لا تترك آثاراً على خلاف تلك التي تترتب على تزوير المستندات الورقية[1].

ب- تقاعس المجني عليه في الإبلاغ عن الجرائم المعلوماتية:

قد يتقاعس المجني عليه عن الإبلاغ عن الجرائم المعلوماتية إلى السلطات المختصة بالكشف عن هذه الجرائم وإثباتها[2]، ويكون بالتالي للمجني عليه دور في صعوبة الحصول على الدليل الإلكتروني، بسبب موقفه السلبي وعدم إبلاغه عن وقوع هذا النوع من الجرائم، فكثير من الجهات التي تتعرض أنظمتها للانتهاك يعمد إلى عدم الكشف عنها تجنباً لعدم الإضرار بسمعته ويكتفي بالإجراءات الإدارية[3].

ففي إحدى الوقائع تعرض أحد البنوك، وهو بنك (Marchant bank city) في بريطانيا لسرقة ٨ مليون جنيه إسترليني من إحدى أرصدته إلى رقم في سويسرا، وتم ضبط الفاعل متلبساً بسحب المبلغ المسروق، وبدلاً من محاكمته قام البنك بدفع مليون جنيه له بشرط التزام الفاعل بعدم الإعلام عن جريمته، وإعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الأمن في حاسوب البنك الرئيس[4].

كما كشفت إحصائيات شركات التأمين في فرنسا عن أن نسبة الإبلاغ عن جرائم الحاسوب تتراوح بين 5 إلى 10% من مجموع الجرائم التي ارتكبت في هذا المجال، ويرجع السبب في ذلك إلى الرغبة في إخفاء ارتكاب الجريمة حتى لا يتم تقليده من جانب الآخرين من ناحية، ولأن في الإبلاغ إهداراً لثقة المتعاملين مع البنوك والمؤسسات المالية من ناحية ثانية، كما أن الإبلاغ قد يسمح لسلطات الضابطة العدلية بالاطلاع على معلومات اسمية لم يقم المجني عليه بالإخطار عنها قبل جمعها من ناحية ثالثة[5].

---

[1] الصغير، 2001م، ص114.

[2] الصغير، 2001، ص116.

[3] مصطفى، 2010، ص47.

[4] فرغلي، و المسماري، 2007، ص10-11.

[5] الصغير، 2001، ص116.

ومن أجل تفعيل عملية الإبلاغ عن الجريمة المعلوماتية، ومن ثم الإسهام بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها، أوصى المؤتمر الدولي الخامس عشر الذي عقد في "ريو دي جانيرو" بالبرازيل في الفترة من 4 – 9 /11/ 1994، بضرورة تشجيع المجني عليهم في هذه الجرائم على الإبلاغ عنها فور وقوعها، وهذا بهدف تخفيض الرقم الأسود للجرائم المعلوماتية في الفضاء الافتراضي[1].

كما أن ثمة مطالبات في الولايات المتحدة الأمريكية بأن تتضمن القوانين المتعلقة بالجرائم المعلوماتية، نصوصاً تلزم موظفي الجهة المجني عليها – أياً كانت – بضرورة الإبلاغ عما يصل إلى علمهم من جرائم تتعلق بهذا المجال، وتقرير جزاءات على الإخلال بذلك الالتزام، إلا أنه لدى عرض هذا الاقتراح على "لجنة خبراء مجلس أوربا" قوبل بالرفض لسبب قانوني مؤداه أن المجني عليه – وهو الشركة التي ارتكبت في حقها جريمة إلكترونية – سوف تصبح متهمة أو جانية بعد أن كانت مجنياً عليها، ولذلك وردت اقتراحات بديلة قد تكون مقبولة، منها الالتزام بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات، وكذلك إصدار شهادة "أمن خاصة" تمنح بعد مراجعة وتدقيق من قبل هيئة خاصة من المراجعين، ويتعين على هذه الهيئة إبلاغ الشرطة بما تكشفه من جرائم[2].

ثالثاً: صعوبات متعلقة بضعف التعاون الدولي في مكافحة الجريمة المعلوماتية:

تتعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بوساطة شبكة الاتصال عن بُعد، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثاً عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية، إذ إن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة[3].

لذلك نادى بعض الفقه بضرورة إنشاء وحدات خاصة بمكافحة الجريمة المعلوماتية بوساطة الحاسوب والإنترنت أسوة بجهات البحث الجنائي الوطنية والدولية – الإنتربول –لإثبات الجريمة عند وقوعها وتحديد أدلتها

---

[1] مصطفى، 2010، ص48.

[2] Hans G. Nilsson, 1993، p. 124.

نقلاً عن: رستم، 2004، ص437.

[3] الصغير،2001، ص115.

وفاعليها، وهو ما يعني كذلك إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات الخاصة في الإنترنت، وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبيها وسبل مكافحتها[1].

وبالرغم من المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية، إلا أن هناك معوقات تحول دون ذلك، وتجعله صعب المنال، وأهم هذه المعوقات:

أ- عدم الاتفاق على صور محددة للنشاط الإجرامي:

إذ إن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى "بإساءة استخدام نظم المعلومات الواجب اتباعها"، كذلك ليس هناك تعريف محدد للنشاط المفروض أن يُتفق على تجريمه، وذلك نتاج طبيعي للتشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي، ومن ثم الجريمة المعلوماتية[2].

ولعل عدم الاتفاق بين الأنظمة القانونية المختلفة على صورة موحدة للسلوك الإجرامي في الجريمة يغري قراصنة الحاسوب على تنظيم أنفسهم وارتكاب جرائمهم من دون تقيد بالحدود الجغرافية[3].

ب- عدم وجود تنسيق بين الدول فيما يتعلق بالأصول الجزائية المتبعة في شأن الجريمة المعلوماتية بين الدول المختلفة:

إن عدم التنسيق وبشكل خاص فيما يتعلق بأعمال الاستدلال أو التحقيق، ولاسيما أن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة، عن طريق الضبط أو التفتيش في نظام معلوماتي معين، أمر غاية في الصعوبة، فضلاً عن الصعوبة الفنية في الحصول على الدليل ذاته[4].

---

[1] حجازي، 2007.أ، ص187.

[2] حجازي، 2007.أ، ص188.

[3] حجازي، 2007.أ، ص189.

[4] حجازي، 2007.أ، ص190.

فمثلاً في غالب الأحيان، يتعذر الحصول على الأدلة من أجهزة الحاسوب الموجودة في دولة أخرى حتى في حال وجود إجراءات دولية تسهل تبادل الأدلة الإلكترونية، فإن معظم هذه الإجراءات معقدة، وهي ليست عملية إلا بالنسبة إلى الجرائم الخطيرة[1].

جـ- عدم وجود معاهدات ثنائية أو جماعية بين الدول للتعاون في مجال هذه الجرائم:

إن عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرائم، وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة، في ظل التقدم السريع لنظم وبرامج الحاسوب والإنترنت، ومن ثم تطور الجريمة المعلوماتية بالسرعة ذاتها على نحو يؤدي إلى إرباك المشرع وسلطات الأمن في الدول، ومن ثم يظهر الأثر السلبي في التعاون الدولي[2].

ولحل ذلك لابد من صدور قانون دولي في صورة اتفاقية دولية، يمثل الحد الأدنى لمتطلبات كل دولة حتى يتم مواجهة ظاهرة الجريمة في فضاء الإنترنت، هذا من ناحية، ومن ناحية أخرى من الممكن تعزيز العلاقات الدولية الثنائية بين كل دولتين باتفاقية ثنائية أو ثلاثية في مجال التعاون الدولي في هذه الجريمة، ويكون هدف هذه الاتفاقيات:

1- التعرف على مكان الجناة وتحديده.

2- تقديم الوثائق المثبتة للجريمة وتبادلها.

3- الحصول على الأدلة والقرائن والأنظمة التي يجب مراعاتها.

4- تنفيذ طلبات البحث والتحري والضبط.

5- المساعدة فيما يتعلق بإجراءات التحقيق الجنائي[3].

---

[1] عبد المطلب، 2006، ص121.

[2] حجازي، 2007.أ، ص190.

[3] حجازي، 2007.أ، ص249 - 250.

د- مشكلة الاختصاص في الجرائم المعلوماتية:

تُعد مشكلة الاختصاص في الجرائم المعلوماتية من المشكلات التي تعرقل الحصول على الدليل فيها، ذلك أن هذه الجرائم من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع جريمة الحاسوب في مكان معين، وتنتج آثارها في مقاطعة أخرى داخل الدولة أو خارجها، ومن هنا تنشأ مشكلة البحث عن الأدلة على شبكة الإنترنت[1].

ونحن نرى أنه لحل مشكلة الاختصاص في داخل إقليم الدولة فإنها تحل على أساس مكان القبض على المتهم أو محل إقامته أو مكان وقوع الجريمة، فأي مكان من الأماكن المذكورة، ينعقد الاختصاص القضائي لسلطات التحقيق والمحاكمة فيه بالجريمة المعلوماتية، وذلك بتطبيق نص المادة (3) الفقرة (1) من قانون أصول المحاكمات الجزائية السوري لعام 1950م الذي جاء فيه: " تقام دعوى الحق العام على المدعى عليه أمام المرجع القضائي المختص التابع له مكان وقوع الجريمة أو موطن المدعى عليه أو مكان إلقاء القبض عليه".

ولكن على المستوى الدولي فإن الأمر في حاجة إلى عقد اتفاقيات دولية ثنائية أو جماعية وتفعيل الإنابات القضائية.

كما نرى أنه لحل مشكلة ضعف التعاون الدولي في مجال الجريمة المعلوماتية ولا سيما في مجال تبادل الأدلة الإلكترونية، فإن الحاجة ماسة إلى إصدار تشريعات جزائية أكثر مرونة تسمح بسرعة التعاون المثمر في تبادل الأدلة الإلكترونية.

---

[1] حجازي، 2007.أ، ص191.

الفرع الثاني

صعوبات متعلقة بالدليل الإلكتروني

هنالك صعوبات كثيرة متعلقة بالدليل الإلكتروني، وهي أولاً، عدم مرئية الدليل الإلكتروني، وثانياً، الحجم الكبير للبيانات التي يوجد فيها الدليل الإلكتروني، وثالثاً، سهولة إخفاء الدليل الإلكتروني، ورابعاً، أن الدليل الإلكتروني دليل ظرفي، وخامساً سهولة التلاعب بالدليل الإلكتروني.

أولاً: عدم مرئية الدليل الإلكتروني:

الأدلة الإلكترونية تتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحواسيب (Hard ware)، واستخدام نظم برامجية حاسوبية (Soft ware) [1].

فليس للدليل الإلكتروني طبيعة مادية ملموسة كما هو الحال في الأدلة التقليدية، فالأجهزة التقنية لا تفرز سكيناً عليها بصمات القاتل، أو مالاً يمكن ضبطه مع السارق في جريمة السرقة وغير ذلك، فكل ما تنتجه التقنية هو عبارة عن نبضات إلكترونية يمكن أن تدل في مجموعها على أنماط السلوك الإنساني[2].

أضف إلى ذلك أن ترجمة الدليل الإلكتروني وإخراجه في شكل مادي ملموس لا يعني أن هذا التجميع يعد دليلاً، بل إن هذه العملية تعد عملية نقل لتلك البيانات من مجالها إلى شكل ملموس يمكن الاستدلال به على معلومات معينة[3].

والواقع أن هذه الطبيعة غير المرئية للدليل الإلكتروني تلقي بظلالها على أجهزة العدالة الجزائية التي تتعامل مع هذه الجرائم المستحدثة، لأن غياب الدليل المرئي يشكّل عقبة كبيرة أمام كشفها[4].

ثانياً: الحجم الكبير للبيانات التي يوجد فيها الدليل الإلكتروني:

يحتوي القرص الصلب مثلاً على حجم كبير من البيانات والمعلومات غير المرتبة، ولكن ما يتعلق بالجريمة قد يشكل جزءاً صغيراً فقط من هذه المعلومات، ويمكن تشبيه حجم المعلومات هذا بموجات الراديو

---

[1] فرغلي، و المسماري، ص14.

[2] الخن، 2012م، ص113.

[3] عريقات، (د.ت)، ص18.

[4] الخن، 2012، ص113.

الموجودة في الهواء، والتي تحتوي على بيانات متشابكة، الأمر الذي يجعل من الصعوبة بمكان معرفة الإشارة المطلوبة وترجمتها إلى بيانات مفهومة، فالوصول إلى الدليل الإلكتروني المطلوب يشكّل تحدياً أمام الخبير المعلوماتي[1].

ثالثاً: سهولة إخفاء الدليل الإلكتروني:

تفرض عملية إخفاء المعلومات تحديات مماثلة لخبراء الأدلة الإلكترونية، وهم الخبراء التقنيون، مما يجعل الأمر صعباً أو مستحيلاً للعثور على البيانات الإلكترونية، فهذه العملية من شأنها خلق عدة مشكلات تتعلق بالدليل الإلكتروني، ومن شأنها التأثير في سير التحقيق في سبيل الحصول على هذا الدليل.

فإخفاء المعلومات الضرورية يعني إخفاء أدلة جوهرية في القضية المراد إثباتها، وهناك عدة حالات لإخفاء المعلومات، إذ يمكن أن يجمع بين إخفاء الهوية وإخفاء المعلومات، أو البيانات المخفية لخلق نظام ملفات آمن تجعل عملية استعادة الأدلة وإعادة تركيبها أمراً في غاية الصعوبة، وفي غاية التعقيد بسبب هذا الأمر[2].

ونظراً إلى أن الحاسوب هو منهج متحرك تتشابك بموجبه كافة المعلومات وكافة طرق المعالجة الواحدة مع الأخرى، فإنه من السهل أن يوضع فيه برنامج تكون مهمته تعديل الإجراءات الضرورية لعمل هذا الذكاء الصناعي، والذي يهدف في النهاية إلى محو كل الدعامات التي توجد في الجهاز. يضاف إلى ذلك أن التخزين الإلكتروني للمعطيات يجعلها غير مرئية وغير مفهومه بالعين المجردة، كما أنه من السهل محو الدليل في زمن قصير، وهذا ما يعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب[3].

كما أنه من المتعارف عليه أن إغلاق جهاز الحاسوب، يعني أن هنالك عدداً كبيراً من الأدلة لا يمكن استرجاعه، وهذا في حالة عدم تخزينها في الذاكرة، ومنها المساس بسلامة الأدلة الموجودة، ولهذا لا يجب غلق الحاسوب فوراً حتى لا يتم مسح الأدلة، كما أن انقطاع التيار الكهربائي المفاجئ عن جهاز الحاسوب يسبب الكثير من المشكلات التي تتمثل في محو المعلومات من الذاكرة، بمعنى فقدان كافة العمليات التي كان يتم

---

[1] الخن، 2012، ص113.

[2] عبد المطلب، 2006، ص122 – 123.

[3] الصغير، 2001، ص114 – 115.

تشغيلها، وأنظمة الملفات الثابتة، فغلق أي نظام قبل الحصول على البيانات في الذاكرة الفعلية يمكن أن يؤدي إلى فقد الأدلة الجوهرية، كما أن هذا الغلق المفاجئ من شأنه أن يؤدي إلى فقدان بيانات مهمة [1].

وهكذا نجد أن انعدام الدليل المرئي والواضح عقبة كبيرة أمام كشف الجرائم، إلا أن هناك من يرى أنه يوجد بعض البرامج والأنظمة التي يمكنها مواجهة هذه المشكلة التي تشكل عائقاً أمام الحصول على الدليل الإلكتروني[2].

رابعاً: الدليل الإلكتروني دليل ظرفي:

الدليل الإلكتروني هو عادة دليل ظرفي، فمعرفة عنوان الإنترنت IP مثلاً يشير إلى الحاسوب الذي ارتكبت الجريمة بواسطته فقط، من دون أن يحدّد مرتكب الجريمة بالذات، الأمر الذي يجعل من الصعوبة بمكان، نسبة النشاط الجرمي إلى شخص ما، ما لم يتم القيام بعدد من التحقيقات للتأكد من ذلك.

ففي إحدى القضايا التي عرضت على المحاكم الأمريكية، نازع المدعى عليه في جميع الأدلة التي وجدت على حاسوبه، لأن المحققين لم يستطيعوا إثبات أنه هو الشخص الذي قام بالنشاطات غير الشرعية على الإنترنت[3].

خامساً: سهولة التلاعب بالدليل الإلكتروني:

إن خاصية صعوبة التخلص من الدليل الإلكتروني قد تقابلها مسألة أخرى ذات علاقة بمسألة التطوير المستمر في تكنولوجيا المعلومات، وهي أن هذا الدليل نتيجة لمرونته وضعفه، فإنه يسهل إتلافه أو فقدانه أو كما يطلق عليه "**Spoliation of Evidence**"، بمعنى إمكانية التخلص منه[4].

فعلى الرغم من تميز الدليل الإلكتروني بصعوبة التخلص منه إلا أن هنالك سهولة بالتلاعب فيه، سواء أكان تعديلاً أو إتلافاً أو إدراجاً في المستندات أو البيانات الرقمية الأخرى[5].

---

[1] هلال، 2015، ص70.

[2] عبد المطلب، 2006، ص122 – 123.

[3] الخن، 2012، ص114.

[4] بن يونس، 2006م، ص11.

[5] عريقات، (د.ت)، ص18.

كما يُخشى كثيراً من التعسف واصطناع الأدلة، إذ لا توجد وسيلة فعالة إلى الآن للتأكد من أن البيانات الموجودة على الأجهزة هي تلك التي تم ضبطها، إذ يمكن بالوسائل العلمية والتقنيات الحديثة تغيير وتعديل وتبديل ومحو البيانات الموجودة على أجهزة الحاسوب[1].

وفي الحقيقة فإن مسألة إتلاف الدليل الإلكتروني هي في الواقع ليست مسألة حقيقية، وإنما الحقيقة أن مسألة إمكانية إتلاف الدليل الإلكتروني تعني أن هناك قصوراً في القدرات التكنولوجية لدى مؤسسات العدالة الجزائية، مما ينبغي معه وجوب العمل على التطوير المستمر لنظم العدالة الجزائية، بالإضافة إلى تطوير قدرات القائمين على مهامها وأعمالها[2].

نستنتج مما سبق أن هنالك عدة مشكلات أقل ما يقال عنها إنها صعبة، وتعرقل عملية جمع واستخراج الدليل الإلكتروني، وهذا يرجع إلى لطبيعة الخاصة للجريمة المعلوماتية، بالإضافة إلى طبيعة الدليل الإلكتروني في حد ذاته، وكذلك شدة الذكاء التي يتميز به المجرمون الذين يقترفون هذا النوع من الجرائم، كما أن هناك مشكلات تتعلق بالحاسوب وطبيعته الخاصة والمعقدة التي تحتاج إلى خبرة فنية وتقنية عالية من الأشخاص الذين يتولون مهمة جمع الدليل الإلكتروني، ومشكلات تتعلق بالأشخاص المرتكبين لهذه الجرائم وقدرتهم الفائقة في إخفاء هويتهم من جهة، وإخفاء المعلومات من جهة أخرى.

لهذا لابد من توافر تقنيين ذوي كفاءة عالية لمواجهة هذه الجرائم المستحدثة، وهؤلاء المجرمين الأذكياء، حتى تسهل عملية جمع الأدلة الإلكترونية[3].

---

[1] رمضان، 2000، ص72.

[2] بن يونس، 2006م. ص11.

[3] هلال، 2015، ص71 – 72.

الفرع الثالث

صعوبات متعلقة بأسباب متعددة

هنالك صعوبات أخرى تواجه الحصول على الدليل الإلكتروني، وترد إلى جملة من الأسباب، وهي أولاً، نقص خبرة أجهزة العدالة الجزائية، وثانياً، صعوبات فنية.

أولاً: نقص خبرة أجهزة العدالة الجزائية:

من الصعوبات التي تواجه عملية استخلاص الدليل الإلكتروني نقص الخبرة لدى رجال الضابطة العدلية، وكذلك لدى أجهزة العدالة الجزائية ممثلة في سلطة التحقيق والمحاكمة، وذلك فيما يتعلق بثقافة الحاسوب والإلمام بعناصر الجرائم المعلوماتية وكيفية التعامل معها، وذلك على الأقل في البلدان العربية، نظراً إلى أن تجربة الاعتماد على الحاسوب وتقنياته وانتشارها في هذه البلدان جاء متأخراً عن أوربا وكندا والولايات المتحدة الأمريكية.

وبالتالي فإنَّ نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدِّي إلى ضياع الدليل بل تدميره أحياناً[1] ذلك أن كشف الجرائم المعلوماتية وتحديد فاعلها ومحاكمتهم يستلزم توافر مهارات خاصة للقائمين على التحقيق والمحاكمة تسمح لهم بتفهم نظام تشغيل الحواسيب وأساليب التلاعب التي تستخدم في ارتكاب الجريمة بوساطة هذا الأخير، فنقص الخبرة في هذا المجال يحول دون كشف الجريمة وضبط مرتكبيها[2]. بل إن المحقق قد يدمر الدليل عن خطأ منه أو إهمال، أو بالتعامل بخشونة مع مختلف الوسائط التي تتضمن الدليل الإلكتروني كالأقراص المرنة أو غيرها[3].

ومن أجل حل هذه الصعوبة فإنَّ إعداد رجال الضابطة العدلية وقضاة التحقيق والحكم، للبحث عن أدلة الإثبات في ميدان الجرائم المعلوماتية، يكتسب أهمية بالغة؛ إذ لا بد لهم من الدراية الكافية بطبيعة هذا النوع من الجرائم، الذي يتسم الكشف عنه وإثباته بصعوبات بالغة، وفي عالم «المعلوماتية وشبكات الحاسوب» القائم على تقنية الاتصالات والتوصيلات والوسائط الإلكترونية، لا تستطيع سلطة البحث والتحري والتحقيق تطبيق الإجراءات

---

[1] الطوالبة، 2009.

[2] الصغير، 2001، ص115.

[3] مصطفى، 2010، ص49.

التقليدية على غالبية جرائم تقنية المعلومات. من أجل ذلك لا بد من تدريب وتكوين رجال الضابطة العدلية والتحقيق والقضاة المختصين بجرائم تقنية المعلومات فيما يتعلق بالأساليب الفنية المستخدمة في ارتكاب الجريمة، وفيما يتعلق بالكشف عنها، والقرائن والدلائل والأدلة المستحدثة في مجال إثباتها، وكيفية معاينتها والتحفظ عليها وفحصها فنياً، مع ضرورة تدريب القضاة على معالجة هذا النوع من القضايا لتمكينهم من الفصل فيها، لذا لا بد من خلق وحدات خاصة تكون مهمتها الأساسية مراقبة وتتبع الشبكة عن طريق الإبحار فيها، ومثل هذه المراقبة السابقة قد تعطي نتائج مهمة على مستوى الحد من الجريمة قبل ارتكابها عن طريق الوقاية منها[1].

كما ينبغي الأخذ بالأساليب المستحدثة في التدريب مثل التدريب عن بُعد، والمؤتمرات المباشرة باستخدام الواقع الافتراضي، وأخيراً فإنه من الضروري أن يكون التدريب ذا بُعد دولي، والسبب في ذلك يعود إلى الطبيعة الخاصة للجريمة المعلوماتية وخصوصاً في جرائم الشبكة العالمية أو جرائم الإنترنيت، لذلك فإن تبادل الخبرات بين العاملين في هذا المجال أمر ضروري لفاعلية التدريب[2].

ثانياً: صعوبات فنية:

هنالك بعض الصعوبات الفنية التي قد تمثل عائقاً أمام الجهة المختصة بجمع الأدلة، ويمكن إجمال هذه الصعوبات فيما يأتي:

أ- وجود جهاز مزود بنظام حماية:

يتم البحث عن الدليل الإلكتروني في وسط افتراضي يحتويه الجهاز الذي ارتكبت به أو ضده الجريمة محل البحث، وغالباً ما يكون هذا الجهاز مزوداً بنظام حماية، بحيث لا يمكن تشغيله إلا باستعمال كلمة مرور معلومة لدى مستعمل ذلك الجهاز، وهو ما قد يحول دون الحصول على المعلومات من خلاله، غير أن التقنية الحديثة قد أسهمت في تفادي هذه المشكلة، إذ بالإمكان الاستعانة بما يسمى قرص التشغيل الذي يُمكّن من تشغيل الجهاز حتى لو كان مزوداً بنظام حماية[3].

---

[1] د. فتح الله، 2012، ص26 – 28.

[2] عبد المطلب، 2006، ص203.

[3] الجملي، 2015، ص58.

ب-انقطاع التيار الكهربائي:

يتم عادة جمع الدليل الإلكتروني من جداول الحالة التشغيلية للبروتوكولات والاتصالات، والمشكلة أن هذه الجداول تظل متاحة لمدة محدودة، إذ تمحى بمجرد فصل التيار الكهربائي عن الجهاز، وهذا من شأنه الحؤول دون الحصول عليها، إلا أنه يمكن التغلب على هذه المشكلة من خلال اتباع أسلوب القص واللصق ووضع تلك الجداول في ملف خاص لجمع الأدلة قبل غلق الجهاز، وهذا يقتضي بالضرورة أن يكون المحقق قد أدرك تلك المعلومات قبل فصل التيار الكهربائي عنها[1].

وهكذا نجد مما تقدم أن صعوبة استخلاص الدليل الإلكتروني ترجع إلى صعوبات متعددة منها ما هو متعلق بالدليل الإلكتروني ذاته مثل إخفاء الدليل وعدم رؤيته، فضلاً عن أن الجريمة المعلوماتية في الغالب لا تترك آثاراً، وأخيراً فإن أجهزة العدالة الجنائية قد تعوق الحصول على الدليل الإلكتروني متى انعدمت أو نقصت خبرتها بشأن كيفية استخلاص هذا الدليل.

وأخيراً تحدثنا في هذا المطلب عن صعوبات الحصول على الدليل الإلكتروني، وقسمنا هذه الصعوبات التي تواجه الحصول على هذا الدليل إلى صعوبات متعلقة بالجريمة المعلوماتية، وصعوبات متعلقة بالدليل الإلكتروني، وأخيراً صعوبات مردها أسباب مختلفة.

---

[1] الجملي، 2015، ص58.

المطلب الثاني

عدم قدرة الوسائل التقليدية في إثبات الجريمة المعلوماتية

يثير إثبات الجريمة المعلوماتية، وبالتالي الحصول على الدليل الإلكتروني بوسائل الإثبات التقليدية إشكالات قانونية، وذلك بالنظر إلى طبيعته الخاصة[1]، وهناك من يذهب إلى إن ما يثيره الدليل الإلكتروني من حيث مشروعية الحصول عليه يتركز بشكل أساسي في إجراءات التفتيش للبحث عن هذا الدليل، وذلك يثير إشكاليتين رئيستين:

الأولى: صفة القائم بالتفتيش.

الثانية: مدى مشروعية التفتيش عن الدليل الإلكتروني وضبطه في الوسط الافتراضي.

ومرد هاتين الإشكاليتين يتعلق بإجراء التفتيش الذي يجب أن يمارس من ذي صفة، وهو عضو الضابطة العدلية أو جهة التحقيق حسب الأحوال، فهل لهؤلاء القدرة على تفتيش الوسط الافتراضي وضبط ما سيسفر عنه من أدلة؟[2].

ومن الجدير بالذكر أن صعوبة إثبات الجريمة المعلوماتية، وبالتالي الحصول على الدليل الإلكتروني، لا تقتصر على التفتيش والضبط، بل تشمل الخبرة ومعاينة مسرح الجريمة المعلوماتية، فهي من الإجراءات التي تهدف إلى الحصول على الدليل الإلكتروني أيضاً.

وبناء على ذلك سنقسم هذا المطلب إلى أربعة فروع:

الفرع الأول: الخبرة.

الفرع الثاني: المعاينة.

الفرع الثالث: التفتيش.

الفرع الرابع: الضبط.

---

[1] الحمداني، 2016م، ص235.

[2] الحلبي، 2011، ص239.

الفرع الأول

الخبرة

تُعد الخبرة وسيلة لجمع الأدلة، والأصل في الخبرة أنها من إجراءات التحقيق الابتدائي، لأنها تهدف إلى الوصول إلى الحقيقة، وبالتالي فإن انتداب الخبير يُعد إجراءً من إجراءات التحقيق، ولابد من التمييز بين تقرير الخبير الذي يعد من الأدلة وإجراء ندب الخبير، الذي يُعد من إجراءات جمع الأدلة، ولبحث الخبرة الإلكترونية لابد من دراسة مفهوم الخبرة الإلكترونية أولاً، ومشروعية الخبرة الإلكترونية ثانياً.

أولاً: مفهوم الخبرة:

إن بحث مفهوم الخبرة يقتضي منا بحث تعريف الخبرة، وكذلك آلية عمل الخبير للحصول على الدليل الإلكتروني، لذلك لابد من دراسة:

أولاً- تعريف الخبرة:

تتضمن الخبرة إبداء رأي علمي أو فني من شخص صاحب اختصاص في شأن واقعة لها أهمية في الدعوى الجزائية، ولا يستطيع القاضي البت فيها لأنه لا يتوافر لديه مثل هذا الاختصاص[1].

ثانياً- آلية عمل الخبير للحصول على الدليل الإلكتروني:

يجب على خبير الأدلة الإلكترونية التعّرف أولاً على الدليل عن طريق تحديد نوع المعلومات المخزنة، ثمّ موقع تخزينها، وكيفية تخزينها، حتى يتمكن من اختيار الطريقة التقنية المناسبة لاستخراجها، وبعد استخراج الخبير الدليل الإلكتروني يلتزم بالحفاظ عليه بتفادي إحداث أي تغيير في البيانات التي يحتويها، لأنّ العكس قد يفقد الدليل قيمته القانونية، وأخيراً يقوم الخبير بتحليل الدليل بتفسير البيانات بطريقة واضحة ومفهومة[2].

---

[1] القدسي، 2011م، ص142.

[2] مليكة، 2013، ص176.

كما يتوجب على الخبير الإلكتروني أن يوثق جميع مراحل عملية البحث، بحيث يشير إلى زمان البحث ومكان المعلومة وكيفية الحصول عليها، وأن يستخدم البرمجيات التي تحافظ على مواقع الويبّ التي عمل فيها؛ لأنه من المعروف أن المعلومات تتغير على الإنترنت من لحظة إلى أخرى[1].

ولابد من جعل ندب الخبرة في الجريمة المعلوماتية وجوبياً من أجل الحصول على الدليل الإلكتروني، نظراً إلى أن طبيعة هذه الجريمة تستلزم التعامل معها بطريقة حرَّفية أو فنية تفوق قدرات فريق التحقيق غير المؤهل، وذلك عن طريق تعديل قوانين الأصول الجزائية التي تجعل من ندب الخبراء أمراً جوازياً.

ويلاحظ أن للخبرة أهمية خاصة في الجريمة المعلوماتية لأن الحواسيب وشبكات الاتصال تحتوي على أنواع ونماذج متعددة، كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة، كما أن التطورات في مجالها سريعة ومتلاحقة إلى درجة قد يصعب معها على المتخصص تتبعها واستيعابها[2]. كما تتجلى أهمية الخبرة المعلوماتية في كونها وسيلة من وسائل الوصول إلى الدليل الإلكتروني في أنها تكشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية[3].

فتشكيل فريق خبراء من أم مطلوب ولا بد منه، وله أهمية خاصة نظراً إلى الطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية عن غيرها من الجرائم، وذلك لأن هذه الجرائم مرتبطة بمسائل فنية وعلمية بحتة، لذلك يصبح لزاماً على القائم بالتحقيق الاستعانة بالخبراء والمختصين، لأن تصدي المحقق لفحص شيء وإبداء الرأي فيه من دون أن تتوافر لديه المعرفة اللازمة يجعل قراره معيباً ويضر بمصلحة التحقيق، ويعوق الوصول إلى الحقيقة، وكل هذا يصب في أهمية التقارير التي يُنجزها خبراء تقنية المعلومات في مجال الجرائم المعلوماتية، ويُعطيها منزلة متميزة من حيث الإلزام[4].

ويمكن إجمال المسائل التي يحتاج رجل الضابطة العدلية أو قاضي التحقيق في وصفها إلى خبير معلوماتي، كما يأتي:

---

[1] الخن، 2012، ص115-116.

[2] حجازي، 2007.ب، ص167.

[3] العدواني، 2015م، ص87.

[4] مطر، 2018م، ص26-27.

1- وصف تركيب الحاسوب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها، بالإضافة إلى الأجهزة الطرفية الملحقة به، وكلمات المرور أو السر، ونظام التشفير وغيرها من الأمور المماثلة.

2- وصف طبيعة بيئة الحاسوب أو الشبكة من حيث التنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية للمعلومات، ونمط وسائط الاتصالات وتردد موجات البث وأمكنة اختراقها.

3- وصف الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها.

كذلك يحتاج رجل الضابطة العدلية إلى معونة الخبير المعلوماتي لبيان كيفية القيام بالآتي:

1- القيام عند الاقتضاء بعزل النظام المعلوماتي من دون إتلاف الأدلة، أو تدميرها أو إلحاق ضرر بالأجهزة.

2- كيفية نقل أدلة الإثبات إلى أوعية ملائمة بغير أن يصيبها تلف.

3- كيفية تجسيد الأدلة في صورة مادية بنقلها إذا أمكن إلى أوعية ورقية، بحيث يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق لذلك المسجل على الحاسوب أو النظام أو الشبكة أو الدعامة الممغنطة[1].

الفرع الثاني

المعاينة

يقتضي بيان مفهوم المعاينة تعريفها ثم بيان مدى صلاحية مسرح الجريمة الإلكتروني للمعاينة، وأخيراً بيان الآلية المتبعة فيها للحصول على الدليل الإلكتروني.

أولاً: مفهوم المعاينة:

يقصد بالمعاينة: "إثبات حالة الأماكن والأشياء والأشخاص، وكل ما يفيد في كشف الحقيقة، والمعاينة بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو إلى أي محل آخر توجد به أشياء أو آثار يرى المحقق أن لها صلة

[1] حجازي، 2007.ب، ص169-170

بالجريمة، غير أن انتقال المحقق قد يكون لغرض آخر غير المعاينة، كما في انتقال المحقق إلى مسكن المتهم أو غيره لتفتيش أو لسماع الشهود"[1].

فالمعاينة هي عبارة عن إعادة تركيب الجريمة وربط مشاهدها، وإعادة تسلسل إحداثها.

وإذا كانت المعاينة تتم بالانتقال إلى محل الواقعة الإجرامية كقاعدة عامة إجرائية مقررة في هذا الشأن، إلا أنه في إطار جرائم الإنترنت، فإن الانتقال يُعد من الموضوعات الجديدة، وذلك أن مسألة الانتقال هذه لا تكون بالضرورة عبر العالم المادي، وإنما يجب أن تكون بالضرورة عبر العالم الافتراضي، فيستطيع عضو سلطة التحقيق أن يقوم بالمعاينة من مكتبه في المحكمة من خلال الحاسوب الخاص به، كما يمكن أن يلجأ إلى مقهى الإنترنت، أو أن ينتقل إلى مقر مزود الخدمة الذي يعد أفضل مكان لإجراء المعاينة، ذلك أنه في كل الأحوال يلزم أن يقوم المحقق بالمعاينة من خلال حاسوب أو حاسوب خادم، ومن ثم فإن مشكلة الانتقال المادي إلى محل ارتكاب الواقعة الإجرامية لا تشكل عائقاً أمام عضو سلطة التحقيق، وإنما المشكلة تكون من خلال الانتقال إلى العالم الافتراضي، إذ يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تمنع زوال أثر الجريمة، ولهذا يجب أن يعجل بإجراء المعاينة خشية ضياع الأدلة[2].

ثانياً- مدى صلاحية مسرح الجريمة الإلكتروني للمعاينة:

لكي نقرر مدى صلاحية مسرح الجريمة الإلكتروني للمعاينة، فإنه يجب التفرقة بين حالتين:

1- الحالة الأولى: الجرائم الواقعة على المكونات المادية للحاسب:

ومن أمثلة هذه الجرائم تلك الواقعة على أشرطة الحاسوب والكابلات الخاصة به، وشاشة العرض الملحقة به، ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسوس، وسرقة الأقراص المرنة بما فيها من معلومات[3].

---

[1] رمضان، 1985، ص371.

[2] مكاري، 2009م، ص125.

[3] عفيفي، 2000م، ص336.

وليس هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل أعضاء الضابطة العدلية، والتحفظ على الأشياء التي تُعد أدلة مادية على ارتكاب الجريمة ونسبتها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل ما استعمل في ارتكاب الجريمة، والتحفظ عليها، والسبب في سهولة المعاينة في هذه الحالة، أنها تتم على مكونات مادية محسوسة كانت محلاً للجريمة أو تخلفت عنها[1].

2- الحالة الثانية: الجرائم المعلوماتية الواقعة على المكونات غير المادية أو بوساطتها:

وفي مقدمة هذه الجرائم، تأتي تلك الواقعة على برامج الحاسوب أو بياناته أو تتم بوساطتها، وكذلك الجرائم التي تتم بطريق الإنترنت، ومنها كذلك جرائم التزوير المعلوماتي والتخريب الذي يتم بطريق الفيروس المعلوماتي[2].

وفي هذه الفروض تظهر عدة صعوبات تحول دون فاعلية المعاينة أو فائدتها، يمكن تلخيصها فيما يأتي:

- الصعوبة الأولى تتمثل في ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلوماتية بصفة عامة، وبرامج الحاسوب وبياناته بصفة خاصة.
- الصعوبة الثانية تتمثل في الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال مدة من زمن وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي مدة طويلة نسبياً، الأمر الذي يعطي الفرصة للجاني أو للآخرين لكي يغيروا أو يتلفوا أو يعبثوا بالآثار المادية للجريمة إن وجدت، الأمر الذي يورث الشك بدلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية [3].
- الصعوبة الثالثة تتمثل في مشكلة زوال الدليل الإلكتروني الذي يمكن تعديله أو تغييره أو محوه في بضع ثوانٍ[4].

---

[1] حجازي، 2007.ب، ص182-183.

[2] حجازي، 2007.ب، ص183.

[3] حجازي، 2002، ص 60-61.

[4] مكاري، 2009، ص125.

ثالثاً- آلية معاينة الدليل الإلكتروني:

هناك من يرى[1] أن الانتقال والمعاينة في الجرائم المعلوماتية تستوجب على القائم بالتحقيق أن يتعامل مع مكان وقوعها على أنه يتكون من مكانين أحدهما تقليدي والآخر افتراضي، والأول مثل غيره من أماكن وقوع الجريمة التقليدية يتكون بشكل أساسي من مكونات مادية ملموسة مثل أجهزة الحاسوب وشاشاتها وملحقاتها، والذي يمكن أن يترك الجاني فيه الكثير من الآثار المادية كبصمات أصابعه أو بعضاً من مقتنياته الشخصية، وهو بصورة عامة يقع خارج البيئة الإلكترونية وتنطبق عليه كافة القواعد المتبعة في معاينة مكان وقوع الجريمة التقليدية، أما الثاني فإنه يقع داخل البيئة الإلكترونية ويتكون من بيانات رقمية (إلكترونية) موجودة في داخل حواسيب أو على شبكة الإنترنت وهو الذي يثير الجانب الأكبر من المشكلات في مجال التحقيق في الجرائم المعلوماتية.

وبالتالي يجب على أعضاء الضابطة العدلية أن يأخذوا في حسبانهم مجموعة من الضوابط خلال معاينة مسرح الجريمة المعلوماتية من أجل الحصول على الدليل الإلكتروني، وتقسم هذه الضوابط إلى:

1- ضوابط قبل التحرك إلى مسرح الجريمة المعلوماتية:

- وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها.
- وجود خريطة توضح الموقع الذي ستتم معاينته، وتفاصيل المبنى أو الطابق موضوع الإخبار، وعدد الأجهزة والخزائن والملفات، ويحدد ذلك من خلال مصادر سرية لجهات الأمن.
- تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية، حتى يتم تحديد كيفية التعامل معها فنياً قبل المعاينة، سواء من حيث الضبط أو التأمين أو حفظ الأوراق والمستندات المتداولة.
- تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة، سواء كانت أجهزة أو برامج صعبة أو لينة.
- إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.

---

[1] خلف، 2016، ص19 - 20.

- إخطار الفريق الذي سيتولى المعاينة، قبل تمامها بوقت كافٍ حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.
- تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حدة، وذلك حتى لا تتداخل الاختصاصات.
- إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكلف بتنفيذها على الوجه الأكمل.
- أن تتم كل هذه الإجراءات وفق مبدأ المشروعية، وفي إطار ما تنص عليه القوانين الجزائية.
- تأمين عدم انقطاع التيار الكهربائي، لأن معاينة الأجهزة وما فيها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي[1].

2- ضوابط في أثناء معاينة مسرح الجريمة المعلوماتية:

هنالك ضوابط يتعين أخذها في الحسبان عند معاينة مسرح الجريمة المعلوماتية، ومن أهمها:

- تحديد أجهزة الحاسوب الموجودة في مكان المعاينة، وتحديد مواقعها بأسرع فرصة ممكنة، وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملف (File server)، وذلك لتعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها[2]، وكذلك إثبات الحالة التي تكون عليها توصيلات وكابلات الحاسوب والمتصلة بمكونات النظام[3].
- فصل التيار الكهربائي من مكان خارج الموقع قبل دخوله، فهذا الإجراء يمنع المستخدم من التلاعب في المعلومات أو محوها، وإن كان لذلك أثره في فقد المعلومات المخزنة في الذاكرة العشوائية لأجهزة الحواسيب، وأيضاً فصل خطوط الهاتف خشية استعمال مودم في جهاز المعالجة الآلية للمعلومات المراد ضبطها[4].

---

[1] حجازي، 2007.أ، ص144 - 145.

[2] خلف، 2016، ص18 - 19.

[3] فتح الله، 2012، ص29.

[4] الصغير، 2001، ص120.

- فصل خطوط الهاتف، حتى لا يسيء الجاني استعمالها كما في حالة التيار الكهربائي، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعمليات الاستدلالات لأنهم قد يسيؤون استغلالها، كما في الهاتف العادي لطمس البيانات[1].
- القيام بتصوير الحاسوب الذي ترتكب عن طريقه الجرائم، وما قد يتصل فيه من أجهزة طرفية ومحتوياته وأوضاع المكان الذي يوجد فيه بصفة عامة، مع العناية بتصوير أجزائه الخلفية وملحقاته الأخرى، على أن يراعي تسجيل زمان ومكان وتاريخ التقاط كل صورة[2].
- التأكد من سلامة الحاسوب أو الحاسوب الخادم، بحيث تكون سلطة التحقيق قد احتفظت بما يسمح بالتأكد من دقة مصدر الدليل الإلكتروني[3]، كما ينبغي التأكد من عدم استخدام خاصية تحويل المكالمات، والتأكد من أن رقم الهاتف يخص جهاز الحاسوب المستهدف[4]، فقد لوحظ أنه من الخدع المعتمدة لدى الهاكرز عند الاختراق، أن يتم ذلك بخط هاتف مسروق تم الدخول عليه، عن طريق الدخول إلى شبكة الهاتف ذاتها والتلاعب فيها، وذلك لأجل تضليل أجهزة المراقبة وأجهزة البحث بعد ذلك[5].
- وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخل مسرح الجريمة، بل ورصد الاتصالات الهاتفية من وإلى مكان مسرح الجريمة[6]، إذ من الممكن أن يتدخل الجاني من خلال وحدة طرفية لإتلاف المعلومات المخزنة في الجهاز (الوحدة الأم)[7].
- إبعاد الموظفين عن أجهزة الحاسوب، بعد الحصول منهم على كلمات السر (Pass word) وكذلك الشفرات في حال وجودها، وكذلك إبعادهم عن الأماكن الأخرى التي توجد فيها أجهزة حاسوب أخرى[8].

---

(1) حجازي، 2007.أ، ص238 – 239.
(2) مكاري، 2009، ص126.
(3) مكاري، 2009، ص126.
(4) الصغير، 2001، ص120.
(5) حجازي، 2007.أ، ص239.
(6) خلف، 2016، ص18 – 19.
(7) الصغير، 2001، ص120.
(8) حجازي، 2007.أ، ص239.

– ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها، ومعرفة السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار، وبروتوكولات الاتصال عبر الإنترنت، وإن تعلقت الجريمة بهذه الشبكة التي تعرف اختصاراً بـ (ip)[1] .

– عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسوب من مجالات القوى المغناطيسية – الممرات المغناطيسية – التي قد تتسبب في محو البيانات[2] .

– التحفظ على محتويات سلة المهملات[3]، والتحفظ على مستندات الإدخال والمخرجات الورقية للحاسوب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات[4].

– عدم التسرُّع في نقل أي مادّة معلوماتيّة من مكان وقوع الجريمة خشية إتلاف البيانات المخزنة[5].

ونستنتج أن هنالك اختلافاً كبيراً بين معاينة الجرائم التقليدية التي تتم في العالم المادي، ومعاينة الجرائم المعلوماتية التي تتم في العالم الافتراضي، إذ يقتضي ذلك السرعة في إجراء هذه المعاينة خشية زوال الدليل الإلكتروني والتخصص الدقيق فيمن يقومون بإجراء هذه المعاينة.

الفرع الثالث

التفتيش

يُعد التفتيش من أهم الأعمال التي تقوم بها الضابطة العدلية، لكونه الفيصل بين نجاح جهود التحقيق الجنائي في العثور على دليل يفيد إثبات وقوع الجريمة أو خيبة أملهم في عدم العثور عليه، هذا من ناحية أما من

---

[1] يعرف **(ip)** وهو اختصار كلمة "**internet protocol**" بأنه وسيلة لنقل البيانات من مكان على الإنترنت إلى مكان آخر، أما **(ip adress)** فهو عنوان مكون من أربعة أرقام، ويستخدم لتحديد هوية كل جهاز يتصل بالإنترنت.

[2] حجازي، 2007.أ، ص148.

[3] رستم، 2004 ، ص486.

[4] رستم، 2004، ص487.

[5] فتح الله، 2012، ص29.

ناحية أخرى فقد ينجح رجال التحقيق في العثور على الدليل المفضي إلى وقوع الجريمة، ولكن يفلت الجاني من قبضة العدالة بسبب عدم اتباعهم القواعد والإجراءات الصحيحة الواجب مراعاتها عند القيام بالتفتيش[1].

وتبدو أهمية بحث التفتيش لإثبات الجريمة المعلوماتية وبالتالي الحصول على الدليل الإلكتروني في أن ما يثيره الدليل الإلكتروني من حيث مشروعية الحصول عليه يتركز بشكل أساسي في إجراءات التفتيش للبحث عن هذا الدليل[2].

أولاً: مفهوم التفتيش:

يُعرف التفتيش بشكل عام بأنه: "إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق، وما يفيد في كشف الحقيقة، وبالتالي هو ليس من الإجراءات التي تتبع في كشف الجرائم قبل وقوعها"[3].

ومما يمكن ملاحظته من هذه التعريفات أن التفتيش إجراء من إجراءات التحقيق ووسيلة للبحث عن الأدلة، وبالتالي فهو ليس دليل إثبات في حد ذاته[4].

في حين يُعرف تفتيش نظم الحاسوب والإنترنت بأنه:" الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الإنترنت"[5].

وبالتالي فإن التفتيش في مدلوله القانوني بالنسبة إلى الجرائم المعلوماتية لا يختلف عن مدلوله السائد في فقه الأصول الجزائية، فهو إجراء من إجراءات التحقيق تقوم به سلطة مختصة، لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات ومخرجات، لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة، أي قد تمت بالفعل وتشكل جناية، أو جنحة، والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى الفاعل[6].

وأهم خصائص تفتيش نظم الحاسوب والإنترنت التي تميزه عن غيره من إجراءات التحقيق الأخرى هي:

---

[1] عبد المطلب، 2006، ص183.

[2] الجملي، 2015، ص59.

[3] سرور، 1993م، ص343.

[4] سرور، 1993، ص359.

[5] الطوالبة، 2004م، ص13.

[6] أحمد، 1997م، ص73.

1- أن التفتيش يحتوي في مضمونه على قدر من الجبر والإكراه، إذ إنه تعرض قانوني لحرية المتهم الشخصية أو لحرمة أسراره الموجودة على جهاز الحاسوب خاصته، أو على برامج خاصة به أو على بريده الإلكتروني عبر شبكة الإنترنت.

2- أن التفتيش يُعد قيداً على حرمة أو حصانة الشخص الذاتية، كما يُعد قيداً على حرمة أسراره الشخصية، أي فيه مساس بحق السر.

3- امتياز التفتيش، بهذه الصورة، بأنه وسيلة للبحث عن الأدلة المادية والمعنوية للجريمة وضبطها، وتشير الخاصية الأخيرة إلى أن الهدف من التفتيش هو ضبط الأدلة التي تفيد في كشف الحقيقة[1].

ثانياً- محل التفتيش:

إن محل التفتيش بشكل عام يوجب البحث في أماكن لها حرمة خاصة كالمساكن ومكاتب المحامين... وهذا يعني المساس بحقوقهم ولو لمدة قصيرة[2].

أما محل التفتيش الإلكتروني فهو كل مكونات الحاسوب، سواء أكانت مادية أم معنوية، وشبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسوب محل التفتيش، وتشمل برامج النظام وبرامج التطبيقات سابقة التجهيز طبقاً لاحتياجات العميل[3].

وجدير بالذكر أن مثل هذا المحل لا يمكن أن يكون قائماً في ذاته، وإنما يشمله مكان أو عقار ما، أو يكون بصحبة مالكه أو حائزه، أي إن الحرز الذي يوجد فيه الحاسوب هو في طبيعته حرز مادي كالمنزل أو شخصه، كما هو الشأن في الحاسوب المحمول، سواء أكان شخصياً أم هاتفاً نقالاً[4].

لذلك لابد من دراسة مدى قابلية هذه المكونات للتفتيش، بالإضافة إلى ذلك سندرس مدى خضوع المشتبه فيه المعلوماتي للتفتيش، وكذلك مدى قابلية التفتيش بالنظر إلى مكان وجود الجهاز المراد تفتيشه.

---

[1] الطوالبة، 2004، ص13.

[2] الحلبي، 2011، ص149.

[3] حجازي، 2007.ب، ص388.

[4] خنفوسي، 2016، ص147.

1- المكونات المادية والمعنوية:

تتكون نظم الحاسوب من مكونات مادية (Hardware) ومكونات معنوية (Software) [1]، لذا فقد ثار تساؤل حول مدى خضوع مكونات الحاسوب المستخدمة للتفتيش، وفي هذا الصدد يجب التفريق بين حالتين:

الحالة الأولى: مدى جواز تفتيش مكونات الحاسوب المادية:

يتكون جهاز الحاسوب من مكونات مادية، وتعرف بأنها: "وسيلة لإدخال الأوامر، والقدرة على استقبال النتائج من هذا الحاسوب"[2]، وهذه المكونات هي:

- **وحدات الإدخال (Input Units)**: وهذه الوحدات هي: **(الفأرة، ومشغل الأقراص الممغنطة، والماسح الضوئي، ومشغل الأسطوانات).**

- **وحدات المعالجة المركزية (Central Processing Unit CPU)**: وهذه الوحدات هي: (وحدات الذاكرة الرئيسة، ووحدة الحساب والمنطق، ووحدات التحكم).

- **وحدات الإخراج (Output Units)**: ومن أمثلة هذه الوحدات: (الراسمات، والطابعات، والشاشات، ومشغل الأقراص، ووحدات تركيب الأصوات أو السماعات).

- **وحدات التخزين (Storage Devices)**: وتشمل: **(الأقراص الصلبة، والأقراص المرنة، وأقراص الليزر).**

- **المودم (Modem).**

- **الكروت أو البطاقات (PCMCIA Cards).**

- **البطاقات الممغنطة،** وبطاقات الائتمان القديمة، والمواد البلاستيكية المستعملة في إعداد هذه البطاقات، وكلها قرائن لإثبات الجرائم المعلوماتية [3].

وبعد استعراضنا لمكونات الحاسوب المادية التي يمكن الاستفادة منها في التحقيق من أجل إثبات دليل الإدانة أو البراءة، سنبحث في مدى جواز تفتيش المكونات المادية للحاسوب.

---

[1] مكاري، 2009، ص127.

[2] حجازي، 2007.أ، ص100.

[3] الطوالبة، 2004، ص19. حجازي، 2002، ص 18.

إن التفتيش المتعلق بمكونات الحاسوب، يسهل إجراؤه على المكونات المادية[1]، وتأتي سهولة هذا التفتيش لأنه يقع على أشياء مادية منصوص عليها في أغلب القوانين الإجرائية[2]، إذ يرى جانب من الفقه[3] أنه لا مشكلة في تفتيش نظام الحاسوب، متى كان التفتيش ينصب على المكونات المادية، أي على معدات الحاسوب وشاشة العرض ولوحة المفاتيح وغيرها، ففي هذا الفرض تطبق القواعد التقليدية للتفتيش.

والواقع أن تفتيش المكونات المادية للحاسوب بأوعيتها المختلفة بحثاً عن شيء يتصل بجريمة إلكترونية يدخل في نطاق التفتيش، طالما تم وفقاً للإجراءات القانونية المقررة، بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، هل هو من الأماكن العامة أم من الأماكن الخاصة، إذ إن صفة المكان لها أهمية خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبالضمانات نفسها المقررة قانونياً في التشريعات المختلفة[4].

وبالنسبة إلى الأماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل مكونات الحاسوب سالفة الذكر أو كان مسيطراً عليها أو حائزاً لها، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبالضمانات والقيود نفسها المنصوص عليها في هذا الصدد[5].

الحالة الثانية: مدى جواز تفتيش مكونات الحاسوب المعنوية:

تشمل المكونات المعنوية للحاسوب، الأنظمة الأساسية كأنظمة التشغيل، والكيانات المنطقية التطبيقية، كالبرامج التي تستخدم للقيام بعمل معين، والبيانات المخزنة في الحاسوب بأنواعها [6]، وكذلك المعلومات المنطقية[7].

---

[1] الحلبي، 2011، ص151.

[2] الطوالبة، 2004، ص28.

[3] حجازي، 2007.ب، ص 384.

[4] أحمد، 1997، ص74.

[5] مكاري، 2009، ص127.

[6] الخن، 2012، ص106.

[7] خنفوسي، 2016، ص147.

وبما أن التفتيش بالمعنى الفني هو إجراء تحقيقي ووسيلة للإثبات المادي، فهو إجراء يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وهذا ما يتعارض مع الطبيعة غير المادية لبرامج وبيانات الحاسوب، وكذلك الشبكات الإلكترونية، فهي برامج وبيانات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي[1]. وهذا ما يطرح السؤال حول **مدى قابلية تفتيش هذه المكونات المعنوية والوسط الافتراضي للحصول على الدليل الإلكتروني.**

إن الإشكالية التي تطرح في شأن قابلية تفتيش المكونات المعنوية أو الوسط الافتراضي ترجع في الواقع إلى تحديد المقصود بمصطلح (الشيء) الذي يفترض أن يكون محلاً للتفتيش والضبط، فإذا كان التفتيش ينصب على شيء فإن التساؤل يثار حول مدى انطباق لفظ (الشيء) على المكونات المعنوية "الوسط الافتراضي"، ولذلك أهمية عملية، فإذا كانت هذه المكونات لا تكتسب صفة الشيء بالمعنى الذي يعبر عنه النص القانوني، فإنه لا يمكن أن تكون محلاً للتفتيش، والمشكلة لا تقتصر على مشروعية التفتيش وإنما أيضاً تمتد إلى مشروعية ضبط البيانات التي توجد في الوسط الافتراضي، إذ إن النص القانوني ينصرف إلى تفتيش الأشياء وضبط ما يوجد فيها من أشياء، فما المقصود بلفظ الشيء؟ وبكلمة أوضح هل يُعد الوسط الافتراضي وما فيه من بيانات شيئاً في تطبيق أحكام التفتيش والضبط؟[2].

يستشعر الفقه صعوبة هذه المسألة نظراً إلى غياب الطبيعة المادية للمعلومات في ذاتها مجردة عن دعامتها المادية[3]، وقد ذهب الفقه في مدى جواز تفتيش المكونات المعنوية إلى ثلاثة اتجاهات:

- الاتجاه الأول: الاتجاه الرافض:

يرى أن المقصود بلفظ الشيء هو ما كان مادياً أي ملموساً، ولذا فإن الوسط الافتراضي والبيانات غير المرئية أو الملموسة لا يمكن عدها شيئاً، ومن ثم سينحسر عنها النص القانوني الذي استعمل مصطلح شيء، ما

---

[1] خنفوسي، 2016، ص146 - 147.

[2] الحلبي، 2011، ص240.

[3] الطوالبة، 2004، ص29.

يجعل تفتيش الوسط الافتراضي وضبط محتوياته مخالفاً للقانون[1]،لأن طبيعة البيانات المعالجة تتطلب قواعد خاصة تحكمها بدلاً من محاولة تطويع القواعد التقليدية وتوسيع نطاقها، وهذا يتأتّى من خلال إجراء تعديل عليها من شأنه توسيع نطاق الأشياء التي تكون مشمولة بالتفتيش والضبط، وتضمينها من الأحكام بما يتلاءم ومتطلبات هذه التقنية الجديدة، فالنصوص الخاصة بالتفتيش بمعناه التقليدي لا ينبغي إعمالها بشأنها مباشرة ، بحسبان أن هذه النصوص تمثل قيداً على الحرية الفردية، ومن ثَم يصبح القياس على الأشياء المادية محظوراً لمنافاته الشرعية الإجرائية[2].

كما يذهب هذا الاتجاه إلى أن المعلومات –المبرمجة في جهاز الحاسوب أو على أسطوانة أو شريط–قد يصعب انطباق وصف المحرر عليها، ويضربون مثالاً على ذلك ليؤيدوا وجهة نظرهم بأن المحرر الذي يحميه تجريم التزوير هو ذلك المحرر الذي يصح الاحتجاج به، وهذا لا يتحقق إلا باستعماله في التعامل، ولا يتحقق بالنسبة إلى المعلومات المبرمجة قبل طباعتها على أوراق[3]. ولذلك يقترح هذا الرأي لمواجهة هذا القصور التشريعي أن يتم تعديل النصوص الخاصة بالتفتيش، وذلك بأن يضاف إليها ما يجعل التفتيش يشمل البحث في الوسط الافتراضي وضبط المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب [4].

وفي بلجيكا، أصدر المشرع البلجيكي القانون المؤرخ بـ 2001/11/28 المتضمن تعديل قانون التحقيق الجنائي، الذي أضاف المادة /88/ إلى هذا القانون، والتي سمحت لقاضي التحقيق بأن يصدر إذناً بتفتيش نظم المعلومات.

– الاتجاه الثاني: الاتجاه المؤيد:

يذهب هذا الاتجاه إلى أن التفتيش والضبط لا يقتصران على الأشياء بمفهومها المادي، لأن الغاية من التفتيش هي البحث عن دليل بشأن جريمة وقعت، ولذا فإن إعمال قواعد التفسير المنطقي تجعل من الكيانات المنطقية مما يمكن تفتيشه وضبط ما فيه من محتويات[5].

---

[1] الحلبي، 2011، ص240 – 241.

[2] أرحومة، 2009، ص7.

[3] حجازي، 2007.أ، ص53 – 54.

[4] الحلبي، 2011، ص241.

[5] الحلبي، 2011، ص241.

ووصولاً إلى النتيجة ذاتها يرى بعض الفقه[1] أن تحديد كلمة شيء أو مادة يجب أن نرجع في شأنه إلى مدلول هذه الكلمة في العلوم الطبيعية، إذ تعني كل ما يشغل حيزاً مادياً في فراغ معين، ولما كانت الكيانات المنطقية والبرامج تشغل حيزاً مادياً في ذاكرة الحاسوب ويمكن قياسها بمقياس معين، وهي أيضاً تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها ذات كيان مادي وتتشابه مع التيار الكهربائي الذي عده الفقه والقضاء في فرنسا ومصر وسورية من قبيل الأشياء المادية، ومن ثم فهي تعد أشياء بالمعنى العلمي للكلمة، لذلك تصلح لأن تكون محلاً للضبط.

وتأييداً لذلك يرى بعض الفقه[2] أن القواعد التقليدية للتفتيش، تطبق على أدلة الجرائم التي يكون محلها برامج الحاسوب، كالسرقة أو الإتلاف أو استعمال هذه البرامج كأداة في ارتكاب بعض الجرائم كالتزوير أو التلاعب في البيانات أو الإتلاف الفني للأنظمة المعلوماتية، وإن القواعد التقليدية كافية لمواجهة هذه الأحوال أياً كانت الوسيلة المستخدمة لارتكاب الجريمة، سواء كانت تقليدية أو غلب عليها الطابع الفني.

إذاً فالمعلومات المبرمجة هي من عداد المحررات، مادامت مدونة على أسطوانة أو شريط أو مسجلة بجهاز الحاسوب نفسه، وذلك استناداً إلى أنه يمكن الاطلاع عليها بالوسيلة المناسبة لذلك[3].

وأيد هذا الاتجاه المجلس الأوربي في التوصية رقم (13) تاريخ 1995/9/11، إذ نصت على أن تسمح الإجراءات الجزائية لجهات التفتيش بضبط برامج الحاسوب والمعلومات الموجودة بالأجهزة وفقاً للشروط ذاتها الخاصة بإجراءات التفتيش العادية[4].

فضلاً عن أن (اتفاقية بودابست) **لعام 2001م**، تقضي في المادة (19) منها بإلزام الدول الأطراف في هذه الاتفاقية بضرورة تبني التدابير والإجراءات التشريعية التي تخول السلطات المختصة ولوج البيئة المعلوماتية، وذلك

---

[1] الحلبي، 2011، ص241 – 242.

[2] عفيفي، 2000، ص344.

[3] حجازي، 2007.أ، ص54.

[4] رمضان، 2000، ص80.

من أجل تيسير إثبات هذه الجرائم[1]، وبالتالي فقد أجازت هذه الاتفاقية تفتيش وضبط البيانات المخزنة في الحاسوب في المادة (19) من هذه الاتفاقية[2].

وبهذا الاتجاه أخذ بعض التشريعات فنص صراحة على أن إجراءات التفتيش تشمل أنظمة الحاسوب، وهذا ما نُصّ عليه في قانون إساءة استعمال الحاسوب في تشريع **المملكة المتحدة**، في القسم الرابع عشر من قانون إساءة استخدام الحاسوب لعام 1990م، وذلك بعد الحصول على إذن بالتفتيش من القاضي المختص.

وفي الأردن، نصت المادة (81) من قانون أصول المحاكمات الجزائية الأردني على أنه لا يجوز دخول المنازل وتفتيشها، إلا إذا كانت هناك أشياء تتعلق بالمجرم، وكلمة أشياء تنطبق على المكونات المادية والمعنوية للحاسوب، وهنا يمكن تطبيق القواعد العامة للتفتيش على الجرائم المعلوماتية [3].

وفي **البحرين**، نصت المادة (22) من قانون جرائم تقنية المعلومات البحريني رقم (6) لعام 2014م، على أنه "في تطبيق أحكام هذا القانون تشمل معنى كلمة (شيء) أو (أشياء) الواردة في قانون الإجراءات الجنائية عبارة (نظام) و(تقنية المعلومات) أو (أي جزء منه) و(بيانات وسيلة تقنية المعلومات) و(أي من وسائط تخزين بيانات وسيلة تقنية المعلومات الواردة في هذا القانون)".

ومن هذا النص نلاحظ أن المشرع البحريني قد وسع من مفهوم الشيء ليشمل جميع المكونات المعنوية.

وأيضاً في سورية فقد عدت المادة (38) والمادة (45) الفقرة (ب) من القانون رقم (20) لعام 2022م البرمجيات الحاسوبية من الأشياء المادية التي يجوز تفتيشها وضبطها، وفق القواعد المنصوص عليها في قانون أصول المحاكمات الجزائية.

ومن الأمثلة الواقعية لتفتيش برامج الحاسوب، أنه بعد تفجير بُرجي مركز التجارة العالمي في الولايات المتحدة الأمريكية في2001/9/11م، ولدى تفتيش الحاسوب النقال العائد للمشتبه به "رمزي يوسف" تبيّن – بحسب رأي الـ FBI –أن هذا الحاسوب كان يحوي الخطط اللازمة للقيام بعمليتي التفجير، كما أدّى هذا

---

[1] أرحومة، 2009، ص 7-8.

[2] الخن، 2012، ص106.

[3] الحلبي، 2011، ص151.

التفتيش إلى الكشف عن دور المدعو "زكريا الموسوي" في عملية التفجير الثانية، وقد تمّ فحص وتفتيش أكثر من مئة قرص صلب في هذه التحقيقات.

وكذلك الشأن في قضية أخرى، تتلخص وقائعها في أن السيدة "شارون لوباتكا" غادرت منزلها بقصد زيارة صديقتها، إلا أنها تغيبت عن المنزل لعدة أيام، ولدى تفتيش الحاسوب الشخصي العائد لها، وجدت الشرطة مئات الرسائل الإلكترونية بين السيدة "شارون" وشخص يدعى "روبرت غلاس"، وقد تضمنت هذه الرسائل تخيلات عن التعذيب والموت، ولدى قيام الشرطة بالتحقيق مع "غلاس"، اعترف بأنه قتل شارون خطأً في أثناء نومه معها، كما قام بإرشاد الشرطة إلى مكان جثتها في شمال كاليفورنيا، حيث وجدت الشرطة أيدي وأرجل شارون مربوطة، ثم تبين أنها ماتت خنقاً[1].

- الاتجاه الثالث: الاتجاه التوفيقي:

يرى ضرورة إهمال الجدال الدائر حول مصطلح الشيء والعبرة عنده بالواقع، فالضبط لا يمكن وقوعه عملياً إلا على أشياء مادية، ولذلك فإن المشكلة ليست مشكلة مصطلح عبر عنه النص القانوني، وإنما هي تتعلق بإمكانية اتخاذ الإجراء، وترتيباً على ذلك فإن تفتيش الوسط الافتراضي يكون صحيحاً إذا أسفر عن وجود بيانات اتخذت فيما بعد شكلاً مادياً، وهذا الاتجاه قد أخذ به قانون الإجراءات الألماني في القسم (94) إذ نص على أن "الأدلة المضبوطة يجب أن تكون ملموسة"، ولذلك فإن البيانات إذا تمت طباعتها تعد أشياء ملموسة وبالتالي يمكن ضبطها[2].

وهناك من يرى[3]جواز ضبط البيانات الإلكترونية بمختلف أشكالها سواء كانت (محسوسة أو غير محسوسة) إذ يعد حلاً يتلاءم مع طبيعة جرائم الانترنت، فالدليل الإلكتروني يمكن التعويل عليه لإثبات وقوع الجريمة ويمكن الاعتماد على الأدلة الإلكترونية إذا قُدمت أيضاً على شكل رقمي أو ورقي.

---

[1] الخن، 2012، ص106 – 107.

[2] أحمد، 1997، ص202. و الحلبي، 2011، ص242.

[3] الحمداني، 2016، ص236 – 237.

ويرى الباحث أنه يمكن تفتيش المكونات المعنوية أو الوسط الافتراضي، وذلك لأن كلمة شيء تشمل الأشياء المادية والمعنوية استناداً إلى التفسير الغائي للنص دون التفسير الحرفي له، وبالتالي فإن تفتيش الوسط الافتراضي يعد صحيحاً وفقاً للقانون، كما أن البيانات في ذلك الوسط يصح ضبطها.

كما يرى ضرورة تدخل قوانين الأصول الجزائية بشكل واضح لأجل تطبيق الإجراءات الخاصة بالوثائق التقليدية، وتطبيقها على المعلومات الموجودة في أجهزة الحاسوب[1].

2- مدى خضوع المشتبه به المعلوماتي للتفتيش:

يقصد بشخص المشتبه به المعلوماتي كمحل للتفتيش "تحسس جسمه وملابسه وفحصه بدقة وإخراج ما يخفيه فيه من محصلات جريمة الإنترنت، وإذا كانت معه أمتعة جاز تفتيشها بحثاً عن أجزاء تتعلق بوحدات معلوماتية محل البحث، سواء أكانت بين يديه أو كانت في سيارته"[2].

ويجوز تفتيش المشتبه به المعلوماتي بناء على رضائه، ومثال ذلك كما لو قام أحد مستخدمي الإنترنت بترديد عبارات أمام الجهات المختصة تفيد بأنه مشترك في البريد الإلكتروني مع أحد الأشخاص الناشطين في تنظيم إرهابي معين، وأنه يتبادل معهم الرسائل الإلكترونية في كل ما يتعلق بنشر أفكار ومبادئ هذا التنظيم الإرهابي، فتطلب منه السلطات المختصة أن تقوم بتفتيش جهازه، فإن وافق فإن التفتيش والضبط يكون صحيحاً[3].

وإذا كان المشتبه به المعلوماتي أنثى، فإن غالبية التشريعات اتفقت على وجوب تفتيش الأنثى من قبل أنثى وذلك مراعاة للقيم والعادات[4].

---

[1] وهذا ما دعا إليه المجلس الأوربي في التوصية رقم (13) تاريخ 1995/9/11م التي جاء فيها أنه "إذا كان القانون يوازي من الناحية العملية بين المعلومات الواردة على أجهزة الكومبيوتر والوثائق التقليدية تعين أن يوضح قانون الإجراءات أن الإجراءات الخاصة بالوثائق تنطبق في شأن المعلومات الموجودة بأجهزة الكومبيوتر". رمضان، 2000، ص81.

[2] خنفوسي، 2016، ص149.

[3] خنفوسي، 2016، ص149.

[4] محمد، 2014م، ص149.

وقد أثار الفقه الجزائي سؤالاً مهماً حول مدى جواز إجبار الأشخاص على الإدلاء ببيانات مخزنة في الحاسوب الآلي وتشكل جريمة، أو مدى إمكانية الحصول منهم على شفرات الدخول لهذه المعلومات المجرمة متى كان يعلمون بها؟

ففي حال كانت المعلومات التي تشكل جريمة توجد مخزنة في ذاكرة الحاسوب الآلي أو على أحد الأقراص الصلبة أو المرنة، فإن التساؤل الذي يثار هو: **ما مدى إمكانية الحصول من الأشخاص على شيفرات الدخول إلى هذه المعلومات إذا كانوا يعلمون بها؟ أو بالأحرى هل يمكن إكراههم على الإفصاح عن كلمة السر وما في حكمها من أجل تسهيل الولوج إلى البيئة المعلوماتية؟**

في الحقيقة لابد من التمييز بين المشتبه به المعلوماتي والشاهد المعلوماتي، كما يأتي:

– **بالنسبة إلى المشتبه به المعلوماتي:** هنا تباينت الآراء بصدد هذه المسألة، فهناك رأي في الفقه[1] يرى أنه لا يجوز قانوناً إجبار المشتبه به على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات، أو إلزامه بالكشف عن الشفرات أو كلمات السر الخاصة بالدخول إلى هذه المعلومات، أو إجباره على تقديم الأمر اللازم لوقف الفيروس، ذلك أن القاعدة الأساسية أنه لا يجوز إلزام الشخص بإقامة الدليل على نفسه بنفسه، سواء عن طريق الاعتراف، أو عن طريق تقديم عناصر الإثبات، كما أنه من حق المشتبه الامتناع عن الإجابة أو الاعتصام بالصمت من دون أن يؤخذ ذلك على أنه إقرار بصحة الاتهام والتسليم بأدلته[2].

ونتيجة لذلك فالمشتبه به له الحرية في عدم الكلام وعدم الإجابة على الأسئلة الموجهة إليه، وهو غير ملزم بالكلام[3].

وهناك من يرى[4] أن هذه الضمانة كما هي مقررة للمشتبه به في الجريمة التقليدية، لا يمنع من الأخذ بها في الجريمة المعلوماتية، ويجب مراعاتها بغرض الحصول على الدليل الإلكتروني.

---

(1) Daragon (E); 1996، N 422، p 242.

(2) النبراوي، 1968م، ص 149.

(3) حجازي، 2007.ب، ص412.

(4) حجازي، 2007.ب، ص414.

إلا أنه إذا كان الراجح أنه لا يجوز إجبار الشخص على الإدلاء بأقوال لها دلالة الشهادة ضد نفسه، إلا أنه يجوز إجباره على تسليم مفتاح خزينة مثلاً، يضاف إلى ذلك أن هناك وسائل للضغط يمكن استعمالها في الواقع العملي ضد المشتبه به، فرفض التعاون مع سلطات العدالة قد يلعب دوراً في تكوين قناعة القاضي ضده، كما أن هذا الرفض قد يدفع قاضي التحقيق إلى توقيفه احتياطياً بحجة عدم التأثير في سير التحقيق أو كشف الأدلة، وذلك بشرط أن تكون الجريمة موضوع المحاكمة، مما يجيز فيها المشرع التوقيف الاحتياطي، كذلك قد توحي سلطات التحقيق للمشتبه به بأن عدم تعاونه الإيجابي معهم في أثناء التفتيش قد يؤدي إلى عدم ضبط النظام المعلوماتي في مجموعه[1].

بينما يذهب رأي آخر إلى القول إنه، وإن كان لا يجوز إجبار الشخص على الإدلاء بأقواله ضد نفسه، لا ينبغي أن يكون ذلك حائلاً دون إجباره على تقديم معلومات يقتضيها ولوج النظام المعلوماتي للسلطات المختصة، متى كانت هذه المعلومات بحوزته، قياساً إلى إجبار الشخص على تسليم مفتاح الخزنة الذي في حوزته[2].

ولكن هذا الرأي الأخير أياً كانت المسوغات التي يقوم عليها، لا يمكن القبول به، فقياس المعلومة التي في حوزة المشتبه به على مفتاح الخزنة وما في حكمه قياس غير صحيح، ذلك أن المعلومة (المتمثلة في كلمة السّرّ وما في حكمها) أمر معنوي بخلاف المفتاح الذي هو شيء مادي محسوس قابل للتسليم، هذا من ناحية، ومن ناحية أخرى فإن هذا الرأي الأخير لا يتفق مع الأصول المستقرة في الإثبات الجزائي، ويتنافى مع مقتضيات حق الدفاع أمام القضاء الجزائي [3].

ومن ناحية ثالثة، وحتى على فرض التسليم بجواز إكراه المتهم أو المشتبه به على تقديم مفاتيح الشفرة التي تمكّن من ولوج النظام المعلوماتي، فإن الأمر تكتنفه صعوبات عملية لا يمكن التغلب عليها، لعل أبرزها أن المتهم يستطيع التذرع بنسيان المعلومة، أو عدم إمكان تذكرها، أو ما شابه ذلك[4].

---

[1] الصغير، 2001، ص105.

[2] بوحويش، 2009، ص100- 101.

[3] أرحومة، 2009، ص 8.

[4] أرحومة، 2009، ص 9.

ويرى الباحث أن الرأي الأول أدعى إلى القبول، وقد أيدته أغلبية التشريعات، إذ أعطى التشريع في بولندا المتهم بارتكاب الجرائم الحق في عدم إفشاء كلمات السر المستخدمة أو حتى الأكواد الخاصة بالبرنامج[1].

ويرى الباحث أنه لا يجوز قانوناً إجبار المشتبه به على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات، أو إلزامه بالكشف عن الشفرات أو كلمات السر الخاصة بالدخول إلى هذه المعلومات، ذلك أن القاعدة الأساسية أنه لا يجوز إلزام الشخص بإقامة الدليل على نفسه، سواء عن طريق الاعتراف، أو عن طريق تقديم عناصر الإثبات، ومن حق المشتبه به الامتناع عن الإجابة أو الالتزام بالصمت من دون أن يؤخذ ذلك على أنه إقرار بصحة الاتهام والتسليم بأدلته، إلا أنه يجوز إجباره على تسليم مفتاح الخزنة التي يوجد فيها النظام المعلوماتي.

– بالنسبة إلى الشاهد المعلوماتي:

أثار الفقه الجزائي سؤالاً مهماً حول مدى جواز إجبار الشاهد المعلوماتي على الإدلاء ببيانات مخزنة في الحاسوب، وتشكل دليلاً على جريمة، أو مدى إمكانية الحصول من الشاهد المعلوماتي على شفرات الدخول لهذه المعلومات المجرمة متى كان يعلم بها.

اختلف الفقه في ذلك، وكان هناك اتجاهان:

الاتجاه الأول: يرى أن الشاهد ليس ملزماً بإفشاء أسرار مهنته، فالشهادة بصفة عامة وظيفة اختيارية من حيث مضمونها، فلا يُلزم الشاهد بالإدلاء ببيانات معينة هو لا يرغب في الإدلاء بها[2]، وإذا كانت الشهادة تنصب على ما أدركه الشاهد بإحدى حواسه فإنه من الصعب أن نطلب منه أن يقدم مساعدته للكشف عن الدليل أو الوصول إليه، فلا يجوز مثلاً إجبار العامل الفني في أحد الأنظمة المعلوماتية أن يقوم – لحساب الضابطة العدلية – بطباعة أو تحليل ذاكرة النظام المعلوماتي ليكشف له عن آثار بعض البيانات، فهذا البحث يدخل في اختصاص الخبير القضائي[3].

---

[1] محمد، 2014، ص 69.

[2] الجملي، 2015، ص58.

[3] Vergucht (P); 1996, N321، p387، 398 et399.

الاتجاه الثاني: يرى أنصاره أنه يمكن إلزام الشاهد بالإدلاء بالمعلومات المتعلقة بموضوع الجريمة ومن ذلك الكشف عن كلمة المرور، بحسبان أنه ليس هناك نص قانوني يمنع من ذلك[1]، وبالتالي يجوز إجبار غير المتهم على تقديم المعلومة التي من شأنها تيسير الدخول إلى المنظومة كمقدم الخدمة مثلاً ، وذلك بحمله على الإفصاح عن كلمة السر التي في حوزته للوصول إلى المصدر أو شبكة الاتصالات؛ لأن الإكراه الواقع على غير المتهم لا يمس حقوق الدفاع خلافاً للوضع بالنسبة إلى المتهم[2].

وذهب بعض الفقه[3] إلى أنه يجب على الشاهد الكشف عن مفاتيح الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة.

كما أنه في غياب النص التشريعي يكون الشاهد مكلفاً بالكشف عن كلمات المرور السرية التي يعرفها وشفرات تشغيل البرامج، ماعدا حالات المحافظة على سر المهنة، فإنه يكون في حل من الالتزام بأداء الشهادة[4]. وفي التشريع الفرنسي وحسب المادتين (62-109) من قانون الإجراءات الجنائية الفرنسي، يمكن إلزام الشاهد المعلوماتي- حسب القواعد العامة- بالإفصاح عن كلمات السر التي يعلمها، ويعاقب جزائياً متى رفض إعطاء هذه الكلمات – مباشرة التزامه بالإعلام- في مرحلة التحقيق الابتدائي والمحاكمة[5].

وفي **اليونان** كذلك يمكن الحصول من مشغل نظام الحاسوب على كلمة المرور السرية للولوج في النظام المعلوماتي، كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني، لكن ليس على الشاهد أي التزامات بالنسبة إلى طباعة ملفات بيانات مخزنة في ذاكرة الحاسوب، وذلك لأنه يجب أن يشهد على معلومات تمت حيازتها بالفعل، وليس الكشف عن معلومات جديدة، وذلك حسب المادة (1/223) من قانون الإجراءات الجنائية اليوناني[6].

---

(1) الجملي، 2015، ص58.

(2) أرحومة، 2009، ص9.

(3) حجازي، 2007.ب، ص346.

(4) محمد، 2014، ص153-154.

(5) حجازي، 2007.ب، ص350.

(6) Vassilaki (Irini); 1993. p371.

وأخذ بهذا الاتجاه أيضاً بعض الدول كالسويد وفنلندا والنرويج، إذ تنص تشريعاتها على أنه يقع على عاتق الشهود واجب بأن ينعشوا الذاكرة بفحص الأماكن والمستندات التي توجد تحت سيطرتهم إذا لم يترتب على ذلك أضرار خطيرة.

وفي قوانين بعض الدول الأنجلوسكسونية فإن الالتزام بالتعاون يتسع ليس فقط لمجرد إصدار الأمر بإحضار الشهود، أو إحضار بعض المستندات، ولكن إلزام الغير بتقديم المساعدة للسلطة القضائية عن طريق تقديم الأدلة أو المساعدة في الوصول إليها، فالقانون الإنكليزي الصادر في عام 1984 م، بشأن البوليس والأدلة الجنائية يعطي للمحققين الحق في أن يطلبوا من الغير أن يمكنوهم من الدخول إلى المعلومات المخزنة في الحاسوب أو الاطلاع عليها أو قراءتها[1].

وتجيز المادة (125) من قانون الإجراءات الجنائية الهولندي لقاضي التحقيق أن يأمر أي شخص، يفترض فيه أنه على علم بكيفية الدخول إلى المعلومات المخزنة في الحواسيب، بالإسهام مع سلطات التحقيق في الكشف عن الحقيقة، طالما أن هذه المعلومات تم تخزينها أو معالجتها أو نقلها عن طريق نظام المعالجة الآلية للبيانات، أو تمكين قاضي التحقيق من الدخول إلى هذه المعلومات، والأمر هنا يقتصر على المعلومات التي استخدمت في ارتكاب الجريمة فحسب.

وطبقاً لهذه المادة إذا كانت مصلحة التحقيق تقتضي فك شفرة البيانات يكون لقاضي التحقيق أن يأمر أي شخص يفترض فيه معرفة تشغيل نظام أمن المعالجة الآلية – في أثناء التفتيش – أن يُمَّكنه من الدخول إلى أنظمة المعالجة الآلية أو في جزء منها، أو أن يقوم بفك الشيفرات، ويجب أن يوجه الأمر إلى الشخص الذي يفترض فيه العلم بكيفية فك الشيفرة[2].

كما يتضمن التشريع الأمريكي قانوناً خاصاً بتعاون متعهدي خدمات الرسائل في مجال الاتصالات الإلكترونية المسجلة.

---

(1) Vergucht (P) ; 1996; p387- 398 et399.

مشار إليه لدى: حجازي، 2007.ب، ص350-351.

(2) Verguht (P); 1996, P 401.

وفي النتيجة فالشاهد أو القائم على تشغيل النظام المعلوماتي يلتزم بالكشف عن الشفرات أو كلمات السر التي يكون على علم بها، ولا يعفيه من هذا الالتزام سوى الاعتصام باحترام السر المهني[1]، ومع ذلك فليس ثمة جزاء جزائي يوقع على الشاهد إذا رفض تقديم المعلومات المطلوبة إلا إذا وقع ذلك في مرحلتي التحقيق الابتدائي والمحاكمة[2].

3- مدى قابلية التفتيش بالنظر إلى مكان وجود الجهاز المراد تفتيشه:

كثيراً ما يقوم مرتكب الجريمة بتخزين معلوماته في حواسيب أو مُخدّمات أخرى؛ بهدف عرقلة التحقيقات [3]، وهنا يثار التساؤل حول إمكانية تفتيش الأنظمة المتصلة بالنظام المأذون بتفتيشه إذا وُجدت في دوائر اختصاص مختلفة، فهل يمتد تفتيش حاسوب معين إلى الأجهزة المرتبطة به؟

في هذه الصورة يمكن التفرقة بين الفرضيتين الآتيتين:

الفرضية الأولى: أن يكون حاسوب المتهم متصلاً بحاسوب أو مُخدّم موجود في مكان آخر داخل الدولة:

إن تفتيش الوسط الافتراضي يأخذ حكم المكان الذي يوجد فيه الجهاز، فإذا وجد في مكان ينطبق عليه وصف المسكن وجب الالتزام في تفتيشه بالأحكام الخاصة بتفتيش المساكن[4].

لكن أثير تساؤل مهم يتعلق بمدى إمكانية امتداد الحق في التفتيش، إذا تبين أن الحاسوب في منزل المتهم متصل بحاسوب آخر مملوك لشخص آخر غير متهم، فهل يمكن تفتيشه في هذه الحالة؟

في الحقيقة هنالك اتجاهان في هذا الفرض، اتجاه مؤيد واتجاه معارض.

- الاتجاه المؤيد:

يرى **الفقه الألماني** بشأن إمكانية امتداد الحق في التفتيش، أنه يمكن أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استناداً إلى المادة (103) من قانون الإجراءات الجزائية الألماني[5].

---

(1) Verguht (P); 1996, P397.

(2) الصغير، 2001، ص108.

(3) الخن، 2012، ص107.

(4) الجملي، 2015، ص27. و الحلبي، 2011، ص244.

(5) حجازي، 2007.ب، ص381.

ويسمح المجلس الأوربي في التوصية رقم (95) تاريخ 9/11/ 1995 في أثناء عملية تنفيذ التفتيش للجهات القائمة بالتنفيذ، ومع احترام الضمانات المقررة، بمد التفتيش إلى أنظمة الحاسوب الأخرى، في دائرة اختصاصهم، والتي تكون متصلة بالنظام محل التفتيش وضبط ما فيها من معلومات، لكن بشرط أن يكون هذا الإجراء ضرورياً[1].

كما تسمح الاتفاقية الأوروبية لجرائم الإنترنت لعام 2001، للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز الحاسوب المعين إلى غيره من الأجهزة المرتبطة به في حال الاستعجال إذا كان يوجد فيه معلومات يتم الدخول إليها في هذا الجهاز من خلال محل التفتيش، فتنص الفقرة الثانية من المادة (19) من القسم الرابع على أنه "من حق السلطة القائمة بتفتيش الحاسوب المتواجد في دائرة اختصاصها أن تقوم في حال الاستعجال بمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الحاسوب الأصلي محل التفتيش"[2].

ولقد حسم بعض القوانين هذه المسألة بإجازة التفتيش في هذه الحالة، إذ وجدت بعض التشريعات المقارنة حلاً لهذه المشكلة كما في **الولايات المتحدة الأمريكية** [3].

كما أن قانون تحقيق الجنايات البلجيكي الصادر في 23 /2000/11، أجاز امتداد التفتيش إلى نظام معلوماتي آخر غير مكان البحث الأصلي، ولكن ليس بصورة مطلقة وإنما بقيود معينة، يمكن إجمالها في أن يكون ثمة ضرورة لكشف الحقيقة فيما يخص الجريمة موضوع البحث، أو أن تكون الأدلة معرضة لمخاطر معينة كالإتلاف أو التدمير وما شابه[4].

وأيضاً المادة (17) فقرة (أ) من القانون الفرنسي رقم 239 لسنة 2003 بشأن الأمن الداخلي الصادر في 18 /2003/3 اعترفت بأنه يمكن لرجال الضابطة العدلية أن يدخلوا من الجهاز الرئيس إلى البيانات التي تهم عمليات البحث والتحري، فنصت المادة (17) منه على أنه "يجوز لرجال الضابطة العدلية من درجة ضباط

---

(1) رمضان، 2000، ص80 – 81.

(2) Verbiest(Thibault); 2002، p.127.

(3) الخن، 2012، ص107.

(4) أرحومة، 2009، ص 10.

وغيرهم من رجال الضابطة العدلية أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم التفتيش على البيانات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر مادامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيس، أو يتم الدخول إليها أو تكون متاحة ابتداءً من النظام الرئيس".

كما أن المشرع الأردني قد أعطى لموظفي الضابطة العدلية الحق في الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المعلوماتية، أي اعترف بامتداد التفتيش إلى حاسوب أو نظام معلوماتي لغير المتهم متى وجدت دلائل في استخدامها لارتكاب جرائم إلكترونية.

كما أعطى المشرع البحريني بموجب المادتين (15– 16) من قانون جرائم تقنية المعلومات البحريني رقم (6) لعام 2014م، للنيابة حق الدخول إلى حواسيب كل من له علاقة بالجريمة حتى لو كان موجوداً في بلد أجنبي، وبغض النظر عن جنسيته.

أيضاً التشريع السوري نص في الفقرة (ج) من المادة (26) من قانون مكافحة الجريمة المعلوماتية رقم /17/لعام 2012 على جواز تفتيش الأجهزة والبرمجيات الحاسوبية المتصلة بأجهزة المشتبه فيه، لكن القانون الجديد رقم(20) لعام 2022م لم يضع نصاً صريحاً بهذا الخصوص.

– الاتجاه المعارض:

على العكس من ذلك فإن هناك من يرى[1] أن هذا الإجراء لا يمكن تطبيقه، لأن هذا النوع من التفتيش ينطوي في الحقيقة على معنى تفتيش غير المشتبه به، ولذلك فإنه لا يجوز تطبيقه إلا في الأحوال التي يجوز فيها للقائم بالتفتيش تفتيش غير المشتبه فيه أو منزله.

كما أن هناك عدداً من التشريعات المقارنة مثل سويسرا وبلجيكا قصرت أثر إذن التفتيش على الأجهزة الموجودة في مكان محدد من دون امتدادها إلى الأجهزة المرتبطة[2].

ونميل إلى تأييد جواز تفتيش حاسوب المشتبه فيه المتصل بحاسوب أو مُخدّم موجود في مكان آخر داخل الدولة إذا كان هناك أساس يدعو إلى الاعتقاد بأن البيانات المطلوبة قد تمّ تخزينها في نظام ذاك الحاسوب، لكن

---

[1] الحلبي، 2011، 245.

(2) Verbiest(Thibault); 2002, p.127.

بشرط أن يكون الدخول إلى النهاية الطرفية الخاصة بغير المتهم لا يحتاج إلى كلمة مرور خاصة لا يستعملها غيره (شفرة)، وأن يكون نظام الحاسوب الآخر ضمن النطاق الإقليمي للدولة، وأن يكون ذلك التفتيش ضرورياً لإظهار الحقيقة، ولا بد من أن يكون أمر هذا التفتيش مسبباً بإيراد الأسباب الذي دعت إليه.

الفرضية الثانية: أن يكون حاسوب المشتبه فيه متصلاً بحاسوب أو مُخدّم آخر موجود في مكان آخر خارج الدولة:

من المتصور طبقاً لهذا الفرض أن يقوم مرتكبي الجريمة المعلوماتية بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصالات البصرية، بهدف عرقلة سلطات الادعاء في جمع الأدلة[1].

فالبيئة المعلوماتية غالباً ما تكون مؤلفة من شبكات منتشرة في كافة أرجاء المعمورة، ومرتبط بعضها ببعضها الآخر عن طريق الإنترنت، بحيث تتيح الفرصة أمام المجرمين للولوج عن بُعد إلى البيانات الإكترونية المخزونة في أية بقعة من بقاع العالم[2]، وقد تكون البيانات التي تثبت حصول الفعل جزءاً من نظام حاسوب يقع خارج الحدود في دولة أخرى[3].

وتتعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بوساطة شبكة الاتصال عن بُعد، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثاً عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية، إذ إن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة[4].

فقد يظهر أحياناً في أثناء التحقيقات أنه من الضروري تفتيش جهاز حاسوب موجود في الخارج كما لو تعلق الأمر بشركة وفروعها في الخارج، إذ ترتبط أجهزة الشركة بعضها ببعضها الآخر، وأحياناً ترتبط بعض الأجهزة بقاعدة بيانات موجودة في الخارج[5].

---

[1] حجازي، 2007.ب، ص382.

[2] خلف، 2016، ص9

[3] الحلبي، 2011، ص150.

[4] الصغير، 2001، ص115 .

[5] مكاري، 2009، ص129.

فمن القواعد المتفق عليها أن نطاق تطبيق قانون أصول المحاكمات الجزائية يرتبط بنطاق تطبيق قانون العقوبات، فكلما كان هذا الأخير واجب التطبيق طبق الأول، ومن القواعد المتفق عليها أيضاً أنه لا تلازم بين تطبيق قانون العقوبات وارتكاب الجريمة على إقليم الدولة، إذ قد ترتكب خارج إقليمها، ومع ذلك قانونها واجب التطبيق، كالاختصاص وفقاً لمبدأ العينية والشخصية والعالمية الجزائية، فضلاً عن ذلك فإن الجريمة قد ترتكب في إقليم دولة ما وتمتد آثارها إلى إقليم دولة أخرى، فإذا كانت هذه الدولة مختصة بالتحقيق في هذه الجريمة لأن قانون عقوباتها واجب التطبيق، فإن التساؤل يثار حول مدى إمكانية تفتيش تلك الآلة الموجودة خارج الإقليم بوساطة السلطات التابعة لهذه الدولة[1].

إذاً قد ترتكب الجريمة بوساطة منظومة لمجموعة من أجهزة الحاسوب تتوزع في أكثر من دولة، والسؤال الذي يطرح نفسه هنا هو: هل يمكن تفتيش تلك الحواسب للبحث عن الدليل الإلكتروني المتعلق بتلك الجريمة، بما في ذلك تلك الأجهزة الموجودة في إقليم دولة أخرى؟

في الواقع هنالك اتجاهان لحل هذه المشكلة:

- الاتجاه الأول: الاتجاه الرافض لتفتيش الحاسوب أو المُخدّم الموجود في مكان آخر خارج الدولة:

تبنى هذا الاتجاه المجلس الأوربي، إذ جاء في تقرير له أن هذا الاختراق المباشر يعد انتهاكاً لسيادة دولة أخرى، مالم توجد اتفاقية دولية في هذا الشأن، ويؤيد ذلك الفقه في ألمانيا، إذ يذهب إلى أن السماح باسترجاع البيانات التي تم تخزينها بالخارج يُعد انتهاكاً لحقوق السيادة لدولة أخرى، وخرقاً للقوانين الثنائية والوطنية المتعلقة بإمكانية التعاون في مجال العدالة القضائية[2].

وأوجبت اتفاقية بودابست الصادرة في 2001/10/22، على هذا النظام في المادة (25) "أن تتفق الأطراف على أوسع نطاق للتعاون بهدف إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وجمع الأدلة في الشكل الإلكتروني لهذه الجرائم".

---

[1] الحلبي، 2011، ص242 – 243.

[2] حجازي، 2007.ب، ص382.

ومن الأمثلة على دور التعاون الدولي ما حدث في ألمانيا، إذ أسفر البحث في إحدى جرائم الغش المعلوماتي عن وجود طرفية حاسوب في ألمانيا متصلة بشبكة اتصالات في سويسرا، إذ كان يتم تخزين بيانات المشروعات فيها، وعندما رغبت سلطات التحقيق الألمانية في الحصول على هذه البيانات لم يتحقق لها ذلك إلا من خلال طلب المساعدة المتبادلة [1].

وفي اليابان، قامت مجموعة من المخربين بمهاجمة عدد من المواقع الخاصة في الحكومة اليابانية، واستخدموا في ذلك حواسيب موجودة في الصين والولايات المتحدة الأمريكية. وقد طلبت الشرطة اليابانية المساعدة من بكين وواشنطن من أجل تسليم المعلومات والبيانات المسجلة على هذه الحواسيب في كلتا الدولتين، حتى تتمكن من التوصل إلى هؤلاء المجرمين[2].

– الاتجاه الثاني: الاتجاه المؤيد لتفتيش الحاسوب أو المُخدّم الموجود في مكان آخر خارج الدولة:

يذهب هذا الاتجاه إلى أنه إذا كانت فكرة السيادة الدولية ترتبط بالمفهوم التقليدي للإقليم، فإنه ليس هناك ما يمنع من تطبيق هذا الحكم في شأن تفتيش النظام المعلوماتي من خلال الولوج من نهاية طرفية في دولة أخرى، فذلك لا ينتهك سيادة الدولة، فالنظام المعلوماتي لا يعرف الحدود، والوحدة التي يتميز بها هي التي تعطي للجهة القائمة بالتفتيش سلطة الولوج وتتبع المعلومات، ولو امتد نشاطها إلى طرف نظام معلوماتي في دولة أخرى، ولا يحد من سلطتها هذه – حسب هذا الاتجاه – إلا وجود نظام شفرة للدخول إلى المعلومات، فذلك يخرج هذا الجزء من نطاق الوحدة المعنوية، وهو ما تفقد معه تلك الجهة صلاحياتها في ذلك الجزء[3].

وفي هذا الاتجاه صدرت عن المجلس الأوروبي توجيهات تجيز تفتيش الحاسوب إلى الشبكة المتصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة، فتنص التوصية رقم (13) في 9/11/ 1995، المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات، على أنه "لسلطة التحقيق عند تنفيذ تفتيش المعلومات لضوابط معينة أن تقوم بمد مجال تفتيش حاسوب معين يدخل في دائرة اختصاصها، إلى غير ذلك من

---

[1] حجازي، 2007.ب، ص383.

[2] حجازي، 2007.ب، ص383.

[3] الجملي، 2015، ص64.

الأجهزة مادامت مرتبطة بشبكة واحدة، وأن تضبط البيانات الموجودة فيها، مادام من الضروري التدخل الفوري للقيام بذلك"[1].

كما أن المادة (32) من **الاتفاقية الأوربية لجرائم الإنترنت لعام 2001م**، قد سمحت بتفتيش حاسوب موجود في دولة أخرى في حالتين:

الحالة الأولى: إذا تعلق التفتيش ببيانات متاحة للجمهور.

الحالة الثانية: إذا رضي صاحب البيانات بالتفتيش.

كما سمحت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة في القاهرة، بتاريخ 2010/12/21م، في المادة (26) منها بإمكانية تفتيش المعلومات المخزنة، وأكدت على ضرورة تبني مجموعة من الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش، أو الوصول إلى تقنية معلومات معينة أو جزء منها، هذا إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية أخرى أو جزء منها في إقليمها، وكانت هذه المعلومات قابلة للوصول قانوناً أو متوافرة في التقنية الأولى، فيجوز توسيع نطاق التفتيش والوصول إلى التقنية الأخرى[2].

وتسمح التشريعات المقارنة بتفتيش الأنظمة المتصلة حتى ولو كانت موجودة خارج إقليم الدولة، فتجيز المادة (17) الفقرة (2) من قانون الأمن الداخلي الفرنسي لرجال الضابطة العدلية أن يقوموا بتفتيش الأنظمة المتصلة، ولو وجدت في خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية[3].

كما نصت المادة (25/أ) من قانون الحاسوب الهولندي الحالي على الاعتداد بالدليل المتحصل عليه في إقليم دولة أخرى إذا تم ذلك تنفيذاً لاتفاقيات التعاون الأمني والقضائي، وأحياناً تكون تلك الدولة مختصة هي الأخرى بالتحقيق في هذه الجريمة، ولذا فإن لم ترغب في مباشرة التحقيق بشأنها فقد تتطوع بتزويد دولة التحقيق بالبيانات التي تم ضبطها وفقاً لما يعرف بنظام تبادل المعلومات أو المساعدات"[4].

---

[1] مكاري، 2009، ص129.

[2] خنفوسي، 2016، ص148 – 149.

[3] مكاري، 2009، ص129.

[4] الحلبي، 2011، ص244.

أيضاً أجاز المشرع البحريني بموجب المادتين (15 – 16) من قانون جرائم تقنية المعلومات البحريني رقم (6) لعام 2014م، للنيابة حق الدخول إلى حواسيب كل من له علاقة بالجريمة حتى لو كان موجوداً في بلد أجنبي.

وفي رأي الباحث أنه لا يحول دون جواز تفتيش الحاسوب أو المُخدّم الموجود في مكان آخر خارج الدولة فيما إذا لم يكن النظام المعلوماتي محمياً بنظام شفرة للدخول إلى المعلومات، لكن في حال وجود نظام شفرة للدخول إلى المعلومات، لا يجوز تفتيش هذا النظام المعلوماتي لتلك الدولة، ولذلك نرى أن السبيل لحل تلك المشكلة هو تعزيز التعاون الدولي، وذلك من خلال تعزيز دور الإنابة المتبادلة بين الدولة المحققة والدولة التي يراد التفتيش فيها.

ثالثاً– آلية تنفيذ التفتيش:

إن المشرع السوري في قانون أصول المحاكمات الجزائية السوري لم يتحدث أو ينص على إجراءات تفتيش الحاسوب وغيرها من الأجهزة التقنية والنظام المعلوماتي، لأنه صدر عام 1950 أي قبل اكتشاف الإنترنت.

وبشكل عام يجب على أعضاء الضابطة العدلية في الأحوال التي يجيز لها القانون إجراء التفتيش أو سلطات التحقيق أن يراعوا الإجراءات الآتية عند قيامهم بتفتيش نظم الحواسيب:

– تأمين حماية مسرح الجريمة، وهذا يتضمن القوة الكهربائية، وأجهزة خدمة الإنترنت، وحلقات الاتصالات الإلكترونية الهاتفية.

– على القائم بالتفتيش أن يحتاط إلى أن المشتبه به قد يتوافر لديه قدرة على الدخول عن بُعد إلى النظام من خلال جهاز الاتصال الوسيط (LAN-bassed) أو (PC-based) أو الإنترنت[1].

– أن يتم التفتيش بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة، وذلك مع مراعاة إبعاد المشتبه فيهم والعاملين على أجهزة الحاسوب عن المكان[2].

---

[1] الطوالبة، 2004، ص58.

[2] الحلبي، 2011، ص154.

- أن يتم عمل نسخة احتياطية من الأقراص الصلبة أو الأسطوانات المرنة قبل استخدامها في البحث والتحقيق، مع استخدام أمر (Disk comp) للتأكد من دقة النسخ.
- القيام بنزع الجهاز المستهدف (الماكينة CPU) للتأكد من عدم وجود أقراص صلبة إضافية.
- نسخ محتوى الاسطوانات والأقراص وتحليلها للكشف عن:
  - الملفات الممسوحة الممكن استعادتها من سلة المهملات، وذلك باستعادتها عن طريق فتح سلة المهملات، ثم تحديد وعمل (Select All) (تحديداً كلياً)، ثم الضغط على قائمة ملف (File) واختيار (Restore) (استرجاع) فتعود الملفات إلى الأماكن التي كانت توجد فيها قبل الحذف، وبالرغم من ذلك توجد ملفات لا يمكن العثور عليها في حالتين: الحالة الأولى: إلغاء الملفات بالضغط على مفتاح (Shift+Delete) في الوقت نفسه، والحالة الثانية: الضغط على (Empty Recycle Bin) من قائمة (File) وذلك بعد الدخول إلى (Recycle Bin).
  - الملفات الخفية باستخدام برنامج (Dos) يتم عن طريق الأمر (DIR/H). وفي حالة استخدام برنامج (Windows 95) يتم الدخول إلى (Windows Explorer)، ثم يتم اختيار قائمة (View)، ثم (Option)، ثم يتم الدخول إلى (Show all Fills)، ثم يتم الضغط على الأمر (OK).
- إجراء بحث نصي على الكلمات المهمة المتعلقة بالقضية، وذلك باتباع الخطوات الآتية:
  - فتح قائمة (START) ويتم اختيار (FIND) ثم اختيار (FILES OR FOLDER) فيظهر بعد ذلك صندوق حواري (DIALOG BOX)، فنختار (Advanced).
  - وأمام التعبير (CONTAINING TEXT) نكتب الكلمة المطلوب البحث عنها، ثم نضغط على الأمر (Find Now)، فتظهر في أسفل الشاشة الملفات التي تتضمن الكلمات المطلوب البحث عنها.
  - تحديد كافة محتويات القرص الصلب من خلال برنامج الـDOS باستخدام الأمر (DIR/S/P).

وفي حالة استخدام برنامج الـ Windows يتم الدخول إلى برنامج (Windows explorer)، فتظهر شاشة نشاهد في بدايتها في أعلى اليسار لفظ (Desktop) وتظهر أسفلها كل محتويات الحاسوب من الأماكن التخزينية لكل الأقراص الصلبة وقرص الليزر (CD. Rom).

- يتم إجراء فحص البرامج وجرد البرامج التطبيقية، وعلى وجه الخصوص البرامج الحسابية التي من المحتمل استخدامها في عملية اختلاس.
- حفظ المضبوطات وتجنب درجات الحرارة العالية أو الأتربة أو أي مجال مغناطيسي[1].

ويلاحظ أن أغلب التشريعات لم تحدد مدة معينة لتنفيذ إجراء التفتيش، بينما نلاحظ أن المشرع الإنكليزي حدده خلال شهر واحد من تاريخ إصدار الإذن[2].

وهناك من يرى[3] أن تنفيذ إجراء التفتيش في نطاق الحاسوب ربما يحتاج إلى مدة أطول من المدة التي يحتاج إليها التفتيش التقليدي، وذلك يعود إلى الاتصال عن بُعد أو حتى من خارج البلاد، فيحتاج الأمر إلى اتصالات قضائية وتنسيق مع الجهاز القضائي الأجنبي لتفتيش وضبط النظم أو البرامج المجرمة عبر شبكة الإنترنت مثلاً.

ويرى الباحث عدم تحديد مدة لتنفيذ التفتيش الواقع على نظم الحاسوب والإنترنت، فمن جهة أولى، هذا النوع من التفتيش يختلف في محله عن التفتيش التقليدي، إذ يقع هذا التفتيش على مكونات الحاسوب المادية والمعنوية، ولاسيما إذا كان هنالك كم هائل من البيانات التي يتطلب تفتيشها وقتاً طويلاً، ومن جهة ثانية، يستلزم هذا التفتيش بعض الإجراءات المعقدة فيما إذا كانت العناصر المكونة للجريمة موجودة في بلد آخر، الأمر الذي يقتضي الحصول على إذن من هذه الدولة بالتفتيش أو إعطائها إنابة قضائية، وهذا كله يتطلب وقتاً طويلاً جداً.

---

[1] الصغير، 2001، ص121 – 122.

[2] الطوالبة، 2004، ص60.

[3] الطوالبة، 2004، ص60.

الفرع الرابع

الضبط

إن الضبط كإجراء من إجراءات إثبات الجريمة المعلوماتية، وبالتالي الحصول على الدليل الإلكتروني يقتضي بحث ما يأتي:

أولاً: مفهوم الضبط:

يقصد بالضبط في قانون أصول المحاكمات الجزائية "وضع اليد على شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها، وعن مرتكبيها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو من إجراءات التحقيق"[1].

فالضبط هو الوسيلة القانونية التي تضع بوساطتها السلطة المختصة يدها على جميع الأشياء التي وقعت عليها الجريمة أو نتجت عنها أو استعملت باقترافها، كالأسلحة والأشياء المسروقة، والثياب الملوثة بالدم، والأوراق وغير ذلك[2].

والضبط هو الأثر المباشر للتفتيش، فالعلاقة وثيقة بين التفتيش والضبط، فإذا بطلت إجراءات التفتيش بطل الضبط، إلا أنه قد يتم الضبط من غير تفتيش، وذلك عندما يقدم المشتبه به باختياره الأشياء المتعلقة بالجريمة[3].

أما الضبط في البيئة المعلوماتية فيقصد به "وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية التي تتصل بالجريمة الإلكترونية"[4].

ثانياً- محل الضبط:

إن الضبط بطبيعته وبحسب تنظيمه القانوني وغايته لا يرد سوى على الأشياء، أما الأشخاص فليسوا محلاً للضبط بالمعنى الدقيق، لكنهم محل للقبض حال حضورهم أو الإحضار في حال غيابهم، وإذا كانت بعض

---

[1] حجازي، 2007.ب، ص 394.

[2] الخن، 2012، ص109.

[3] الخن، 2012، ص109.

[4] خنفوسي، 2016، ص150.

القوانين تتحدث عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف تماماً عن ضبط الأشياء[1].

كما أن القانون لا يفرق في مجال الضبط بين المنقول والعقار، ذلك أن كليهما يمكن ضبطه كذلك، ويستوي أن يكون الشيء المضبوط مملوكاً للمشتبه به أو لغيره[2].

وضبط الأدلة الإلكترونية أو ما يتعلق بالجرائم المعلوماتية يتصل بضبط المكونات المادية لأنظمة الحاسوب، وضبط المكونات المعنوية والبرمجيات، وضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط الحواسيب معاً وما يتصل بها[3].

إذاً فيما يتعلق بالضبط الإلكتروني للحصول على الدليل الإلكتروني، فإننا نميز بين ضبط المكونات المادية، وضبط المكونات المعنوية، ومدى قابلية البريد الإلكتروني للضبط.

1- مدى قابلية المكونات المادية للضبط:

لا تثير المكونات المادية مشكلة من حيث إمكانية ضبطها لأنها أشياء مادية[4]، وبالتالي يجوز ضبط الحاسوب والأسلاك والمودم ووحدة الذاكرة ووحدة التحكم، وبما في ذلك مخرجات الحاسوب الموجودة في صورة مخرجات ورقية أو أوعية التخزين المادية كالأقراص المغناطيسية أو الذاكرات الإلكترونية الخارجية، إذ يتم ضبط الأداة التي يتم فيها التخزين[5].

وضبط الأجهزة الإلكترونية لا يعد دليلاً في الإثبات، وإنما هو خطوة نحو الإثبات أو تمهيد للدخول إلى الإثبات أو النفي، فالجرائم المعلوماتية ليست مثل الجرائم التقليدية، فحيازة المخدرات تشكل جريمة لذات الحائز، أما حيازة الأجهزة فليست جريمة[6].

---

(1) الحلبي، 2011، ص170.

(2) حجازي، 2007.ب، ص 394.

(3) الحلبي، 2011، ص169.

(4) الجملي، 2015، ص59.

(5) المخول، 2024، ص 390.

(6) محمد، 2014، ص37.

ويرى الباحث أن ضبط المكونات المادية للحاسوب والمتمثلة في معدات الحاسوب وكابلات الشاشة وشاشة العرض ومفاتيح تشغيله...، يمكن أن يطبق بصددها القواعد التقليدية ذاتها للضبط من دون أدنى صعوبة.

2- مدى قابلية المكونات المعنوية للضبط:

إن الضبط محله، في مجال الجرائم المعلوماتية، البيانات المعالجة إلكترونياً، وقد أثير هنا التساؤل الآتي: **هل يصلح هذا النوع من البيانات لأن يكون محلاً للضبط الذي يعني كما رأينا وضع اليد على شيء مادي ملموس؟**

انقسم الفقه في هذا الصدد إلى اتجاهين:

الاتجاه الأول: الاتجاه الرافض:

يرى هذا الاتجاه أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم المادي لا ينطبق على بيانات الحاسوب غير الملموسة [1].

وقد أيد هذا الاتجاه جانب من الفقه الفرنسي مثل (Gassin) إذ يرى[2] أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة، وبالتالي لا تعد شيئاً مادياً بالمعنى المصطلح عليه، ولذلك لا يمكن ضبطها.

ويقترح هذا الاتجاه، إزاء النقص التشريعي، ضرورة أن يضاف إلى الغاية التقليدية للتفتيش إمكانية البحث وضبط المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب، وبذلك تصبح الغاية من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة المادية أو أية مادة معالجة بوساطة الحاسوب[3].

وبالتالي يذهب هذا الاتجاه إلى أنه بما أن بيانات الحاسوب لا تصلح لأن تكون محلاً للضبط، لانتفاء الكيان المادي عنها، فلا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو

---

[1] حجازي، 2007.ب، ص379.

[2] Gassin R, 1982، p. 38.

[3] حجازي، 2007.ب، ص379-380.

بنقلها على دعامة مادية أو غيرها من الوسائط المادية، ويستند هذا الاتجاه إلى أن النصوص التشريعية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة[1].

وقد أخذ بهذا الاتجاه القانون الألماني في المادة (161) من قانون الإجراءات الألماني، عندما نص على أن البيانات المعالجة إلكترونياً لا يمكن ضبطها مجردة إلا إذا تم تحويلها إلى كيان مادي مطبوعة على ورق، أو عن طريق التصوير الفوتوغرافي[2].

ويرى الباحث أنه لابد من تطوير النصوص القانونية المتعلقة بالضبط، لتشمل إمكانية ضبط معطيات الحاسوب والبيانات المعالجة إلكترونياً.

وهذا ما ذهب إليه المشرع البلجيكي، وذلك بمقتضى قانون 28 /2000/11، المعدل لقانون التحقيق الجنائي الذي أضاف المادة (39مكرر) والتي سمحت بضبط الأدلة الإلكترونية مثل: نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية[3].

الاتجاه الثاني: الاتجاه المؤيد:

يرى هذا الاتجاه أن البيانات المعالجة إلكترونياً ما هي إلا ذبذبات إلكترونية أو موجات كهرومغناطيسية تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره[4].

وبالتالي فهذا الاتجاه ينفي الطابع المعنوي لهذه البيانات، ويؤكد أنها شيء مادي يمكن تلمسه في المحيط الخارجي، وأنها كيان مادي لا يمكن إنكاره، وذلك استناداً إلى حكم صدر من محكمة جنح بروكسل في بلجيكا، أكد على أن هذه البيانات أشياء مادية محسوسة، وبالتالي يمكن خضوعها لقواعد التفتيش التقليدية ومن ثم إمكانية ضبطها[5].

---

[1] الحلبي، 2011، ص171.

[2] الحلبي، 2011، ص175.

[3] فرغلي، و المسماري، 2007، ص15.

[4] الحلبي، 2011، ص171.

[5] حجازي، 2007.ب، ص385.

وهكذا ينصب الضبط على الأشياء المادية وغير المادية، كما هو الحال في مراقبة المحادثات الهاتفية وتسجيل المحادثات الخاصة، وعلى ما هو مخزن في أجهزة الحاسوب، أو مخزن على الأقراص أو على الدعامات الأخرى[1].

ومن التشريعات التي أيدت ضبط المكونات المعنوية التي يجري تبادلها في نطاق شبكة المعلومات الإنترنت، قانون الإجراءات الجنائية اليوناني وذلك في المادة (251) التي خولت سلطات التحقيق إمكانية القيام بأي شيء ضروري لجمع وحماية الدليل الجزائي، ويفسر الفقه الجزائي عبارة – أي شيء– بأنها تمتد لتشمل ضبط البيانات المخزنة أو تلك التي تمت معالجتها إلكترونياً، لذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسوب لا تشكل أية مشكلة في اليونان، إذ بإمكان المحقق أن يعطي أمراً للخبير الخاص بالحاسوب، والذي يقوم بجمع البيانات وتكون مقبولة كدليل في إجراءات المحاكمة الجزائية.

كذلك فإن المادة (487) من القانون الكندي تمنح سلطة إصدار إذن الضبط – لأي شيء–طالما توافرت أسس معقولة للاعتقاد بأن الجريمة وقعت أو يشتبه في وقوعها، أو أن هناك نية في ارتكاب الجريمة بوساطته، أو سوف ينتج دليلاً على وقوع الجريمة، وهكذا فإن هذا النص يفسر بطريقة جلية أنه يسمح بضبط بيانات الحاسوب غير المحسوسة[2].

كما أن المشرع الأردني قد أجاز ضبط المكونات المعنوية بشكل صريح وواضح في قانون جرائم أنظمة المعلومات الأردني لسنة 2010م، وذلك في الفقرة (ب) من المادة (12) منه[3].

وقد أجاز القانون السوري ضبط كل ما يعدّ من آثار الجريمة، وسائر الأشياء والأوراق التي تساعد على إظهار الحقيقة، سواء أكانت تؤيد التهمة أم تنفيها، وقد أوجب القانون عرض الأشياء المضبوطة على المدعى عليه أو على من ينوب عنه للمصادقة والتوقيع عليها، فإذا امتنع، صرّح القائم بالضبط بذلك في المحضر[4].

---

[1] الحلبي، 2011، ص170.

[2] حجازي، 2007.ب، ص379.

[3] "…. يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون، والأموال المتحصلة منها والتحفظ على المعلومات، والبيانات المتعلقة بارتكاب أي منها".

[4] المواد (32)، (34)، (97) من قانون أصول المحاكمات الجزائية السوري.

أما بالنسبة إلى **إجراءات ضبط المكونات المعنوية للحاسوب،** فإن البيانات والمعلومات لا يمكن ضبطها بشكل منفصل عن أجهزة وأدوات التخزين، فالحاسوب والأجهزة الملحقة به، هي بمنزلة الأوعية المادية التي تحتوي هذه المعلومات والبيانات، وهي تشبه الحقيبة التي تُحفظ فيها الأوراق، وقد أجاز المشرع السوري في المادة (39) والمادة (35) من قانون مكافحة الجريمة المعلوماتية للضابطة العدلية الحصول على **نسخة** من البيانات والمعلومات والبرمجيات الحاسوبية التي تم تفتيشها؛ **ويمكن للضابطة العدلية في حالات الضرورة ضبط الأجهزة** والبرمجيات الحاسوبية المستخدمة أو جزء من مكوّناتها.

ومن هذا النص نستنتج أن المشرع السوري قد أحسن فعلاً عندما أجاز ضبط المكونات المعنوية بنص صريح وواضح.

3- مدى قابلية البريد الإلكتروني للضبط:

في الواقع يخضع هذا البريد للنص القانوني الوارد في قانون أصول المحاكمات الجزائية الخاص بضبط الخطابات والرسائل والجرائد والمطبوعات والطرود، وجميع البرقيات لدى مكاتب البريد، وبالتالي فإن التشريعات مازالت تخضع البريد الإلكتروني إجرائياً للقواعد الخاصة بالبريد العادي، لكن بالنظر إلى طبيعة البريد الإلكتروني أصبح من الملح أن تتطور هذه القواعد، وأن تتحدث عن ضبط البريد الإلكتروني، ومراقبته ووضع قواعد إجرائية خاصة به لكي يصبح من السهل الوصول إلى هذا الدليل وحفظه قبل أن يتم محوه بسرعة، تفوق الإجراءات الخاصة بالبريد العادي، والتعامل معه كدليل معنوي قائم في ذاته، ومنفصل عن إمكانية إفراغه في مستندات ورقية تقليدية[1].

ونحن نرى ضرورة تطوير قواعد الضبط لتتلاءم مع طبيعة البريد الإلكتروني وتخصيص إجراءات تتصف بالمرونة والسرعة تفوق الإجراءات الخاصة بالبريد العادي لضبط هذا البريد، وذلك نظراً إلى سهولة التخلص من الأدلة الإلكترونية الموجودة فيه.

---

[1] حمودة، 2017، ص122.

ثالثاً- آلية الضبط:

إن على عضو الضابطة العدلية عندما يصل إلى مسرح الجريمة، أن يتبع في ضبط المعلومات الإلكترونية الإجراءات الآتية[1]:

1- تأمين مسرح الجريمة المعلوماتية من العبث، إذ يجب عزل الحواسيب عن الشبكة، لتجنب إجراء أي تغيير على الأدلة الإلكترونية من قبل الغير، فلا بد من إجراء عملية الفصل الضرورية بين الحاسوب وكل شخص ليس له علاقة بالقائمين على التحقيق [2]، وذلك خشية قيام المشتبه فيه أو من له علاقة أو مصلحة ما بتدمير الأدلة بإزالتها من الحاسوب.

2- رفع البصمات عن الأجهزة لمقارنتها فيما بعد ببصمة المشتبه به.

3- حجز أو مصادرة الحاسوب أو القرص الصلب، وجميع الحاويات المادية والذواكر، كالسواقات والأقراص الممغنطة، فقد قام المشرع الأمريكي في المرشد الفيدرالي بإجازة ضبط القطع الصلبة (في الحاسوب ومكوناته المادية) إلا أن هذا الإجراء قد لا يكون هناك إمكانية لاتخاذه كما لو كان الضبط يتم عن بُعد في حالة اتخاذ إجراءات جزائية عن بُعد، وبالتالي يتم اللجوء إلى أساليب أخرى تصلح لكي يتم الضبط بمقتضاها مثل النسخ (copy) في حالة عدم وجود إمكانية لضبط القطع الصلبة، فيتم مثلاً نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها، وبالتالي يكون أسلوب النسخ صالحاً تماماً لأن ينتج عنه دليل إلكتروني مقبول أمام القضاء، وإلى جوار النسخ يوجد أيضاً أسلوب تجميد التعامل مع الحاسوب أو أحد القطعات المكونة له التي تم استخدامها في ارتكاب الجريمة، والتي تحتوي على ما يفيد الأدلة على ارتكابها، ومثل هذا الإجراء يصلح لأن يتخذ في مواجهة الحواسيب الخادمة التي تحتوي على مواقع القرصنة، وكذلك يصلح أسلوب التجميد إذا كان القرص الصلب يحتوي على ملفات مشفرة وتحتاج بالتالي إلى فك شفرتها لكي يمكن

---

[1] الخن، 2012 ، ص109.

[2] سلامة، (د.ت)، ص358 .

التعرف على محتوياتها الإجرامية، أو يكون الدخول إلى الحاسوب يحتاج إلى كلمة مرور (password) فالتجميد هنا يساعد خبراء المعمل الجنائي على القيام بعملهم من دون خوف من ضياع الدليل[1].

4- وضع ملصقات على الأشياء المضبوطة، وتوثيقها وتغليفها، وتحضيرها لنقلها بالحالة التي كانت عليها إلى مكان الاختبار والفحص.

5- تحرير محضر بعد إجراء عملية الفحص، يتضمن ذكر جميع الإجراءات السابقة، والنتائج التي تم التوصل إليها بنتيجة الفحص.

كما وضعت المنظمة الدولية لدليل الحاسوب[2]عدة معايير لضبط الدليل الإلكتروني، وقد تمت المصادقة على هذه المعايير خلال المؤتمر الدولي للبحث المعلوماتي والجريمة المعلوماتية، المنعقد في تشرين الأول عام 1999 (IHCFC)[3]، وهذه المعايير هي:

- عدم تغيير الدليل في أثناء ضبطه.
- أن تتم عملية الضبط من قبل شخص مؤهلٍ في المعلوماتية.
- جميع النشاطات المتعلقة بالضبط والوصول والتخزين ونقل الدليل الإلكتروني، يجب أن تكون موثقة ومحفوظة بغرض التدقيق.
- أن يكون الشخص الذي في حوزته الدليل الرقمي مسؤولاً عن جميع الإجراءات المتعلقة بهذا الدليل.
- أن تكون الجهات المسؤولة عن ضبط وتخزين ونقل الدليل الإلكتروني والوصول إليه مسؤولة عن تطبيق هذه المبادئ[4].

---

[1] بن يونس، 2005، ص219.

[2] تأسست المنظمة الدولية لدليل الحاسوب **(International Organization on computer) Evidence** في عام 1995، وتتكون من الجهات الحكومية المسؤولة عن تطبيق القانون، أو من الهيئات الحكومية التي تزاول التحقيق في مجال الحاسوب. وتهدف هذه المنظمة إلى تزويد الجهات الدولية القانونية بكيفية تبادل المعلومات بتحقيقات جرائم الحاسوب والمسائل ذات الصلة بالمعلوماتية الشرعية. كما تقوم بتنظيم عملية الاتصال بين أعضائها، وتقدم التوصيات اللازمة في هذا المجال، وتقيم المؤتمرات المتعلقة بنشاطاتها.

[3] وهو اختصار لـ International Hi - tech crime and Forensics conference.

[4] الخن، 2012، ص121.

ولابد من أن يكون ضبط الدليل الإلكتروني متناسباً مع ماهيته، بحيث ينصبّ الضبط على جميع الأجهزة والأدوات التي تمّ تخزين المعلومات فيها، لأن ضبط المعلومات والبيانات لا يمكن أن يتم بمعزل عن وسائط التخزين.

ولا بد من ضرورة الاستغناء عن طلب الإذن لضبط الأدلة الإلكترونية في الجرائم المعلوماتية استثناء، وذلك خشية محو وطمس الدليل بسهولة، ومن ثم يكون من الصعب ملاحقة المجرم أو كشف شخصيته.

وأخيراً درسنا في هذا المبحث، مدى قدرة الوسائل التقليدية في إثبات الجريمة المعلوماتية من أجل الحصول على الدليل الإلكتروني، فتناولنا في المطلب الأول منه الصعوبات التي تعترض إثبات الجريمة المعلوماتية بالوسائل التقليدية، وتبين لنا أن هذه الصعوبات منها ما يتعلق بالجريمة المعلوماتية ومنها ما يتعلق بالدليل الإلكتروني، ومنها ما يتعلق بأسباب متعددة لعل من أهمها نقص خبرة أجهزة العدالة وصعوبات فنية، كما درسنا في المطلب الثاني مدى ملاءمة الوسائل التقليدية لإثبات الجريمة المعلوماتية، فدرسنا الخبرة، وأيضاً المعاينة وذلك بتعريفها ومحل إجراءها وآلية المعاينة، وكذلك درسنا إجراءات التفتيش والضبط، وعرضنا لمدى خضوع المكونات المادية والمعنوية لإجراء التفتيش والضبط وآلية التفتيش والضبط للحصول على الدليل الإلكتروني.

ونستنتج أن الوسائل التقليدية لم تعد كافية بشكل فعال لإثبات الجريمة المعلوماتية، وبالتالي للحصول على الدليل الإلكتروني، مما أدى إلى ظهور إجراءات حديثة، إذ إن التطور المستمر الذي يتصف به الدليل الإلكتروني أدى إلى تطور وسائل الحصول عليه، وسنعرض هذه الإجراءات الحديثة في الفصل الثاني.

الفصل الثاني

إثبات الجريمة المعلوماتية بالوسائل المستحدثة

إن من أهم سمات هذا العصر أنه عصر التكنولوجيا الرقمية، إذ بات يتحرك من خلال تكنولوجيا المعلومات والاتصالات، وواكبته حركة إجرامية كبيرة، فقد ظهر ما يسمى بالجرائم المعلوماتية، ويمكن تعريف الجريمة المعلوماتية بأنها كل فعل أو امتناع عن فعل يتم إعداده أو التخطيط له، يتم بموجبه استخدام أي نوع من الحواسيب الآلية سواء الحاسوب الشخصي أو شبكات الحاسوب أو الأنترنت أو وسائل التواصل الاجتماعي لتسهيل ارتكاب جريمة، أو عمل مخالف للقانون، أو جريمة تقع على الشبكات نفسها عن طريق اختراقها بقصد تخريبها أو تعطيلها أو تحريف أو محو البيانات أو البرامج التي تحويها، كما تشمل الجرائم المعلوماتية جرائم الاعتداء على سلامة أنظمة المعلومات والبيانات وسريتها، وجرائم الاعتداء على الحياة الخاصة للأفراد، وجرائم الاعتداء على الأموال والاحتيال المعلوماتي، وجرائم التدليس المعلوماتي[1].

وحتى تقوم الجريمة المعلوماتية لابد من إثباتها وإقامة الدليل على وجودها، فالحق أن موضوع التقاضي يجرد من كل قيمة إذا لم يقم الدليل على الواقعة التي يستند إليها، ويمكن إثبات الجرائم المعلوماتية بوسائل متعددة، فمن الممكن إثباتها بوساطة وسائل الإثبات التقليدية كما ذكرنا، غير أن التطور التكنولوجي أدى إلى ظهور وسائل إثبات جديدة[2].

وإن بحث إثبات الجريمة المعلوماتية بالوسائل المستحدثة، يقتضي عرض وبيان ماهية الوسائل المستحدثة في إثبات الجريمة المعلوماتية، ومن ثم بيان فاعلية الوسائل المستحدثة في إثبات الجريمة المعلوماتية وموقف التشريعات منها وضماناتها، وبناءً على ذلك سنقسم هذا الفصل إلى المبحثين الآتيين:

المبحث الأول: ماهية الوسائل المستحدثة في إثبات الجريمة المعلوماتية.

المبحث الثاني: فاعلية الوسائل المستحدثة في إثبات الجريمة المعلوماتية وموقف التشريعات منها وضماناتها.

---

[1] حجازي، 2007.أ، ص.137.

[2] غنيمي، (د.ت)، https://www.da5ira.com/ ص 1.

المبحث الأول

الوسائل المستحدثة في إثبات الجريمة المعلوماتية

إذا كانت الوسائل التقليدية قد تكفي لإثبات الجرائم التقليدية فإنها قد تعجز عن إثبات الجرائم المعلوماتية، وقد ظهرت وسائل إثبات حديثة تساعد وتسهل في إثبات الجرائم المعلوماتية، وتتمثل في وسائل مادية ووسائل إجرائية، وإن بحث الوسائل المستحدثة في إثبات الجريمة المعلوماتية يستلزم بيان الوسائل المادية الحديثة، ومن ثم بيان الوسائل الإجرائية الحديثة، وهذا يقتضي تقسيم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: الوسائل المادية الحديثة.

المطلب الثاني: الوسائل الإجرائية الحديثة.

المطلب الأول

الوسائل المادية الحديثة

يقصد بالوسائل المادية تلك الأدوات الفنية التي تستخدم في نظم المعلومات، والتي تثبت وقوع الجريمة وتحدد الجاني، فالوسائل المادية عبارة عن أدوات او برامج ذات طبيعة تقنية يتم استخدامها بغرض إثبات وقوع الجريمة وتحديد مرتكبيها، أو بالأحرى وسائل فنية الهدف منها جمع مختلف الأدلة الجنائية الرقمية التي يمكن من خلالها الكشف عن ملابسات الجريمة المعلوماتية، ومن بين هذه الوسائل استخدام بروتوكول IP/TCP والبروكسي Proxy والمعلومات التي تحتويها ملفات الكوكيز Cookies ، واستخدام معلومات البروكسي: Proxy ، وبرامج التتبع وكشف الاختراق، وسنبحث ذلك كله في الفروع الآتية:

الفرع الأول: استخدام بروتوكول:IP/TCP .

الفرع الثاني: استخدام معلومات الكوكيز Cookies .

الفرع الثالث: استخدام معلومات البروكسي : Proxy .

الفرع الرابع: استخدام برامج التتبع وكشف الاختراق.

الفرع الأول

استخدام بروتوكول: IP/TCP

يُعد بروتوكول IP/TCP من أكثر البروتوكولات المستخدمة في الإنترنت، لأنه يعد جزءاً أساسياً منه، وهو المسؤول عن تراسل حزم البيانات عبره وتوجيهها إلى أهدافها، فهو يوجد بكل جهاز مرتبط بالإنترنت، ويتكون من أربعة أجزاء، يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني إلى مزود الخدمة، والثالث إلى مجموعة الحواسيب الآلية المترابطة، وأما الجزء الرابع فيحدد الحاسوب الذي تم الاتصال منه.

ويقوم بروتوكول IP بعنونة كل حزمة مع إضافة معلومات أخرى إليها، فيتم استخدام عنوان IP من خلال البحث عن رقم الجهاز وتحديد موقعه الجغرافي، بالإضافة إلى إمكانية مراقبة المستخدم من طرف مزود خدمة الإنترنت وتقديم المعلومات التي تفيد في التحقيق بناء على أن لكل جهاز حاسب آلي يتصل بالإنترنت عنوان IP خاص به، وزيادة على ذلك يعمل عنوان IP بشكل متزامن مع بروتوكول آخر هو بروتوكول التحكم بالنقل TCP الذي تكمن وظيفته في تقسيم المعلومات إلى حزم معلوماتية.

وبالرغم من المعلومات المهمة التي يحتويها بروتوكول IP/TCP، إلا أنه يُثار عدد من الصعوبات في استخدامه، إذ إنه يحتوي على معلومات عن جهاز الحاسوب وليس الأشخاص، لذلك فمن الصعوبة إثبات أن شخصاً قد ارتكب جريمة معلوماتية، ومع ذلك يمكن أن يستخدم كقرينة ضد مالك أو صاحب هذا الجهاز إلى أن يثبت العكس، كما أن هناك إمكانية لاستعمال عناوين زائفة بوضع معلومات غير صحيحة من أجل تجنب التعرف إليهم، أو حتى استخدام برامج معينة تؤمن لهم سرية تحركاتهم عبر الشبكة، وذلك بإخفاء عنوان IP عن المواقع التي يزورونها.

الفرع الثاني

استخدام معلومات الكوكيز :Cookies

استخدام معلومات الكوكيز :Cookies يتم عند زيارة مستخدم الإنترنت أي موقع من مواقع الويب، إذ يفتح هذا الأخيرة ملفاً صغيراً على القرص الصلب يسمى كوكيز Cookies بهدف جمع بعض المعلومات عنه وتحسين عملية تصفح الموقع، فهو يسجل عدداً من المعلومات التي يمكن أن تساعد في التحقيق، من بينها تاريخ زيارة الموقع الإلكتروني، أو تاريخ إجراء التعديلات عليه أو الانتهاء منها، وزيادة على ذلك الاحتفاظ بكلمات السر الخاصة بالمستخدم عند زيارته للموقع[1].

الفرع الثالث

استخدام معلومات البروكسي :Proxy

تم تطوير تقنية البروكسي Proxy لاستخدامها كحواجز نارية Firewalls لشبكة الإنترنت والحاجز الناري عبارة عن نظام أمني يفرض توليد جميع الرزم المرسلة أو الواردة من خلال جهاز وحيد، وتمريرها من خلال الحاجز الناري، فالدور الأساسي الذي تقوم به هو قيامها بدور الوسيط بين مستخدم الإنترنت ومواقعها، وذلك بطلب المعلومات من تلك المواقع وتقديمها للمستخدم، ومن بين أهم ما تتميز به مزودات البروكسي Proxy هو قدرتها في تسريع الوصول إلى شبكة الإنترنت، بالإضافة إلى احتوائها على تدابير أمنية للتحكم بعملية الاتصال بالإنترنت، ومثال ذلك التعرف على الأشخاص المسموح لهم بالاتصال بالشبكة، وتحديد الخدمات التي يمكن استخدامها، أو حتى تحديد الأيام والأوقات المسموح بها بزيارة الإنترنت. وعليه فكل هذه العمليات والمعلومات التي يحتويها البروكسيProxy ، يتم حفظها في قاعدة بياناته، مما يجعل دورها قوياً في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المشتبه به والموجودة عند مزود الخدمة، وبالرغم من المزايا التي تتمتع بها مزودات البروكسي Proxy إلا أنها تحتوي على عدة مساوئ قد تشكل عائقاً في التحقيق،

---

[1] المختار و أبو بكر، 2010، ص 112.

من بينها منع الوصول إلى صفحات مواقع إلكترونية معينة، أو الحصول على صفحات قديمة أو ناقصة أحياناً، إلا أن هذا كله لا يمس في أنها وسيلة مفيدة في التحقيق.

الفرع الرابع

استخدام برامج التتبع وكشف الاختراق

إن طبيعة عمل هذه البرامج تكمن في التعرف على محاولات الاختراق، وكشف كافة المعلومات المتعلقة بمن قام بها، وأيضاً إشعار الجهة المتضررة من هذه العملية. ومن بين هذه البرامج، برنامج Hack Tracer V1.2، فعندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسوب يسارع بإغلاق منافذ الدخول أمام المخترق، ثم يبدأ في عملية اقتفاء أثره حتى يصل إلى الجهاز الذي حدثت العملية من خلاله، ويستعرض هذا البرنامج مجموعة شاملة من بيانات المخترق من حيث عنوان IP الخاص به، وتاريخ حدوث الاختراق باليوم والساعة، وفي الأخير المعلومات الخاصة بمزود الخدمة.

المطلب الثاني

الوسائل الإجرائية الحديثة

إن المقصود بالوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية: " الإجراءات التي تستعمل أثناء تنفيذ طرق التحقيق الثابتة والمحددة والأساليب المتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، فالوسائل الإجرائية عبارة عن أساليب محددة قانوناً تهدف إلى إثبات وقوع الجريمة وتحدد شخصية مرتكبها، وذلك باستخدام تقنيات وبرامج إلكترونية مختلفة"[1].

وتتمثل هذه الوسائل الإجرائية الحديثة، بالوسائل المتعلقة بالبيانات الساكنة، وكذلك بالوسائل المتعلقة بالبيانات المتحركة، وبناءً على ذلك سنقسم هذا المطلب إلى الفرعين الآتيين:

الفرع الأول: الوسائل المتعلقة بالبيانات الساكنة.

الفرع الثاني: الوسائل المتعلقة بالبيانات المتحركة.

---

[1] غنيمي، (د.ت)، ص 4.

الفرع الأول

الوسائل المتعلقة بالبيانات الساكنة

تتمثل هذه الوسائل في التحفظ المعجل على البيانات المخزنة، وفي الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك، وسنبحثهما كالآتي:

أولاً: التحفظ المعجل على البيانات المخزنة.

ثانياً: الأمر بتقديم بيانات معلوماتية عن المشترك.

أولاً: التحفظ المعجل على البيانات المخزنة:

إن التعرض لمفهوم هذه الوسيلة، يقتضي منا تحديد المقصود بمزودي الخدمات بما أنهم هم من يحوزون هذه البيانات، وكذلك تعريف التحفظ المعجل على البيانات المخزنة.

أ – تعريف مزودي الخدمات:

يُعرف مزود الخدمات بأنه: " الشخص الذي يقدم خدماته إلى الجمهور بوجه عام في مجال الاتصالات الإلكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود".

وقد عرفه المشرع السوري في المادة الأولى من القانون رقم /20/ لعام 2022 بأنه الشخص الطبيعي أو الاعتباري الذي يقدم خدمة النفاذ أو الاستضافة أو التطبيقات منفردة أو مجتمعة وما في حكمها، والحاصل على ترخيص لتقديم الخدمة.

كما عرف المشرع القطري في المادة الأولى من القانون رقم (14) لسنة 2014م، الخاص بمكافحة الجرائم الإلكترونية، مزود الخدمة بأنه " أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة تخزين المعلومات"[1].

وأيضاً عرف القانون الفلسطيني رقم (16) لسنة 2017م، بشأن الجرائم الإلكترونية مزود الخدمة بأنه " أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو أي

---

(1) الذيب، 2019م، ص220 –228.

شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب نيابة عن أية خدمة إلكترونية أو مستخدمي هذه الخدمة".

ب – تعريف التحفظ المعجل على البيانات المخزنة:

يقصد بهذا الإجراء: "توجيه السلطة المختصة لمزود الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش، أو الأمر بتقديم بيانات معلوماتية"[1].

ويسوغ هذا الإجراء في أن البيانات في البيئة الإلكترونية قابلة للمحو أو التغيير أو العبث بها بسرعة، وقد يكون الدافع هو طمس كل ما يؤدي إلى كشف شخصية فاعل الجريمة، فمثلاً قد يعلم أعضاء الضابطة العدلية بوجود صور إباحية للأطفال في اليوم الأول فيقومون باتخاذ إجراءات الحصول على إذن تفتيش في اليوم التالي، وفي اليوم الثالث يحصلون على الإذن ثم يصل إلى علمهم أن المزود قام بشطب السجلات كالمعتاد في اليوم الثالث المذكور، فالتحفظ من خلال هذا المثال يتضح أنه إجراء أولي أو تمهيدي الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها[2].

كما أن البيانات المذكورة في الأمر تتضمن أيضاً بيانات المرور المتعلقة بالاتصالات السابقة، وهذا بغرض تحديد خط سير الاتصال، أي مكان ومصدر وصول هذه الاتصالات، والتي تُعد من الأمور الجوهرية للتعرف على هوية الأشخاص الفاعلين، وقد عرفت المادة الأولى الفقرة (د) من اتفاقية بودابست هذا النوع من البيانات بأنها صنف من بيانات الحاسوب التي تشكل محلاً لنظام قانوني محدد، إذ يتم استخراج هذه البيانات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة، وبذلك تتمثل مجموعة من البيانات في: مصدر الاتصال ووجهته المقصودة، وخط السير، ووقت أو زمن الاتصال وفقاً لتوقيت غرينتش، وحجم الاتصال ومدته، ونوع الخدمة المعطاة مثل نقل الملفات أو البريد الإلكتروني أو المراسلات الفورية، وغالباً ما يحوز مزود الخدمة بمفرده بيانات المرور، ما يكفي لتحديد مصدر أو نهاية الاتصال

---

[1] مصطفى، 2010، ص159.

[2] هلال، 2015، ص59.

بدقة، بل إن كل واحد منهم يكون لديه بعض أجزاء اللغز، ويتعين أن توضع هذه الأجزاء تحت الاختبار بقصد تحديد مصدرها والجهة المرسل إليها[1].

ثانياً: الأمر بتقديم بيانات معلوماتية عن المشترك:

يقصد به: " أن تصدر السلطة المخولة أمراً إلى مقدم الخدمة على الشبكة أو أي شخص في حيازته أو تحت سيطرته بيانات معينة ليقوم بتقديمها، سواء أكانت هذه البيانات تتعلق بالمحتوى أم بخط السير"[2].

كما يقصد بهذا الأمر "تمكين السلطة المختصة من إلزام مزودي الخدمة بتقديم بيانات موجودة بحوزتهم أو تحت سيطرتهم تتعلق بالمستخدم".

وقد حددت اتفاقية بودابست المقصود بهذه البيانات بقولها إنها تتعلق بنوع خدمة الاتصال التي اشترك فيها الشخص والوسائل الفنية لتحقيقها، والعنوان البريدي أو الجغرافي ورقم الهاتف، ودخول المشترك للحصول على تلك الخدمة والفواتير التي ترسل إليه، وأي معلومات تتعلق بطريقة الدفع، وأي معلومات أخرى تتعلق بأداء الخدمة أو الاتفاق بين المشترك ومزود الخدمة[3].

ويمتد الأمر الذي يمكن للسلطة المكلفة بالتحقيق إصداره ليشمل نوعين من البيانات المتعلقة بالمستخدم:

أ- البيانات المتعلقة بالمرور[4]:

وهي التي تكون في الغالب في حيازة مزود الخدمة فقط، والمقصود بهذا النوع من البيانات تلك التي تعالج الاتصالات التي تمر من خلال نظام معلوماتي، فتحدد الاتصال ومقصده وسيره وتاريخه ووقته، ويتضمن هذا النوع من البيانات (بيانات المرور المتعلقة باتصالات سابقة)، إذ إنه من خلال هذه البيانات يمكن تحديد خط سير الاتصال، فيتيح إمكانية تحديد هوية من أسهم في ارتكاب الجريمة محل التحقيق.

---

[1] مصطفى، 2010، ص159 - 161.

[2] المخول، 2024، ص393.

[3] هلال، 2015، ص61.

[4] حددت المادة (1) فقرة (د) من اتفاقية بودابست لعام 2001م، بيانات المرور بأنها: " أي بيانات كومبيوتر متعلقة باتصال عن طريق منظومة كومبيوتر، والتي تنشأ من منظومة كومبيوتر تشكل جزءاً من سلسلة الاتصالات، توضح مصدر الاتصال، والوجهة المرسلة إليها، والطريق الذي تسلكه، ووقته وتاريخه، وحجمه، ومدة وقوع الخدمة المذكورة ".

ب- البيانات المتعلقة بمحتوى الاتصال:

المقصود بها مضمون المعلومات المنقولة عن طريق الاتصال الإلكتروني.

وليس هناك اختلاف جوهري بين هذين النوعين من البيانات من ناحية المضمون، وإنما يتمثل الاختلاف بينهما في درجة تعلق كل منهما بحماية الحق في الخصوصية.

الفرع الثاني

الوسائل المتعلقة بالبيانات المتحركة

يقصد بالإجراءات المتعلقة بالبيانات المتحركة المراقبة الإلكترونية، ويمكن تعريف المراقبة الإلكترونية بأنها "ذلك العمل الذي يقوم به المراقب، باستخدام التقنية الإلكترونية، لجمع المعلومات عن المشتبه فيه، سواء أكان شخصاً أم مكاناً أم شيئاً، وذلك لتحقيق غرض أمني"[1].

وإن المراقبة الإلكترونية تتم من خلال مراقبة المكالمات الهاتفية أو المكالمات الإلكترونية على الإنترنت[2]، ودراسة إجراء المراقبة على المكالمات الهاتفية والإلكترونية للحصول على الدليل تقتضي بيان ماهية مراقبة المكالمات الهاتفية أولاً، ومن ثم بيان ماهية مراقبة المكالمات الإلكترونية ثانياً، وذلك فيما يأتي:

أولاً: ماهية مراقبة المكالمات الهاتفية.

ثانياً: ماهية مراقبة المكالمات الإلكترونية.

أولاً: ماهية مراقبة المكالمات الهاتفية:

إن المراقبة تعني أن المحادثات الصادرة من هاتف معين أو إليه أو أي عنوان هاتفي آخر، ينصت إليه بشكل سري، أو يلتقط باستخدام وسائل تقنية مساعدة من أجل الحصول على محتويات تلك المكالمات موضوع المراقبة[3].

---

[1] الخن، 2012، ص100.

[2] خالد، 2007، ص219.

[3] خالد، 2007، ص220.

وتتم المراقبة عادة باستخدام ميكروفونات مخفية عندما تكون الضابط العدلية بحاجة إلى استخدام هذه الوسائل – ضمن الحدود القانونية – للكشف عن بعض الجرائم خاصة المنظمة منها، كجرائم المخدرات والجرائم الواقعة على أمن الدولة، ومن أجهزة التنصت الاعتيادية المعتمدة من قبل الضابطة العدلية في العالم ميكروفونات صغيرة الحجم مرتبطة بسلك رفيع متصل بمسجل صغير الحجم أيضاً، بحيث تستخدمها الضابطة العدلية وتتكلم مع المشتبه به وتسجل صوته مثلاً من دون أن تكشف الضابطة العدلية عن هويتها لغرض إلقاء القبض على ذلك الشخص واستخدام المكالمة المسجلة في الإثبات[1].

ومن الجدير بالذكر أن التنصت على المكالمات الهاتفية وتسجيلها قد لا يتطلب اتصالاً فعلياً بالخط الهاتفي المراد مراقبته، لأنه يكون هناك مجال كهربائي كافٍ حول الخط يسهل عملية التقاط المحادثات، كما قد لا يتطلب الدخول إلى المسكن أو المكان المراقب لغرض وضع بعض أجهزة المراقبة والتسجيل، إذ من الممكن وضع أجهزة دقيقة معدة لهذا الغرض تثبت خارج جدران المكان المراقب، كما أن هناك من الأجهزة ما يمكن دسها في ملابس الشخص المراقب من دون علمه[2].

وتختلف مراقبة المكالمات الهاتفية عن التسجيل الصوتي، في أن الأولى تتم دائماً خلسة وبصورة سرية ومن دون علم الأشخاص المراد مراقبتهم، كما تتميز المراقبة بخاصية أخرى هي أن تسجيل المكالمات الهاتفية من خلال عملية المراقبة أو التنصت لا يقتصر على أحاديث الشخص المتهم فحسب، بل يتعدى ذلك إلى الطرف الآخر الذي يبادله الحديث أيضاً[3].

ويؤخذ على استراق السمع أو التنصت على المحادثات الهاتفية أنه لا يوجد ما يؤكد صدور الحديث عن الشخص المراقب، ولا سيما إذا كانت الأصوات تتشابه، كما أنه من السهل أن يستعمل الغير هاتف المشتبه فيه

---

(1) Frank J. Donner; 1981، P.110 - 112.

(2) خالد، 2007، ص220.

(3) خالد، 2007، ص220 – 221.

في غيبته مثلاً، ويزعم بأنه المشتبه فيه، وعليه يجب الحذر في قبول الدليل الذي يتم الحصول عليه عن طريق مراقبة المحادثات الهاتفية لما يشوبه من شكوك، إلا إذا أقر المشتبه به بصحة محتوى المراقبة أو التسجيل[1].

وتتبنى التشريعات الجزائية معيارين لتحديد خصوصية المكالمة الهاتفية وتسجيل المحادثات الشخصية، وهما: معيار طبيعة المكان، ومعيار طبيعة الكلام، بحيث تمد التشريعات التي تأخذ بالمعيار الأول حمايتها إلى الأحاديث التي تتم في الأماكن الخاصة فقط، من دون الأخذ في الحسبان طبيعة المكالمات الهاتفية أو الأحاديث الشخصية، ومنها ما يوفر الحماية معتمداً على طبيعة الحديث من حيث عده من قبيل الخصوصية أو العلانية من دون الاهتمام بالمكان الذي يجري فيه ذلك الحديث[2].

وينتقد بعض الفقه[3] موقف التشريعات التي تأخذ بمعيار خصوصية المكان، **والباحث يؤيد هذا الانتقاد، لأن معيار طبيعة المكان من حيث كونه مكاناً خاصاً يصح الاستناد إليه في حالة حرمة المساكن والمحال الخاصة، في حين أن حرمة المحادثات ينبغي أن تصان سواء أكانت في مكان خاص أم عام، وأن المحادثات الهاتفية هي في طبيعتها سرية، ولها خصوصية بصرف النظر عن المكان الذي يجري فيه الحديث الهاتفي.**

ثانياً: ماهية مراقبة المكالمات الإلكترونية:

إن بحث ماهية مراقبة المكالمات الإلكترونية، يقتضي تعريف هذا الإجراء ومحله، وكذلك الآلية المتبعة لإجرائه.

أ- تعريف مراقبة المكالمات الإلكترونية:

مراقبة المكالمات الإلكترونية والذي يطلق عليه أيضاً الاعتراض الإلكتروني هو إجراء يتعلق بالبيانات المتحركة وإجراءاتها، ويُعرَّف بأنه: "اعتراض الاتصالات الإلكترونية الخاصة، والمقصود بهذا الإجراء مراقبة الاتصالات الإلكترونية أثناء بثها، أي في الزمن الفعلي لنقلها بين الأطراف"[4].

---

[1] خالد، 2007، ص221.

[2] خالد، 2007، ص236 – 237.

[3] عوض، 1999، ص311.

[4] هلال، 2015، ص62.

ومن أهم خصائص الإنترنت أنه يسهل مراقبته، فالمعلومات تنتقل من خلال أجهزة الحاسوب التي يتصل بعضها ببعضها الآخر عن طريق الخادم ضمن الإنترنت، وبالتالي فإن كل جهاز أو موقع يسهل متابعته ومراقبته من أي جهاز مرتبط بالإنترنت[1].

ب- محل مراقبة المكالمات الإلكترونية:

ميزت اتفاقية بودابست بين نوعين من البيانات المعلوماتية محل مراقبة المكالمات الإلكترونية، وهما: البيانات المتعلقة بالمرور والبيانات المتعلقة بمحتوى الاتصال، لذلك لابد لنا من دراسة هذين النوعين من البيانات.

النوع الأول: البيانات المتعلقة بالمرور:

عرفت المادة الأولى من اتفاقية بودابست البيانات المتعلقة بالمرور بأنها: "كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي، والتي يتم إنتاجها بوساطة هذا النظام المعلوماتي بوصفه عنصراً في سلسلة الاتصال، مع تعيين المعلومات الخاصة بأصل الاتصال، ومقصد الاتصال أو الجهة التي تقصد من الاتصال، وخط السير، والساعة والتاريخ، وحجم ومدة الاتصال، ونوع الخدمة".

النوع الثاني: البيانات المتعلقة بمحتوى الاتصال:

إن الاتفاقية لم تورد تعريفاً لها، ولكنها تشير إلى المحتوى الإخباري للاتصال، أي مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال، فيما عدا البيانات المتعلقة بالمرور.

وهناك من يلاحظ أن هناك تقارباً في المعنى بين كلا النوعين، إلا أنهما مختلفان تماماً من حيث درجة المساس بالحق في الخصوصية، إذ يكون ذلك أكثر أهمية بالنسبة إلى مراقبة محتوى الاتصال أو المراسلة، ومن ثم تفرض ضمانات أكبر عند تجميع محتوى البيانات في الزمن الفعلي عن حركة البيانات، سواء من حيث الجرائم التي من أجلها يتم توظيف هذا الإجراء، أو من حيث السلطة المختصة بإصدار أمر المراقبة.

---

[1] الحلبي، 2011، ص53.

وعلى العكس تضع بعض الدول كفرنسا مفهوماً موحداً لكل من تجميع حركة البيانات ومراقبة محتوى البيانات الإلكترونية، ومن ثم تسري عليهما الضمانات الخاصة نفسها عند اتخاذ أحد الإجراءات، من دون الأخذ في الحسبان الحساسية التي تحيط بموضوع مراقبة محتوى البيانات، ويرجع ذلك إلى عدم وجود تمييز في القانون الذي لا يوجد فيه اختلافات حول المصلحة في الخصوصية أو تشابه إجراءات التجميع التقني [1].

وفي إطار تحديد محل المراقبة الإلكترونية ثارت مشكلة تحديد طبيعة البريد الإلكتروني غير المفتوح في صندوق خطابات مقدم خدمات الإنترنت، **فهل يجب عدها اتصالات إلكترونية مخزنة أم اتصالات إلكترونية متحركة، وبالتالي تطبق عليها الإجراءات المتعلقة بالبيانات المتحركة والمتمثلة في اعتراض الاتصالات الإلكترونية، ومن ثم لا يتم الحصول عليها إلا عن طريق سلطة الاعتراض؟** وحسم المشرع الأمريكي هذا الأمر، وعد الاتصالات الإلكترونية المخزنة من قبيل البيانات الساكنة، وبالتالي تطبق عليها كل الإجراءات التي تتناسب مع هذا النوع من البيانات من تفتيش وأمر بالتحفظ العاجل، بدليل أنه قام بتعديل قانون خصوصية الاتصالات الإلكترونية، ليشمل حماية الاتصالات الإلكترونية المخزنة من البريد الإلكتروني والرسائل الصوتية غير المفتوحة والمخزنة لدى مزود الخدمة[2].

وقد تم تأكيد هذه القاعدة في عدد من القضايا مثل قضية (United States v.Smith) إذ قرر القضاء الأمريكي بأنه لا يمكن مراقبة الاتصالات السلكية وهي في حالة التخزين الإلكتروني[3].

جـ- الآلية المستخدمة في مراقبة المكالمات الإلكترونية:

إن السؤال الذي يطرح نفسه هو: **ما التقنية المستخدمة في مراقبة المكالمات الإلكترونية؟**

في الحقيقة تعددت التقنيات المستخدمة في مجال اعتراض المكالمات الإلكترونية، فهناك برامج مخصصة لفحص الرسائل الإلكترونية الصادرة والواردة، وبرامج تقوم باستعادة الرسائل التي تمّ إلغاؤها أو محوها، وأخرى تقوم بتعقب المواقع الإباحية، وغير ذلك من هذه البرمجيات. وسنتناول فيما يأتي أبرز أنواع هذه البرمجيات:

---

[1] مصطفى، 2010، ص165 - 167.

[2] هلال، 2015، ص62.

[3] مصطفى، 2010، ص165 - 167.

- تقنية برنامج "كارنيفور" للتنصت على البريد الإلكتروني:

طورت إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفيدرالي الأمريكي FBI، برنامج أطلق عليه اسم "كارنيفور"، إذ يقوم هذا البرنامج بتعقب وفحص رسائل البريد الإلكتروني الصادرة والواردة عبر المخدمات المستخدمة من قبل مزودي خدمة الإنترنت، فيما إذا كان هناك اشتباه بأن هذه الرسائل تحمل معلومات عن جرائم أو حوادث جرمية، وهذا البرنامج يقوم بفحص وتسجيل الرسائل التي تحتوي على كلمات أو معلومات يشتبه في أن لها علاقة بالجرائم، ويتجاهل الرسائل الأخرى[1].

- برامج استعادة الوثائق الإلكترونية الممحوة:

في عام 1988م، أسس الأمريكي "جون جيسين" شركة تدعى "اكتشاف الأدلة أو القرائن الإلكترونية". وقد اتجهت هذه الشركة لتسهيل عملها في البحث والتحري نحو الوثائق الإلكترونية، بحسبان أن هذه الوثائق تترك وراءها أثراً لا يُمحى، ويمكن استعادتها مهما اجتهد الفاعل في محوها، وذلك على عكس الوثائق الورقية التي تتحول إلى مادة يصعب استرجاع المعلومات منها بعد تمزيقها أو يستحيل بعد إحراقها.

ومن أشهر القضايا الذي اعتمدت على هذا الأسلوب، القضية التي رفعتها وزارة العدل الأمريكية وتسع عشرة ولاية ضد شركة مايكروسوفت، لمحاولتها احتكار أنظمة تصفح الإنترنت، فبعد البحث في نظام البريد الإلكتروني العائد لهذه الشركة، تم اكتشاف رسائل إلكترونية تتعلق بمحاولة الإضرار بالمنافسين التجاريين، التي اعتقد أصحابها أنهم قاموا بمحوها، ومن أشهر الرسائل الممحوة التي استخدمت في هذه القضية، الرسالة التي سأل فيها رئيس مايكروسوفت عدداً من كبار الموظفين في شركته عمّا إذا كان لديهم خطة تتعلق بما يمكن فعله من أجل إلحاق الضرر بالخصوم التجاريين[2].

- برنامج مراقبة البريد الإلكتروني:

وهو برنامج صمّمه المبرمج الأمريكي "ريتشارد إتوني"، ويقوم هذا البرنامج بسبر محتوى البريد الإلكتروني موضوع المراقبة، وقراءة الرسائل التي قام صاحبها بإتلافها، أو تلك التي لم يقم بتخزينها أصلاً، ويمكن تحميل

---

[1] موسى، 2005، ص189.

[2] موسى، 2005، ص193 - 194.

هذا البرنامج على أي جهاز حاسوب بهدف مراقبة بريده الإلكتروني، وقد استخدمت المخابرات الأمريكية هذا البرنامج لكشف مشتبه به من الجنسية الروسية حاول اختراق بعض المواقع على شبكة الإنترنت[1].

ومن الأمثلة الشهيرة للمراقبة الإلكترونية عن طريق مراقبة البريد الإلكتروني، أنه تمّ الكشف عن العلاقة الغرامية بين الرئيس الأمريكي السابق "بيل كلينتون" والآنسة "مونيكا لوينسكي"، عن طريق مراقبة البريد الإلكتروني لهما[2].

- برنامج تعقب المواقع الإباحية:

ويُعرَّف هذا البرنامج باسم "نوبد شرطة الإنترنت" وهو يقوم بالبحث عن الصور الجنسية المخلّة بالأخلاق في أنظمة الحواسيب التي تعمل وفق برنامج تشغيل ويندوز بإصداراته الحديثة، ثم يقوم بتبليغ الهيئات الحكومية عنها، بهدف تطهير شبكة الإنترنت من هذه المواقع والصور[3].

---

[1] موسى، 2005، ص216.

[2] الخن، 2012، ص102.

[3] موسى، 2005، ص217.

المبحث الثاني

فاعلية الوسائل المستحدثة في إثبات الجريمة المعلوماتية وموقف التشريعات منها وضماناتها

إن بيان دور الوسائل المستحدثة في إثبات الجريمة المعلوماتية وموقف التشريعات منها، يقتضي تسليط الضوء على أهمية الوسائل المستحدثة في إثبات الجريمة المعلوماتية، ومن ثم بيان موقف التشريعات من الوسائل المستحدثة وضماناتها، وبناءً على ذلك سنقسم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: أهمية الوسائل المستحدثة في إثبات الجريمة المعلوماتية.

المطلب الثاني: موقف التشريعات من الوسائل المستحدثة وضماناتها.

المطلب الأول

أهمية الوسائل المستحدثة في إثبات الجريمة المعلوماتية

إن بحث أهمية الوسائل المستحدثة في إثبات الجريمة المعلوماتية، يقتضي بيان أهمية الوسائل المتعلقة بالبيانات الساكنة في إثبات الجريمة المعلوماتية، ومن ثم بيان أهمية الوسائل المتعلقة بالبيانات المتحركة في إثبات الجريمة المعلوماتية، وبناء على ذلك سنقسم هذا المطلب إلى الفرعين الآتيين:

الفرع الأول: أهمية الوسائل المتعلقة بالبيانات الساكنة في إثبات الجريمة المعلوماتية.

الفرع الثاني: أهمية الوسائل المتعلقة بالبيانات المتحركة في إثبات الجريمة المعلوماتية.

الفرع الأول

أهمية الوسائل المتعلقة بالبيانات الساكنة في إثبات الجريمة المعلوماتية

تتمثل هذه الوسائل كما سبق أن ذكرنا في التحفظ المعجل على البيانات المخزنة، وفي الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك، وهناك من يرى[1] أن الإجراءات المتعلقة بالبيانات الساكنة لها أهمية في استخراج الدليل الإلكتروني، وخاصة أنها تكون تحت إشراف مختصين في الحاسوب وملحقاته وشبكاته، على الرغم من أن فيها اعتداء على الحياة الشخصية للأفراد بسبب الاطلاع على بياناتهم الخاصة، إلا أنه يمكن التغاضي عن هذا الاعتداء في سبيل كشف الحقيقة في الجريمة الواقعة والحصول على الدليل الإلكتروني وهو الهدف المنشود، ونسبة الجريمة المعلوماتية لأشخاص معينين، وعلى الرغم من الخلاف حول السلطة التي لها حق في الاطلاع على البيانات، وكذلك الخلاف فيما يتعلق بإلزام مزود الخدمات بإعطاء المعلومات، إلا أن الهدف يبقى هو إيجاد الدليل الإلكتروني.

فلا بد من الإشارة أن إجراء التحفظ العاجل على البيانات المخزنة، الذي يعد إجراء أولياً تمهيدياً الهدف منه محاولة الاحتفاظ بالبيانات قبل فقدانها وضمان السرعة اللازمة للحفاظ على الأدلة المتعلقة بالجريمة المعلوماتية وتجميعها ولاسيما أن آثارها يمكن أن تندثر بسرعة وفي ظرف وجيز، يتلاءم وطبيعة البيئة المعلوماتية من حيث قابلية البيانات فيها للمحو والفقد بسرعة.

ولما كان التحفظ العاجل والتجميع الفوري للمعطيات والبيانات يتطلب أحياناً اعتراض محتوى هذه البيانات الإلكترونية، فقد استحدثت آليات تعطي الصلاحية للسلطات المختصة في التجميع الفوري لبيانات الحاسوب من خلال جمع أو تسجيل أو إجبار مقدم الخدمة في نطاق قدرته الفنية على جمع أو تسجيل سير البيانات المرتبطة باتصالات معينة وكذا صلاحية الاعتراض على محتوى هذه البيانات.

---

[1] هلال، 2015، ص62.

أمام هذه الشكليات المستحدثة التي تهم البحث عن الجريمة المعلوماتية كان لابد من وجود جهة معينة تتعاون مع الأجهزة المكلفة بالبحث والتحري وتزودهم بمختلف المعلومات التي قد تساعدهم في الوصول إلى الحقيقة لضمان البحث في مواجهة الأشخاص الذي يحوزون إحدى الوثائق أو البيانات المعلوماتية.

وقد ظهرت إلى الوجود إجراءات وتدابير مستحدثة تفرض على مزودي الخدمات الإلكترونية التعاون مع الأجهزة المكلفة بالبحث عن الجرائم المعلوماتية، وتضع التزاماً على عاتق هؤلاء الأشخاص بتزويد هذه الأجهزة بكل المعلومات المفيدة التي يتوفرون عليها في سبيل إظهار الحقيقية[1].

الفرع الثاني

أهمية الوسائل المتعلقة بالبيانات المتحركة في إثبات الجريمة المعلوماتية

شهد عالمنا المعاصر قفزة جبارة في المجال التكنولوجي، لكن هذا التطور استغله المجرمون لتطوير إجرامهم الذي أصبح يرتكب بأساليب مستحدثة جعلت الجريمة أكثر تعقيداً وصعبة الكشف على المحققين، فقد سمح التطور التكنولوجي بتحول الجرائم التقليدية إلى مستحدثة تبعاً للتغيير الذي طالها بفعل التقنية العالية، بالإضافة إلى ظهور جرائم أخرى جديدة، فكان من الطبيعي أن تتطور في المقابل أساليب البحث والتحري، ولعل من أهمها "المراقبة الإلكترونية"، وهي إجراء ليس بالجديد، فطالما اعتمده جهاز الشرطة القضائية للبحث والتحري عن الجرائم والمجرمين، لكون المراقبة هي الصورة الحية والمرئية التي تمثل الواقع الفعلي للحدث الإجرامي؛ لكن تطور الجريمة طوّر من المراقبة أيضاً، فإلى جانب المراقبة المادية ظهرت أيضاً المراقبة التقنية[2].

وإن الهدف الرئيس من المراقبة الإلكترونية التي يسعى إليها المحقق الجنائي من وراء اتخاذ هذا الإجراء هو الحصول على دليل يسهم في كشف غموض الجرائم المعلوماتية، وتأكيد الأدلة المستخلصة من البحث والتحقيق حتى يتم إسناد الجريمة المرتكبة في الفضاء السيبراني للمتهم، وعليه فلا يجوز اللجوء إلى مراقبة

---

[1] قجاج، خصوصية البحث عن الجريمة الإلكترونية: https://www.hespress.com تاريخ الدخول في 2024/4/5

[2] التجاني، 2022م، ص1187.

الأحاديث الخاصة في البحث عن الأدلة إلا إذا توفرت لدى المحقق أدلة جادة تحتاج إلى أن تدعم بإجراء هذه المراقبة.[1]

وتعد اتفاقية بودابست[2]، الأبرز في تبنيها لهذا الإجراء نظراً إلى مسايرتها خصوصية الجرائم المعلوماتية، فالإطار التشريعي لهذه الجرائم ومعاقبة المجرمين يتطلب تبني إجراء خاص وفعال تتمكن من خلاله الأجهزة الأمنية والقضائية والمكلف بالتحقيق الجنائي من الوصول إلى الأهداف المرجوة.

المطلب الثاني

موقف التشريعات من الوسائل المستحدثة وضماناتها

إن بحث موقف التشريعات من الوسائل المستحدثة في إثبات الجريمة المعلوماتية، يقتضي بيان موقف التشريعات الجزائية المقارنة، ومن ثم موقف التشريع السوري، وضمانات الوسائل المستحدثة للحفاظ على خصوصية الأفراد، وبناءً على ذلك سنقسم هذا المطلب إلى الفروع الآتية:

الفرع الأول: موقف التشريعات الجزائية المقارنة.

الفرع الثاني: موقف التشريع السوري.

الفرع الثالث: ضمانات الوسائل المستحدثة للحفاظ على خصوصية الأفراد.

الفرع الأول

موقف التشريعات الجزائية المقارنة

أولاً: التحفظ المعجل على البيانات المخزنة:

فقد نص المشرع الأمريكي على هذا الإجراء في القسم (18 U S.C2703 (f) من قانون خصوصية الاتصالات الإلكترونية الأمريكي (ECPA).

---

[1] سرور، 1993، ص 583-584.

[2] اتفاقية بودابست لمكافحة الجرائم المعلوماتية الصادرة بتاريخ 23 نوفمبر 2001.

أما المشرع الفرنسي فرأى أن هذا الإجراء يُعد اعتداء على حق الخصوصية، واحتراماً منه لحرمة الحياة الخاصة، وألزم مزودي الخدمة بمحو البيانات التي تتعلق بالاتصالات الإلكترونية بين مستخدمي هذه الشبكة، وعاقب بالغرامة من يتقاعس عن محو هذه البيانات[1]، إلا أن القانون الفرنسي الخاص بالأمن القومي والصادر في 2001/11/15م، أقر بمشروعية هذا الإجراء وذلك في حالين: الأول يتعلق بمتطلبات المحاسبة المالية بين مزودي الخدمات والمشتركين في خدماتهم، إذ يقدم مزودو الخدمات لبعض هؤلاء المشتركين بعض الخدمات مدفوعة الأجر، أما الثاني فيتعلق بتقديرات التعاون مع القضاء التي تسوغ الاحتفاظ بتلك البيانات لمدة لا تزيد عن السنة.

وهذا الاستثناء يؤكد ما ذهب إليه التوجه الأوربي رقم (58) لسنة 2002م، والذي قرر بدوره أنه من حق الدول الأعضاء اتخاذ التدابير اللازمة لحماية الأمن العام والدفاع القومي وأمن الدولة والتدقيق في الجرائم، بما يتضمنه ذلك من استثناءات على الحق في الخصوصية، ومن بين هذه الاستثناءات ضرورة التحفظ المعجل على البيانات المعلوماتية المخزنة حفاظاً عليها من التلف والتغيير.

وتجدر الإشارة إلى أنه توجد بعض الاستثناءات على التزام مزودي الخدمات بالتعاون مع سلطات التحقيق، إذ يستبعد القانون الفرنسي البيانات التي تحوزها جهات معينة من القاعدة السابقة، والتي تفرض واجب التعاون مع رجال العدالة بوجه عام، مثلما جاء في نص المادة (31) في الفقرة الثانية من القانون رقم (78/17) الصادر في يناير 1978، الخاص بالمعلوماتية والحريات في فرنسا، إذ تنص هذه المادة على عدم جواز مراقبة المعلومات التي تجمعها الكنائس أو أي تجمعات دينية أو فلسفية أو سياسية، أو نقابية والتي تتعلق بأعضائها أو المتراسلين معها، كما يستثنى أيضاً من هذه القاعدة أنواع معينة من المعلومات نصت عليها المادة (18) من قانون الأمن الداخلي الذي عدل قانون الإجراءات الجزائية الفرنسي، وأدخل المادة (1/60) الخاصة بالمعلومات

---

[1] تنص الفقرة الأولى من المادة (23) من قانون البريد والاتصالات الفرنسي على أنه " يجب على مقدمي خدمة الاتصالات محو وإخفاء أية بيانات تتعلق بالاتصال من اللحظة التي ينتهي بها الاتصال".

التي تكتسي طابع سر المهنة، إذ تنص هذه المادة على أنه "باستثناء المعلومات التي تُعد من أسرار المهنة التي أوردها القانون، والمتواجدة في الأنظمة المعلوماتية أو أي أجهزة للمعالجة الآلية....."[1].

كما نص على هذا الإجراء قانون مكافحة الجرائم الإلكترونية المصري لسنة 2016م، إذ نص في المادة (27) منه على التحفظ على أدلة الإثبات، وهي متعلقة بمزودي الخدمة الإلكترونية، بإلزامهم بحفظ وتخزين بيانات خط سير الحركة، ووسائل البيانات، وذلك لمدة مائة وثمانين يوماً.

وبالتالي نص المشرع المصري على التحفظ على الأدلة وربطه بمدة زمنية معينة محددة وهي ستة أشهر. كما أن المشرع البحريني نص على هذا الإجراء في قانون تقنية المعلومات البحريني رقم (6) لعام 2014م، إذ جاء في المادة (1/12) منه أن "للنيابة العامة الحق بأمر أي شخص سواء مزود الخدمة أم غيره بحفظ الأدلة لمدة 90 يوماً قابلة للتجديد، وكذلك الحفاظ على سرية الأدلة وعدم الإفشاء بها".

وأيضاً نص المشرع القطري في المادة (21) الفقرة (4) من القانون رقم (14) لسنة 2014 م، الخاص بمكافحة الجرائم الإلكترونية، على أنه "يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة، بالآتي: الاحتفاظ المؤقت والعاجل ببيانات تقنية المعلومات أو بيانات المرور أو معلومات المحتوى لمدة تسعين يوماً قابلة للتجديد، بناءً على طلب الجهة المختصة أو جهات التحقيق والمحاكمة".

أما بالنسبة إلى بعض الدول، فمن الملاحظ أن التحفظ على البيانات يُعد بالنسبة إليها، سلطة قانونية جديدة، فهو إجراء تحقيقي مستحدث في سبيل مكافحة الجريمة المعلوماتية، كما أنه متماشٍ مع البيئة الإلكترونية التي تكون فيها البيانات قابلة للمحو والفقد[2].

ثانياً: تقديم بيانات معلوماتية عن المشترك:

فقد جاء في توصية المجلس الأوربي رقم 13 تاريخ 9/11/ 1995، أنه مع احترام الحصانات والامتيازات المقررة قانوناً تجيز القوانين الإجرائية توجيه أوامر لمن يحوز أشياء تفيد في الكشف عن الحقيقة

---

[1] هلال، 2015، ص58 – 59.

[2] هلال، 2015، ص58.

بتسليمها، ولذلك يتعين تعديل القوانين الإجرائية بإصدار مثل هذه الأوامر لمن يحوز معلومات (برامج –قواعد – بيانات) تتعلق بأجهزة الحاسوب بتسليمها للكشف عن الحقيقة.

كما يتعين ومع احترام الحصانات والضمانات المقررة قانوناً إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول إلى نظام من أنظمة المعلومات أو للدخول على ما يحويه من معلومات باتخاذ اللازم للسماح لرجال التحقيق بالاطلاع عليها، وأن تخول سلطات التحقيق إصدار أوامر لأي شخص آخر لديه معلومات عن طريقة التشغيل والمحافظة على المعلومات [1].

كما أن بعض التشريعات المقارنة تسمح لأعضاء الضابطة العدلية بأن يأمروا الأشخاص بتسليم ما تحت أيديهم من موضوعات يُطلب تقديمها كدليل، ومن بينها البيانات المتعلقة بالشخص المشترك في الجريمة، والتي يحوزها مزود الخدمات، وهذا الأخير يلزمه القانون الفرنسي رقم (719) لسنة 2000م، المعدل للقانون (1067) لسنة 1986م، الخاص بحرية الاتصالات، إذ تنص المادة (9/43) من هذا القانون على أنه: "يتعين على مزودي خدمات الدخول المحافظة على بيانات مستعملي خدماتهم، وذلك تمهيداً لطلب السلطات منهم تلك البيانات التي قد تفيد كدليل في جريمة معينة وقعت بالفعل"[2].

أما فيما يتعلق بالقانون الأمريكي، فإنه في قانون خصوصية الاتصالات الإلكترونية أجاز لأعضاء الضابطة العدلية، في إطار ما يقومون به من جمع المعلومات، الاطلاع على البيانات الموجودة في حوزة مزودي الخدمات، والتي تخص مستخدمي شبكة الإنترنت وذلك من خلال توجيه تكليف إلى مزود الخدمات بتقديم تلك المعلومات، وهذه المعلومات تتمثل في ثلاث أنواع: يتمثل النوع الأول في المعلومات الشخصية الخاصة بالمشترك مثل اسمه ورقم هاتفه وعنوانه، والنوع الثاني هو المعلومات الشخصية الخاصة بالمتعامل مع المشترك، أي كل من يتصل به، أو يدخل معه في صفقة مثلاً، وبالنسبة إلى النوع الثالث فهو المعلومات المتعلقة بمحتوى البيانات، كمضمون المحادثات ومضمون الملفات[3].

---

[1] رمضان، 2000، ص81 – 82.

[2] هلال، 2015، ص60.

[3] بن يونس، 2005، ص271.

وهناك قوانين لا تجيز إصدار مثل هذا الأمر لأعضاء الضابطة العدلية وإنما تجيزه لقاضي التحقيق، مثل القانون المصري، إذ جاء في نص المادة (99) من قانون الإجراءات الجنائية المصري أنه "لقاضي التحقيق أن يأمر الحائز لشيء يرى ضبطه أو الاطلاع عليه بتقديمه".

ولا تختلف سلطة النيابة العامة في ذلك عن سلطة التحقيق، كما أن للمحكمة أن تصدر مثل هذا الأمر وفقاً للقانون المصري، وتنص المادة (291) من القانون نفسه على أن "للمحكمة أن تأمر ولو من تلقاء نفسها في أثناء نظر الدعوى بتقديم أي دليل تراه لازماً لظهور الحقيقة"[1].

أما فيما يتعلق باتفاقية بودابست، فقد نصت في المادة (18) منها على أنه: "يجوز تمكين السلطات المختصة من إلزام مقدمي الخدمات إعطاء البيانات المتعلقة بالمشترك، سواء كانت في حيازته المادية أو تحت سيطرته، ويشترط في هذه البيانات أن تكون مخزنة، وبالتالي فإنه لا يدخل فيها أي معلومات متعلقة بحركة ومحتوى البيانات ذات العلاقة باتصالات مستقبلية".

وأيضاً نص المشرع القطري في المادة (21) الفقرة (1) و (3) من القانون رقم (14) لسنة 2014 الخاص بمكافحة الجرائم الإلكترونية، على أنه: "يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة، بالآتي:

1- تزويد الجهة المختصة، أو جهات التحقيق والمحاكمة، بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على أمر من النيابة العامة.

3- الاحتفاظ بمعلومات المشترك لمدة سنة".

ثالثاً: المراقبة الإلكترونية:

هناك من يرى[2] أنه لا يجوز استخدام وسيلة إثبات تنافي الأخلاق السليمة كالتنصت على الهاتف، والمذياع السري، لأن مراقبة المحادثات الهاتفية تتم من دون علم الشخص المستهدف وتتيح سماع وتسجيل أدق أسرار حياته الخاصة[3].

---

[1] هلال، 2015، ، ص61.

[2] محمد، 2014، ، ص 44.

[3] طوالبة، 2004، ص 154.

إلا أن الرأي السائد هو مشروعية اعتراض المحادثات الهاتفية، لأن الغرض من مشروعية المراقبة هو تحقيق نوع من التوازن بين حق الأفراد في الخصوصية والسرية، وحق المجتمع في مكافحة الجريمة بوسائل فعالة ليعيش آمناً ومطمئناً[1].

وبالنسبة إلى موقف التشريعات، فقد أجاز قانون الإجراءات الجنائية الفرنسي مراقبة الاتصالات الخاصة بخصوص تحقيق قضائي، على أن تكون الجريمة على درجة جسيمة من الخطورة، وتكون كذلك عندما تكون العقوبة المقررة لها الحبس لمدة سنتين أو أكثر وفقاً للمادة 100 من قانون الإجراءات الجنائية الفرنسي. ووضع أجهزة المراقبة يتعين أن يكون من قبل أشخاص مؤهلين من العاملين في مرفق الاتصالات العام، ويجب ألا تزيد المراقبة في جميع الأحوال على أربعة أشهر قابلة للتجديد[2].

كما أن القانون الفرنسي الصادر في 10 /1991/7، في شأن الاتصالات يجيز اعتراض الاتصالات البعدية[3]، في حالة المراقبة الإدارية على الاتصالات الخاصة، فقد حدد المشرع الفرنسي حالاتها على سبيل الحصر في المادة الثالثة من قانون 10 /1991/7 بشأن سرية المراسلات، فلا تجوز المراقبة إلا للبحث عن معلومات تتعلق بالأمن القومي والمحافظة على المركز العلمي والاقتصادي لفرنسا، ولمكافحة الإرهاب والجريمة المنظمة وإعادة تنظيم الجماعات التي تم حلها بمقتضى قانون عام 1936 بشأن جماعات القتال والفرق الخاصة، كما تستهدف التجارة غير المشروعة في المخدرات، وتجارة السلاح وتزييف العملة والمتاجرة في العنصر البشري. ويقدر رئيس الوزراء حدود المراقبة الأمنية بناء على توصية مكتوبة ومسببة من قبل وزير الدفاع أو وزير الداخلية أو وزير الجمارك، ويقوم هؤلاء جميعاً بمباشرة هذا الاختصاص بأنفسهم، ولا يجوز لهم تفويض الغير في مباشرته إلا لاثنين من معاونيهم، ويتعين إعدام متعلقات التسجيلات والمراقبة بانتهاء الغرض منها، ولقد أنشأ قانون 1991 لجنة تسمى باللجنة القومية لمراقبة التسجيلات الأمنية (Commission nationale de contrôle des interceptions de sécurité)، وتتكون اللجنة من ثلاثة أعضاء، ويتولى تعيين رئيسها رئيس الجمهورية،

---

[1] طوالبة، 2004، ص 154.

[2] Bensoussan Alain: 1996، p.89.

رمضان، 2000، ص78.

[3] حجازي، 2007.ب، ص 383.

ويتولى تعيين عضو من النواب من قبل رئيس مجلس النواب، ويعين عضو آخر من أعضاء مجلس الشيوخ من قبل رئيس المجلس، وتنعقد هذه اللجنة بناء على دعوة من رئيسها، ويجوز لها أن تتصدى من تلقاء نفسها أو بناء على طلب من أصحاب المصلحة للتأكد من أن أعمال المراقبة تتم في إطار القانون، وكل المعلومات التي تصل إلى اللجنة تعد سرية، وتقوم كل عام بنشر تقرير عن نشاطها[1].

كما أن المشرع الجزائري أجاز مراقبة المحادثات الهاتفية في التعديل الأخير لقانون الإجراءات الجزائية بالقانون 22/6 المؤرخ في 2006/12/20م، في نص المادة (14)، المتممة للباب الثاني من الكتاب الأول من الأمر رقم 155/66، في الفصل الرابع تحت عنوان: "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"، في المواد من (65 مكرر 5 إلى 65مكرر 10).

وإذا أخذنا عبارة (الفائدة من ظهور الحقيقة) بالمعنى الواسع، أي بالمعنى الذي يفيد المصلحة العامة، فالمصلحة العامة تقتضي السماح بمراقبة المحادثات الهاتفية، ولاسيما في الجرائم المعلوماتية، ومنها جرائم الاتصالات التي تتميز بصعوبة إثباتها وطبيعتها الخاصة والتي تختلف عن الجرائم التقليدية، لأن هذه المراقبة تحقق فائدتين:

الفائدة الأولى: تتمثل في المساعدة في كشف الجريمة.

الفائدة الثانية: هي تشكيل حماية وقائية مسبقة في هذا النوع من الجرائم.

ويذهب بعض الفقه[2] إلى أنه من الصحيح أن مراقبة الاتصالات الإلكترونية فيه اعتداء على الحياة الخاصة للأفراد وسرية اتصالاتهم، التي كفلها مختلف التشريعات، إلا أن هذا الأمر ضروري في بعض الأحيان في هذه الجرائم المستحدثة التي لا تكفي الإجراءات التقليدية فقط لإثباتها والحصول على الدليل الإلكتروني، وكان لابد من اتباع إجراءات حديثة تتماشى مع طبيعة كل من الدليل الإلكتروني، والجرائم المعلوماتية.

---

(1) Bensoussan Alain: 1996, .p.89.

رمضان، 2000، ص78 – 79.

(2) هلال، 2015، ص69.

فعلى الرغم من أن التنصت مثير للجدل، إلا أنه مسموح به تحت ظروف معينة في جميع الدول تقريباً، فقد أكد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل 1994 على السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسوب ذاته[1].

أما الاتفاقية الأوربية حول جرائم الإنترنت لعام 2001، فقد سمحت المادتان /20/ و/21/ منها بمراقبة حركة البيانات ومحتواها في أثناء عملية التراسل.

وفي فرنسا، أجاز القانون الفرنسي الصادر في 1991/7/10م، اعتراض الاتصالات عن بُعد بما في ذلك شبكات تبادل المعلومات[2]، وحينما أصدر المشرع الفرنسي القانون المؤرخ في 2000/8/1، الذي عدّل قانون حرية الاتصالات المؤرخ في 1986/9/30م، سمح بمقتضى هذا التعديل لمزودي الخدمات بمراقبة حركة أعضاء الإنترنت[3].

وفي فلسطين أجاز المشرع في قانون الجرائم الإلكترونية رقم (16) لعام 2017م، لقاضي الصلح أن يأذن للنيابة العامة بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها؛ للبحث عن الدليل المتعلق بالجريمة، وذلك في الفقرة (1) من المادة (35) منه.

كما تبنّى المشرع الجزائري إجراء المراقبة الإلكترونية كإجراء خاص واستثنائي في الجرائم الخطيرة التي من ضمنها الجرائم المعلوماتية وفق ضوابط وشروط، والمشرع الجزائري سار على نهج اتفاقية بودابست من خلال نصه على آليات خاصة ذات طابع إلكتروني تكشف غموض الجرائم المعلوماتية، ثم أضاف آلية أخرى ضمن القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ومن الأمثلة الواقعية على التنصت على المكالمات الإلكترونية قيام مجرم معلوماتي من الأرجنتين في آب عام 1995م، بالدخول إلى شبكة الحاسوب في مركز آمرية الرقابة البحرية للاستطلاع المحيطي في سانيتاغو بكاليفورنيا، بصورة غير مشروعة إلى مالا يقل عن (395) موقعاً عبر العالم وعلى مدى (836) مناسبة، وتشمل

---

[1] لموسخ، 2009.

[2] هلال، 2015، ص62.

[3] الخن، 2012، ص100.

(12) دائرة أمريكية لمواقع البحرية، و لـ (38) مرة منفصلة، واستهداف (138) موقعاً في (23) بلداً بـ (395) مناسبة، وقام بتعديل بعض الملفات، لكن غالبية النشاط الإجرامي تركز في تركيب ملفات، وقام بتعديل بعض الملفات، لكن غالبية النشاط الإجرامي تركز في تركيب ملفات استكشاف (Sniffer) لإزالة أسماء وكلمات السر الشخصية للمستخدم، وقدرت الخسارة المادية نتيجة ذلك في شبكة ناسا (NASA) وحدها بأكثر من مائة ألف دولار، وتعاونت عدة جهات لمتابعة هذا المجرم، ونتيجة للتحريات التي أجرتها هذه الجهات تم الحصول على أمر قضائي من المحكمة المختصة يسمح لها بالدخول والتنصت على الاتصالات الإلكترونية، إذ تم ربط الحاسوب لديها مع جامعة هارفارد، الأمر الذي مكنها من تحديد هوية المجرم بنجاح من بين (16500) حساب من حسابات المستخدمين، في شبكة الحواسيب التي يتراوح عددها بين (8000) و (9000) حاسوب، ومما (200) إلى (300) مستخدم للخطوط المباشرة، مما يعني ما يقارب (60،000) رسالة بريد إلكتروني في اليوم الواحد، وتم تحديد هوية المجرم باستخدام عملية التقليص الأوتوماتيكي[1].

وهكذا نستنتج أن معظم الدول أخذت بالتنصت على المكالمات الإلكترونية وأجازتها، بهدف رصد الجرائم المستحدثة والحصول على الدليل الإلكتروني.

[1] الطوالبة، 2008، ص5.

الفرع الثاني

موقف التشريع السوري

أولاً: التحفظ المعجل:

نص عليه المشرع السوري في المادة (8) من قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة السوري رقم (17) لعام 2012م القديم، كما يأتي: " أ- يعاقب مقدم الخدمات على الشبكة الذي يهمل تنفيذ التزامه بحفظ نسخة من المحتوى لديه وحفظ بيانات الحركة التي تسمح بالتحقق من هوية الأشخاص الذين يسهمون في وضع محتوى على الشبكة بالغرامة من مئة ألف إلى خمسمائة ألف ليرة سورية.

ب- إذا كان الإهمال المشار إليه في الفقرة /أ/ من هذه المادة مقصوداً وأدى إلى عرقلة التحقيق في جريمة أو الشروع فيها أو إلى عدم التمكن من وقف وقوعها تكون العقوبة الحبس من ثلاثة أشهر إلى سنتين والغرامة من مئتي ألف إلى مليون ليرة سورية".

كما نصت المادة (6) من قانون الجرائم المعلوماتية السوري الجديد رقم 20 لعام 2022 على أنه: "يعاقب الامتناع عن حفظ نسخة من المحتوى الرقمي أو المعلومات أو بيانات الحركة بالحبس من شهر إلى ستة أشهر وغرامة من (2000000) ل.س مليوني ليرة سورية إلى (4000000) ل.س أربعة ملايين ليرة سورية، مقدم الخدمات على الشبكة الذي يمتنع عن تنفيذ التزامه بحفظ نسخة من المحتوى الرقمي أو المعلومات المخزنة لديه أو بيانات الحركة التي تسمح بالتحقق من هوية الأشخاص الذين يسهمون في وضع هذا المحتوى على الشبكة، أو يهمل تنفيذ هذا الالتزام".

ونستخلص من هذه المادة أن المشرع السوري نص على مشروعية هذا الإجراء وإجازته، وذلك بجعله التزاماً وعاقب على الإخلال به بعقوبات جزائية.

ثانياً: تقديم بيانات معلوماتية عن المشترك:

نصت المادة (11) من قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة السوري رقم (17) لعام 2012م السابق، تحت عنوان "الامتناع عن إجابة أمر السلطة القضائية" على ما يأتي: "يعاقب مقدم

الخدمات على الشبكة الذي يمتنع عن إجابة أمر السلطة القضائية بسحب أي جزء من المحتوى المخزن لديه من التداول أو بمنع الوصول إليه بالعقوبة المنصوص عليها على جرائم الامتناع عن تنفيذ قرار السلطة القضائية".

ومن هذا النص نستنتج أن المشرع السوري قد أجاز تقديم بيانات معلوماتية واعترف بمشروعيته وعاقب على عدم تنفيذ الأمر من قبل مقدم الخدمات بعقوبات جزائية.

وفي قانون الجريمة المعلوماتية الجديد رقم (20) لعام 2022م نصت المادة (2) منه التي جاءت بعنوان "التزامات عامة" على أنه: "يلتزم مقدم الخدمات على الشبكة بالآتي: ب- تقديم أي معلومات تطلبها منه السلطات القضائية المختصة".

ثالثاً: المراقبة الإلكترونية:

في التشريع السوري نصت المادة (96) من قانون أصول المحاكمات الجزائية على إعطاء الحق لقاضي التحقيق بمراقبة المحادثات الهاتفية متى كان لذلك فائدة في ظهور الحقيقة.

كما سمحت الفقرة (أ) من المادة 26 من قانون مكافحة الجريمة المعلوماتية رقم /17/ لعام 2012 بالتقصي الإلكتروني أو المراقبة الإلكترونية.

كما نص القانون الجديد للجرائم المعلوماتية رقم (20) لعام 2022م في المادة (18) فقرة (أ) منه على جريمة اعتراض المعلومات، وذلك بمفهوم المخالفة كما يأتي:" أ- يعاقب بالحبس من ثلاثة أشهر إلى سنة وغرامة من خمسمئة ألف ليرة سورية إلى مليون ليرة سورية كل من اعترض أو التقط بوجه غير مشروع المعلومات المتداولة على نظام معلومات أو الشبكة، أو تنصت عليها باستخدام إحدى وسائل تقانة المعلومات".

الفرع الثالث

ضمانات الوسائل المستحدثة للحفاظ على خصوصية الأفراد

سنعرض ضمانات الوسائل المستحدثة للحفاظ على خصوصية الأفراد، كما يأتي:

أولاً: ضمانات التحفظ المعجل على البيانات المخزنة للحفاظ على خصوصية الأفراد:

من أجل ضمان التحفظ المعجل على البيانات المخزنة للحفاظ على خصوصية الأفراد، لابد من مراعاة ما يأتي:

1 – تقييد التحفظ المعجل على البيانات المخزنة بمدة معينة:

يجب أن يتم تقييد التحفظ المعجل على البيانات المخزنة بمدة معقولة تمكن من الرجوع إلى مرتكب الجريمة[1]، وقد قيدت اتفاقية بودابست التحفظ المعجل بمدة 90 يوم كحد أقصى، وهذه المدة قابلة للتمديد.

وهي المدة نفسها التي أخذ بها المشرع البحريني في قانون تقنية المعلومات البحريني رقم (6) لعام 2014م. في المادة (1/12)، وكذلك المشرع القطري في المادة (21) الفقرة (4) من القانون رقم (14) لسنة 2014 الخاص بمكافحة الجرائم الإلكترونية.

وقد أغفل المشرع السوري النص على هذه الضمانة، **ونرى أن تقييد التحفظ المعجل على البيانات المخزنة بمدة معينة يعد من أهم ضمانات مشروعية إجرائه.**

2 – صدور إذن من الجهة القضائية المختصة:

لابد من صدور إذن من الجهة القضائية المختصة للاطلاع على هذه البيانات، وذلك احتراماً لحق الخصوصية.

وقد نص على هذه الضمانة المشرع القطري في المادة (21) الفقرة (4) من القانون رقم (14) لسنة 2014 الخاص بمكافحة الجرائم الإلكترونية، عندما نص على أن الاحتفاظ المؤقت والعاجل ببيانات تقنية المعلومات أو

---

[1] محمد، 2014، ص 84.

بيانات المرور أو معلومات المحتوى، يجب أن يكون بناءً على طلب الجهة المختصة أو جهات التحقيق والمحاكمة.

3- الحفاظ على سرية الأدلة وعدم الإفشاء عنها أو الانتفاع منها:

احتراماً لحق الخصوصية يجب أن تبقى المعلومات المخزنة على الأقراص طي الكتمان حتى تظهر الحاجة إلى استخراج بعض المعلومات منها، وذلك بعد صدور إذن خاص من الجهات المختصة.

إذ نص المشرع البحريني على هذه الضمانة في قانون تقنية المعلومات البحريني رقم (6) لعام 2014م، وذلك في المادة (1/12) منه، حين فرض التزاماً على الأشخاص أو مزودي الخدمة الذين تكلفهم النيابة العامة بالوصول إلى الأدلة والتحفظ عليها بعدم إفشاء أي سر يتعلق بدليل من أدلة الدعوى أو حتى إخبار المشتبه فيهه، وأيضاً أي محاولة من قبلهم للانتفاع من هذه الأدلة[1].

ثانياً: ضمانات الأمر بتقديم بيانات معلوماتية عن المشترك للحفاظ على خصوصية الأفراد:

من أجل ضمان تقديم بيانات معلوماتية عن المشترك للحفاظ على خصوصية الأفراد، لابد من مراعاة ما يأتي:

1- أن يتخذ هذا الإجراء في الجرائم الخطيرة:

من ناحية الجرائم التي يجوز من أجل مكافحتها اتخاذ هذا الإجراء، فإنه يجب حصرها في أشد الجرائم جسامة.

ونرى أنه يجب قصر هذا الإجراء على الجنايات والجنح فقط دون المخالفات، نظراً إلى بساطتها التي لا تسوغ انتهاك خصوصية الأفراد.

2- تحديد السلطة المختصة للقيام بهذا الإجراء:

أكدت اتفاقية بودابست في المادة (18) منها على ضرورة تحديد السلطة المختصة بإصدار أمر تقديم البيانات، إذ يسمح لرجال السلطة العامة بإصدار مثل هذا الأمر إذا تعلق الأمر ببيانات المشترك المعلنة

---

[1] حمودة، 2017، ص131.

للجمهور، في حين أن هناك دولاً تشترط أن يكون هذا الأمر صادراً فقط من السلطات القضائية كالتشريع السوري في المادة (11) من قانون مكافحة الجريمة المعلوماتية وتنظيم التواصل عبر الشبكة السوري رقم (17) لعام 2012م، ولاسيما عند الحصول على نوع معين من البيانات المتعلقة بالحق في الخصوصية مثل رقم بطاقة الائتمان، أو حساب بنكي للمشترك، كما أن المادة /2/ من القانون رقم /20/ لعام 2022 الجديد نصت على ذلك.

ثالثاً: ضمانات المراقبة الإلكترونية للحفاظ على خصوصية الأفراد:

من أجل ضمان إجراء المراقبة الإلكترونية للحفاظ على خصوصية الأفراد، لابد من مراعاة ما يأتي:

1- أن يكون هنالك جريمة خطيرة ارتكبها المشتبه فيه:

لا بد من أن يكون هنالك جرائم خطيرة ارتكبها المشتبه فيه لإمكان مراقبته إلكترونياً.

وقد أكد المجلس الأوربي في التوصية رقم 13 تاريخ 1995/9/11م، على أنه يجب مراجعة القوانين الإجرائية بغرض توفير إمكانية المراقبة والتسجيل في أثناء نقل المعلومات، وبخصوص التحقيقات بشأن بعض الجرائم الخطيرة المتعلقة بسرية وتكامل وتوفير أنظمة المعلومات والاتصالات[1].

من هذه التوصية نستنتج أن المجلس الأوربي رهن إجازة المراقبة والتسجيل فقط بخصوص التحقيقات بشأن بعض الجرائم الخطيرة، وليس كل الجرائم، مما يستوجب تحديد الجرائم التي يجوز فيها المراقبة.

2- أن يكون هنالك مشتبه فيه إلكترونياً:

المشتبه فيه الإلكتروني يمكن أن يكون شخصاً، أو موقعاً، أو بريداً إلكترونياً مخالفاً للقانون، وتشمل المراقبة الإلكترونية جميع تحركات المشتبه فيه عبر الإنترنت، بما في ذلك بريده الإلكتروني[2].

3- فائدة المراقبة في إظهار الحقيقة:

ترى التشريعات المعاصرة أن القول بوجود فائدة من المراقبة من خلال إظهار الحقيقة، هو السند الشرعي المسوغ للاعتراض، على أساس أن هذا الإجراء فيه اعتداء على الحياة الخاصة للأفراد، ولهذا فهو جائز في

---

[1] رمضان، 2000، ص81.

[2] الخن، 2012، ص100.

حالات ضيقة، وذلك برجاء ظهور الحقيقة وإلقاء القبض على الفاعلين، أما مدى فائدة اعتراض الاتصالات الإلكترونية فهي خاضعة لتقدير إما قاضي التحقيق أو قاضي الحكم، وهذا التقدير بدوره يخضع لرقابة قضاء الموضوع[1].

4- صدور إذن بإجراء المراقبة الإلكترونية من السلطة المختصة:

تعد السلطة القضائية بصفة عامة هي المختصة في إصدار هذا الإذن، وُيعد هذا الأمر ضمانة ضرورية حتى يكون هذا الأمر مشروعاً [2].

5- تسبيب الإذن الصادر بشأن مراقبة الاتصالات الإلكترونية:

لم تنص التشريعات التي أخذت بالمراقبة الإلكترونية على ضرورة تسبيب الإذن الصادر بشأن مراقبة الاتصالات الإلكترونية، ونرى أن ذلك يعد ثغرة قانونية ينبغي معالجتها بأسرع وقت بالنظر إلى أهمية التسبيب كضمانة مهمة لتسويغ هذه المراقبة.

6- تحديد الأشخاص المخولين بإجراء المراقبة على المكالمات الهاتفية والإلكترونية.

7- توفير السرية والاحترام للمعلومات:

جاءت هذه الضمانة في توصية المجلس الأوربي رقم 13 تاريخ 9/11/ 1995م التي أكدت على أنه في حالة جمع المعلومات بطريق المراقبة والتسجيل يتعين توفير السرية والاحترام للمعلومات التي يفرض القانون لها حماية خاصة وبصورة مناسبة[3].

وفي نهاية هذا المبحث نجد أن الإجراءات المستحدثة تُعد في غالبيتها إجراءات فنية، وتتميز بالفعالية والسرعة في الحصول على الدليل الإلكتروني، وبالتالي الكشف عن الجرائم وإسنادها إلى مرتكبها.

---

[1] هلال، 2015، ص68.

[2] مصطفى، 2010، ص174 – 175 .

[3] رمضان، 2000، ص81.

الخاتمة

ناقشنا في هذه الرسالة التي كانت بعنوان: " فعالية الوسائل التقليدية في إثبات الجريمة المعلوماتية"، مدى قدرة الوسائل التقليدية في إثبات الجريمة المعلوماتية بحسبانها جريمة مستحدثة ومختلفة في طبيعتها وخصائصها عن الجريمة التقليدية، فكان لابد من تسليط الضوء على قدرة هذه الوسائل التقليدية ونجاعتها في إثبات هذا النوع المستحدث من الجرائم، نظراً إلى انتشاره بشكل كبير وخطورته، وذلك من أجل الوصول إلى أفضل الوسائل لإثباتها، وقد توصلنا في النهاية إلى مجموعة من النتائج والمقترحات نجملها فيما يأتي:

أولاً: النتائج:

– إن الوسائل التقليدية لم تعد كافية وقادرة على ضبط الجريمة المعلوماتية، كما أن البحث عن الجريمة المعلوماتية يتطلب وضع وتبني وسائل مستحدثة تتماشى وتنسجم مع خصوصية وطبيعة هذا النوع من الجرائم.

– تعد إجراءات البحث و التحري أكثر الإجراءات تأثرا بالتحولات العامة الاجتماعية و الاقتصادية والتكنولوجية التي يعرفها محيطها القانوني، فلما كانت الجريمة المعلوماتية بفعل طبيعتها و خصوصيتها قد قلبت كثيراً من المفاهيم القانونية السائدة، سواء على مستوى القانون الموضوعي من حيث التجريم و العقاب بفعل ازدواجية طبيعتها بين جريمة معلوماتية محضة تستهدف الأنظمة و البيانات الإلكترونية في حد ذاتها، أو كجريمة عادية مرتكبة بوساطة تقنية المعلومات كآلية من أجل التواصل و التخطيط لتنفيذ المشاريع الإجرامية ، فلقد فرضت تحدياً إجرائياً يتعلق بإثباتها.

– إن البحث عن الجريمة المعلوماتية في بيئة رقمية تختلف عن البيئة التي اعتادت أجهزة إنفاذ القانون البحث والتحري فيها، قد أسهم في ظهور مجموعة من الوسائل المستحدثة للبحث عن الجريمة المعلوماتية لإثباتها تتناسب مع خصوصية وطبيعة هذا النوع من الجرائم.

– إن إجراء المراقبة الإلكترونية مهم، ويقوم بدور فاعل للحصول على الدليل الإلكتروني، وذلك لعدم كفاية الإجراءات التقليدية للحصول على هذا الدليل، والتي لا تتناسب مع طبيعته.

ثانياً: المقترحات:

– من أجل تفعيل عملية الإبلاغ عن الجريمة المعلوماتية، ومن ثم الإسهام بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها، تظهر ضرورة تشجيع المجني عليهم في هذه الجرائم على الإبلاغ عنها فور وقوعها، وذلك بإبلاغ جهة خاصة، أو بإبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات.

– ضرورة إقامة دورات تدريبية لتأهيل أعضاء الضابطة العدلية وقضاة التحقيق والحكم، وإمدادهم بالخبرة المطلوبة اللازمة لمواكبة الوسائل المستحدثة في إثبات الجريمة المعلوماتية.

– ضرورة تأهيل رجال الضابطة العدلية للتعامل مع مسرح الجريمة المعلوماتي، لما له من أثر كبير في سهولة الحصول على الدليل الإلكتروني، وكذلك في عدم اتلافه، ونقترح جواز أن يلتمس المشتبه فيه في المعاينة من القاضي أن يصرح له بتعيين خبير فني متخصص في الانترنت ليكون بصحبة المحقق في حال كان غير مؤهل، حتى يمنع أي تشكيك في صحة الدليل المستمد من المعاينة.

– ضرورة امتداد تفتيش حاسوب المتهم المتصل بحاسوب أو مُخدّم موجود في مكان آخر داخل الدولة، لكن بشرط أن يكون الدخول للنهاية الطرفية الخاصة بغير المتهم لا يحتاج إلى كلمة مرور خاصة لا يستعملها غيره (شفرة)، وأن يكون نظام الحاسوب الآخر ضمن النطاق الإقليمي للدولة، وأن يكون ذلك التفتيش ضرورياً لإظهار الحقيقة، ولا بد من أن يكون أمر هذا التفتيش مسبباً بإيراد الأسباب الذي دعت إليه.

– ضرورة السماح بتفتيش الحاسوب أو المُخدّم الموجود في مكان آخر خارج الدولة فيما إذا لم يكن النظام المعلوماتي محمياً بنظام شفرة للدخول إلى المعلومات، إذ إن النظام المعلوماتي لا يعرف الحدود، والوحدة التي يتميز بها هي التي تعطي للجهة القائمة بالتفتيش سلطة الولوج وتتبع المعلومات ولو امتد نشاطها إلى طرف نظام معلوماتي في دولة أخرى وذلك لا ينتهك سيادة الدولة، أما في حال وجود نظام شفرة للدخول إلى المعلومات، فنرى أنه لا يجوز تفتيش هذا النظام المعلوماتي لتلك الدولة، ولذلك نرى أن السبيل لحل تلك المشكلة هو تعزيز التعاون الدولي، وذلك من خلال تعزيز دور الإنابة المتبادلة بين الدولة المحققة والدولة التي يراد التفتيش فيها.

– ضرورة عدم تحديد مدة لتنفيذ التفتيش الواقع على نظم الحاسوب والإنترنت، فمن جهة أولى، هذا النوع من التفتيش يختلف في محله عن التفتيش التقليدي، إذ يقع هذا التفتيش على مكونات الحاسوب المادية والمعنوية، ولاسيما إذا ما كان هنالك كم هائل من البيانات التي يتطلب تفتيشها وقتاً طويلاً، ومن جهة ثانية، يستلزم هذا التفتيش بعض الإجراءات المعقدة فيما إذا كانت العناصر المكونة للجريمة موجودة في بلد آخر، الأمر الذي يقتضي الحصول على إذن من هذه الدولة بالتفتيش، أو إعطائها إنابة قضائية، وهذا كله يتطلب وقتاً طويلاً جداً.

– جواز أن يقع التفتيش في إطار تفتيش نظم الحاسوب والإنترنت على غير المتهم، لكن بشرط أن يكون إجراء التفتيش قد تم بناء على أدلة قوية، ولا يكفي أن تشير الدلائل إلى أن في حوزته أشياء تظهر الكشف عن الحقيقة.

– ضرورة توسيع سلطات الجهة المعنية بإجراء التفتيش، ولو استلزم الأمر ولوج النظام المعلوماتي من دون الحصول على إذن عند الضرورة، إذا كان من شأن انتظار صدور الإذن أن يفوت فرصة الحصول على الدليل الإلكتروني.

– وضع استثناء على ضمانة حضور المشتبه فيه أو صاحب المحل أو المسكن أو من ينوب عنهما أو الشهود لإجراء التفتيش في حالة الخشية من العبث بالدليل، أو للإفلات من الاتهام، أو تهديد أحد الشهود، أو الإضرار بسير التحقيق، أو تأخير المحاكمة.

– عدم تحديد وقت معين لتنفيذ التفتيش في إطار تفتيش نظم الحاسوب والإنترنت فقط، وذلك لأجل الحصول على الدليل الإلكتروني قبل التلاعب فيه أو إتلافه من قبل المجرمين.

– بالرغم من أن كلاً من المعاينة والتفتيش من إجراءات التحقيق، والهدف منهما جمع الأدلة التي تثبت وقوع الجريمة ونسبتها إلى المتهم، إلا أن المعاينة بطبيعتها لا تشكل مساساً بأسرار وحقوق الأفراد وحرمتهم، سواء تعلقت بالأشخاص أو الأشياء أو الأماكن بالقدر الذي يمثله التفتيش الذي هو إجراء يمس بمستودع أسرار المتهم وحرمته، وسواء انصب على شخصه، أو مسكنه أو أمتعته، لذلك يتوجب إحاطة التفتيش بضمانات قانونية بشكل أكبر من المعاينة لضمان مشروعية الحصول على الدليل الإلكتروني.

– لابد من تطوير النصوص القانونية المتعلقة بالضبط، لتشمل إمكانية ضبط معطيات الحاسوب والبيانات المعالجة إلكترونياً.

– ضرورة تطوير قواعد الضبط لتتلاءم مع طبيعة البريد الإلكتروني، وتخصيص إجراءات تتصف بالمرونة والسرعة تفوق الإجراءات الخاصة بالبريد العادي، لضبط هذا البريد، وذلك نظراً إلى سهولة التخلص من الأدلة الإلكترونية الموجودة فيه.

– ضرورة الاستغناء عن طلب الإذن لضبط الأدلة الإلكترونية في الجرائم المعلوماتية استثناء، وذلك خشية محو وطمس الدليل بسهولة، ومن ثم يكون من الصعب ملاحقة المجرم أو كشف شخصيته.

– تحديث الأساليب الإجرائية التقليدية في قانون أصول المحاكمات الجزائية السوري من خبرة معاينة وتفتيش وضبط، لتستوعب الحصول على الدليل الإلكتروني، وتحديثها على نحو يكفل استجابتها بشكل كاف للحصول على هذا الدليل المستحدث، بغير أن تتعرض حقوق الإفراد وحرياتهم للخطر عند الإثبات به.

– أثبتت الإجراءات التقليدية المنصوص عليها في قانون الأصول الجزائيّة قصورها في كشف مرتكبي الجرائم المعلوماتيّة، ممّا اضطرّ المشرّعين إلى استحداث جملة من الوسائل الإجرائية الاستثنائية الكفيلة بضمان مكافحة فعّالة لهذا النوع الإجرامي المستجد، لذلك نقترح على التشريعات التي لم تتبنّ هذه الوسائل المستحدثة ضرورة تبني هذه الوسائل لنجاعتها في إثبات الجريمة المعلوماتية.

– سَنّ القوانين والأنظمة الخاصَّة التي تسدُّ كافَّة ثغرات الحصول على الدليل الإلكتروني، ولا سيما الاهتمام بالإجراءات الفنية الحديثة للحصول على الدليل الإلكتروني لكونها تساعد كثيراً في اكتشاف الدليل الإلكتروني، وحفظه، إذ إن الطرق العلمية والفنية للحصول على الدليل الإلكتروني قد أصبحت هي الأكثر فاعلية للحصول على هذا الدليل.

– نظراً إلى أهمية تقييد التحفظ المعجل على البيانات المخزنة بمدة معينة لكونه من أهم ضمانات مشروعية إجرائه، يمكن للمشرع السوري الأخذ بهذه الضمانة لما فيها من حماية أكبر لحق خصوصية الفرد.

– ضرورة إحاطة الإجراءات المتعلقة بالبيانات الساكنة، بضمانات معينة تكفل مشروعية الدليل الإلكتروني، وأهم هذه الضمانات وقوع جريمة معينة، وأن تكون هذه الجريمة من نوع الجناية والجنحة فقط دون المخالفات، والاشتباه بالمدعى عليه أنه مرتكب الجريمة، وإعطاء هذه السلطة لسلطة التحقيق فقط دون غيرها، لخطورة هذا الإجراء.

– بالنسبة إلى تحديد خصوصية المكالمة الهاتفية وتسجيل المحادثات الشخصية، فإنه من الضرورة بمكان تبني معيار طبيعة الكلام وعدم الأخذ بمعيار طبيعة المكان، وذلك لأن حرمة المحادثات ينبغي أن تصان سواءٌ أكانت في مكان خاص أم عام، وأن المحادثات الهاتفية هي بطبيعتها سرية، ولها خصوصية، بصرف النظر عن المكان الذي يجري فيه الحديث الهاتفي.

– عدم جواز إجراء المراقبة الإلكترونية إلا في الجنايات والجنح، أما المخالفات فلا يمكن أن يسوغ إجراء المراقبة الإلكترونية فيها، نظراً إلى بساطتها التي تمنع انتهاك حرمة الاتصالات الإلكترونية، ولا يكفي ذلك بل لابد من تحديد الجنايات والجنح كما فعل المشرع الجزائري، على أن يكون معاقباً عليها بحد أدنى من العقوبة لتجوز فيها المراقبة الإلكترونية.

– ضرورة تسبيب الإذن الصادر بشأن مراقبة الاتصالات الإلكترونية، بالنظر إلى أهمية التسبيب كضمانة مهمة لتسويغ هذه المراقبة.

– ضرورة مراعاة الإجراءات التقليدية والفنية الحديثة للحصول على الدليل الإلكتروني جميع الضمانات المنصوص عليها في القوانين والدساتير والمواثيق الدولية، وذلك من أجل الحصول على دليل إلكتروني مشروع يمكن الاعتماد عليه أمام أجهزة تنفيذ العدالة الجزائية، ويكون ذلك عن طريق تدريب القائمين على هذه الإجراءات سواء التقليدية (الخبرة– المعاينة – التفتيش – الضبط)، أو الفنية الحديثة، ولا سيما المراقبة الإلكترونية لاتباع إجراءات صحيحة ومشروعة لا تمس حقوق الأفراد أو حرياتهم، وتضمن في الوقت نفسه مصلحة المجتمع في أن تبقى حقوقه مصونة ومحمية من جميع المجرمين الذي قد يعتدون عليه.

المراجع

أولاً: باللغة العربية:

1- الكتب العامة:

- رمضان، عمر السعيد (1985م). **مبادئ قانون الإجراءات الجنائية**، ج1، دار النهضة العربية، القاهرة، مصر.

- سرور، أحمد فتحي (1993). **الوسيط في قانون الإجراءات الجنائية**، دار النهضة العربية، القاهرة، مصر.

- سلامة، مأمون (د.ت). **شرح قانون الإجراءات الجنائية**، دار الفكر العربي، الإسكندرية، مصر.

- القدسي، بارعة (2011م). **أصول المحاكمات الجزائية- سير الدعوى العامة**، ج2، الطبعة الأولى، منشورات جامعة دمشق، دمشق، سورية.

- عوض، عوض محمد (1999). **الوجيز في قانون الإجراءات الجنائية**، ج1، دار المطبوعات الجامعية، الإسكندرية، مصر.

- النبراوي، محمد سامي (1968م). **استجواب المتهم**، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر.

2- الكتب المتخصصة:

- المختار، خالد و أبو بكر، إسماعيل (2010). **التحقيق الجنائي في جرائم الحاسوب (سيكولوجيته ـ أساليبه القانونية ـ أدواته العلمية)**، دار عزة للطباعة والنشر، الخرطوم.

- أحمد، هلالي عبد اللاه (1997م). **تفتيش نظم الحاسب وضمانات المتهم المعلوماتي**، الطبعة الأولى، دار النهضة العربية، القاهرة.

- أحمد، هلالي عبد اللاه (2006م). **حجية المخرجات الكمبيوترية في المواد الجنائية**، دار النهضة العربية، القاهرة، مصر.

- بحر، عبد الرحمن (1999م). **معوقات التحقيق في جرائم الإنترنت «دراسة مسحيَّة على ضباط الشرطة في دولة البحرين»**، أكاديمية نايف العربية للعلوم الأمنيّة، السعودية.

- بن يونس، عمر (2005م). **الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية**، الطبعة الأولى، دار النهضة العربية، القاهرة.
- بن يونس، عمر محمد (2007م). **الدليل الرقمي**، الطبعة الأولى، مصر.
- حجازي، عبد الفتاح بيومي (2002م). **الدليل الجنائي والتزوير في جرائم الكومبيوتر والإنترنت**، دار الكتب القانونية، المحلة الكبرى، مصر.
- حجازي، عبد الفتاح بيومي (2007.أ). **الإثبات الجنائي في جرائم الكومبيوتر والإنترنت**، دار الكتب القانونية، المحلة الكبرى، مصر.
- حجازي، عبد الفتاح بيومي (2007.ب). **مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت**، دار الكتب القانونية، المحلة الكبرى، مصر.
- حجازي، عبد الفتاح بيومي (2009م). **جرائم الكومبيوتر والإنترنت**، بهجات للطباعة والتجليد، القاهرة، مصر.
- الحلبي، خالد عياد (2011م). **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن.
- خالد، كوثر أحمد (2007م). **الإثبات الجنائي بالوسائل العلمية– دراسة تحليلية مقارنة**، الطبعة الأولى، مكتب التفسير للنشر والإعلان، أربيل، العراق.
- الخن، محمد طارق (2012م). **الجريمة المعلوماتية**، منشورات الجامعة الافتراضية، دمشق، سورية.
- رستم، هشام محمد فريد (1994م). **الجوانب الإجرائية للجرائم المعلوماتية– دراسة مقارنة**، الطبعة الأولى، مكتبة الآلات الحديثة، أسيوط، مصر.
- رمضان، مدحت (2000م). **جرائم الاعتداء على الأشخاص والإنترنت**، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر.

- الصغير، جميل عبد الباقي (2001م). **أدلة الإثبات الجنائي والتكنولوجيا الحديثة (أجهزة الرادار، الحاسبات الآلية، البصمة الوراثية) دراسة مقارنة**، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر.
- الطوالبة، علي حسن (2008). **التعاون القضائي في مجال مكافحة الجرائم الإلكترونية**، مركز الإعلام الأمني، جامعة العلوم التطبيقية، البحرين.
- الطوالبة، علي حسن محمد (2004م). **التفتيش الجنائي على نظم الحاسوب والإنترنت- دراسة مقارنة**، الطبعة الأولى، عالم الكتب الحديث، إربد، الأردن.
- الطوالبة، علي حسن (2009). **مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي**، دراسة مقارنة"، مركز الإعلام الأمني، البحرين.
- عبد المطلب، ممدوح عبد الحميد (2006م). **البحث والتحقيق الجنائي الرقمي في جرائم الكومبيوتر والإنترنت**، دار الكتب القانونية، مصر.
- عفيفي، عفيفي كامل (2000م). **جرائم الكومبيوتر**، د. ن، القاهرة، مصر.
- فرغلي، عبد الناصر محمد محمود و المسماري، محمد عبيد سيف سعيد (2007م). **الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية- دراسة تطبيقية مقارنة**، جامعة نايف العربية للعلوم الأمنية، الرياض.
- المخول، عيسى مد الله (2024م). **الجريمة الإلكترونية**، الطبعة الأولى، دار القلم، دمشق، سورية.
- مصطفى، عائشة بن قارة (2010م). **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، دار الجامعة الجديدة، مصر.
- مكاري، نزيهة (2009م). **إثبات جرائم الاعتداء على حق المؤلف عبر الإنترنت في التشريع الجزائري، دراسة مقارنة**، الطبعة الأولى، دار هومة، الجزائر.
- موسى، مصطفى محمد (2005). **دليل التحري عبر شبكة الإنترنت**، الطبعة الأولى، دار الكتب القانونية، القاهرة، مصر.

3- الرسائل الجامعية:

- رسائل الدكتوراه:

- الذيب، عيسى غازي (2019م). **مشروعية الدليل الإلكتروني في الإثبات الجزائي- دراسة مقارنة**، رسالة دكتوراه في القانون الجزائي، كلية الحقوق جامعة دمشق، دمشق.

- محمد، معمر علي إبراهيم (2014م). **حجية الأدلة التقنية في الجرائم الإلكترونية**، رسالة دكتوراه، جامعة الرباط الوطني، كلية الدراسات العليا والبحث العلمي، السودان.

- مليكة، بهلول (2013م). **دور الشرطة العلمية والتقنية في الكشف عن الجريمة**، رسالة دكتوراه، كلية الحقوق، جامعة الجزائر 1، الجزائر.

- رسائل الماجستير:

- آل ثنيان، ثنيان ناصر (2012م). **إثبات الجريمة الإلكترونية -دراسة تأصيلية تطبيقية**، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية،.

- هلال، آمنة (2015م). **الإثبات الجنائي بالدليل الإلكتروني**، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر.

- بوحويش، عطية عثمان محمد (2009م). **حجية الدليل الرقمي في إثبات جرائم المعلوماتية**، رسالة ماجستير مقدمة إلى أكاديمية الدراسات العليا، بنغازي.

- عريقات، سهى إبراهيم داود (د.ت). **الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي**، ورقة بحثية، كلية الحقوق، جامعة القدس.

- العدواني، محمد نافع فالح رشدان (2015م). **حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية (دراسة مقارنة بين القانونين الكويتي والأردني)**، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن.

4- المجلات:

- التجاني، زليخة (2022م). المراقبة كإجراء للبحث والتحري عن الجرائم، **مجلة أبحاث قانونية وسياسية**، المجلد7، العدد1، الجزائر.

- الجملي، طارق محمد (2015). الدليل الرقمي في مجال الإثبات الجنائي، **مجلة الحقوق**، المجلد الثاني عشر، العدد الأول، الصفحات (40-73)، جامعة بنغازي، ليبيا.

- حمودة، أمجد خليل (2017). الوسائل الحديثة لإثبات الجرائم التي ترتكب بواسطة الأجهزة الإلكترونية، **مجلة جامعة الأزهر**، عدد خاص بمؤتمر كلية الحقوق الخامس المحكّم، المجلد التاسع عشر، الصفحات (113-136)، غزة، فلسطين.

- الحمداني، ميسون خلف حمد (2016م). مشروعية الأدلة الالكترونية في الإثبات الجنائي، **مجلة كلية الحقوق**، جامعة النهرين، المجلد الثامن عشر، العدد الثاني، الصفحات (195-254)، بغداد، العراق.

- خلف، جاسم خريبط (2016). صعوبات الدليل الجنائي في الجرائم المعلوماتية، **مجلة القانون للدراسات و البحوث القانونية**، العدد12، قسم القانون، كلية شط العرب الجامعة.

- خنفوسي، عبد العزيز (2016). مدى حجية أدلة الإثبات الجنائي التقليدية في إثبات جرائم الإرهاب المعلوماتي، **مجلة دراسات وأبحاث**، المجلد8، العدد22، الصفحة (142-155).

- لموسخ، محمد (2009). تنازع الاختصاص في الجرائم الإلكترونية، **مجلة دفاتر السياسة والقانون**، العدد الثاني، جامعة قاصدي مرباح ورقلة، الجزائر، ص:151-167.

- المنشاوي، محمد أحمد (2012م). سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، **مجلة الحقوق**، السنة السادسة والثلاثون، العدد الثاني، الصفحة (515-568)، الكويت.

5- مؤتمرات وأوراق عمل:

- أحمد، هلالي عبد اللاه (2004م). **حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة**، بحوث مؤتمر القانون والكومبيوتر والإنترنت، من 1 – 3 مايو، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، الصفحة (713-789).

- أرحومة، موسى مسعود (2009م). **الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية**، مقدَّم إلى المؤتمر المغاربي الأول حول: المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا . طرابلس خلال الفترة 28- 29 /10/.

- رستم، هشام محمد فريد (2004م). **الجرائم المعلوماتية، أصول التحقيق الجنائي الفني**، بحوث مؤتمر القانون والكومبيوتر والإنترنت، من 1 – 3 مايو، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، الصفحات (401-506).

- عرب، يونس (2002). **جرائم الكمبيوتر والإنترنت، (إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات)**، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 10-2/12/.

- غنام، غنام محمد (2004م). **عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر**، بحوث مؤتمر القانون والكومبيوتر والإنترنت، من 1 – 3 مايو، كلية الشريعة والقانون، جامعة الأمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، الصفحات (625-660).

- فتح الله، محمود رجب (2012م). **دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول**، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان الشقيقة خلال الفترة 23-25 /9/ الموافق 7-1433/11/9هـ.

- مطر، حسين خليل (2018م). **إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية**، بحث مقدم الى مؤتمر (الإصلاح التشريعي طريق نحو الحكومة الرشيدة ومكافحة الفساد) الذي أقامته مؤسسة النبأ للثقافة والإعلام وجامعة الكوفة، كلية القانون، في الفترة بين 25-26 /4/.

6- القوانين:

- قانون الإجراءات الجزائية الجزائري الصادر بموجب الأمر 155/66 في 1966م وفقاً لآخر التعديلات.
- قانون الإجراءات الجزائية الفرنسي وفقاً لأحدث التعديلات.
- قانون أصول المحاكمات الجزائية السوري الصادر بالمرسوم 112 في 1950/3/13م.
- قانون أصول المحاكمات الجزائية اللبناني رقم 328 الصادر في 2001/8/2م.
- قانون الإمارات الاتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات.
- قانون الجرائم الإلكترونية الفلسطيني رقم (16) لسنة 2017م.
- قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري الصادر بالمرسوم التشريعي رقم (17) بتاريخ 2012/2/8م.
- قانون جرائم أنظمة المعلومات الأردني المؤقت لسنة 2010م.
- قانون جرائم تقنية المعلومات البحريني رقم (6) لعام 2014م.
- قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.
- مشروع قانون مكافحة الجرائم الإلكترونية المصري لسنة 2016م
- نظام مكافحة جرائم المعلوماتية السعودي الصادر في 2007/3/26م.

7- الاتفاقيات والمؤتمرات الدولية:

- الاتفاقية الأوربية لمكافحة جرائم الحاسوب والإنترنت (بودابست 2001/10/22م).
- المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكومبيوتر (4-9 تشرين أول 1994م- البرازيل/ ريو دي جانيرو).

8- الإنترنت:

- غنيمي، جابر (د.ت). " **إثبات الجرائم الإلكترونية**"، تونس، https://www.da5ira.com

- يوسف قجاج، خصوصية البحث عن الجريمة الإلكترونية، بحث منشور على الموقع الآتي:

https://www.hespress.com تاريخ الدخول في 2024/4/5.

ثانياً: باللغة الأجنبية:

-Hans G. Nilsson، Computer crimes and other crimes aginst information Technology whin the working programme of the council of Europe، R.I.D.P. 1993.

-Vassilaki (Irini); Computer crimes and other crimes against information technology in Greece، R.I.D، 1993

– Gassin R، le droit et l'informatique، Dalloz، Paris ، France، 1982.

- Frank J. Donner; The age of Surveillance، Washington، DC، 1981.

- VERBIEST(THIBAULT) ; cyber consommateur، Litec، Paris، France، 2002.

- VERGUCHT (P); La répression des délits informatiques dans une perspective international. Thèse، Montpellier 1، 1996.

- BENSOUSSAN ALAIN: Internet. Aspects juridiques، memento - guide، hermes، 1996.

-R.E.Anderson، Bank Security، Butter worth (publishers) INC، 1981.

- Brian Carrier. Defining Digital Forensics Examination and Analysis Tools. In Digital Research Workshop II، 2002، Available at:

http://www.Dfrws.org/dfrws2002/papars/papars/Brian Carrier.pdf accessed 5April 2024.

Summary

It did not include that the legal development of technological progress that the world witnessed in the middle of the twentieth century not only had positive effects، but went beyond that، as most people took advantage of this to commit various crimes using modern technological techniques، as criminals were able to develop criminal methods in a way There is a high level of technology in the electronic environment، which has become necessary to develop means of control to keep pace with the development of electronic crime methods، and it has become required of criminal justice agencies to deal with new forms of evidence in the field of criminal proof.

Law No. 20 of 2022 regulating communication on the Syrian network and cybercrime did not include any individualization of the procedural rules related to proof. In light of the above، the problem of this topic is one of the most important problems raised by cybercrime at the procedural level، which is represented in: the effectiveness of traditional means of proof. In proving cybercrime، to what extent can it be said that traditional means of proof are sufficient to prove cybercrime alone?

In order to study this research، we followed the descriptive approach to describe information crime، the analytical approach to analyze the legal texts contained in the Syrian Code of Criminal Procedure، and the comparative approach between Syrian legislation and some Arab and Western legislation whenever necessary.

In order to become familiar with the various aspects of the topic and to answer the various questions raised by the problem، we relied on a binary division of the plan، which consists of two chapters. The first chapter is the adequacy of traditional means in proving cybercrime، and the second chapter is proving cybercrime using modern means.

We have shown the inability and insufficiency of traditional means of proof of inspecting، inspecting and controlling information crimes، both from a legal and technical standpoint، and we have shown the extent of the need for the legislator to introduce new means of legislation appropriate to this type of crime، in addition to establishing technical bodies specialized in information crimes to be entrusted with them. The process of collecting technical evidence for these crimes.

Keywords: effectiveness - means - proof - information crimes - traditional - new.

Syrian Arab Republic

Damascus University

Faculty of Law - Department Criminal Law

The suitability of traditional means in proving cybercrime

A dissertation submitted in partial fulfillment of the requirements for the degree of Master in criminal law

By

Ali Kharma

Supervisor

Dr. Issa Altheeb

Professor in the Department of Criminal Law

2024