جامعة الشهيد الشيخ العربي التبسي - تبسة
كلية الحقوق والعلوم السياسية - تبسة
- قسم الحقوق -

مطبوعة مقدمة لطلبة السنة الأولى ماستر تخصص
جريمة وأمن عمومي
- السداسي الأول -

محاضرات في مقياس التحقيق في الجريمة الإلكترونية

إعداد الدكتورة/ خذيري عفاف
أستاذ محاضر قسم - أ -

مقدمة

شهد العالم منذ نهاية القرن العشرين ثورة عظيمة في مجال المعلوماتية سميت بالثورة المعلوماتية، حيث حققت هذه الأخيرة العديد من المزايا على جميع الأصعدة وفي شتى ميادين الحياة، إذ تلاشت معها الحدود السياسية والحوافز بين الدول والشعوب، لما تتميز به من عنصري الدقة والسرعة في جميع المعلومات وتخزينها ونقلها وتبادلها عن بعد داخل الدولة الواحدة أو بين العديد من الدول عبر العالم، الأمر الذي جعل العديد من العلماء و المفكرين يصفون هذه الثورة بالشورة المعلوماتية.

و بالرغم من هذه المزايا التي حققتها هذه الثورة في مجال تقنية المعلومات إلا أنه قد رافقتها جملة من الانعكاسات السلبية الخطيرة نتيجة الانحراف في استخدام هذه التقنية واستغلالها بشكل غير مشروع، وبطرق من شأنها المساس بمصلحة الفرد والجماعة، إذ ازدادت هذه المخاطر تفاقما في ظل البيئة الافتراضية التي تملكها شبكة الانترنت، مما أدى إلى ظهور نمط جديد من الجرائم المستحدثة و التي لم تكن معهودة من قبل، إذ أصبح من الصعب التعامل مع هذا النوع من الجرائم و تكييفها القانوني على أساس النصوص القانونية التقليدية، سواء تلك النصوص الموضوعية التي تبين الفعل المجرم و العقوبة المقررة له، أو تلك النصوص الإجرائية التي تبين مراحل الدعوى الجزائية بما فيها مرحلة البحث و التحري ومرحلة التحقيق و كذا الأجهزة المنوط بها مباشرة هذه الإجراءات.

ونتيجة عدة ثغرات التي تثيرها المواجهة الإجرائية لهذه الجرائم زاد اهتمام الحكومات والهيئات الدولية بمكافحتها لذلك عملت معظم التشريعات ومن بينها المشرع الجزائري

على تعديل نصوص القوانين الإجرائية بما يتلازم وخصوصية التحقيق في هذه الجرائم عن طريق استحداث آليات وأساليب خاصة تعتمد بالضرورة على التقنيات الحديثة.

أهمية الموضوع:

يعتبر موضوع التحقيق في الجريمة الالكترونية من بين أهم المواضيع المستحدثة و التي لا تزال محل نقاش و بحث مستمر نتيجة ارتباطيها بمجال تقنيات المعلومات و التكنولوجيا الحديثة، التي لا تنفك في تطور مستمر يوم عن يوم، هذا ما جعل أساليب الجريمة الالكترونية بحد ذاتها في تطور مستمر يوم عن يوم، هذا ما جعل أساليب الجريمة بحد ذاتها في تطور مستمر، إذ أصبحت تهديد الأفراد و الجماعات وأمن الدول، وخاصة ما تعلق منها بالجانب الإجرائي، الذي لقي العديد من التحديات و الإشكالات القانونية و العملية التي وقفت عائقا أمام أجهزة التحري و التحقيق في الجرائم الالكترونية، نظرا للخصوصية التي تتمتع بها هذه الأخيرة من حيث أساليب ارتكابها ومرتكبيها و الآثار الناتجة عنها، ومن هنا ظهرت أهمية استحداث إجراءات وقائية و أخرى وردعية لمواجهة هذا النوع من الإجرام، بما يتماشى مع خصوصية و طبيعته التقنية البحثية.

الإشكالية:

لقد تأثرت الجريمة بالتطورات التكنولوجية الحديثة، وظهرت أساليب إجرامية تستخدم أساليب لم تكن معروفة من قبل. وأمام هذا التطور وجب على أجهزة العادلة السعي أكثر في مجال الإثبات الجنائي باستخدام تقنيات وأساليب للتحقيق في هذا النوع

من الجرائم ولذلك طرح الإشكال الآتي: ما هي أهم الإجراءات التي إتباعها المشرع للتحقيق في الجرائم الالكترونية؟

وسيتم التطرق ضمن هذه المطبوعة للمحاور المقررة وفقا للبرنامج التعليمي المتضمن في عرض التكوين الموجه لطلبة السنة الأولى ماستر جريمة وأمن عمومي على النحو التالي:

المحور الأول: إجراءات التحقيق في الجرائم الإلكترونية.

المحور الثاني: القيمة الثبوتية للدليل الإلكتروني أمام القضاء الجزائي.

المحور الثالث: عقبات التحقيق الجنائي في الجرائم الإلكترونية.

المحور الأول: إجراءات التحقيق في الجرائم الإلكترونية

إن طبيعة الجريمة السيبرانية وأركانها ووسائل ارتكابها قد تدفع المشرع الجنائي إلى إعادة النظر في عدد من المسائل الإجرائية، ولا سيما فيما يتعلق بأهم موضوع في هذا القانون، وهو مسألة الأدلة.

وذلك لأن الأدلة التي يمكن أن تثبت هذا النوع من الجرائم يجب أن تكون ذات طبيعة فنية، وهو أمر غير ممكن في ظل القواعد الإجرائية التقليدية لاستخلاص الأدلة. ولهذا السبب، من الضروري أن يتدخل المشرع من أجل وضع قواعد إجرائية يمكن أن تستند إليها السلطات المكلفة بالتحقيق والتحري في الجرائم السيبرانية من أجل إيجاد الأدلة المناسبة لإثبات الجريمة السيبرانية.

ويعتبر هذا الدليل فريد من نوعه لأنه مستمد من البيئة الرقمية التي تحدث فيها الجرائم الإلكترونية، بخصائصها (خصائص البيئة الرقمية)، وهو الأمر الذي يقودنا إلى الحديث عن مسألة قبول هذا الدليل أمام القضاء و مدى كشفه للحقيقة وحتى لو تم التأكد من موثوقية وشرعية هذا الدليل، فإن المسألة تتجاوز ذلك إلى مسائل أكثر أهمية تتعلق بمدى خضوع هذا الدليل ذي الأصل العلمي لتقدير القاضي، وفقاً لمبدأ القناعة الشخصية للقاضي الجنائي، الذي يشكل جوهر أي قرار.

المبحث الأول: آليات التحقيق في الجرائم المعلوماتية

يعد التحقيق القضائي من أهم الإجراءات التي يتم اتخاذها بعد وقوع الجريمة، وتكمن أهميته في إثبات وقوع الجريمة وإثبات جدية نسبة الجاني إلى مرتكبها بمختلف

أنواع الأدلة، وهو كما يوحي به الاسم، بحث عن الحقيقة بهدف الوصول إلى إدانة المتهم أو توجيه الاتهام إليه بعد جمع الأدلة القائمة على الجريمة.

من المعروف أن الإجراءات الجنائية تمر بمرحلتين: مرحلة التحقيق ومرحلة المحاكمة. وتمر إجراءات التحقيق أيضاً بمرحلتين: مرحلة التحقيق الأولي ومرحلة التحقيق.

المرحلة الأولى، وهي مرحلة جمع الأدلة، يقوم بها ضباط الشرطة القضائية، أما المرحلة الثانية فهي من اختصاص قاضي التحقيق، الذي يؤيد الآراء والميول التي تقسم التحقيق:

– التحقيقات الأولية، التي يعهد بها إلى ضباط الشرطة القضائية.

– والتحقيقات القضائية، وهي متروكة للقضاء، وتنقسم إلى تحقيقات ابتدائية من قبل قاضي التحقيق، وتحقيقات نهائية في مرحلة المحاكمة من قبل القاضي.

وفي كلا هذين النوعين من التحقيقات، يتمتع مأمورو الضبط القضائي والقضاة بسلطة القيام بإجراءات تحري وتحقيقات محددة وفقا لقانون الإجراءات الجزائية، وهو ما يمكن فهمه بشكل أفضل من خلال قراءة أحكام المادتين 12 و38 من قانون الإجراءات الجزائية الواردتين في الفصل الأول "التحقيق والتحري في الجرائم" من هذا القانون. وتنص الفقرة 3 من المادة 12 على أن "يتولى مأمورو الضبط القضائي التحقيق والتحري في الجرائم المنصوص عليها في قانون الإجراءات الجنائية".

القانون الجنائي" ..... وتنص المادة 38 من نفس القانون على أنه "يناط بقاضي التحقيق إجراءات البحث والتحري".

وعليه فإن إجراءات التحري والتحقيق في الجريمة، سواء كانت أولية أو ابتدائية، هي من اختصاص سلطات التحقيق، ومن هذا المنطلق فإن إجراءات التحري والتحقيق التي يقوم بها مأمورو الضبط القضائي تدخل في إطار التحقيقات الأولية، أما تلك التي يقوم بها مأمورو التحري فتعتبر تحقيقات ابتدائية.

وإذا كانت التحريات بصفة عامة تعتمد على ذكاء وبصيرة وملاحظة ودهاء المحققين الذين يبذلون كل جهد في التحري والتتبع والدراسة وكشف الأدلة من أجل كشف الحقيقة، فإن التحريات في البيئة الإلكترونية تضاف إلى ذلك وتواكب حركة الجريمة وتطور أساليب العمل الإجرامي في هذه البيئة هناك حاجة إلى تطوير الأساليب ووضع الأجهزة المتخصصة لوضعها موضع التنفيذ من أجل مواكبة حركة الجريمة وتطور أسلوب العمل الإجرامي في هذه البيئة.

المطلب الأول: مزايا التحقيقات في الجرائم السيبرانية

تتسم الجرائم الإلكترونية بحداثة تنفيذها، وسرعة تنفيذها، وسهولة إخفائها ودقة وسرعة محو آثارها، مما ينتج عنه عدد من الصعوبات والمشاكل العملية التي تعيق المؤسسات القضائية في مواجهة هذا النوع من الجرائم. وعلى وجه الخصوص، تواجه أجهزة التحري والتحقيق العاملة في مجال جمع الأدلة الإلكترونية مشاكل وصعوبات إجرائية في القيام بمهامها في الكشف عن هذا النوع من الجرائم وملاحقة مرتكبيها وتقديمهم للعدالة.

وإزاء هذا الوضع، ثار جدل حول ما إذا كان من الممكن الاكتفاء بالقواعد الإجرائية العادية للتحقيق في الجرائم السيبرانية أم أنه من الضروري وضع قواعد إجرائية خاصة

تتماشى مع خصوصيتها وطبيعتها. وأشار بعض أصحاب المصلحة إلى أنَّ القواعد الإجرائية التقليدية للتحقيق والتحري في الجرائم ليست خاصة بجرائم معينة.

بل هي قواعد عامة تنطبق على جميع الجرائم المرتكبة ضد القانون الجنائي، بما فيها الجرائم السيبرانية، وعلى الرغم من أنَّ الجريمة السيبرانية تختلف عن غيرها من الجرائم من حيث طبيعتها وخصائصها، فإنها تظل خاضعة، من حيث المبدأ، للقواعد العامة المنطبقة على جميع الجرائم، كما أنَّ التحقيق في الجرائم السيبرانية يخضع لعدد من أنواع الجرائم، لأنها قد تكون ذات صلة، وتتضمن جميع عناصر التحقيق وتمر بنفس المراحل الفنية والشكلية التي تتبع في الجرائم التقليدية.

ولذلك يجوز للسلطات القضائية أن تستخدم القواعد الإجرائية القائمة عند التعامل مع الجرائم السيبرانية، ولا تتغير هذه القواعد القائمة أو تتأثر بالجريمة السيبرانية، إذ لا ينبغي تطوير بعض المفاهيم فقط والتعامل معها بطريقة قانونية.

واعتبر آخرون أن القانون الإجرائي القائم يحتوي على مقتضيات عامة تنطبق على الجريمة السيبرانية، ولكن لا يلزم سوى بعض التعديلات لإعطاء إجراءات التحقيق والتحري لهذا النوع من الجرائم نوعاً من الخصوصية التي تناسب طبيعة هذا النوع من الجرائم التي تتسم بخصوصيتها وذاتيتها التي تختلف عن الجرائم الأخرى وقد اقترح البعض أن قانون التحري والتحقيق في هذا النوع من الجرائم يحتاج فقط إلى بعض التعديلات من أجل إضفاء نوع من الخصوصية التي تناسب طبيعة هذا النوع من الجرائم.

إلا أن هذه الفرضية – أي أن القانون الإجرائي العادي قاعدة عامة تنطبق على الجريمة السيبرانية – لا يمكن الأخذ بها على الإطلاق، وذلك بسبب طبيعة وخصوصية الجريمة السيبرانية وصعوبات الضبط، والتي لا تتناسب، كما هو موضح أدناه، مع البيئة التقليدية التي ترتكب فيها مختلف الجرائم الأخرى.

ويعتبر القانون الإجرائي وقواعده الإجرائية وثيقة أساسية لحماية الحقوق الفردية وتأكيد احترام المبادئ الأساسية المعترف بها دولياً وتحقيق التوازن بين مصلحة الدولة في تقصي الحقيقة والحريات الفردية للمواطنين، وبما أن القواعد الإجرائية على اتصال دائم بحقوق الأفراد وحرياتهم، فإن مشروعية الإجراءات تتطلب أن تكون إجراءات البحث وجمع الأدلة متوافقة مع القانون ولا تحيد عن روح أحكامه. ولذلك، هناك أحكام لبعض الإجراءات لأن التفسيرات المتوسعة في تنفيذ الإجراءات أو تفسيرات هذه الإجراءات المقررة تهدد حقوق الأفراد وحرياتهم.

ولذلك يجب تحقيق التوازن بين حقوق الفرد المشتبه فيه من جهة وحقوق المجتمع من جهة أخرى، وبين هذه الحقوق وضرورة احترام القواعد القانونية والنظامية في البحث عن الأدلة في مجال البحث الجنائي بصفة عامة والجرائم الإلكترونية بصفة خاصة.

ومن ثم يمكن القول إن القواعد الإجرائية العادية تظهر محدوديتها وقصورها، وذلك لأن تطبيقها في بيئة لا تتفق مع القواعد الإجرائية العادية قد يشكل انتهاكا لشرعية الإجراءات بشكل عام ولحقوق الأفراد بشكل خاص. ولذلك، فقد أدى التحقيق في هذا النوع من الجرائم إلى ضرورة وجود قواعد خاصة مكرسة للتحقيق في هذا النوع من الجرائم، تضمن في الوقت نفسه تحقيق التوازن بين متطلبات فعالية أنشطة الهيئات

الجنائية الإجرائية في مجال المعلومات ومتطلبات حماية الحريات الشخصية وحقوق الخصوصية.

المطلب الثاني المؤسسات المكلفة بالتحقيق في الجرائم السيبرانية والتحقيق فيها

تتقدم الجريمة المعلوماتية بوتيرة هائلة تضاهي تقدم التكنولوجيا ذاتها، إلا أن الحركة التشريعية والثقافة الأمنية والقانونية المتعلقة بهذه الجرائم لا تتقدم بنفس السرعة، وهذا الاختلاف في التقدم والتطور هو نتيجة لعملية جمع الأدلة والتحقيق في القضايا الجنائية للجرائم المعلوماتية، وبالتالي ينعكس سلبًا على تقييم نوعية وتحقيقات وملاحقات وقرارات السلطات الأمنية. ويتطلب التعامل مع هذه المعلومات جهود فريق من الشرطة والطب الشرعي والنيابة العامة والبرمجة وتحليل النظم. وقد يكون ضابط الشرطة على دراية بالإجراءات التقنية والقانونية المستخدمة في الربط بين الجرائم والتحقيق فيها وحماية حقوق الإنسان، ولكنه قد لا يكون على دراية بعلوم الحاسوب والحوسبة والاتصالات، وبالتالي لا يستطيع فهم الأدلة الجنائية التي يبحث عنها فهماً كاملاً، كما أن محللو النظم والمبرمجين المهندسون الذين يفهمون كل شيء عن تقنية المعلومات وشبكات الاتصالات وطريقة عملها، قد لا يدركون ما يتصل بمتطلبات الإجراءات القانونية وقواعد البيانات وكيفية التعامل معها حتى تبقى الأدلة ذات قيمة برهانيه مقبولة أمام المحاكم.[1]

[1] محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الالكترونية، مجلة الفكر الشرطي، المجلد 21، العدد 81، ص 20-21.

الفرع الأول: الضبطية القضائية

تعتبر الضبطية القضائية صاحبة الاختصاص الأصيل في كل الجرائم بما فيها الجريمة الإلكترونية، وقد منحها القانون أساليب تحري جديدة نبينها فيما يلي:

1. **على مستوى جهاز الشرطة:** أنشأت المديرية العامة للأمن الوطني مخبرا مركزيا بمركز الشرطة **بشاطوناف** بالعاصمة الجزائر، ومخبرين جهويين الأول بمدينة قسنطينة والثاني بمدينة وهران تحتوي على فروع تقنية من بينها خلية الإعلام الآلي وفرق متخصصة مهمتها التحقيق والكشف عن جرائم الإنترنت، بالإضافة لإنشائها ثلاث مخابر على مستوى بشار، ورقلة وتمنراست قيد الإنجاز بهدف تعميم هذا النشاط عبر أرجاء الوطن[2].

كما يظم المخبر الجهوي للشرطة العلمية على مستوى قسنطينة ووهران مخبرا خاصا يتولى مهمة

التحقيق في الجريمة الإلكترونية تحت اسم» دائرة الأدلة الرقمية والآثار التكنولوجية «وتضم الأقسام التالية:

- قسم استغلال الأدلة الرقمية الناجمة عن الحواسيب والشبكات.
- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات، وذلك بالاستعانة بأجهزة مادية للكشف عن الجرائم الالكترونية.

[2]فلاح عبد القادر وآيت عبد المالك نادية، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019، ص 1695.

2. **على مستوى جهاز الدرك الوطني:** تعمل مؤسسة الدرك الوطني على مكافحة الجريمة الإلكترونية بواسطة المعهد الوطني للأدلة الجنائية وعلم الإجرام الكائن مقره **ببوشاوي** التابع لقيادة الدرك العامة، قسم الإعلام والإلكترونيك الذي يختص بالتحقيق والكشف عن الجرائم الالكترونية، وأيضا بواسطة مديرية الأمن العمومي والاستغلال والمصلحة المركزية للتحريات الجنائية، وهي هيئة ذات اختصاص وطني مهمتها التصدي للجريمة الإلكترونية[3].

الفرع الثاني: مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية عن طريق المرسوم الرئاسي رقم 261 -15 ومقره **بئر مراد رايس**، وهو تابع لمديرية الأمن للدرك الوطني، وقد حددت المادة الأولى منه تشكيل وتنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، 37 وتمارس الهيئة العديد من المهام في مجال التصدي للجريمة الإلكترونية ورد النص عليها في المادة 14 من القانون 04-09 سالف الذكر وهي:

-ضمان المراقبة المستمرة لشبكة الإنترنت.

-مراقبة الاتصالات الإلكترونية لفائدة وحدات الدرك الوطني المشاركة في عمليات البحث والتحري عن الجرائم الإلكترونية وفقا لما يسمح به القانون[4].

المبحث الثاني: ضوابط التحقيق والتفتيش في الجرائم المعلوماتية

---

[3] فلاح عبد القادر وآيت عبد المالك نادية، المرجع السابق، ص 1696.

[4] فلاح عبد القادر وآيت عبد المالك نادية، المرجع السابق، الصفحة 1697.

قد لا تكون أساليب التحقيق التقليدية مناسبة للكشف عن الجرائم أو القبض على الجناة أو الحفاظ على الأدلة. ويمكن إجراء التحريات الأولية قبل البحث والضبط والتفتيش من أجل كشف غموض الجريمة تمهيداً للقبض على الجاني وجميع الأدلة المتعلقة بالجريمة.

ويمكن أن تكون المعلومات التي يقدمها المجني عليه للشرطة مفيدة للغاية في تحديد طبيعة الجريمة، وكيفية ارتكابها، والأدوات المستخدمة في الجريمة، والمشتبه به، والدافع وراء الجريمة، وما إذا كان هناك أي شهود.

وبسبب هذه الخصائص العامة، فإن سلطات التحقيق والتحري وحتى سلطات الادعاء العام لديها درجة عالية من المعرفة بأنظمة الحاسوب وكيفية عملها وكيفية ارتكاب الجرائم على أنظمة الحاسوب أو من خلالها، وهي قادرة على كشف غموض هذه الجرائم وكشف الجرائم وكشف يجب أن يكون لديهم القدرة على التصرف بسرعة من حيث ضبط الأدوات المستخدمة في الجرائم ومصادرة البيانات والمعدات المستخدمة في الجرائم أو الخاضعة لها.[5].

المطلب الأول: جمع الإستدلالات في جرائم تقنية المعلومات

تسبق مرحلتي التحقيق الأولي والتحقيق النهائي (المحاكمة) مرحلة تُعرف باسم "مرحلة جمع الأدلة". وتعتبر هذه المرحلة من أهم مراحل الإجراءات الجنائية، فهي

[5]محمد أبو العلاء عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، مقال منشور على الموقع التالي: https://www.bibliotdroit.com/2021/12/blog-post_77.html تمت الزيارة بتاريخ 12-08-2022.

ليست مرحلة قضائية، بل هي المرحلة التي تسبق بدء الإجراءات الجنائية وهي الأساس الذي تبنى عليه جميع الإجراءات الجنائية. وعلى الرغم من أنها الأساس الذي تبنى عليه التحقيقات القضائية، إلا أن جمع الأدلة ضروري في معظم الجرائم لأن الجرائم غالباً ما ترتكب في الخفاء ومن الضروري كشف الجريمة وضبطها ومعرفة أسباب الجريمة وملابساتها ودوافعها لتسهيل أعمال التحقيق ومنع هروب الجاني أو فراره وحصره تمهيداً لضبطه وهي خطوة تمهيدية ضرورية[6].

تعد هذه المرحلة من أهم إجراءات العدالة الجنائية وأكثرها حساسية، فبالإضافة إلى كونها ترتبط بشكل مباشر ووثيق بالحرية الفردية والحق في العيش بأمان بعيداً عن أي اعتداء من السلطات، فهي بداية الطريق إلى العدالة الجنائية وضمانات الحقوق وطريق مواجهة الجريمة من أجل منعها وكشفها كما أنه أهم إجراءات العدالة الجنائية وأكثرها حساسية، فهو بداية الطريق إلى منع الجريمة والكشف عنها. كما أنه المعيار الذي تقاس به كفاءة أجهزة الشرطة والأمن وقدرتها على تحقيق السلامة العامة، من خلال منع الجريمة والحد منها وكشفها والقبض على الجناة عند وقوعها وتقديمهم للمحاكمة العادلة.[7].

---

[6]إسكندر إسلام،ماهية مرحلة جمع الاستدلالات، مقال منشور على الموقع التالي:

http://lawpractice-iskandar.blogspot.com/2011/06/blog-post_7371.html تمت الزيارة بتاريخ 15-08-2022.

[7]- عثماني عزالدين، التحقيق في الجريمة الالكترونية، مطبوعة مقدمة لطلبة السنة الأولى ماستر- تخصص جريمة وأمن عمومي، قسم الحقوق، جامعة تبسة،2022،ص9.

وعليه يمكن بيان إجراءات جمع الاستدلالات لمواجهة جرائم تقنية المعلومات من خلال تقسيم المطلب إلى فرعين، الفرع الأول: الإبلاغ والبحث والتحري في جرائم تقنية المعلومات، والفرع الثاني: الإنتقال والمعاينة في جرائم تقنية المعلومات.

الفرع الأول: البلاغ والبحث والتحري في جرائم تقنية المعلومات

يجب على مأموري الضبط القضائي تلقي البلاغات المتعلقة بالجرائم المجني عليهم، وتلقي الشكاوى المتعلقة بالجرائم التي يوجب المشرع على المجني عليهم تقديم شكوى بشأنها، وتقييدها في محضر تحقيق وإحالتها إلى النيابة، وإجراء جميع التحريات التي من شأنها المساعدة على إظهار الحقيقة وإثبات وقوع الجريمة أو نفيها ونسبتها إلى مرتكبها. ويجب إجراء التحريات اللازمة لجمع الأدلة والإثباتات. ومن ثم سيتناول هذا القسم الإجراءات التالية لقبول بلاغ المجني عليه، وقبول الشكوى، وإجراءات التحقيق والتحري في جرائم تقنية المعلومات:

أولا: تلقي الشكاوى والبلاغات في جرائم تقنية المعلومات

الأصل أنه يجب على رجال البلاغ بصورة عامة، إبلاغ السلطات المختصة بأن جريمة قد ارتكبت أو على وشك أن ترتكب، أو أن هناك اتفاقاً جنائياً أو دليلاً أو قرينة أو نية ارتكاب أو اشتباه أو خوفاً من ارتكاب جريمة. "إبلاغ السلطات المختصة عن وقوع الجرائم المنصوص عليها في القانون الجنائي".

وقد نصت المادة(12) من ق.إ.ج الجزائري[8] على أن الشرطة القضائية تختص بمهام البحث والتحري عن الجرائم المنصوص عليها في قانون العقوبات وجمع الأدلة حولها وكشف مرتكبيها مادام لم يبدأ فيها تحقيق قضائي"، كما نصت المادة (17) من ذات القانون على أنه يباشر ضباط الشرطة القضائية الصلاحيات المنصوص عليها في المادتين 12 و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات"، كما نصت المادة (19) من القانون ذاته على قيام أعوان الضبطية القضائية الذين لا تتوفر فيهم صفة ضابط الشرطة القضائية بمعاونة ضباط الشرطة القضائية في مباشرة وظائفهم ويثبتون الجرائم المقررة في قانون العقوبات ممثلين في ذلك لأوامر رؤسائهم مع الخضوع لنظام الهيئة التي ينتمون إليها ويقومون بجمع كافة المعلومات الكاشفة عن مرتكبي تلك الجرائم". كما نصت المادة (18) من القانون ذاته على أنه يتوجب على ضباط الشرطة القضائية أن يحرروا محاضر بما قاموا به وأن يبادروا فورا إلى إخطار وكيل الجمهورية المختص بالجنح والجنايات التي يعلمون بوقوعها".

وتنص هذه المواد على وجوب التبليغ عن الجرائم إلى السلطة العامة المختصة، سواء كانت من أفراد الجمهور أو من الموظفين العموميين أو الموظفين العموميين. ويتطلب ذلك العلم بالجريمة من جانب المبلِّغ. وليس من الضروري أن يكون على علم تام بالجريمة وملابساتها ووقائعها، ولكن يكفي أن يكون على علم تام بالجريمة. ثم يرتفع مستوى المعرفة بعد ذلك، فكلما زادت المعلومات والتفاصيل عن الجريمة كان ذلك أفضل، ويكون المخبر ملزمًا بالإفصاح عنها دون إخفاء أي شيء.

---

[8] الأمر رقم 66 – 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، التضمن قانون الاجراءات الجزائية الجزائري، المعدل والمتمم.

ينص المشرع الجزائري على المسؤولية الجنائية لمن لا يقوم بالإبلاغ عن الجرائم.

ولذلك، فبمجرد أن يتلقى ضابط الشرطة القضائية أو سلطة التحقيق المختصة بلاغا يشير إلى أن شخصا ما يرتكب فعلا يشكل جريمة تقنية معلومات في موقع أو جهاز معين ووفقا للغة برمجة معروفة بما في ذلك، على سبيل المثال، معلومات عن نشر فيروس مدمر عبر شبكة إلكترونية، فإنه تبدأ ممارسة سلطاته.

وهناك معلومات يجب استيفاؤها من مقدم البلاغ أو الشكوى في الجرائم المعلوماتية نسبة لتباين جرائم الحاسب الآلي والانترنت ويمكن لمتلقي البلاغ أو الشكوى الحصول على هذه المعلومات عن طريق أسئلة تتناول جوانب محددة منها ما يلي:[9]

1- تحديد المكان الذي وقع فيه الفعل غير القانوني يجب على المبلّغ تحديد المكان الذي وقع فيه الفعل غير القانوني ووصفه بطريقة يمكن تحديدها، على سبيل المثال موقع الشركة، العنوان، البنك، المنزل الذي وقع فيه الاعتداء.

2- تحديد نوع الجريمة: لا يكفي أن يحدد المبلّغون موقع الجريمة، بل يجب أن يشيروا أيضًا إلى نوع الجريمة، مثل الاعتداء على الممتلكات أو الاحتيال على بطاقات الائتمان أو القرصنة أو تعطيل المواقع الإلكترونية أو الاعتداء على البيانات أو المعلومات الإلكترونية.

3-تحديد مسرح الجريمة: يجب على المبلِّغين تحديد الجهاز الذي ارتُكبت فيه الجريمة والمكان الذي وقع فيه الهجوموبالتالي، فإن هذه العناصر مهمة وضرورية في

9- إيهاب محمد التاج، المرجع السابق، ص 392

أي بلاغ يتعلق بالجريمة السيبرانية لتمكين موظفي إنفاذ القانون من توصيف الجريمة ووضع خطة استجابة تقنية وقانونية.

الإبلاغ هنا يمكن أن يتم عبر الإنترنت، أو ما يسمى بالإبلاغ الرقمي، وذلك بإرسال رسالة إلكترونية إلى الجهات المختصة للتحقيق والاستفسار عن وجود صفحات أو مواقع إلكترونية غير قانونية، تمارس جرائم تقنية المعلومات، وقد تكون بلاغا مباشرا أمام أحد مقرات الأمن الوطني.

يجب أن تكون لدى المبلِّغين عن جرائم تكنولوجيا المعلومات معرفة كافية بالجوانب التقنية للحواسيب والشبكات الإلكترونية لكي يتمكنوا من تقديم معلومات تشرح القضية بشكل جيد وتسمح لضابط الشرطة القضائية أو المحقق بتحديد طبيعة الجريمة بطريقة مرضية من أجل المضي قدما في التحقيق. ولذلك يجب أن يكون لدى الشخص الذي يتلقى البلاغ معرفة كافية بالجوانب التقنية للحواسيب والشبكات الإلكترونية ليتمكن من مناقشة المخبر في الجوانب العديدة ذات الصلة بالجريمة موضوع البلاغ.

ثانيا: البحث والتحري وكشف غموض جرائم تقنية المعلومات

عملية التحقيق عبر الإنترنت: إجراء أمني يقوم به محقق عبر الإنترنت باستخدام التكنولوجيا الإلكترونية الرقمية لتحقيق هدف معين، وتخزين النتائج في ملف رقمي يعمل على إثبات وقوع جريمة إلكترونية ونسبها إلى شخص معين، وهو أحد عناصر الأدلة الجنائية، أو وإتاحتها للجمهور في شكل مكتوب.

ولتحقيق ذلك، يجب تدريب الضباط الذين يجرون التحريات والتحقيقات على استخدام خبراتهم الفنية المتخصصة في هذا المجال، وكذلك تطوير الإجراءات الجنائية، لتحقيق الأهداف المطلوبة.[10].

وحددت المادة (17) من قانون الإجراءات الجزائية اختصاصات رجال الضبطية القضائية بالقول بأنه يمارس ضباط الشرطة القضائية الصلاحيات الموضحة في المادتين 12 و13، ويتلقون البلاغات والشكاوى ويجمعون الأدلة.

وعلى هذا الأساس؛ فالتحري عبر الشبكة المعلوماتية يعتبر عمل أمني وقانوني يقوم به رجل الضبط القضائي المختص عبر الشبكة بواسطة الحصول على بيانات ومعلومات تعريفية أو وصفية عن الأشخاص أو الأماكن أو الأشياء عن طريق تكنولوجيا المعلومات من أجل منع أو مكافحة جرائم تكنولوجيا المعلومات أو لتحقيق الأمن السيبراني، أو لأي غرض آخر.

ويتمتع المحققون الجنائيون بسلطة تقديرية واسعة في جمع المعلومات لاستخدامها في الكشف عن الجرائم السيبرانية والحد منها وفي اختيار أدوات التحقيق الإجرائية التي يرونها مناسبة وضرورية لإنجاز مهامهم بفعالية، وهناك عدة مصادر للمعلومات لهذا الغرض:

---

[10]- محمد أبو العلاء عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، مقال منشور على الموقع التالي: **https://www.bibliotdroit.com/2021/12/blog-post_77.html** تمت الزيارة بتاريخ 12-08-2022.

– **المراقبة الإلكترونية:** عمل يقوم به مشغّل المراقبة باستخدام التكنولوجيا الإلكترونية لجمع بيانات أو معلومات عن شخص أو مكان أو شيء مشتبه به سواء كان شخصًا أو مكانًا أو شيئًا ذا طبيعة خاصة.

لتحقيق غرض أمني أو لأي غرض آخر.

ولم يتصد المشرع الجزائري لم يعرّف نص قانون الإجراءات الجزائية ولا نص القانون 09-04 المتعلق بالأنظمة الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات ومكافحتها المراقبة الإلكترونية، بل تُرك ذلك للاجتهادات القضائية التي اختلفت هي الأخرى في تحديد تعريف دقيق وموحد لإجراءات المراقبة الإلكترونية. فبعض الاجتهادات الفقهية تعرّف التنصت والتسجيل بأنه إجراءات متعمدة تشمل المحادثات الخاصة سواء كانت مباشرة أو غير مباشرة، أي المتبادلة وجهاً لوجه أو عبر وسائل الاتصال السلكية واللاسلكية.[11].

تعتبر المراقبة الإلكترونية من أهم وسائل التحقيق والتحري باستخدام تكنولوجيا المعلومات لجمع البيانات عن المشتبه بهم في جرائم تكنولوجيا المعلومات. ومع ذلك، تعتبر المراقبة الإلكترونية من الإجراءات التي تنتهك الحق في الخصوصية التي يحميها الدستور والقانون (مثل مراقبة البريد الإلكتروني للمشتبه بهم)، وبالتالي يجب على مأموري الضبط القضائي الحصول على إذن من السلطات القضائية المختصة قبل الشروع في ذلك.

---

[11]- بن بادة عبد الحليم، المراقبة الالكترونية كإجراء لاستخلاص الدليل الإلكتروني "بين الحق في الخصوصية ومشروعية الدليل الإلكتروني، المجلة الأكاديمية للبحث القانوني، المجلد 10، العدد 03-2019، الصفحة 390.

وفي هذا السياق، فإن المراقبة الإلكترونية هي وسيلة لجمع البيانات والمعلومات عن جرائم تقنية المعلومات ويقوم بها مأمورو المراقبة الإلكترونية المتمثلة في مأموري الضبط القضائي من ذوي المهارات الفنية العالية المناسبة لنوع جريمة تقنية المعلومات التي يتعاملون معها، باستخدام التكنولوجيا الإلكترونية والشبكات الإلكترونية، كان يقوم بمراقبة أحد قراصنة البيانات الذين قاموا باختراق الحاسوب الآلي الخاص بالمجني عليه وبريده الإلكتروني، أو اختراقه للمواقع.

ويسمح القانون رقم 09-04 الذي يحدد قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لضباط الشرطة القضائية بالوصول عن بعد إلى الأنظمة المعلوماتية أو أجزاء منها والبيانات المعلوماتية المخزنة فيها، وكذا أنظمة تخزين المعلومات المفيدة لعملية التحقيق.[12].

لا ينتهك موظفو مقدمي خدمات الاتصالات السلكية واللاسلكية القانون عندما يراقبون الاتصالات ويكشفون عن عمليات الاختراق التي يقوم بها مجرمو الإنترنت ويكشفون عنها للسلطات من أجل حماية حقوق مقدمي الخدمات. يتمتع مزودو الخدمات الذين يحققون في الاستخدام غير القانوني لأنظمة المعلومات بصلاحيات واسعة للمراقبة والحق في الكشف عن أدلة الاستخدام غير القانوني.

وعلى هذا الأساس، فإن المشكلة هنا أنه ليس من السهل إجراء المراقبة السرية الإلكترونية في جرائم تكنولوجيا المعلومات التي تحدث من خلال الشبكات الإلكترونية

---

[12] المادة05 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الصادر بالجريدة الرسمية الجزائرية، بالعدد رقم 47، الصفحة 5.

ووسائلها. إذ يجب أن تتوافر في هيئات الضبط القضائي التي تقوم بذلك المؤهلات العلمية والفنية اللازمة للقيام بهذه المهمة على الوجه الصحيح، ولا يمكن تحقيق ذلك إلا بإسناد مثل هذه المهمة إلى هيئة ضبط قضائي خاصة تنشأ وتعد خصيصاً لهذا الغرض ضمن هيئة شرطية مخصصة لمكافحة جرائم تقنية المعلومات والتحقيق فيها ولا يمكن أن يتحقق ذلك إلا من خلال ما يلي: أن يكون أعضاء هذه الهيئات على دراية وإلمام بالبيانات الإلكترونية المتعلقة بمفهوم الحياة التي لا يجوز مراقبتها إلا بما يسمح به القانون.

وللحصول على هذه المعرفة، من الضروري من ناحية أن تقوم السلطة التشريعية بتنظيم إجراءات المراقبة التي تعتبر إجراءات تحقيق، ومن ناحية أخرى تزويد موظفي هذه السلطات بالثقافة القانونية اللازمة لهذا الغرض من خلال تنظيم دورات تدريبية خاصة لهم.

وفي سبيل تحديد شخصية المجرم الإلكتروني ورصد تحركاته، يمكن الاستعانة بالعناصر الآتية:

أ- مقدمو الخدمات: يمكنهم مراقبة هذه التحركات من خلال اكتشاف العناوين التي تم الوصول إليها.

ب- الرسائل المرسلة والملفات التي تم تنزيلها من الشبكة.

ج- بروتوكول الإنترنت: وهو البروتوكول الخاص بالاتصال بالإنترنت الذي يمكن- من خلاله- تحديد الشخص المستخدم للإنترنت، وتحديد موقعه.

د- نظام الـ **PROXY**: يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصالات بالشبكات قدرتها لإدارة الشبكة

وضمان الأمن وتوفير خدمات الذاكرة الجاهزة[13]، جهاز كمبيوتر يعمل كوكيل لتقليل الوقت اللازم للدخول المتكرر إلى موقع معين على شبكة الإنترنت..

هـ- مراقبة عمل العاملين على الشبكة: تعتبر رقابة إدارية تصب في مصلحة صاحب العمل للتأكد من عدم إهدار العاملين لوقت عملهم لتحقيق مكاسب شخصية أو العمل لصالح الغير.

و- التحريات الإلكترونية: في بعض الدول يكلف مأمورو الضبط القضائي بالتحقيق في جرائم تقنية المعلومات، ولديهم خبرة فنية في التحقيق الجنائي والمعالجة الإلكترونية للبيانات.

- عملية توثيق وتحريز الأدلة الجنائية الرقمية

تحتاج الأدلة الجنائية الرقمية، مثلها مثل الأدلة المادية، إلى التوثيق والتأكد من مصداقيتها وخلوها من العيوب لعدة أسباب، منها

1) التوثيق الذي يحفظ الدليل الرقمي بصيغته الأصلية، والذي يُستخدم لعرض وتأكيد صحة الدليل والتأكد من عدم وجود تحريف أو تعديل في الصور المسجلة بالفيديو – على سبيل المثال – من خلال مطابقة النص الرقمي مع النص الملتقط على الشاشة بين الطرفين يمكن استخدامه لتأكيد صحة المناقشات المباشرة[14].

2 – يجب أن يشهد الشخص الذي يجمع الأدلة على الاتساق بين الأدلة التي تم جمعها والأدلة المقدمة في المحكمة، والتوثيق أمر أساسي. ويعتبر عدم قدرة المحقق على التمييز بين الدليل الأصلي وصورته المقدمة إلى القضاء سبباً لإبطال الأدلة.

---

[13] إيهاب محمد التاج، المرجع السابق، ص 407.

[14] محمد قاسم أسعد الردفاني، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، المجلة العربية للدراسات الأمنية والتدريب المجلد 31، العدد (21) 157-192، 2014، الرياض، ص 181.

3- يجب توثيق موقع الأدلة الرقمية أثناء إعادة بناء الجريمة، حيث أن تشابه معدات الحاسوب وملحقاته يجعل من الصعب نقلها دون توثيق مناسب ومفصل يحدد بدقة الأجزاء والملحقات وموقعها الأصلي.

4- يشكل التوثيق جزءاً من الحفاظ على الأدلة الرقمية حتى نهاية عملية التحقيق والملاحقة القضائية. ويرجع ذلك إلى أن التوثيق ينطوي على التحديد الدقيق للجهة التي تحتفظ بالأدلة وقنوات التوزيع، والتي يجب أن تكون محدودة قدر الإمكان.

عند توثيق الأدلة الرقمية، يجب تحديد متى وأين وكيف تم الاستيلاء على الأدلة وتأمينها ومن قام بذلك. من الضروري أيضًا توثيق الأدلة الرقمية بعدة طرق، بما في ذلك التصوير الفوتوغرافي وتصوير الفيديو ورسم الخرائط والنسخ المطبوعة من الملفات المخزنة على أجهزة الكمبيوتر وتلك المخزنة على الأقراص، وإذا كانت مخزنة على أقراص أو أشرطة فيجب تسجيل البيانات وفقًا لما يلي لكل منها المعلومات التالية مطلوبة:

- التاريخ والوقت.
- توقيع الشخص الذي قام بعمل النسخة.
- اسم أو نوع نظام التشغيل.
- اسم البرنامج أو الأمر المستخدم لإنشاء النسخة.
- المعلومات الموجودة في الملف المحفوظ.[15].

الفرع الثاني: الإنتقال والمعاينة في جرائم تقنية المعلومات

[15] محمد قاسم أسعد الردفاني، المرجع السابق، ص 181.

وهي من أهم إجراءات مرحلةجمع الأدلة التي يقوم بها رجال الضبط القضائي، وهي العمود الفقري وركيزة التحقيق الجنائي.

فهي تقدم عرضا صادقا للوقائع والحقائق، دون كذب أو محاباة أوخداع، وتعطي رجال الشرطة صورة حقيقية وواقعية لمسرح الجريمة والمواد والآثار ذات الصلة، وتكشف عن خفايا الجريمة التي قد تساعد على إثبات وقوع الجريمة وتحديد مكان الجاني (الجناة).

وفي كلتا الحالتين، بعد تلقي بلاغ عن جريمة إلكترونية والتحقق من البيانات اللازمة الواردة في البلاغ، يتوجه ضابط الشرطة إلى مسرح الجريمة ويجري تحققاً في الموقع، وهو تحقق إلكتروني لأنه في حالة الجريمة الإلكترونية نادراً ما تترك آثار مادية بعد ارتكاب الجريمة، مما يقلل من الأدلة، وأيضاً لأن وقوع الجريمة وارتكابها تختلف عن تلك الخاصة بالجرائم التقليدية بسبب طول الفترة الزمنية بين وقوع الجريمة واكتشافها ولأن الآثار الناتجة يمكن أن تتعرض للتلاعب أو المحو أو التلف، مما يؤثر سلباً على الآثار الناتجة[16].

أولا: المقصود بالانتقال والمعاينة في مسرح جرائم تقنية المعلومات

الانتقال: والهدف منه أن يذهب المحقق إلى مكان الجريمة أو إلى مكان توجد فيه آثار أو أشياء تفيد في كشف الجريمة في أسرع وقت ممكن قبل أن تختفي آثارها،

[16] مليكة أبوديار، الإثبات الجنائي في الجرائم الإلكترونية، المجلة الإلكترونية للأبحاث القانونية 2018، العدد 02، ص 101-102.

وذلك لجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وأشياء أخرى تفيد في كشف الحقيقة.

وَفِي الفقه الجنائي يعَرَف الإنتقال بأَنه، "المعاينة البصرية للوقوف على حالة المكان والأشخاص والأشياء؛ وضبط أي أشياء ضرورية لإظهار الحقيقة؛ ومعاينة مسرح الجريمة الإلكترونية: فحص الآثار التي تركها مستخدمو الشبكات الإلكترونية والإنترنت، بما في ذلك الرسائل المرسلة والمستلمة من قبل المستخدمين وجميع الاتصالات التي تمت عبر الحواسيب والشبكات الإلكترونية"، فيقصد بالمعاينة إثبات حالة المكان الذي وقعت فيه الجريمة، أو ضبط أشياء تفيد في كشفها، أو حالة الأشخاص بالمشاهدة والوصف، سواء بالكتابة، أو الرسم التخطيطي، أو بالتصوير، أو مشاهدة آثار الجريمة على فاعلها – المجني عليه– وكل ما له علاقة بها[17].

في مجال كشف ألغاز الجريمة الرقمية، لا يكتسي الاختبار أهمية في مجال كشف ألغاز الجريمة الرقمية:

ونادرا ما يكون للجريمة الرقمية الإلكترونية أي آثار مادية مرئية، ففي الفترة الفاصلة بين ارتكاب الجريمة والكشف عنها، قد يزور العديد من الأشخاص موقع أو مسرح الجريمة الإلكترونية الرقمية، مما قد يؤدي إلى تغيير الآثار المادية أو إتلافها أو التلاعب بها أو فقدانها جزئيا، وبالتالي إلقاء الشك على الأدلة المستخدمة في المعاينة.

[17]طارق عبد الرحيم الردايدة، التفتيش الإلكتروني في الجرائم الرقمية – دراسة وصفية مقارنة –، مذكرة ماجستير ضمن تخصص أمن نظم المعلومات والجرائم الرقمية، جامعة الأميرة سمية للتكنولوجيا، الأردن، 2017، الصفحة 27.

ولكي تكون معاينة مسرح الجريمة الإلكترونية الرقمية مفيدة في الكشف عن حقيقة الجريمة ومرتكبيها يجب مراعاة عدة قواعد وإجراءات زمنية أهمها:

1) وصف الموقع:

ويتضمن ذلك تصوير محتوى الموقع والوضع العام، والتركيز على الحاسوب الرقمي وملحقاته المتصلة به، وتصوير الجزء الخلفي للحاسوب وملحقاته، ومراعاة الوقت (التاريخ والتوقيت) والموقع الذي التقطت منه كل صورة فوتوغرافية.

2) المراسلات: التوصيلات والكابلات المتصلة بمكونات نظام الحاسب الآلي بحيث يمكن حصرها عند تقديمها للقضاء.

3) التعيينات التالية:

مستندات الإدخال/ الإخراج الورقي للحاسوب الرقمي المتعلقة بالجريمة.

المستندات المهملة أو الممزقة، وورق الكربون المستعمل، والأشرطة، ومحتويات حاويات نفايات الأقراص الممغنطة، السليمة وغير السليمة، وحساب فحصها والتحقيق فيها وإزالتها ورفع بصماتها إن وجدت[18].

والسبب في الانتقال الفوري إلى مسرح الجريمة للمعاينة هو التأكد من أن الأدلة التي تم الحصول عليها غير مشكوك فيها، حيث قد يتمكن الجاني من إزالة العناصر

[18] ـ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الاولى، القاهرة، 2008، ص172.

الرئيسية التي يمكن أن تساعد في كشف الحقيقة في الوقت الفاصل بين الجريمة والمعاينة.

وبمجرد تلقي البلاغ، تكون الخطوة التالية هي الانتقال إلى معاينة مسرح الجريمة، والتي غالبا ما يقوم بها ضباط الشرطة للتنقيب عن مسرح الجريمة وفحصه والحفاظ على الآثار والبقايا والأدلة المادية المتعلقة بالجريمة ومرتكبيها، وتصوير مسرح الجريمة وإعداد مسودة سيناريو لكيفية وقوع الجريمة ووقت ارتكابها والظروف المحيطة بها، وذلك من أجل إقامة دعوى ضد الجناة ارتكاب الجريمة من أجل إثبات القضية ضد مرتكبيها.

ثانيا: ضوابط المعاينة في جرائم تقنية المعلومات

وتبدأ العملية الإجرائية بنزول فريق متخصص يتمتع بكافة الاختصاصات اللازمة لضبط واحتجاز كافة المعدات والأشخاص المتورطين فيها بعيدًا عنهم، مع مصادرة الأقراص المحمولة والأقراص الصلبة والهواتف المحمولة.

ثم يتم الاتصال بالمبلغ وتزويده بكافة المعلومات المتاحة للفريق. ويتم ذلك بالاشتراك مع النيابة العامة والخبراء المتخصص ينفي هذا المجال، بإتباع الإجراءات الموضحة حتى يتسنى تقديمها إلى السلطات القضائية كأدلة إثبات دون أي قصور.[19]، يتم ذلك على النحو التالي:

1 – مسرح الجريمة التقليدي: يقع خارج البيئة الحاسوبية ويتألف أساسا من المكونات المادية الملموسة للمكان الذي ارتكبت فيه الجريمة، وهو أقرب ما يكون إلى

[19] محمد قاسم أسعد الردفاني، المرجع السابق، ص 180.

مسرح الجريمة التقليدي، حيث قد يترك الجاني بعض الآثار، مثل البصمات والمتعلقات الشخصية ووسائط التخزين الرقمية، وقد يقوم أعضاء فريق التحقيق بالتعامل مع الأدلة هناك وفقاً لذلك. وفي هذه الحالة لا توجد صعوبات كبيرة في تحديد مدى ملاءمة مسرح الجريمة الذي يحتوي على هذه العناصر للمعاينة من قبل عنصرالضبط القضائي، وفي ضبط وإسناد عناصر معينة تشكل دليلاً مادياً على ارتكاب الجريمة، وفي وضع الأختام في المكان الذي جرت فيها لمعاينة.

– مسرح الجريمة الافتراضي: يتألف من بيانات رقمية موجودة في بيئة إلكترونية، موجودة ومتحركة في بيئة الحاسوب والإنترنت، في الذاكرة وعلى الأقراص الصلبة. لا ينبغي أن يتم التعامل مع الأدلة الموجودة في هذا المسرح إلا من قبل محترفين متخصصين في التعامل مع هذا النوع من الأدلة الرقمية.

وتنشأ في مثل هذه الجرائم صعوبات تعيق صحة شهادة الخبراء وفائدتها، ويمكن تلخيصها على النحو التالي:

أ – تتمثل الصعوبة الأولى في ندرة الآثار المادية التي تخلفها الجرائم التي تقع عادة على أدوات الحاسوب، ولا سيما البرامج والبيانات الحاسوبية.

فالفترة الزمنية الطويلة نسبياً التي غالبا ما تنقضي بين وقوع الجريمة والكشف عنها، وكثرة عدد الأشخاص الذين يزورون مسرح الجريمة خلال تلك الفترة، يمكن أن تخلق فرصاً للتلاعب أو تلفيق أو تزوير الآثار المادية، أو ضياع أجزاء من الآثار المادية، مما يلقي بظلال من الشك على الأدلة المستخلصة من الفحص.

وعلى العكس من ذلك، يمكن استخدام المعلومات والآثار الرقمية المستخرجة من الحواسيب في إنشاء صفحات الويب، ورسائل البريد الإلكتروني، والفيديو الرقمي،

والصوت الرقمي، وغرف الدردشة، والملفات المخزنة على الحواسيب الشخصية، والصور المرئية، والوصول إلى الخدمات، والدخول إلى الإنترنت من خلال مزودي الخدمة والشبكات، وقد تحتوي على ثروة كبيرة من المعلومات، بما في ذلك الاتصالات بالشبكات.

لذا، يجب مراعاة القواعد والإرشادات الفنية التالية عند التحقيق في مسرح جريمة تقنية المعلومات:

1-) تصوير جهاز الحاسوب وأجهزته الطرفية ومحتوياته والوضع العام للمكان الذي يوجد فيه، مع الانتباه إلى الجزء الخلفي والملحقات الأخرى.

2-) راقب بعناية كيفية إعداد نظام الحاسوب.

3- توثيق حالة كابلات الحاسوب وتوصيلاتها بمكونات النظام لتسهيل المقارنة والتحليل عند تقديمها إلى محكمة مختصة.

4- التأكد من خلو البيئة الخارجية من المجالات المغناطيسية وعدم التسرع في نقل المواد المعلوماتية من مسرح الجريمة قبل إجراء الاختبارات اللازمة للتأكد من أن التداخل بين المجالات المغناطيسية لا يضر بالبيانات المخزنة.

5- يجب ملء صناديق القمامة بالوثائق المهملة أو الممزقة وورق الكربون المستخدم والأشرطة السليمة أو التالفة والأقراص المغناطيسية، ويجب فحصها لإزالة أي بصمات قد تكون مرتبطة بالجريمة.

-يجب أن تقتصر أعمال الفحص على ضباط إنفاذ القانون سواء كانوا باحثين أو محققين مدربين تدريباً جيداً، ولديهم الكفاءة العلمية والخبرة الفنية في مجال استرجاع

المعلومات والحاسب الآلي ومواجهة هذا النوع من الجرائم والتعامل مع الأدلة التي قد تترك في مسرح الجريمة التقليدي.

وقبل وصول المحقق أو الفني إلى مسرح الجريمة، يجب وضع خطة عمل شاملة تتضمن الخطوات التالية

1 – إعداد المواد والمغلفات المطلوبة لمسارح الجريمة الرقمية بمختلف أحجامها وأشكالها

2 – إعداد النماذج الأولية للوثائق المطلوبة لتسجيل المعاينة.

3 – التأكد من أن جميع المهنيين والفنيين على دراية بأشكال الأدلة والتعامل السليم معها.

4 – تقييم العواقب القانونية المترتبة على معاينة مسرح الجريمة الرقمي.

5 – التحقق من الأثر المادي المتوقع على مسرح الجريمة الرقمية.

6 – تعيين شخص مسؤول قبل الوصول إلى مسرح الجريمة.

7 – إعداد مهام الطاقم الأساسية قبل الوصول.

8– تقييم مهام الطاقم المطلوبة للتعامل بنجاح مع مسرح الجريمة.[20]

ويتبين مما تقدم أن جهاز الشرطة المتمثل في عناصر الضبط القضائي يعملون من خلال البحث والتحري عن الاستدلالات التي تدين المجرم الإلكتروني؛ فحين تلقيهم البلاغات والشكاوى المرتبطة بجرائم تقنية المعلومات عبر الشبكة الإلكترونية؛ يقومون بالبحث والتحري عن مرتكب تلك الجريمة، وكشف غموضها بواسطة الإرشاد الجنائي

[20] محمد رضوان هلال وكاظم محمد عطيات، كيفية التعامل التقني والآمن مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص، ص 45.

والمراقبة الإلكترونية للشبكة عبر الإنترنت، وذلك من خلال التقنية الإلكترونية للحصول على بيانات ومعلومات تفيد في التعرف على مرتكب جرائم تقنية المعلومات، للحد منها وضبطها لتحقيق الأمن الإلكتروني.

وعلى هذا الأساس يجب على القائمين بعملية البحث والتحري ومعاينة مسرح الجرائم الإلكترونية أن يكونوا على درجة عالية من التأهيل والتدريب الفني الكافي لمواجهة هذه النوعية من الجرائم، وأن تعطى هذه الاختصاصات في البحث والتحري والمعاينة في العالم الافتراضي إلى سلطة مختصة بمكافحة الجرائم الإلكترونية، لكون مرتكبي هذه الجرائم على درجة عالية من الذكاء والتخصص في اختراق المواقع أو النظام المعلوماتي.

الفرع الثالث: إجراءات التفتيش

على الرغم من أن القانون المقارن لايعرّف معنى التفتيش، إلا أنه ينص على أن التفتيش هو أحد الإجراءات التي يقوم بها الموظفون المخولون وفقاً للإجراءات التي يقرها القانون بغرض الحصول على أدلة مادية على جريمة محققة تنسب إلى شخص معين في مكان يتمتع فيه بالحرمة والخصوصية. ويمكن اعتبار أن عمليات التفتيش، كمبدأ عام، من مسؤولية سلطات التحقيق.[21]

ويختلف التفتيش بحسب نوعية الجرائم، فالجرائم العادية يتعلق التفتيش بها على أشياء مادية، أما الجرائم المعلوماتية فهي تطرح العديد من الصعوبات لأنها تخص

[21] ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، مذكرة ماجستير تخصص السياسة الجنائية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض 2012، ص 64.

برامج في الحاسوب أي مكونات معنوية كما أن الدليل الناتج عن هذا الإجراء قد يتصف بعدم المشروعية بسبب الغموض الذي يطرح حول مدى إتباع الأصول العامة في التفتيش؟

والأصل أن قواعد التفتيش شرعت لأجل حماية الخصوصية وحقوق الإفراد، كما أنه لابد من تحقيق أفضل ضمانات للمتهم تتفق ومقتضيات البراءة، لذا لا بد من إتباع القواعد العامة فيما يخص استصدار مذكرات التفتيش كما أنه لضبط حدود التفتيش لابد من مراعاة ما يلي:

– أولا: إذا كانت الجريمة الإلكترونية مرتبطة بأحد أنظمة الكمبيوتر فإن مذكرة التفتيش يجب أن تكون واضحة في تحديد النظام محل التفتيش حتى لا يؤدي إلى كشف بيانات شخصية، وكذا الخاصة بسرية المهنية.

– ثانيا: إذا كان النظام أو مكان وجود الدليل غير معروف فيتعين أن تكون عبارة مذكرات التفتيش عامة على سبيل المثال، إذا كان نظام المعلومات في مكان واحد ونقاط النهاية في مكان آخر، بحيث يملك الجاني الفرصة لتدمير البيانات.

– ثالثا: إستصدار أمر كف يد المشتبه بمجرد البدء بإجراءات التفتيش.

– رابعا: من خلال مراقبة كيفية إعداد نظم المعلومات والأثر الذي تتركه، ومعرفة السجلات الإلكترونية التي توفرها شبكات المعلومات، والوصول إلى الأنظمة والمواقع، والدخول إلى بروتوكولات الحوار والاتصال عبر الإنترنت، ومعرفة أماكن الاتصال

وأنواع الأجهزة المتصلة بها، ومعرفة متى تكون الجريمة مرتبطة بهذه الشبكة إذا كانت كذلك، فإنها تُعرف بالاختصار (ip).[22]

خامسا :قياسا على منع ضباط الشرطة القضائية من الإطلاع على الأوراق المختومة أو المغلقة أثناء التفتيش فإنه يمنع عليهم الإطلاع على نظام الحماية الآلية للبيانات المخزنة و المحمية بطريق التشفير أو الترميز أو بأي وسيلة تقنية أخرى ضد القرصنة، وذلك لاتفاقهما في نفس العلة وهي رفض مسبق لعمليات الاطلاع الغير مصرح به، لكن يجب أن يقابل ذلك رسم حدود للقاعدة العامة الموجودة في التشريعات العقابية وهي "إعفاء المشتبه في ارتكابه للجريمة من تقديم ما من شأنه أن يدينه بشكل مباشر" بحيث يجبر المتهم على تقديم أكواد الدخول و الكلمات السرية للمرور للملفات.

سادسا: لا بد من مراعاة خاصية هذه الجرائم من كونها عابرة للحدود أثناء التفتيش فالجرائم العادية يسهل تحديد مكان ارتكابها في حين أنه من الصعب تحديد مكان وقوع ارتكاب الجريمة في جرائم الإنترنت، لأنه لا يحولدون تنقل الملفات والرسائل الحاسوبية حدود مكانية، كما أنه لا توجد معاهدات واتفاقيا تتيحالتعاون الدولي في هذا المجال أو عدم قدرتها إن وجدت على مواجهة المتطلبات الخاصة بجرائم الكمبيوتر ومواكبة التحريات وكفالة السرعة للحصول على أدلة الإثبات[23].

---

[22] سحتوت نادية، التنظيم القانوني للجريمة المعلوماتية (أدلة إثبات الجريمة المعلوماتية)، مجلة دراسات وأبحاث، المجلد 1، العدد 1، 2009، ص51.

[23]سعيد سالم المزروعي وعزمان عبد الرحمان، إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقا للتشريع الإماراتي، مجلة العلوم الإقتصادية والإدارية والقانونية، المجلة العربية للعلوم ونشر الأبحاث، العدد 13، المجلد الثاني، أكتوبر 2018، ص 111-124.

سابعا – القضاء على الدور السلبي للمجني عليهم: خشية أن تهتز سمعة المجني عليهم أمام العملاء، خاصة في قطاع الأعمال والمصارف فيحجمون عن الإبلاغ على الجرائم المعلوماتية ويكتفون بإجراءات تأديبية للموظف ومحو آثار الجريمة وإصلاح الضرر بدل المحافظة على مسرح الجريمة، مما يؤدي إلى ضياع الدليل والبراهين بحيث يصبح التفتيش الذي تقوم به الجهات المختصة دون فائدة مرجوة منه[24].

المطلب الثاني: إجراءات التحقيق الابتدائي في جرائم تقنية المعلومات

التحقيق الإبتدائي اختصاص هام يباشره قضاء التحقيق بإجراءات مختلفة تتسم بالحياد، وأعضاؤه هم الذين يباشرونه في الأصل ضد متهم معين، لبحث الجريمة ومدى ثبوتها أو عدم ثبوتها بأنفسهم توصلا إلى مدى توافر أركانها.

وعلى ذلك فإذ يباشر قضاة التحقيق عملهم لايريدون من ورائه سوى الوصول إلى الحقيقة؛ بهدف الوصول إلى تطبيق متطلبات القانون وتحقيق العدل،ويجوزللنيابةالعامةأن تعين ضباط إنفاذ القانون للقيام بنشاط أو أكثرمن أنشطة التحقيق المحددة ، مثل عمليات التفتيش و المصادرة والنقل و التفتيش ، باستثناء استجواب المشتبه بهم[25].

وعليه قسمنا هذا المطلب إلى فرعين، الفرع الأول بعنوان التفتيش في جرائم تقنية المعلومات وجمع الأدلة وضبطها، والفرع الثاني: ندب الخبراء والاستجواب في جرائم المعلومات.

---

[24]سحتوت نادية، المرجع السابق، ص53.

[25]- عثماني عزالدين، المرجع السابق، ص21

الفرع الأول: التفتيش في الجرائم المعلوماتية.

الغرض من التفتيش هو ضبط كل ماله صلة بالجريمة ويساعد على كشف حقيقة الجريمة ومرتكبيها.

وقد يلزم أن يتم التفتيش في أماكن ذات حرمة خاصة، ويحيط القانون عمليات التفتيش بعدد من الضمانات والضوابط.

وقد يكون مكان التفتيش مسكنًا أو شخصًا، وفي كلتا الحالتين قد يتعلق بالمتهم أو بشخص آخر.

والغرض من التفتيش هوضبط أي شيء له صلة بالجريمة ومفيد للتحقيق الجاري، سواء كان ذلك الشيء أداة استعملت في ارتكاب الجريمة، أو شيئاً ناشئاً عن الجريمة، أو شيئاً آخر يساعد على كشف الحقيقة. وهنا كمكان خاص للتفتيش في ما يتعلق بالحواسيب هو جميع مكونات الحواسيب.

سواء كانت مادية أو عقلية، أو شبكات الاتصالات الخاصة، أو البيانات المسجلة في ذاكرة الحاسوب أو مخرجاته، أو السجلات المنشأة باستخدام نظم المعالجة الآلية للبيانات، أو يوميات التشغيل، أو المعاملات الخاصة عند الدخول إلى نظم المعالجة الآلية للبيانات، أو كلمات السر ومفاتيح فك التشفير، سواء كانت السجلات المتعلقة بمفاتيح الدخول أو مفاتيح فك التشفير، بالإضافة إلى الشخص الذي يستخدم الحاسوب

الذي تم فحصه، والمكونات المادية للحاسوب، ووحدة الذاكرة، ووحدة الحاسوب، والوحدة المنطقية، ووحدة الإخراج، وأخيرًا وحدة التخزين الثانوية.[26].

كما تنقسم المكونات المادية والمعنوية للحاسب الآلي إلى نوعين، وفقاً لاحتياجات العميل:

الكيانات المنطقية الأساسية أو برامج النظام والكيانات المنطقية التطبيقية أو البرامج التطبيقية، والبرامج التطبيقية والبرامج التطبيقية، والمكونات المذكورة أعلاه. وتتطلب الحواسيب بمكوناتها مجموعة من الأشخاص ذوي الخبرة والمهارات في تكنولوجيا نظم المعلومات، سواء كانوا مشغلي حواسيب وأخصائيي برامج، أو مخططي برامج تطبيقية، أو مهندسي صيانة واتصالات أو مدير ينظم معلومات.[27]

وليست الغاية من التفتيش التعدي على الحريات والخصوصيات المصانة في جميع الدساتير والقوانين العالمية وإنما محاولة الوصول إلى حل لغز الجريمة الرقمية، وكشف ستار الحقيقة سواء كانت تصب ضد مصلحة المتهم أو في مصلحته، وذلك مع مراعاة عدم الوقوع في التعدي أو التعسف على حقوق الأفراد أثناء تطبيق هذا الإجراء الخطير فالمشرع قد وضع عدة ضوابط تقدم ضمانات للمتهم سواء بفترة ما قبل إجراء التفتيش أو أثناءها.

---

[26]سعيد سالم المزروعي وعزمان عبد الرحمان، المرجع السابق، ص 111-124.

[27] إيهاب محمد التاج، المرجع السابق، ص 400.

ومن هذه الضوابط؛ الحصول على الإذن للقيام بعملية التفتيش، وتحديد الأشخاص المنوط بهم القيام بهذا الإجراء، والوقت المناسب لإجرائه، وغيرها من الضمانات.[28]

أولا: السلطة المخولة بالتفتيش في الجرائم المعلوماتية:

التفتيش مخول- بحسب الأصل- إلى جهة التحقيق، ويخضع للخصائص العامة التي تخضع لها كل إجراءات التحقيق التمهيدي، والقانون سمح لعناصر الضبط القضائي بالقبض على المتهمين وتفتيشهم وتفتيش مساكنهم في حالات معينة ووفقا لضوابط محددة، بما يعد استثناء من القاعدة العامة، حيث أن القضاء غير مطالب بإجراء التفتيش بنفسه، فربما لا يتوفر لقاضي التحقيق وقت لتنفيذه، خصوصا إذا كان هناك العديد من الأشخاص أو تمت الجريمة في أماكن متفرقة أو تعدد الحاسبات محل التفتيش، لذا جرت العادة في الغالب على تفويض أحد ضباط الشرطة القضائية وبناء على إذن صادر عن السيد وكيل الجمهورية للقيام به بمنحه "إذن أو أمر التفتيش" الذي يجب أن يراعى في إقراره وتحريره كل الشروط الخاصة بالندب.

البحث الإلكتروني هو إجراء تحقيقي، بإذن قضائي مسبق، يهدف إلى البحث داخل نظام حاسوبي أو شبكة الإنترنت، سواء كان هذا النظام يتكون من حاسوب واحد أو عدة حواسيب متصلة ببعضها البعض من خلال شبكة في مكان لا يمكن اقتحامه قانوناً والغرض من ذلك هو استخراج المعلومات الاستدلالية والتحقيق فيها، والمتمثلة في

---

[28] طارق عبد الرحيم الردايدة، التفتيش الالكتروني في الجرائم الرقمية - دراسة وصفية مقارنة -، مذكرة ماجستير ضمن تخصص أمن نظم المعلومات والجرائم الرقمية، جامعة الأميرة سمية للتكنولوجيا، الأردن، 2017، ص 54.

المعلومات والبيانات التي يمكن أن تساعد في الوصول إلى نوع الجناية أو الجنحة التي وقعت، بغض النظر عما إذا كانت مكونة من حواسيب.[29].

ثانيا: محل التفتيش في الجرائم المعلوماتية

إن تفتيش نظم المعالجة الآلية يعد من أعقد العمليات عند اتخاذ الإجراءات الجزائية حيال من يرتكب الجريمة المعلوماتية، كون محل التفتيش فيها هو نظام المعالجة الآلية ذو الطابع غير المادي، ولا يعدو أن يكون إلا معلومات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي[30]، ويجب اتباع قواعد وإجراءات تفتيش الأماكن في الجرائم الالكترونية أولا وقواعد وإجراءات تفتيش الأشخاص في الجرائم الالكترونية ثانيا

أولا- قواعد وإجراءات تفتيش الأماكن في الجرائم الالكترونية:

– يتم تحديد المكان الذي سيجرى تفتيشه وتحديد مداخله ومخارجه والمباني المتصلة به أو المؤدية إليه.

– تدرس ظروف المنطقة المحيطة بالمكان المراد تفتيش هو التحري عن مدى ردود الأفعال والاحتمالات التصدي للقوة أو التعدي عليها، ويتم إجراء تقييم مسبق لحالة الأفراد المراد تفتيشهم، وتتخذ كافة الاحتياطات اللازمة لكل حالة.

– تعيين قوات لمحاصرة المكان من الخارج تحدد وفق كل حالة.

---

[29] سعيد سالم المزروعي وعزمان عبد الرحمان، المرجع السابق، ص 111-124.

[30] سعيداني نعيم، المرجع السابق، ص 143.

-يجرى تفتيش المنازل في حضور الشخص المأذون بتفتيش مسكنة أو المتهم الذي ضبط متلبسا أو بحضور شاهدين من الأشخاص الذين تربطه بهم صلة قرابة أو القانطين رفقته بنفس المنزل أو جيرانه على أن يثبت ذلك في محضر الضبط.

-تنظيم عملية التفتيش بحيث لا يفصل جانب من المكان المراد تفتيشه أو ملحقاته.

-عدم السماح للأشخاص المتواجدين في الأماكن الجاري تفتيشها بمغادرة هذه الأماكن لأي سبب من الأسباب خشية انتهاز الفرص للتخلص من الأدلة الرقمية.

ثانيا- وقواعد وإجراءات تفتيش الأشخاص في الجرائم الالكترونية.

- لا يجوز أن يتعدى التفتيش شخص المقصود به إلى غيره، إلا أنه إذا حدث أثناء تفتيش مسكن أن قامت قرائن إزاء المتهم أو كان الشخص الموجود يظهر على أنه يحوز شيء مفيد في الكشف عن الحقيقة يجوز لضباط الشرطة القضائية تفتيشه وفقا للقانون.

- ينبغي أن يجرى التفتيش في مكان مغلق إلا إذا كانت الظروف تدعو لإتمامه في أماكن مفتوحة أما بالنسبة لتفتيش النساء فينبغي أن تتم داخل مكان مغلق أو بعيد عن الأنظار.

- قبل البدء في تفتيش أحد الأشخاص ينبغي السيطرة عليه أولا للحد من خطورته ومقاومته ومنع تأثير ذلك على إتمام تفتيشه، وتختلف وسائل الحد من خطورة الشخص ومقاومته تبعا لظروف كل حالة، فليس لذلك قواعد ثابتة لإتباعها إلا أنه يمكن إجمالها في أنها تقييد لحركة هذا الشخص ووضعه تحت السيطرة من أجل التفتيش، ويتم إثبات نتائج التفتيش في محضر[31].

[31]- مصطفى محمد موس، المرجع السابق، ص206.

كم أن هناك قواعد وإجراءات احتياطات الأمن في التفتيش في الجرائم الالكترونية:

أ – على ضباط الشرطة القضائية التنسيق بالاتصال عن طريق رؤسائهم برئيس قسم مكافحة الجرائم الالكترونية وشبكاتها المختص قبل حصولهم على أوامر التفتيش أو الضبط وقبل شروعهم في ضبط الدليل الالكتروني لاحتمال أن يكون لديه من المعلومات ما يفيد في إجراءات التفتيش أو الضبط أو التخطيط.

ب – يقوم رئيس قسم مكافحة قسم الجرائم الالكترونية وشبكاتها بتزويد ضابط الشرط القضائية بما لديه من معلومات وإرشادات وعليه الاشتراك معهم في التفتيش والضبط في الأحوال الآتية:

– إذا تعلق الأمر بضبط عصابات

– إذا كان المطلوب ضبطه ممن عرف عنهم استخدام السلاح.

– إذا كان المطلوب يباشر نشاطه في مناطق صحراوية أو نائية.

– إذا كانت هناك ظروف أخرى تقتضي هذا الاشتراك.

ج – إذا رأى رئيس قسم الجرائم الالكترونية وشبكاتها أن ظروف التفتيش تقتضي الاستعانة بقوات أكثر فاعلية أن يلجأ إلى الشرطة المحلية على أن هذه القيود لا تشل يد ضابط الشرطة القضائية في حالة وقوع حالة تلبس بحيازة الدليل الإلكتروني.

الفرع الثاني: استخلاص الأدلة الإلكترونية وإحرازها

الغرض من القيام بالتفتيش هو الحصول على الأدلة أو الأشياء المفيدة في إظهار الحقيقة في الجريمة الواقعة، فالضبط في غالب الأحوال هو الغاية من التفتيش، غير أن ذلك ليس الهدف الوحيد من التفتيش فقد يتم استنادا لأسباب أخرى غير التفتيش، وكمثال على ذلك المعاينة وما يقدمه المتهم والشهود أمام مراكز الشرطة.

في قانون الإجراءات الجنائية، يُقصد بالضبط في قانون الإجراءات الجنائية ضبط أي شيء يتعلق بالجريمة ويفيد في كشف الحقيقة عن الجريمة ومرتكبيها، ويمكن أن تكون طبيعته القانونية إما إجراء استدلالي أو إجراء تحقيقي.

والغرض من التفتيش هو ضبط أي شيء يفيد في الكشف عن الحقيقة، بصرف النظر عن الشخص أو المكان أو الشيء، مادام له صلة بالجريمة. وقد ينطوي جمع الأدلة في الجرائم السيبرانية على عناصر مادية مثل الحواسيب وملحقاتها والأقراص الصلبة والأقراص الممغنطة والأشرطة والطباعة والبرمجيات والبطاقات الممغنطة وبطاقات الائتمان وأجهزة المودم وغيرها من المعدات المستخدمة في شبكات الإنترنت، وفي هذه الحالة يمكن ضبطها وفقا لإجراءات الحجز والمصادرة التقليدية، ومن ثم لا تطرح أي مشاكل قانونية أو عملية[32].

ولذلك، فإن الأشياء التي ينبغي أن تخضع لإجراءات المصادرة في جرائم تقنية المعلومات هي الكيانات ذات القيمة التي يمكن استخدامها لإثبات الجريمة أو لإسناد الجريمة إلى مرتكبها:

1-) ضبط المستندات والكيانات الورقية التي يتم التلاعب بها إلكترونياً وتعتبر ذات صلة بالجريمة أو مرتكبها، والتي قد تكون مستندات مزورة في نظام حاسوبي، أو مستندات في أي موقع خارج النظام أو مستندات في سلة المهملات.

2- جهاز إدخال يتكون من لوحة مفاتيح، وشاشة، وفأرة، وخادم، وجهاز جمع البيانات، وماسح ضوئي، وبرنامج معالجة النصوص، وبرنامج عرض الشرائح.

---

[32] براهيمي جمال، براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه في القانون، جامعة تيزي وزو- الجزائر، نوقشت بتاريخ 2018/06/27، ص 47

3- تحتوي هذه الوسيلة على نظام حماية يتألف من رمز أو شيفرة لايمكن رؤيتها إلا إذا تعرف عليها الطرف المتلقي، حيث يمكن أن تحتفظ بنسخ من المواد المرسلة والمستلمة وتسترجعها وتستعرضها وتديرها.[33].

4- الأشرطة المغناطيسية:

جميع الأشرطة ووسائط النقل والتخزين التي قد تحتوي على مواد مفيدة في البحث عن الحقيقة أو في تحديد هوية الجناة.

5- طابعات المراقبة وآلات التصوير بجميع أنواعها.

وعلى وجه الخصوص، المعدات الحديثة القادرة على تخزين الوثائق والمواد المطبوعة أو المصورة بحيث يمكن إعادة استخراجها وتحديد محتوياتها.

6- التنسيق بين وحدة الذاكرة الرئيسية ووحدة التحكم والمودم (الوسيلة التي تتواصل بها أجهزة الكمبيوتر مع بعضها البعض عبر خطوط الهاتف).

الفرع الثالث: الإستعانة بالخبراء والاستجواب في الجرائم المعلوماتية

الخبرة هي إجراء بشأن موضوع ما يتطلب معرفة بعلم أو تقنية معينة يمكن أن يُستمد منها الدليل.

وبالتالي فإن معرفة الخبرة تفترض وجود شيء مادي أو حقيقة مادية يستمد منها الخبير رأياً[34].

---

[33] سعيد سالم المزروعي وعزمان عبد الرحمان، المرجع السابق، ص 111-124.

[34] إبراهيم رمضان إبراهيم عطايا، الجريمة الالكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، العدد 30، الجزء الثاني،2015، ص 382

وهي وسيلة لاستخدام المعلومات العلمية في تحديد التفسير الفني للأدلة والإثباتات، وهي ليست مستقلة عن الأدلة الشفوية أو المادية، بل هي تقييم فني لهذه الأدلة. والعنصر الذي يميز الخبرة عن غيرها من إجراءات الإثبات الأخرى، مثل المعاينة والشهادة والتحقيق، هو رأي الخبير الفني في توضيح الأدلة أو تحديد قيمتها الإثباتية في الإثبات.

وذلك لأن معرفة الخبير مفيدة في إثبات ارتكاب الجريمة، ونسبة الجريمة إلى المتهم، وتحديد خصائص الشخصية الإجرامية للمتهم.

الاستجواب هو أحد أهم إجراءات التحقيق المستخدمة للكشف عن الحقيقة. وترجع أهمية الاستجواب إلى أنه يمكّن سلطات التحقيق من طرح الأسئلة الصحيحة، والتعمق في موضوع القضية والوقوف على أدق التفاصيل حول الجريمة. يُعرّف الاستجواب بأنه "إجراء تحقيق يتم فيه استجواب المتهم عن الجريمة المتهم بها ويُطلب منه إما دحض الأدلة ضده أو الاعتراف بها".

أولا: ندب الخبراء في الجرائم المعلوماتية

أدى التطور التقني في نظم المعالجة الآلية إلى تغييرات كبيرة في المفهوم العام للأدلة، وقد أدت هذه البيانات في الواقع إلى زيادة دور الأدلة العلمية، وأعلنت عن إضافة الخبرة التكنولوجية إلى عالم الخبرة القضائية، حيث إن استنباط الأدلة الرقمية

اللازمة لإثبات الجريمة السيبرانية وكشف أنماطها يتم على أيدي خبراء متخصصين في هذا المجال.[35].

لذلك هناك حاجة دائمة لخبراء وفنيين في حال وقوع جرائم تقنية المعلومات، وتتراوح مهامهم بين فحص وتدقيق عمليات البيانات الآلية وتطوير البرمجيات وتشغيل الحاسب الآلي وعلومه، ويتوقف نجاح أو فشل أعمال جمع الأدلة والتحقيق في هذه الجرائم على كفاءة وخبرة هؤلاء الخبراء، ومن المعروف أنه

يجب على المحققين الجنائيين تحديد الدور الدقيق للخبير الاستخباراتي في القضية التي يكون مسؤولاً عنها.

وهذا يعيدنا إلى ضرورة تأهيل ضباط إنفاذ القانون وسلطات التحقيق الأولي في جرائم تقنية المعلومات من أجل إنجاح التحقيق في جرائم تقنية المعلومات. ومن الضروري أيضا عدم تشجيع البعض على الادعاء بأن الخبراء أنفسهم هم من يحددون إطار ولايتهم، لأن ذلك من شأنه أن يقوض دور المحققين والقضاة في القضايا الجنائية المتعلقة بجرائم تكنولوجيا المعلومات.

تتمتع النيابة العامة وقضاء التحقيق بالسلطة التقديرية في الاستعانة أو عدم الاستعانة بخبراء تحت إشراف محكمة الموضوع.

والاستعانة بالخبراء في مجال جرائم تقنية المعلومات ضرورية بصفة خاصة عندما يتعذر على المحقق فهم الجوانب التقنية والعلمية للجريمة أثناء التحقيق، والتي تتطلب درجة عالية من الخبرة لكشف غموضها أو فهم طبيعتها، ويقتضي القانون الاستعانة بأشخاص وهيئات فنية ومختبرية ومهنية متخصصة في المسائل المتخصصة.

---

[35] سعيداني نعيم، المرجع السابق، ص165.

وتجدر الإشارة إلى أن القانون يجيز استخدام الاستعانة بالخبراء كجزء من عملية التحقيق لكشف غموض الجريمة وإثبات أو دحض الأدلة ضد الجاني أو المشتبه به.

ثانيا: الاستجواب في الجرائم تقنية المعلومات

يعتبر الاستجواب الإلكتروني أحد إجراءات التحقيق في الجريمة الالكترونية للكشف عن هوية المتهم وعلاقته بالجريمة، كما أنه محاط بجملة من الشروط والضمانات التي تكفل تحقيقا عادلا[36].

وتجري سلطات التحقيق الاستجوابات في الجرائم الإلكترونية. فعند مثول المتهم لأول مرة للتحقيق، يجب على قاضي التحقيق تسجيل جميع البيانات المتعلقة بهويته وإخباره بالتهم الموجهة إليه وتسجيل البيانات المتعلقة بها في محضر.

ويؤدي الاستجواب بهذا المعنى وظيفتين: أولاً، التأكد من هوية المتهم ومناقشة التهم الموجهة إليه بالتفصيل.

ثانياً، تحقيق الدفاع عن المتهم.

فمناقشة الأدلة ضد المتهم قد تؤدي إلى اعتراف المتهم بالجرم المنسوب إليه، وفي الوقت نفسه تمهد الطريق لتفنيد الأدلة ضد المتهم إذا كان المتهم بريئاً، وبالتالي تجنب خطر إقامة الدعوى ضد المتهم أو تقديمه للمحاكمة كمتهم. كما أنه يساعد النظام القضائي على معرفة الحقيقة والكشف عن الجناة الحقيقيين[37].

---

[36] حاحة عبد العالي وقلات سمية، المكافحة الإجرائية للجرائم الالكترونية –دراسة حالة الجزائر –، مجلة المفكر، المجلد 13/ العدد 2 (جانفي2018)، ص 233.

[37] سعيد سالم المزروعي وعزمان عبد الرحمان، المرجع السابق، ص 111-124.

إلا أن الاستجوابات لا تخلو من المخاطر، كالرغبة في تضييق الخناق على المتهم والأسئلة المتعددة التي تهدف إلى استدراج المتهم إلى النطق باعترافات قد تكون صحيحة أو كاذبة، أو مجحفة بحق المتهم، أو غير واقعية أو خادعة لنظام العدالة.

لذلك يجب أني كون المحقق خلال مرحلة الاستجواب على دراية بجرائم تقنية المعلومات وكيفية ارتكابها، ومبادئ ومصطلحات الحاسب الآلي والإنترنت وما يتعلق بها، ومبادئ وأصول أمن المعلومات، حتى يتمكن من التواصل الجيد مع الشهود والمتهم من جهة ومع خبراء الحاسب الآلي في فريق التحقيق من جهة أخرى، ومن المحتمل أن يكون أفضل نهج أثناء عملية الاستجواب هو ضرورة حضور خبير الحاسوب أثناء عملية الاستجواب وأن يكون قادراً على المشاركة في الاستجواب من خلال طرح أسئلة ثانوية على الشهود والمتهم.

وبدلاً من ذلك، يمكن لخبير الحاسوب أن يكتب الأسئلة على ورقة ويضعها أمام المحقق حتى يتمكن المحقق من اختيار الفرصة المناسبة لطرح الأسئلة[38].

والقواعد المتبعة في المناقشات والمقابلات هي نفسها إلى حد كبير، بما في ذلك ضرورة عزل الشاهد والمتهم حتى لا يتأثر أحدهما بأقوال الآخر، والترتيب الذي يتم به أخذ الأقوال، وضرورة قراءة المحققين للإيماءات ونبرة الصوت[39].

---

[38] سعيد سالم المزروعي وعزمان عبد الرحمان، المرجع نفسه، ص 111-124.

[39] محمد حسن السراء، المرجع السابق، ص 52.

المحور الثاني: القيمة الثبوتية للدليل الإلكتروني أمام القضاء الجزائي

اتجه الفقه الجنائي إلى أن الإثبات عملية متكاملة تهدف إلى البحث عن الأدلة التي تثبت حدوث الواقعة الجنائية و ظروف ارتكابها و أسبابها و تنسبها إلى مرتكبيها وتقديمهم للعدالة، ولكن دور الدليل ينحصر في اقناع المحقق و القاضي بتورط الجاني في اقتراف الجريمة أو براءة، إذن الإثبات الجنائي يشمل الوسائل و الإجراءات المشروعة للبحث عن الأدلة و تحقيقها، وعند ظهور الدليل يبدو واضحا التمييز بين وسيلة الإثبات و النتيجة التي تتجسد في الدليل، لذلك يُعرّف إثبات الوقائع الجنائية بأنها لإجراءات التي تتخذها السلطات القضائية لتوضيح الغموض في مجال التحقيق والحكم، وإظهار الحقيقة وحماية الحياة الخاصة و مراعاة قرينة البراءة .

وعملية الإثبات الجنائي تتشكل من عدة مراحل متعاقبة ومترابطة تنطلق من إثبات حدوث الواقعة الجنائية وكونها فعل ملموس كأثر لمخالفة القانون ونتيجة لنشاط محضور واضح الأركان و المعالم و الظروف و الأسباب و الدوافع، قد تظهر مراحله عقب الارتكاب و الضبط الفوري للجاني، وقد يتخلف الكشف عن هذه المراحل والتعرف على الحقيقة لما بعد ذلك وإزالة الغموض، وفي كل هذه الأحوال تعرف الدعوى الجنائية مراحل رجحان الأدلة وإحالة الواقعة للمحاكمة ولا يشترط هنا في الأدلة اليقين، لكن يكفي فيها الإحتمال، ولكن في مرحلة الحكم تخضع الوقائع الجنائية للإثبات بأدلة يقينية وحازمة إضافة إلى لمسها المباشر ليقين القاضي وقضى بأن المغزى في المحاكمات باقتناع القاضي بشكل يقيني بأي دليل أو قرينة يطمئن إليها، مما يجعله ينطق بالحكم وهو مطمئن إلى تحقيق العدالة فيجب أن تبنى أحكام الإدانة على حجج و أدلة و براهين قاطعة الثبات تفيد الجزم و اليقين، ويكفى للحكم بالبراءة التشكيك في نسبة التهمة إلى المتهم أو عدم كفاية أدلة الثبوت[40].

المبحث الأول: الأحكام الاجرائية لاستخلاص الدليل الرقمي

نظرا للطبيعة التقنية للجريمة المعلوماتية وكذلك الدليل الرقمي والمعوقات التي تواجه رجال الأمن والتحقيق للوصول إلى أدلة الإثبات فإنه لابد من وجود طرق إجرائية مستحدثة تتناسب مع طبيعتها التقنية والتكنولوجية، وهو ما أدى بالتشريعات في مختلف الدول إلى إرساء قواعد جزائية مستحدثة تقوم بتكريس تقنية المعلومات من أجل استخلاص الدليل الرقمي.

---

[40]- محمد محمد عنب، استخدام التكنولوجيا الحديثة في الاثبات الجنائي، مطبعة السلام الحديثة، مصر، 2008، ص 10، 11.

والمشرع الجزائري وكغيره من التشريعات قام بإرساء جملة من المقومات التشريعية لمكافحة الجريمة المعلوماتية من خلال ما جاء به القانون 22-06 المؤرخ في العشرون من ديسمبر من سنة ألفين وستة المعدل والمتمم لـ ق.إ.ج الأمر (66/155) من خلال إجرائي التسرب واعتراض المراسلات، وكذلك بموجب إصدار قانون إجرائي خاص به القانون 04-09 المتضمن القواعد الخاصة بالوقاية من الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقام باستخدام إجراء المراقبة الإلكترونية، إلى جانب إجراء التفتيش، وسوف نتعرض في هذا المبحث إلى كل من هذه الإجراءات المستحدثة في مجال المعلوماتية.

المطلب الأول: المراقبة الإلكترونية

تناول المشرع الجزائري هذا الإجراء من خلال المادة الرابعة من القانون رقم 09-04 المتعلق بالقواعد الخاصة بالرقابة عن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بعنوان مراقبة الاتصالات الإلكترونية –الحالات التي تسمح باللجوء إلى الرقابة الإلكترونية.

الفرع الأول: تعريف المراقبة الإلكترونية

المراقبة الإلكترونية هي واحدة من أهم موارد التحقيق التي غالبًا ما تُستخدم في التحقيقات والتحريات المتعلقة بالجرائم الإلكترونية، وهي جزء لا يتجزأ من عمل المحققين والعملاء.[41]

[41] محمد حسن السراء، المرجع السابق، ص 51.

ونجد أن المشرع الجزائري لم يعرف هذا الإجراء من خلال القانون رقم 04-09 ولهذا سيتم التطرق إلى التعريف الفقهي، الذي وضع له العديد من التعريفات منها: المراقبة الإلكترونية "تعتمد على التنصت والتسجيل ومحلها الدردشات الخاصة سواء كانت مباشرة أو غير مباشرة، بمعنى سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية واللاسلكية"، ورأي أخر أن المراقبة هي نوع خاص من استراق السمع يسلط على الأحاديث الشخصية والمحدثات.

وتستخدم كلمة المراقبة للدلالة على مراقبة الشبكات الخاصة بالإنترنت وقد عرفها قانون المراقبة السلكية واللاسلكية الفيدرالي الأمريكي بأنها "الالتقاط السمعي، أو أي التقاط سمعي أو أي التقاط لمحتويات أي اتصال إلكتروني أو شفهي باستخدام أي جهاز آخر.[42]

الفرع الثاني: شروط وآليات المراقبة الإلكترونية

يمكن أن نستنتج شروط وآليات المراقبة الإلكترونية في التشريع الجزائري من خلال نص المادة 65 مكرر 5 من قانون الاجراءات الجزائية على أنها:

- اعتراض الاتصالات عن طريق الاتصالات السلكية واللاسلكية
- القيام بترتيبات تقنية دون موافقة الأشخاص المعنيين من أجل بث أو تسجيل ما قاله شخص أو أكثر في مكان خاص أو عام أو التقاط صور فوتوغرافية لشخص أو أكثر في مكان خاص.

[42] عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية مجلة الفكر الشرطي، المجلد 22، العدد 86، 2013، ص 270.

وتشير المادة 04 من القانون رقم 09-04 إلى الجرائم التي تضر بالأمن الوطني.

- عندما تكون هناك معلومات تفيد بإمكانية الاعتداء على نظم المعلومات بطريقة تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

- عندما يكون من الصعب، بسبب احتياجات التحقيقات القضائية والتحقيقات، التوصل إلى استنتاجات فيما يتعلق بتحقيق جارٍ دون اللجوء إلى المراقبة الإلكترونية.

- كجزء من تنفيذ طلب التعاون القضائي الدولي.

أما بالنسبة لإجراءات تنفيذ المراقبة الإلكترونية وفقا لما جاء في القانون 09-04 ونصت عليه المادة 04 منه، فهي:

الإذن المكتوب: ويتضمن

- التعريف والمراقبة.
- طبيعية الجريمة.
- تسليم الإذن.
- كتابة وتحديد المدة التي لا تتجاوز 4 أشهر قابلة للتجديد.

طرق التنفيذ: وتشمل:

- سرية الإجراءات.

- التسيير: حيث أنه يمكن لوكيل الجمهورية أو قاضي التحقيق أو ضابط الشرطة الفضائية أن يسخر عونا مؤهلا لدى هيئة مكلفة بالاتصال (العامة، الخاصة) للقيام بهذا الإجراء.

- المحاضر: حيث يحرر الشخص المكلف بالعملية محضرا يحتوي على العناصر الأساسية للعملية.

المطلب الثاني: التسرب واعتراض المرسلات

يعد التسرب إجراء من إجراءات البحث والتحقيق الحديثة التي اعتمدتها معظم تشريعات العالم الحديثة لمكافحة الجرائم الإلكترونية، وقد كانت اتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية مبادرة لاحتواء هذا الإجراء من خلال المادة العشرون على أساليب التحري الخاصة بما فيها التسرب الذي عبرت عنه بـ "الأعمال المستترة".[43]

أما المشرع الجزائري فقد تبنى بدوره هذا الإجراء، عقب تصديق الجزائر على اتفاقية منظمة الأمم المتحدة أعلاه بموجب المرسوم الرئاسي رقم 05-02 المؤرخ في 02/2/ 2002 مع التحفظ واتفاقية مكافحة الفساد لسنة 2003 بتاريخ 19/ 4/ 2004.

الفرع الأول: التسرب

وهو الإجراء المستحدث الذي نص عليه قانون الإجراءات الجزائية في نصوص المواد من مكرر 11 إلى المادة مكرر 18.

أولا تعريفه:

تقنية يسمح بموجبها بالدخول إلى وسط مغلق مثل جماعة إجرامية أو شبكة تتاجر في الممنوعات

[43] براهيمي جمال، المرجع السابق، ص 82-83.

كالأسلحة أو المخدرات، وتتم هذه العملية بعد اختيار ضابط الشرطة القضائية لأحد العناصر التابعة له الذين تتوفر فيهم بعض الصفات الخاصة للتأقلم والتكيف مع الوسط المستهدف.

ثانيا: شروطه

– وبعد إبلاغ المدعي العام، يجب الحصول على إذن خطي مسبق من المدعي العام أو قاضي التحقيق؛ والجريمة التي تبرر استخدام التسريب؛ وهوية ضابط الشرطة الذي ينسق العملية؛ ومدة العملية (التي يتم تحديثها وفق المتطلبات التحقيق أو التحقيق، والتي لا يمكن أن تتجاوز أربعة أشهر).

– يجب أن تكون الجريمة واحدة من الجرائم المحددة في المادة 65–2 (5) من قانون الإجراءات الجنائية، بما في ذلك الجرائم ضد أنظمة المعالجة الآلية للبيانات.

ثالثا– مراقبة إجراءات التسرب:

يراقب التسرب و.ج المتخصص أو قاضي التحقيق وفقا لنص المادة 65 مكرر 11 ق.إ.ج.ج، ويمكن لهما الأمر بوقف التسرب في أي مرحلة وذلك من أجل تأمين خروج متسلسل من الشبكة الإجرامية أو عدم جدوى التسرب.

رابعا– التسرب في مجال الإجرام المعلوماتي:

تكون عملية التسرب في الجرائم الإلكترونية بدخول ضابط أو عون شرطة إلى العالم الافتراضي وذلك عن طريق اشتراكه في المحادثات كغرف الدردشة، أو اختراق مواقع معينة استخدام أسماء وهمية أوصفات أو أسماء مستعارة في طريقة اقتحام

القراصنة للمواقع الإلكترونية ومحاولة الاستفادة منها، أو الاتصال بالمشتبه فيهم عن طريق البريد الإلكتروني.

لا يجوز لموظفي الشرطة القضائية المشاركة بأنفسهم في إجراءات التسريب دون إذن مسبق من السلطة القضائية المختصة. ويجب أن تتم الإجراءات تحت الإشراف المباشر للسلطة التي أصدرت الإذن، حسب الحالة[44].

الفرع الثاني: اعتراض الاتصالات والتسجيل الصوتي والتصوير الفوتوغرافي

يتعلق الأمر بمسألة بالغة الأهمية كونها تشكل انتهاكا لحرمة المراسلات التي كفلها الدستور الجزائري، غير أن المشرع الجزائري قد سمح بموجب وتسمح المادة 65-2-05 من قانون الإجراءات الجزائية باعتراض الاتصالات عن طريق الاتصالات السلكية واللاسلكية في حالة جرائم المخدرات والجريمة المنظمة الدولية والجرائم المرتكبة ضد أنظمة المعالجة الآلية للمعطيات إذا كان ذلك ضروري التحقيق في الجرائم المرتكبة في الوقت الحاضر. وتجدر الإشارة إلى أن هذه المادة تجيز للمشرع الجزائري الترخيص بهذا الإجراء في حالة الجرائم المرتكبة ضد أنظمة المعالجة الآلية للمعطيات حتى تتمكن جهات التحقيق من استخلاص أدلة الإثبات والوصول إلى الحقيقة.

وتنص المادة03 من قانون منع ومكافحة الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات على ما يلي:

"وفق القانون المتعلق بالاتصالات وسرية الاتصالات، أو الحاجة إلى حماية النظام العام أو الحاجة إلى التحقيقات أو الاستفسارات القضائية، وفق اللقواعد

---

[44] براهيمي جمال، المرجع السابق، ص 85-86.

المنصوص عليها في الإجراءات الجزائية لهذا القانون، يجوز مراقبة الاتصالات الالكترونية وجمعها وتسجيل محتوياتها وتسجيلها في الوقت الحقيقي ووضع الترتيبات التقنية للقيام بإجراءات البحث والضبط داخل النظام" في الماضي كانت وسيلة الاتصال في الماضي عن طريق الهاتف، أما في الوقت الحاضر فقد انتقلت إلى البريد الإلكتروني وغرف الدردشة على الإنترنت. ويعرّف المشرع الجزائري الاتصالات في المادة 09 من القانون 03-2000 على النحو التالي: "كما يعرّف وسائل الاتصال الإلكترونية بأنها وسيلة "نقل أو إرسال أو استقبال الإشارات أو النصوص أو الصور أو الأصوات أو المعلومات المختلفة بأي وسيلة إلكترونية". وبالتالي، فإن مراقبة محتوى الاتصالات عبر الإنترنت والرسائل الإلكترونية تعتبر جريمة يعاقب عليها القانون لأنها تتعلق بحرمة الحياة الخاصة، كما أشار المشرع إلى ذلك في المادة 137 من قانون المتعلق العقوبات الجزائري، العقوبات الجزائري إلا في الحالات التي أجازها القانون كما سبق الذكر في المادة 03 من قانون، 04-09 ولهذا فإن المشرع الجزائري فرض الحماية القانونية على جميع الاتصالات الإلكترونية باعتبارها جزء من الخصوصية وأجاز ذلك في الحالات التي يسمح بها القانون من أجل مقتضيات التحري والتحقيق والوصول إلى أدلة الإثبات ووفقا لما تتطلبه العدالة الجنائية.

المبحث الثاني: حجية الدليل الرقمي في الإثبات الجنائي

ينص الفقه والقانون الموضوعي على أن القضاة يتمتعون بصلاحيات واسعة لتقييم الأدلة واستخلاص الاستنتاجات من الأدلة وآثارها الوقائعية. ومع ذلك، يجب أن تكون الأدلة مثبتة على وجه اليقين، وأن تكون ذات صلة بالوقائع الرئيسية ومتسقة مع التسلسل المنطقي للأحداث، وبالتالي يجب أن يكون هذا الرأي متسقًا أيضًا مع أدلة

الجرائم الرقمية. والأدلة الجنائية الرقمية هي شكل من أشكال الأدلة المادية العلمية التي تحكمها قواعد علمية ورياضية لا تترك مجالا للتأويل، ومن ثم فهي أكثر حجية في الإثبات ومعالجتها بواسطة تكنولوجيا المعلومات، ومن ثم يجري استغلالها في الجريمة السيبرانية الجديدة (والافتراضية،أي الإلكترونية) هناك: على الرغم من عدم وجود تشريعات جوهرية ورسمية تنظم استخدام الحواسيب وتكنولوجيا المعلومات، إلا أن المحاكم لم تواجه أي مشاكل في التعامل مع الأدلة الجنائية الرقمية للأسباب التالية

1. الموثوقية التي اكتسبتها الحواسيب والكفاءة التي حققتها النظم المعلوماتية الحديثة في مختلف المجالات، وربط الأدلة الجنائية الرقمية وآثارها بالجريمة محل المحاكمة، ووضوح ودقة الأدلة الرقمية في إثبات العلاقة بين الجاني والمجني عليه، أو بين الجاني والفعل الإجرامي (1) أن تكون الأدلة واضحة ودقيقة؛ و

(2) إمكانية تعقب الأدلة الرقمية والوصول إلى مصادرها، وحقيقة أن الأدلة الرقمية تستند إلى نظريات رياضية مثبتة وغير قابلة للشك، مما يعزز يقين الأدلة الرقمية.

3) حقيقة أن العلم يمكن أن يتوصل إلى رأي واستنتاج قاطع بشأن صحة النتائج التي يتوصل إليها علم الحاسوب.

4) أن الأدلة الجنائية الرقمية عادة ماتكون مدعومة برأي الخبراء، وأن الخبرة في المسائل الجنائية لها دور في الكشف عن الأدلة والتحقيق فيها وتقييمها وتقديمها للمحكمة وفق شروط وقواعد ينظمها القانون وتقرها السلطات القضائية.

5 ومع بروز الجريمة السيبرانية والجرائم ذات التقنية العالية كظاهرة جديدة، لم يعد هناك مجال لاستكشاف سبل تحقيق العدالة في سياق هذا النوع من السلوكيات إلا من خلال استخدام التقنيات الافتراضية ذاتها.

وقد تم إدخال البيئات السمعية والبصرية عن بُعد من خلال التحقيقات التي تأخذ أقوال الشهود وتكشف عن الصور والبيانات التي توضح الجريمة السيبرانية والجريمة التقليدية من خلال الوسائل الحديثة.

وبموجب هذه القواعد، فإن التقارير والمعلومات والبيانات المحفوظة بأي شكل من الأشكال، وكذلك الوقائع والأحداث والآراء والتحليلات التي ينقلها أشخاص من ذوي المعرفة والخبرة في مجال الأنشطة والممارسات المنظمة، هي على عكس الأدلة السمعية الأخرى، بيانات أكثر دقة ومحفوظة بطريقة علمية وبالتالي فهي جنائية تعتبر أدلة مقبولة في المحاكم.[45]

المطلب الأول: مفهوم الدليل الرقمي

وبشكل عام، تلعب الأدلة الجنائية دورًا مهمًا في الكشف عن حقيقة الوقائع قيد التحقيق أو في المحاكمة وغالبًا ما تكون حجر الزاوية الذي تُبنى عليه القضية، كما تلعب الأدلة الجنائية دورًا حاسمًا في تشكيل معتقدات القاضي.

الفرع الأول: تعريف الدليل الرقمي:

[45] محمد قاسم أسعد الردفاني، المرجع السابق، ص 185.

أدلة من أجهزة الكمبيوتر فيشكل مجالات ونبضات مغناطيسية وكهربائية يمكن جمعها وتحليلها باستخدام برامج الكمبيوتر، مثل برامج الرؤية الحاسوبية ومعلومات في أشكال متنوعة يمكن إتاحتها لوكالات إنفاذ القانون.

كما يعرف على أنه مجموعة من المجالات والنبضات المغناطيسية التي يمكن جمعها وتحليلها باستخدام برامج وتطبيقات خاصة وعرضها في شكل صور وتسجيلات صوتية وفيديو[46].

الفرع الثاني: خصائص الأدلة الرقمية

الأدلة الرقمية هي أدلة مجمعة بالحاسوب في شكل حقول ونبضات مغناطيسية وكهرومغناطيسية يمكن جمعها وتحليلها باستخدام برمجيات وتطبيقات وتقنيات خاصة. وهي المكوّن الرقمي للمعلومات المقدمة في شكل رسوم بيانية لاعتمادها من قبل وكالات الإنقاذ وإنفاذ القانون.

وتتميز الأدلة الرقمية عن الأدلة المادية المأخوذة من مسرح الجريمة العادي بالطرق التالية

تقلل طريقة نسخ الأدلة الرقمية من الحاسوب من خطر إتلاف الأدلة الأصلية أو تلغيه فعلياً، لأن طريقة النسخ هي نفسها طريقة الإنشاء.

من السهل، باستخدام التطبيقات والبرمجيات المناسبة، تحديد ما إذا كان قد تم التلاعب بالأدلة الرقمية أو تغييرها.

---

[46]مركز هردو لدعم التعبير الرقمي، الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، مصر، 2014، ص 23-31.

ونظراً للصعوبة النسبية لإتلاف الأدلة أو محوها، يمكن إعادة كشف الأدلة الرقمية من خلال القرص الصلب للحاسوب حتى لو أمر الجاني بحذف الأدلة من الحاسوب.

كما يتم تسجيل فعل الجاني بمحو الدليل كدليل، حيث يتم تسجيل نسخة من هذا الفعل (فعل الجاني بمحو الدليل) على الحاسوب ويمكن استرجاعها لاحقًا واستخدامها كدليل ضد الجاني.

ويسمح الانتشار العالمي لمسرح الأدلة الرقمية لمتلقي الأدلة الرقمية بتبادل المعارف القيّمة بسرعة وعلى نطاق عالمي وعلى نطاقات متنوعة، مما يسهم بسرعة نسبية في تحديد هوية الجناة وأفعالهم.

ويمكن للأدلة الرقمية أن سجلت حركات الفرد وعاداته وسلوكه وشؤونه الشخصية، مما يسهل العثور على التحقيقات الجنائية أكثر من الأدلة[47].

الفرع الثالث: مميزات الدليل الرقمي

– يمكن أن تظهر الأدلة الرقمية مرة أخرى من خلال ذاكرة الجهاز الذي يحتوي على هذا الدليل، حتى لو حاولت إصدار تعليمات لحذف هذا الدليل.

– يتم تسجيل محاولة الجاني لمحو الدليل الرقمي نفسه فيه كدليل، حيث يتم تسجيله في ذاكرة الجهاز أنه يفعل ذلك.

– الطبيعة الفنية للدليل الرقمي هو أنه يحتوي على العديد من البرامج و التطبيقات لتحديد ما إذا كان قد تم العبث به أوتحريفه.

[47]- مصطفى محمد موسى، المرجع السابق، ص217.

الفرع الرابع: أنواع الدليل الرقمي

لم يتطرق أغلب فقهاء القانون الجنائي إلى دراسة شاملة ودقيقة للأدلة الجنائية الرقمية نظرا لحداثة هذا النوع من الأدلة وبيئته التي تمتاز بالتطور المستمر، وبالرغم من ذلك نشير إلى محاولة فقهية قسمت الدليل الرقم الى[48]:

ألف–الأدلة المعدة كوسيلة للإثبات:

يمكن تلخيص هذا النوع من الأدلة الرقمية على النحو التالي::

– السجلات التي تم إنشاؤها تلقائيا بواسطة الجهاز، و تعتبر هذه السجلات من مخرجات الجهاز التي لميساهما لإن سانفي إنشائها، مثل سجلات الهاتف و فواتير الكمبيوتر. 1 . السجل هوجزء منه يتم حفظه بواسطة الإدخال ويتم إنشاؤه بواسطة الجهاز، ومثال على ذلك الإدخال إلى الجهاز وإجراء العمليات الحسابية على تلك البيانات.

ص. لم يعد الدليل وسيلة للإثبات:

حدث هذا النوع من الأدلة الرقمية دون إرادة الشخص. أي الأثر الذي تركه الجاني دون الرغبة في الوجود، يسمى هذا النوع من الأدلة ببصمة رقمية، وتسمى أيضا تتبعا لمعلومات الرقمية ،وسجلال رسائل المرسلة منه أو التي يتلقاها، وجميع الرسائل التي

---

[48] عيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي آفلو – الأغواط، العدد 06، مارس 2021، ص 154.

يتم إجراؤها من خلال جهاز أو شبكة معلومات عالمية للاتصال، يتجسد في الآثار التي تركها مستخدمو شبكات المعلومات.

في الواقع، لم يعد هذا النوع من الأدلة هو الأساس للحفظ من قبل الشخص الذي أصدره، ولكن الوسائل التقنية الخاصة، حتى بعد مرور بعض الوقت على ظهوره، يمكن الاستيلاء على جميع الاتصالات التي تتم عبر الإنترنت، وتلك التي يصدرها أو يتلقاها ذلك الشخص، بواسطة تقنية خاصة.

الفرع الخامس: أشكال الدليل الرقمي

المبدأ الأساسي هو أن الأدلة الرقمية ليست مهمة، فهي تتكون من بيانات ومعلومات فيشكل رقمي غير ملموس،ومخرجاتها في شكل مادي ملموس تتطلب استخدام أجهزة الكمبيوتر و أدواتها وأنظمة برامج الكمبيوتر ،والتي تتميز بسرعة وسهولة وصعوبة محوها أو إتلافها، وعندما يحاول الجاني محو الأدلة الرقمية،فإن هذه المحاولة ليست هذا يعني أنه سيتم تسجيلها كدليل.[49].

وللدليل الالكتروني ثلاث أنواع وهي:

– أولا: إخراج طبيعة الورق، حيث يتم تسجيل المعلومات على الورق، ويتم استخدام الطابعة والرسومات لطباعة الرسومات بدرجات مختلفة من الوضوح على الورق.

ثانيا: يتم استخدام إخراج الطبيعة الإلكترونية لتخزين المعلومات بدلا من المستندات الورقية مثل الشريط المغناطيسي أو الورقة المغناطيسية.

---

[49] إبراهيم رمضان إبراهيم عطايا، المرجع السابق، ص 383.

ثالثا: يتم عرض الإخراج المرئي بواسطة شاشة الكمبيوتر نفسها، ويمكن لهذا النوع عرض البيانات التي يعالجها الكمبيوتر على شاشة خاصة.

أما بالنسبة لأنواع الأدلة الإلكترونية كدليل على ما إذا كان يمكن تقسيمها إلى 2 أنواع رئيسية:

1-يتم إعداد الأدلة لتكون وسيلة للإثبات، مثلا لسجلات التي يتم إنشاؤها تلقائيا بواسطة الأدلة، والسجلات المحفوظة بواسطة المدخلات، و الأجزاء التي تم إنشاؤها بواسطة الآلات،والأدلة لمتعد وسيلة للإثبات من خلال ترك الجاني غائبا.

2-لم يعد الدليل وسيلة للإثبات، وهذا النوع من الأدلة الرقمية يحدث بدون إرادة الشخص، أي أنه لا يسمح للجاني بالبقاء على استعداد للوجود.[50]

الفرع السادس: مشروعية الدليل الرقمي

يتسع ويضيق مدى قبول الدليل الرقمي تبعا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة، وفي هذا الصدد نجد المشرع الجزائري وكغيره من المشرعين أفرد نصوص تحفز القاضي على الأخذ أو عدم الأخذ بأي دليل بما فيها الدليل التقني[51].

تعني شرعية الوجود أن الأدلة معترف بها، ويسمح القانون للقضاة بالاعتماد عليها لتشكيل إدانة للإدانة، ويمكن القول أن النظام القانوني مختلف في الموقف عن الأدلة المقبولة كأساس للإدانة.اعتماداعلى الاتجاه الذي يتبنونه، هناك

2 الاتجاهات الرئيسية: 1 هو نظام الأدلة القانونية و 2 هو نظام الأدلة الإقتناعية.

---

[50]- حسين طاهري، الجرائم الالكترونية، دار الخلدونية، الطبعة الأولى، 2021، ص267.

[51] فلاح عبد القادر وآيت عبد المالك نادية، المرجع السابق، ص 1701.

أولا – نظام الأدلة القانونية:

يقوم نظام الأدلة القانونية على الدور الرئيسي الذي يضطلع به المشرع في النص على قواعد الإثبات حيث يحدد مسبقا الأدلة التي يستند إليها القاضي في حكمه، فقد يشترط دليل معين أو شروط مضافة إلى الدليل الذي يحكم القاضي بناء عليه بعقوبة معينة.

إن هذا النظام لا يعرف اقتناع القاضي ويقوم مقامه اقتناع المشرع المبني على افتراض صحة الدليل، وعملية الإثبات تتم من خلال وضع المشرع لقواعد علمية مبنية على أسس ثابتة تحدد للقاضي طريق اقتناعه، ويقتصر دور هذا الأخير على الحرص على تطبيق القانون من حيث توافر الدليل وشروطه، فدور القاضي إذا مجرد عملية حسابية بحتة يجب عليه تطبيقها[52].

وفقا لهذا النظام، فإن المشرع هو الذي يحدد فقط الدليل على أن القاضي يمكنه الاعتماد على الأدلة و يحدد القيمة المقنعة لكل دليل، لذلك يقتصر دور القاضي على مجرد فحص الأدلة، ولاتوجد طريقة للقانون للثقة فيدور القاضي في تقييم القيمة المقنعة للأدلة للتأكد من استيفاء الشروط المحددة في القانون. يسمى نظام الأدلة القانونية أو المقيدة ، يقيد القانون القاضي بقائمة الأدلة التي حدد تقيمته الإثباتية، وهذا هو السبب في أن القانون يقيد القاضي بقائمة الأدلة التي حددت قيمته الإثباتية. ينتمي النظام إلى نظام معا لثقافة، وبالتالي، فإن الأنجلوسكسونيين، مثل المملكة المتحدة و المملكة المتحدة والولايات المتحدة،إلخ،لا يمكن للنظام الذي يعتمد هذا النظام التعرف على

---

[52]يقاش فراس، أنظمة الإثبات الجنائي وخصائصها، مجلة الحضارة الإسلامية، المجلد رقم 10، العدد 13، الصفحات 381-396 ص 381-382.

الأدلة الرقمية ذات القيمة الاستدلالية مالم ينص القانون صراحة على ذلك في قائمة الأدلة الاستدلالية،لذلك إذا لم ينص القانون على ذلك،فسيتم إهدار القيمة الاستدلالية،ومهما كانت شروط اليقين، سيعتمد القاضي عليها. لا يجوز تكوين اعتقاد بأي وسيلة.

بناء على هذا الفهم، قدم قانون أدلة الجريمة في المملكة المتحدة قبول اللأدلة الرقمية وحدد قيمتها الإثباتية بالاتفاق وطبيعة النظام القانوني في المملكة المتحدة.

ويقوم نظام الأدلة القانونية على أساس مبدأ حماية مصلحة المتهمين من تعسف القضاة، فقد يعتبر ضمان لحماية المتهم من تعسف القاضي بحيث لا يحكم على أحد إلا بالعقوبة التي حددها المشرع وبشرط الاطمئنان لها من حيث صحتها.[53]

قد يكون نظام الأدلة القانونية يقيد القاضي بحيث يفقد سلطته في الحكم وفق اللواقع،وغالبا ما يحكم ضد معتقداته من أدلة غير معترف بها فيذلك النظام،لذلك يصبح القاضي مثل آلة في طاعة أحكام القانون،لك يوسع هذا النظام نطاقه. حتى في البلدان التي تعتبر الأكثر تكريسا لها،على سبيل المثال، نجد أن بريطانيا بدأت في تخفي فصرامتها، فإنما يسمى بقاعدة الاعتقاد، و هي أن القاضي يمكن أن يكون إدانته، قد ظهر دون أدنى شك. من أي دليل، ولا حتى من بين الأدلة المقدمة عندما تكون هذه الأدلة قاطعة.

ثانيا – نظام الإتبات الحر:

[53]يقاش فراس، المرجع نفسه، ص 382.

تسود الأدلة الحرة في ظلال نظام اللاتيني، ووفقا لهذا النظام، يتمتع ضابط العدالة الجنائية بحرية مطلقة في إثبات الحقائق أمامه، ولا يلزمه القانون بالاعتماد على الأدلة في تكوين إدانته، ويجوز له أن يبني هذه الإدانة على أي دليل، حتى لو لم يتم تقديمها ،و لكن هذا النظام هو المشرع بطريقة لا يهتم النظام بأحكام الأدلة الاستدلالية، فكل الأدلة لها قيمة إثباتية متساوية في نظر المشرع، والقاضي هو الشخص الذي يختار من بين ما يعتبره صالحا للوصول إلى الحقيقة. وفي هذا يكون لها لحرية المطلقة في قبول الأدلة أو رفضها إذا لم يفع لذلك، على الرغم من توفر شروط صحة الأدلة، يحق للقاضي إعادتها تحت مبرر عدم الإدانة،لذلك يتمتع قضاة مثل هذا النظام بدور نشط في مجال الأدلة مقابل تراجع دور المشرع.

والمبدأ الأساسي الذي يقوم عليه هذا النظام هو أن اقتناع القاضي ويقينه الخاص النابع من ضميره فقط هو الذي يبني على أساسه أحكامه دون مراعاة لطريقة معينة يمليها عليه المشرع في الوصول إلى الحقيقة.[54]

لذلك،في مثل هذا النظام، بالنظر إلى أن المشرع غير مكلف بسياسة تقديم قائمة بالأدلة الاستدلالية، فإن مسألة شرعية الأدلة الرقمية لا تنشأ من حيث الوجود، وبالتالي فإن مسألة قبول الأدلة الرقمية تتأثر فقط بمدى اقتناع القاضي بها إذا كان هذا النوع من الأدلة قد يخضع لتقدير قضائي. ليس كذلك.

[54]يقاش فراس، المرجع السابق، ص 384.

وفقا لهذا النظام، إذا كان أصلا لدليل شرعيا في وجوده، فسيكون الدليل الرقمي شرعيا من حيث وجود الأصل واستحسانه.

ثالثا – حجية الدليل الاكتروني أمام المحاكم الجزائية الجزائرية:

إن الطبيعة التقنية الخاصة للأدلة الرقمية تجعل من الممكن العبث بمحتواها بطريقة تشوه الحقيقة، حتى بدون قدرة غير المحترفين على التعرف على التزوير، بالإضافة إلى أن معدل الأخ. نظرا لأن مثل هذه الفكرة تثير تساؤلات، فسيكون من الممكن استبعاد الأدلة الرقمية من دائرة الأدلة الجنائية لتناقضاتها وافتراض البراءة طاءفي إجراءات الحصول على أدلة صادقة عند الحديث عن الحقيقة يبدو مرتفعا في مثل هذه الأنواع.

بموجب النظام القانوني الذي يعتمد نظام الأدلة اللاتينية، يتمتع القضاة بسلطات واسعة لتقييم الأدلة من حيث قيمة الأدلة. يجوز للقاضي قبول أو رفض الأدلة، اعتمادا على إيمانه الشخصي بهذه الأدلة.

ولم ينص المشرع الجزائري صراحة على قبول الدليل الإلكتروني ، وهذا على الأساس يمكن الاعتماد على ما جاء بنص المادة 212 من قانون الإجراءات الجزائية الذي ينص على مبدأ حرية الإثبات في المواد الجنائية تطبيقا لنظام الإثبات الحر، حيث يقابله نص المادة 427 من قانون الإجراءات الجزائية الفرنسي الذي ينص على؛ في حالة عدم وجود نص على خلاف ذلك، يمكن إثبات الجريمة من خلال جميع الأدلة، ويبت القاضي على أساس معتقداتها لشخصية. من ناحية أخرى، ينص قانون الإجراءات على أنه يمكن إثبات الجريمة بأي دليل، مالم ينص القانون على خلاف

ذلك، ويمكن للقاضي اتخاذ قرار وفقا لإدانته، ولا يسمح للقاضي باتخاذ قرار يستند فقط إلى الأدلة المقدمة إليه فيسيا قال التماس والحجج المقدمة أمامه مباشرة.

ومن جهة أخرى يأتي إدراج المشرع لهذه المادة ضمن الأحكام المشتركة بطرق الإثبات، مما لا يدع مجالا للشك في تطبيقها أمام كل الجهات القضائية، وبالتالي اعتمد المشرع الجزائري نظام الإثبات الحر كأصل عام ونظام الإثبات المقيد كاستثناء، وقد ساير المشرع الجزائري الاتجاه العالمي المساير نحو الاعتراف أكثر فأكثر بحجية الأدلة الإلكترونية على اختلاف أنواعها مثل الإثبات بالكتابة في الشكل الإلكتروني، والتوقيع والتصديق الإلكترونيين.

كذلك نص المشرع الجزائري على مراقبة الاتصالات الإلكترونية وحفظ المعطيات المتعلقة بحركة السير وإلزام مؤدي الخدمات بحفظ الأدلة الإلكترونية والاستعانة بكل شخص له مؤهلات لمساعدة الجهات القضائية المختصة.

فيتبين لنا جليا أن المشرع الجزائري قد أخذ بحجية الأدلة الإلكترونية في الإثبات الجنائي ، نتيجة لانتشار الجرائم الإلكترونية بكافة أنواعها، وقصد تحقيق الفاعلية في مكافحتها، وهناك اتجاه دولي للاعتراف بحجية المراسلات الإلكترونية بمختلف أنواعها والإعتراف بحجية الملفات المخزنة في النظم و مستخرجات الحاسوب والبيانات المسترجعة، وحجية الملفات ذات المدلول التقني البحت والإقرار بالإثبات بالكتابة في شكلها الإلكتروني وبصحة التوقيع الإلكتروني وتساويه في الحجية مع التوقيع الحقيقي، والتخلي تدريجيا عن عدة عقبات تحد من الإثبات في الوسط الرقمي ومع كل هذا يجب مراعاة المبادئ والشروط التي تحكم الأدلة الإلكترونية، كمبدأ المشروعية، ومبدأ وجوب

مناقشة الأدلة ، وتأمين الدليل الرقمي ضد التلاعب إضافة إلى صحة الوقائع الواردة بالدليل[55].

المطلب الثاني: أساليب تقييم الدليل الرقمي

سنتناول وسائل تقييم الأدلة الرقمية من حيث السلامة من العبث، ومن ثم وسائل تقييمها من حيث سلامة الإجراءات التي تتبع للحصول عليها من الناحية الفنية وفقا للسياق التالي:

الفرع الأول: تقييم الدليل الالكتروني من حيث سلامته من العبث

يمكن ضمان سلامة الأدلة الرقمية من العبث بعدة طرق،بما في ذلك:

– تلعب علوم الكمبيوتر دورا مهما في توفير المعلومات التقنية التي تساهم في فهم محتويات وأشكال الكتيبات الرقمية، وتستخدم هذه العلوم للكشف عن درجة تشغيل محتويات هذا الدليل، وتعتبر فكرة التحليل التناظري الرقمي وسيلة مهمة للكشف عن موثوقية الكتيبات الرقمية، يعتقد أنه أحد أكثر أشكال التلاعب شيوعا، والتيمن خلالها سيرى الرقمي إلى أي مدى حدث العبث في النسخة المستخرجة.

–حتى إذا لم يتم الحصول على النسخة الأصلية من الدليل الرقمي أو تم العبث بالأصل، فمن الممكن استخدام عملية رياضية خاصة تسمى الخوارزمية.

---

[55] عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة دكتوراه تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، 2018/2017، ص 199-200.

– هنا كنوع من الأدلة الرقمية يسمى الدليل المحايد، وهو دليل لاعلاقة له بموضوع الجريمة،لكنه لا يغيرأو يغير نظام (الكمبيوتر).

تسمح لنا هذه الأساليب ضمان سلامة الأدلة الرقمية و مطابقتها للواقع.

الفرع الثاني: تقييم الدليل الالكتروني من حيث السلامة التقنية للإجراءات المتبعة في الحصول على الدليل الرقمي

عادة ما يتبعون سلسلة من الإجراءات الفنية للحصول على أدلة رقمية، ويمكن أن تعاني هذه الإجراءات من أخطاء قد تشكك في سلامة نتائجها.:

أ– باتباع اختبارين رئيسيين، يمكن كاستخدام الأدوات المستخدمة في العديد من التجارب للتأكد من دقتها في إعطاء النتيجة المرجوة.::

– اختبار سلبي كاذب: هذا الاختبار هو أداة تستخدم للحصول على الدليل، يمكنه عرض جميع البيانات المتعلقة بالدليل الرقمي.

– اختبار إيجابي كاذب: هذا يعني أن الأداة المستخدمة للحصول على الأدلة الرقمية تتطلب اختبارا تقنيا للتأكد من أن هذه الأداة لا تعرض أي بيانات إضافية جديدة.

لذلك ،من خلال اختبارات 2 هذه، يتم التأكد من أن الأدوات المستخدمة تعرض جميع البيانات المتعلقة بالأدلة الرقمية وفي نفس الوقت لاتتم إضافة بيانات جديدة، مما يعطي الموثوقية بأن النتائج التي يوفرها هذا الجهاز تثبت الواقع.

ب–الاعتماد على الأدوات التي أثبت تكفاءتها في تقديم نتائج أفضل للبحث العلمي:

تظهر الأبحاث المنشورة في مجال تكنولوجيا المعلومات الطريقة الصحيحة التي يجب اتباعها للحصول على الأدلة الرقمية، وبالتالي تثبت هذه الدراسات أدوات الكفاءة المشكوك فيها وهذا يساهم في تحديد موثوقية المخرجات المستمدة من هذه الأدوات[56].

إذا استوفت الأدلة الرقمية الشروط العامة لما يمكن أن يكون أساسا للإفراج عن الثقة بها،فقد يبدو من غير المقبول للقاضي إعادة تقييم هذه الأدلة ووضعها من جديد في مجال الدراسة، والأدلة الرقمية كدليل علمي، وأهميتها قاطعة فيما يتعلق بالحقائق المذكورة عنها، وقابليته اللتلاعب وخطوات الحصول عليها. إذا كنا قد اعترفنا سابقا بإمكانية التشكيك في سلامة الأدلة الرقمية بسبب معدل الخطأ، فهذه مشكلة فنية حيث لا يستطيع القاضي إبداء رأي نهائي، حتى لو لم يفعل ذلك الأشخاص في الولاية القضائية. **Therefore** لذلك، إذا استوفت الأدلة الرقمية الشروط المذكورة أعلاه فيما يتعلق بالسلامة من العبث والخطأ، فلا يمكن إرجاع هذه الأدلة حسب تقدير القاضي وفقا للمادة، فمن الضروري لتنفيذها أن يكون هناك مستوى مكافئ من الشك في الأدلة، حيث أن سلطة القاضي في إعادة الأدلة على أساس فكرة الشك، والقاضي هو دور القاضي سوف يقتصر على فحص الصلة بين الأدلة والجريمة.

[56]مركز هردو لدعم التعبير الرقمي، الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، مصر، 2014، ص 23-31.

في هذه الحالة، ليس هناك شك في أن التجربة تلعب دورا مهما في إثبات صحة هذا الدليل كأساس لتشكيل إدانة القاضي، لأن فحص موثوقية هذا الدليل ليس للقاضي، ولكن من جوهر فن الخبير.

وتجدر الإشارة إلى أن هذه القيمة التي ندعيها حول الأدلة الرقمية لا يمكن اعتبارها خروجا جديدا عن القواعد العامة للأدلة الجنائية للقانون، حيث توجد بعض الأدلة التي لا يستطيع ضابط العدالة الجنائية تقييمها وفقا لسلطته بموجب المادة 212 ،على سبيل المثال، سجل الانتهاكات.

نشير هنا إلى عدم الخلط بين الشك في أن الأدلة الرقمية ملوثة بأسباب العبث المحتمل أو وجود أخطاء في الحصول عليها معا لقيمة المقنعة لهذا الدليل. القضية الأولى لم يتخذ القاضي قرارا لأنها مسألة فنية، لذا فإن المثل بينهم هو أن القاضي ليس لديه خيار سوى قبول هذا الدليل ولا يمكنه التشكيك في قيمتها لإثباتية.

لأنه ،بطبيعته التقنية ،يمثل بيانا صادق اللوقائع، ما لم تثبت الأدلة عدم أهمية الجريمة المراد إثباتها[57].

المطلب الثالث: مدى حجية الدليل الإلكتروني في الإثبات الجزائي أمام القضاء

يقصد بحجية الدليل الإلكتروني أن لديها سلطة الإثبات للكشف عن الحقيقة والصدق في إسناد النشاط الإجرامي إلى شخص معين أوكذبه، فبمجرد الحصول على الأدلة وتقديمها إلى القضاء، لا يكفي اعتمادها كدليل على الذنب، ولكن من الضروري

[57] مركز هردو لدعم التعبير الرقمي، المرجع السابق، ص 23-31.

تقييمها والنظر في قيمتها في إثبات قضية جنائية. الفقه العام هو أن سلطة القاضي الجنائي هي تقييم السلوك الإجرامي.يخضع الدليل لمبدأ حرية القضاة في تكوين معتقداتهم الخاصة،والنتيجة المهمة حتما هي "حرية القضاة في تقييم الأدلة" ،والتي تهدرها أيضا في هذا المبدأ.

ومقابل ذلك لا ينبغي أن يفهم من حرية القاضي في الاقتناع التحكم المطلق في الأمور والقضاء كيفما شاء وفقا لأهوائه ومزاجه الشخصي، إنما هو مطالب بتحري المنطق الدقيق في تفكيره الذي قاده إلى اقتناعه واستلهام عقيدته، وألا يكون تفكيره هذا قد جافى الأصول المسلّم بها في الاستدلال القضائي.

ولتحقيق ذلك، أحاطه القانون بمجموعة من القيود التي تشكل في مجملها شروطا لإعمال المبدأ وتطبيقه التطبيق السليم بما يضمن بلوغ الحقيقة دون المساس بالحقوق والحريات العامة للأفراد.

مما لاشك فيه أن تطبيق هذا على الأدلة الإلكترونية يمكن أن يسبب بعض الصعوبات، حيث أن القاضي الجنائي، بثقافته القانونية وعدم كفاءته الفنية في مجال المعلوماتية، غير قادر على إدراك الحقائق المتعلقة بصحة الأدلة الإلكترونية. كما أن تمتع هذا الدليل بالقيمة الاستدلالية لقوة الإثبات التي يمكن أن تصل إلى نقطة اليقين، و الأدلة العلمية بشكل عام، يجعل من الممكن العبث بمحتوياته بسهولة بطريقة تشوه الحقيقة دون قدرة غير خبير، ناهيك عن الطبيعة التقنية للأدلة الإلكترونية.

في حالة حدوث هذه الصعوبات أو غيرها، من المهم أن تقوم المحكمة الجنائية بتقييم ومناقشة الأدلة الإلكترونية بمصداقية وقبولها أو رفضها لأنها غير مقتنعة بها.

بناء على ما سبق، سنراجع الشروط التي يجب توافرها في الدليل الإلكتروني للتعبير عن الحقائق العلمية الحقيقية (الفرع الأول) ، ثم نسلط الضوء على دور ذلك في تكوين الإدانات الشخصية للقضاة الجنائيين (الفرع الثاني).

الفرع الأول: شروط حصول الدليل الإلكتروني على حجية في الإثبات

تمتاز الجرائم الحاسوبية (ذات الطبيعة عبر الوطنية) على الشبكة الدولية بالقدرة الكبيرة على تحريف الأدلة أو إتلافها فتثير مشكلة تحديد صحتها، فعند الحصول عليها من خلال التفتيش عبر الحدود تظهر مشكلة تحديد صحتها، وذلك يعني ضرورة الحاجة إلى وضع إجراءات أو بروتوكولات في استخدامها في عمليات التفتيش الحاسوبية لضمان صحة البيانات المسترجعة أو لا ولحفظ شفافية وسلامة الإجراءات التي من شأنها إثبات صحة البيانات ثانيا.[58]

والدليل الالكتروني في حقيقة الأمر يعتبر صورة من صور الدليل العلمي يعكس حقيقة علمية محددة، وبالتالي فهو يحوز على حجية قوية في الإثبات، وذلك بما يميزه من دقة وموضوعية وحياد، ولكونه ناتج عن عمليات علمية حسابية دقيقة لا تقبل التأويل مما يجعله ذا حجة بالغة، ويعين القاضي من خلال التقليل من الوقوع في الأخطاء القضائية والاقتراب أكثر للوصول إلى الحقيقة، لأن التقنية العلمية توفر منهاجا دقيقة لجمع الأدلة ذات قوة علمية ثابتة إلى حد بعيد.

[58] طيبة جواد حمد المختار، صعوبات الملاحقة القضائية في الجرائم الحاسوبية، مجلات جامعة بابل، المجلد 14، العدد الأول، 2007 ص 05.

ومع هذا فرغم أن الدليل الإلكتروني بحكم طبيعته العلمية وموضوعى تهو حياديه مثل إخبارا حقيقيا عن الواقع، إلا أن ذلك لا يجعله بمنأى عن الشك في سلامته من العبث من خلال التغيير أو التحريف من ناحية، وفي صحة الإجراءات التي تم التحصل عليه من خلالها من ناحية أخرى.

وإذا كان الشك في مصداقية الدليل الإلكتروني مرتبطا أساسا بعوامل خارجية مستقلة عنه لا بمضمونه، فاكتسابه حجية داحضة في الإثبات وكذا قبوله كدليل تبنى عليه الحقيقة في الدعوى الجزائية يتطلب توافر الشروط التالية:

أولا- يقينية الدليل الإلكتروني

من الشروط الهامة على وجوب الأخذ بالأدلة المستمدة من الحاسوب وشبكة الإنترنت أن لا تكون ظنية، ولهذا اشترط قانون البوليس والإثبات في بريطانيا لسنة، 1984م "أنه لتحقيق حجية الأدلة الرقمية أن تكون المعطيات المستخرجة دقيقة ومتحصلة عن الحاسوب بصورة مشروعة".

وأن الدليل الرقمي له من جهة قوته القانونية الإثباتية التي تصل إلى حد اليقين، وهذا لا يعني ألا يكون الدليل الرقمي محل شك من سلامته من التغيير أو العبث، أو خطأ في صحة الإجراءات المتبعة في كيفية الحصول عليه وقد يرجع ذلك إلى عدم استخدام الأدوات المناسبة في الحصول على الدليل الرقمي وما قد يترتب عليه من أخطاء في أثناء عمليات استخراج الدليل الرقمي[59].

[59] طارق عبد الرحيم الردايدة، المرجع السابق، ص 172.

عادة ما تكون أدلة الطب الشرعي الرقمية مدعومة برأي الخبراء، وتلعب خبرة مواد الطب الشرعي دورها في الكشف عن الأدلة وفحصها وتقييمها وتقديمها أمام المحاكم وفقا للشروط والقواعد التي ينظمها القانون و يوافق عليها القضاء.

الأول هو المعرفة الحسية التي يتم استنتاجها من الحواسب عد فحص وفحص هذه المخرجات،والثاني هو المعرفة العقلية التي يدركها القاضي من خلال تحليل المخرجات الإلكترونية واستقراءها واختتامها وربطها بالظروف المحيطة بها.

إذا لم يأت القاضي لتأكيد نسبة الجرائم الإلكترونية إلى المتهم، في جبت برئته، حيث سيتم تفسير الشك لصالح المتهم.

و بغية تحقيق قدر أكبر من اليقين بشأن الأدلة الإلكترونية، مثل ماتخضع الأدلة الإلكترونية لقواعد وإجراءات معينة تحكم طريقة الحصول عليها، فإنها تخضع أيضا لقواعد أخرى تحكم قيمتها الإثباتية من وجهة نظر علمية، وربما يمكن النظر في أهم هذه التدابير لضمان سلامتها من العبث، وهي : في هذه الحالة، ينبغي أن تخضع المحكمة لتقييم تقنيبا لوسائل التقنية لطبيعة هذه الأدلة، مما يسمح للمحكمة بأن تقرر ما إذا كانت ستمضي في الإجراءات أملا.:

. تقدير الدليل الإلكتروني من حيث خلوه من العبث:

غالبا ما تخضع الطبيعة الفنية للأدلة الإلكترونية للشك والشك في سلامتها بسبب إمكانية تزويرها واكتشافها بطريقة تتعارض مع الحقيقة. يمكن تقديم هذه الأدلة بطريقة لا يستطيع غير الخبير التعرف على العبث بها والتعبير عن حقيقة محددة تم إنشاؤها خصيصا للتعبير عنها ضد الحقيقة،ويمكن القول أن هذا صحيح عند النظر في الأدلة

الفنية الأخرى المقدمة إلى القضاء. تجعل التكنولوجيا الحديثة من الممكن العبث بسهولة ويسر بالأدلة التقنية الإلكترونية لإظهار نفسها على أنها أصلية في التعبير عن الحقيقة.

لضمان سلامة الدليل الإلكتروني من العبث والعبث، عادة ما يتم استخدام مجموعة الآليات التالية:

أ-تقنية التحليل التناظري والرقمي:

هي تقنية لمقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بواسطة الآلة الرقمية والتحقق مما إذا كانت النسخة المستخرجة منه قد تم العبث بها، وهي تقنية لتوفير المعلومات الفنية التي تساهم في فهم محتوى الدليل الفني ووجوده و الكشف عن درجة تشغيل محتوى هذا الدليل. و يستخدم تكنولوجيا المعلومات الآلية التي أثبتت دورا فعالا.

ب- استخدام العمليات الحسابية الخاصة تسمى ب**Algorithm**الخوارزمية[60]:تستخدم هذه العملية عادة إذا لم يتم الحصول على النسخة الأصلية من الدليل الإلكتروني أو إذا كان هناك شك في أن العبث قد أثر على النسخة الأصلية. تتيح هذه التقنية ضمان موثوقية الدليل الإلكتروني وسلامته من العبث به أو التشويه.

[60]الخوارزميات في البرمجة هي وصفة يتم تقديمها للحاسب، يوجد فيها خطوات مفصلة ليقوم الحاسب بحل مشكلة أو يصل إلى هدف معين.

ج–استخدام الأدلة المحايدة: هونوعا من الأدلة الإلكترونية الرقمية المخزنة في بيئة افتراضية، والتي لاعلاقة لها بموضوع

الجريمة، ولكنها تساهم في التحقق من سلامة الأدلة الإلكترونية المقصودة في حالة عدم وجود تغييرات أو تعديلات على أنظمة الكمبيوتر.

2. تقييم الدليل الإلكتروني في السلامة الفنية لإجراءات التحصيل باعتباره تطبيق أدلة علمية دقيقة كما هو موضح أعلاه، إذا كانت نسبة الأخطاء الفنية في الحصول على الدليل الإلكتروني صغيرة جدا، فهذا لا يعني أنهم فقود تماما، ولكن قد يحدث خطأ أثناء الاستخراج، والذي قد يكون عيبا في الكود المستخدم، أو معلومات غير صحيحة و هذا يرجع إلى أخطاء عند استخدام الأدوات المناسبة لاستخراج الأدلة، مثل استخدام المواصفات.

أيضا، نظرا للأخطاء عند استخدام أدوات بدقة أقل من 100 ٪ (100٪) ،غالبا ما نقوم بتقليل البيانات أو معالجتها بشكل مختلف عن الطريقة الأصلية التي تم تقييمها.

ثانيا: وجوب مناقشة الدليل الإلكتروني

من شروط مشروعية الدليل الرقمي إمكانية مناقشة الأدلة المستخرجة من الحاسوب، الهواتف النقالة وغير من الأجهزة الرقمية، حيث تتم المناقشة بحضور جميع الأطراف إظهارا للحق، مع العلم أن القاضي يبني قناعته على الأدلة التي طرحت

ونوقشت أمامه في جلسة المحاكمة وتمت مناقشتها من طرف أطراف الدعوى جميعهم[61].

وتحقق شرط سلامة الدليل الإلكتروني من العبث وسلامته من الخطأ في إجراءات من الضروري أيضا مناقشة هذه الأدلة علانية في المحاكمة وفقا للمبادئ الأساسية للإجراءات الجنائية، و مبادئ الشفوية والمواجهة. لا يجوز لموظف العدالة الجنائية أخذ الأدلة المقدمة من أحد أطراف القضية أو بناءا لحكم عليها مالم يتم تقديمها شفويا في المحاكمة لإبلاغ الطرف الآخر حتى يمكن مناقشتها والرد عليها. وإبداء آرائهم في قيمتها القانونية.

ويترتب على ذلك عدم جواز اقتناع القاضي بمعلومات شخصية حصل عليها خارج الجلسة أو في غير نطاق المرافعات والمناقشات التي جرت فيها، وإلا يكون بذلك قد جمع في شخصه صفاتين متعارضتين هما صفة الشاهد وصفة القاضي، مما يبعث الحرج في نفسية الخصوم ويعيقهم عن مناقشة شهادته والرد عليها بحرية، لأن اعتماده على علمه الشخصي يجعله عرضة للتهم والشبهات وهو الأمر الذي يجب أن يتنزه القضاء عنه عموما.

كما أنه لا يجوز لضابط العدالة الجنائية الإدانة على أساس رأي الآخرين إلا إذا كان أحد الخبراء والفنيين الذين استشار هم وفقا للقانون وكان ضميره راضيا عن رأيهم وقرر الاعتماد عليهم نبين الأدلة المتبقية في ورقة قضيته السابقة.

---

[61] طارق عبد الرحيم الردايدة، المرجع السابق، ص 172.

لذلك ، إذا كان القاضي غير قادر على الحكم على جريمة إلكترونية بناء على معرفته الشخصية أو بناء على آراء الآخر ينكما هو موضح أعلاه، فمن الضروري أن يعيد التحقيق و مناقشة جميع الأدلة الناتجة عن الكمبيوتر الإلكتروني الموجود في ملف القضية. – بالنسبة لشهود الجريمة، يجب الاستماع إليه ممرة أخرى أمام المحكمة الابتدائية، وكذلك يجب على المهنيين من اختصاصاتهم المختلفة المثول بموجب هذا القانون لدى القاضي، لذلك قبل أن تناقش المحكمة تقاريرهم أنهم خلصوا إلى أن هي تحكم بشكل فعال في خطورة الأدلة التي تم الحصول عليها في مرحلة التحقيق ويعرض عليه مرة أخرى وسلطات التحقيق لمراقبة التقييمات المبرمة لوقائع الجرائم الإلكترونية[62].

تنص المادة 427 ،الفقرة 2،من قانون الإجراءات الجنائية الفرنسي على أنه "لا يجوز للقاضي إصدار حكم إلا على الأدلة المقدمة أثناء المحاكمة والتي نوقشت أمامه في مواجهة الأطراف . "وفي السياق نفسه، تنص المادة 302 من قانون الإجراءات الجنائية المصري على أنه" لا يمكن للقاضي أن يصدر حكمه على أساس أدلة لمتعرض عليه في جلسة استماع " ، لكن المشرع الجزائري اعتمد شرطا لمناقشة الأدلة في الفقرة الثانية من المادة 212 من قانون الإجراءات الجنائية على النحو التالي: "لا يمكن للقاضي أن يقدم له إلا في معرض". قراره غير مبرر على أساس الأدلة المقدمة. جرت المناقشة أمامه".

يبدو أن المشكلة في مناقشة الأدلة الإلكترونية هي أن معظم هذه الأخيرة تعتبر أدلة غير مرئية للعين المجردة ويتم تسجيلها بوسائل إلكترونية لا يمكن قراءتها أو

---

[62]براهيمي جمال، االمرجع السابق، ص 158.

استخلاصها إلا باستخدام الأجهزة الإلكترونية، وكذلك يمكن التلاعب بها عن طريق محو المعلومات المسجلة أو استبدال الآخر دون علم أحد، مما يجعلها مصدرا للنقاش العام عن بعد. الباقي هو مجرد نسخة تم الوصول إليها عن بعد، لأنها تثير مسألة الاحتمال. في هذه الحالة، تعتبر الأدلة المستردة أو التي تم الحصول عليها من المراقبة الإلكترونية دليلا أصليا، لذلك يمكن تقديمها إلى القضاء ومناقشتها في أدلة القضية.

لحل هذه المشكلة من وجهة نظر قانونية، ينص قانون الأدلة الأمريكي (3/1001) على أنه "من خلال قاعدة تؤكد على الانعكاس الدقيق للبيانات إذا تم تخزين البيانات على جهاز كمبيوتر أو جهاز مشابه – أفضل دليل–" ذهب المشرعون الأمريكيون إلى أبعد من ذلك واعترفوا بنسخة تلقى المشرعون الإنجليز واليابانيون إخراج الكمبيوتر تحويلها إلى صورة مرئية. من خلال المادة (224) من الفقرة الثانية من قانون الإجراءات الجنائية للنواب الألمان سواء كانوا أصليين أو نسخا مستخرجة من هذا الأصل، قام النواب الألمان بعمل مخرجات حاسوبية لأنواع مختلفة من البيانات من مصادر يجب على المحكمة قبولها كدليل أو طباعة أو نسخ[63].

هذا هو نفس الشيء الذي اعتمده المشرع اليوناني في المادة 364 من قانون الإجراءات الجنائية.

ربما كانت الطبيعة التقنية لهذا الدليل هي التي دفعت هذه الدول إلى الاعتراف بمنطق افتراض الأصالة في الدلائل الإلكترونية الرقمية على المستوى القانوني، وعندما يتم إزالة محتواه من نظام المعلومات، فإنه لا يمثل أصله **value.lt** يبقى في المكان الذي تم استخراجه واستدعائه.

---

[63]براهيمي جمال، المرع السابق، ص 160.

و نعتقد أنه إذا اشترط القانون الإثبات الإلكتروني للحصول على سلطة الإثبات ليتم مناقشته علنا في المحكمة، فإن دور القاضي في هذا يظل محدودا للغاية بسب بافتقاره الشديد لثقافة المعلومات، و مع توسع مجال الإثبات الإلكتروني، تطغى التطورات العلمية على نظام الإدانة القضائية، والقاضي في التقييم، الذي ينطوي على القول بأن القاضي لا يمكن أن يؤجل إلا إلى أخصائي مختص دون أي تقييم من جانبه. و تخلص إلى أن الحكومة أصبحت تؤمن بتناقص وتناقص دور موظفي العدالة الجنائية في نظام العدالة الجنائية.

هذه المشاكل تدفع إلى التحقيق في دور الطبيعة العلمية للأدلة الإلكترونية في تشكيل الإدانات الشخصية للقضاة الجنائيين[64].

[64] براهيمي جمال، المرجع نفسه، ص 161.

المحور الثالث: عقبات التحقيق الجنائي في الجرائم الإلكترونية

لعل من أهم العناصر المتعلقة بالجريمة هو مكان وقوع ذلك المشهد أو زاويته، وهو العنصر الأساسي للسيطرة على الجريمة و التحقيق فيها وملاحقة مرتكبها ،و هذا هو نفسه فيما يتعلق بالجريمة الإلكترونية، حتى لو كانت مختلفة عن المشهد المادي الإجرامي التقليدي، حيث أنذلك المشهد متاح وهو مسرح أخلاقي، لذا فإن الإنترنت الشخص المتجول على الإنترنت يعتبر كبصمة أخلاقية على المواقع التي يزورها، حيث أن عنوانه الإلكتروني الدائم مخصص له، ونوع الجهاز الذي يستخدمه وحيث يدخله يعتبر كبصمة أخلاقية على المواقع التي يزورها، المواقع التي يزورها، حيث يتم تحديد نوع الجهاز الذي يستخدمه.قررنا.

يمكن أحيانا تتبع هذه العناصر بطريقة بسيطة، بعضها متاحل لمستخدمين العاديين، والذي يمكن أن يكشف عن معلومات المستخدم، وأولئك الذين يرغبون في تتبعت حركات الجاني، وما يقوم به المحترفون، وحتى أن الكمبيوتر الشخصي للمجرم نفسه يحمل ملفات تعريف الارتباط للموقع الذي دخله. هناك.

ربما ليس الأمر بهذه البساطة، وربما من الممكن اكتشاف المجرمين البسيطين بهذه الطريقة، ولكن حتى المجرمين والهواة الخاصين يمحوون الآثارالمسجلة بعدة طرق. مسح ملفات تعريف الارتباط على جهازك و إخفاء العناوين الإلكترونية على جهازك بطرق مختلفة.

تحاول الدول والشركات المختلفة التي تقدم خدمات الإنترنت التغلب على هذه الاختراقات من خلال برامج خاصة، وأحيانا أكوا دأخرى، و إذا حاولت استخدامها لأغراض استقصائية، فإن تعاون مزود الخدمة ضروري لأن هذه الأكواد تنتمي إلى مزود الخدمة وتتعرف على هوية المتصل من خلال الخط. فمن الضروري.

تعتمد مراقبة الجريمة و إثباتها بشكل أساسي على جمعا لأدلة، ووسائل الإثبات التي يحددها المشرع حصريا، لانتهاك الحرية الفردية وحقوقها الأساسية، ولا يسمح للأدلة التي تم جمعها بالانحراف عن الأدلة التي اعترف بها المشرع القيمة القانونية، وهي الوسيلة الرئيسية للإثبات و التفتيش والاستيلاء على الأشياء المتعلقة بالجريمة، في حين أن وسائل الإثبات الأخرى، مثل الاستجواب والمواجهة والاستماع إلى الشهود، هي المرحلة التالية من إجراءات التحقيق وجمع الأدلة[65].

و تعترض سلطة جمع الاستدلالات والتحقيق صعوبات بالنسبة للدليل ذاته وكذا إجراءات التحري لذا سنتعرض لكل منهما من خلال المبحثين التاليين:

المبحث الأول: صعوبات تتعلق بالدليل ذاته

[65] عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية - دراسة مقارنة-، مذكرة ماجستير في القانون العام، جامعة الشرق الاوسط 2014، ص 74-75.

هنا كأوجه تشابه كبيرة بين التحقيق في جرائم الإنترنت والتحقيق في الجرائم الأخرى، ولكن بالإضافة إلى جمع الأدلة، هناك طرق تحقيق مماثلة بشكل عام، مثل الفحص والفحص والشهادة والخبرة.

ومعذلك، تتميز الجرائم المتعلقة بالإنترنت عن الجرائم الأخرى بعدد من الخصائص، والتي تتطلب بالطبع تطوير أساليب وإجراءات التحقيق الجنائي بطريقة مناسبة لهذه الخصوصية، حتى يتمكن المحققون من اكتشاف الجرائم والتعرف على الجناة بالسرعة اللازمة وaccuracy.To التحقيق في هذا النوع من الجرائم، بالإضافة إلى عرض عدد كبير من السجلات حول خلفية المنظمة وموظفيها، من الضروري الإشارة إلى عدد كبير من السجلات التي يجب عرضها، مثل أدلة الكمبيوتر، والملفات التي تسجل عمليات الكمبيوترإلخ.، وفي سبيل الوصول لتحصيل الدليل الالكتروني يعاني القائم بالتحقيق من العديد من الصعوبات والمعوقات نوردها على النحو التالي:

المطلب الأول: عدم ظهور الدليل المادي

يمكن للجاني عن طريق نبضات إلكترونية لا ترى بالعين المجردة العبث في بيانات الحاسب أو برامجه، في وقت وجيز جدا وهذه البيانات التي يتم التلاعب بها يمكن محوها أيضا في وقت وجيز جدا قبل أن تصل إلى المحققين. فالجريمة المعلوماتية عكس الجرائم العادية الأخرى تتم دون رؤية دليل الإدانة حتى عند وجود الدليل يمكن للجاني محو الدليل وفي حضور أجهزة العدالة غير المختصة بعد تنفيذه للجريمة، ولذلك فمعظم الجرائم المعلوماتية يتم اكتشافها بمحض المصادفة وليس بطريقة التبليغ عنها.

فقد دلت دراسة ميدانية قامت بها إدارة الصحة وخدمات الإنسان بالولايات المتحدة عام 1983 أن الحوادث المصادفة مثلا (الانتقام– الفضول –الشكوى)من المبلغ ضدهم أو النشاط غير المعتاد للمجرمين شكلت نسبة 49% من عوامل ساهمت في كشف الإحتيال، أما الرقابة الداخلية والخارجية فكان لها ذات الأثر بنسبة 26% ومن بين بعض أنواع الجرائم التي يختفي فيها الدليل:

– اختلاس المال مثلا عن طريق الجريمة المعلوماتية: قد يكون أساس النشاط الإجرامي هو التلاعب في نظام الحاسب الآلي ويتم ستر وإخفاء الدليل عن طريق العبث بالبيانات النهائية التي تخرج من الجهاز وذلك بمعالجته في نظام الحاسب ذاته.

– وقد ترتكب السرقة عن طريق التجسس على ملفات البيانات واختراقها كما هو الحال في إيطاليا حيث حاول الجاني سرقة المعلومات والبيانات عن طريق اختراق النبضات الإلكترونية عبر الألياف الضوئية المرسلة بين البنوك و أجهزة الصراف الآلي بهدف الحصول على المال.

ويقسم المجرمون بحسب خفاء الدليل إلى:

– المحتالون: لديه مقدرة عالية على إخفاء أدلة جرائم المعلومات، وتركز جرائمهم على تشغيل شبكات التحويلات والحسابات المصرفية.

يهدف الجناة هنا إلى إعاقة وصول سلطات التحقيق إلى الفضاء الأخلاقي الذي يحتوي على أدلة من خلال وضع أنظمة حماية تمنع التسلل غير القانوني للأنظمة والبرامج والملفات وصعوبة نسخها. يستخدم الجناة كلمات مرور محددة لهذا أو يضعون تعليمات لتدمير الأدلة عند محاولة الوصول غير المصرح به، مثل هذه الأوامر المتطورة جدا

ذات خطورة كبيرة يمكن أن تضيع فرصة الاتهام على النيابة العامة، والفرصة الوحيدة للنيابة العامة في حفظ وحماية الدليل تكمل في اكتشاف لمعادته وتحديدها وفكر رموزها قبل عمل أي شيء بالحاسب الآلي، وهو الأمر الذي يحتاج إلى خبرة وفن واختصاص[66].

– التجسس: يحاول هؤلاء جمع المعلومات لصالح بلدهم أو لصالح بعض الأشخاص والشركات التي تتنافس فيما بينها، فهم لديهم مقدرة فائقة على طمس الأدلة.

المطلب الثاني: فقدان الآثار التقليدية للجريمة

و كما ورد في جانب واحد من الفقه، فإن سبب عدم وجود آثار تقليدية هو أن هناك عدة عمليات يتم فيها إدخال البيانات مباشرة في الكمبيوتر دون الاعتماد على وجود مستند أو مستند يتم فيه إجراء النقل كما لو كان البرنامج قد تم إعداده وتخزينه على الكمبيوتر، ويمكن هنا ارتكاب بعض أنواع الجرائم، مثل الاختلاس والتزوير، ويتم إخراج النتائج على أهواء مستخدم الكمبيوتر، دون استخدام الورق، عن طريق إدخال البيانات غير ضرورية و معتمدة من قبل نظام الكمبيوتر،أوعن طريق تغيير البرامج المخزنة على الكمبيوتر. نظرا لأنها وثيقة أو وثيقة، فإن الجريمة تفقد تأثيرها أحد الأسباب التي تساهم في عدم القدرة على الحصول على آثار تقليدية هو حقيقة أن الجاني نفسه لديه القدرة على محو أو إتلاف أدلة الجريمة فيوق تقصير جدا، وحتى إذا تم القبض عليه، فقد تكون هذه الجريمة بسبب خطأ في نظام الكمبيوتر أو الشبكة.

---

[66]محمد حسن السراء، المرجع السابق، ص 41-42.

عند البحث عن آثار أو أدلة على جريمة المعلومات، سواء كانت موظفين أوتجار، من خلال مراقبة حركة التجارة و مراقبة المشتبه به مداخل وخارج المؤسسات المالية، و توجيه التحقيق إلى إدارة التاجر في نطاق المؤسسة التي وقعت فيها الجريمة، يجب على أفراد الأمن جمع معلومات سرية حول تحركات السوق وتداول وتغيير الأموال والممتلكات. فمن الصعوبات التي قد يتعرض لها المحقق في مجال جرائم الحاسوب والإنترنت سهولة محو الدليل من قبل المتهم، فباستخدام بعض الأدوات الجنائية الخاصة يستطيع المحقق استرجاع الأدلة غير أن ذلك لا يكون متاحا دوما[67]. يتم تنفيذ الجرائم المرتكبة على الكمبيوتر (تدمير البيانات) أو بواسطته (الشتائم والسرقة) بالإشارات والأوامر الأخلاقية التي يقدمها الجانب المنفذ للكمبيوتر، بحيث يمكن تنفيذ هذه الإجراءات، خاصة إذا كانت الجريمة ناتجة عن تصرفات الجاني، ممثلة بالضغط على زر واحد من على لوحة التحكم الخاصة بالكمبيوتر نفسه. مشكلة التخلص من الأمر بسيطة للغاية. مشكلة تؤدي إلى مشكلة أخرى أكثر تعقيد او خطورة– صعوبة تحديد الجاني واكتشافه، ما يجعل المصادفة المحضة الوسيلة الوحيدة لذلك[68].

المطلب الثالث: تعذر الحصول على الأدلة بسبب طريقة الحماية الفنية والقانونية وآثار ذلك إجرائيا

بالرغم من محاولة الجهات ذات الأنظمة المعلوماتية حماية أنظمتها عن طريق الترميز والتشفير فإن قراصنة الحاسب الآلي والعاملين في ذات المؤسسات يستطيعون اختراق هذه الأنظمة، ومن ثم يجعلون حمايتها عديمة الجدوى، وليست الأمور تقف

---

[67] طارق عبد الرحيم الردايدة، المرجع السابق، ص 173.

[68]محمد حسن السراء، المرجع السابق، ص 41-42.

عند هذا الحد بل إن هؤلاء يقومون بفرض تدابير أمنية لمنع التفتيش المتوقع بحثا عن أدلة إدانتهم وذلك باستخدام كلمات سر حول مواقعهم، تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة الإطلاع على أي دليل يخلفه نشاطهم الإجرامي.

كذلك استخلاص الدليل العلمي في الجريمة المعلوماتية هو من المسائل الفنية التي يقوم بها الخبير وهو يخضع لوزن وتقدير القاضي في ضوء الأدلة التي قدمت في الدعوى، وهناك من اعتبر الوسائل العلمية في أغلب حالاتها ليست دليلا مستقلا في ذاته وإنما هي قرائن يتم دراستها واستخلاص دلالتها وهذا القول يؤدي إلى إفلات المجرم المعلوماتي من العقاب، لذا على المشرع التحرر من القواعد التقليدية شرط عدم المساس بالحقوق الدستورية ومبدأ المشروعية.

وفي كثير من الأحيان تجد جهات التحقيق نفسها مجبرة على تفتيش نظم الحاسب الآلي برمته بحثا عن الدليل، وهو الأمر الذي يحتاج إلى فحص آلاف الصفحات خصوصا عندما لا تثبت تلك الصفحات شيئا، بالإضافة إلى الحالات التي يكون فيها الحاسب متصلا بشبكة الاتصالات العالمية فتزداد الصعوبة وترتفع والتكاليف، والأمر هنا يتطلب خبرة فنية وقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجود الدليل واقصر وأيسر السبل لضبطه[69].

المبحث الثاني: صعوبات تتعلق بالأشخاص

نظرا لطبيعة الجرائم المتعلقة بالحاسوب، يلزم معرفة واضحة بأنظمة الكمبيوتر وطرق التشغيل ووسائل إساءة الاستخدام من قبل المستخدمين، ولا تتحقق هذه المعرفة التقنية

[69]محمد حسن السراء، المرجع السابق، ص 41-42.

فقط من خلال تدريب المحققين والمشاركين في التحقيق في الجرائم الإلكترونية، ويدعو البعض إلى الحاجة إلى الشرطة المهنية والمحاكمات المهنية في هذا المجال.

المطلب الأول: طبيعة المجرم في الجرائم الإلكترونية

- معلومات مشابهة للجرائم التقليدية تتطلب الجرائم درجة عالية من الاحتراف، سواء عند ارتكابها أو عند العمل على اكتشافها من الشخص الذي يرتكبها. أي أن الشخص يجب أن يكون خبيرا في المدى الضروري والكافي لمشاكل الحوسبة و**Internet.So** يمكن كأن ترى أن معظم الأشخاص الذين ارتكبوا هذه الجرائم هم خبراء في مجال أجهزة الكمبيوتر، وعندما يرتكبون هذا النوع من الجرائم، تبحث الشرطة عن خبراء الكمبيوتر أولا.
- وبالتالي، يقوم المجرمون بتشفير الملفات الإلكترونية أو البيانات التي تحتوي على محتوى غير قانوني لمنع الأطراف الثالثة من رؤيتها أو اكتشافها، كما في حالة نقل البيانات المتعلقة بجرائم غسل الأموال على الإنترنت بعد التشفير.
- يحرص مرتكب الجريمة، بعد ارتكابه لجريمته، على محو آثاره التي تشير إلى حدوثها من خلال الخروج بتقنيات مصممة لهذا الغرض، مع مراعاة سهولة وسرعة إمكانية محو البيانات الإلكترونية وتغييرها، وهو ما يمكن القيام به في وقت قياسي قصير جدا،يقاس باللحظات والثواني.
- على هذا الأساس، غالبا ما يكون ضحايا الجرائم الإلكترونية هم السبب في صعوبة اكتشاف هذه الجرائم لعدة أسباب.:
  - – نقص الخبرة الفنية والتقنية;
  - عدم اتخاذ الحيطة والحذر.

- الإمتناع عن الإخبار.
- عدم إدراك خطورة الجرائم المعلوماتية[70].

المطلب الثاني: صعوبات تتعلق بعمل القائمين بالتحقيق في الجرائم الإلكترونية

جمع الأدلة عن طريق المعاينة والتفتيش يطرح العديد من الصعوبات ولذا سنتعرض لهما بشيء من التفصيل:

الفرع الأول: معوقات المعاينة في الجرائم المعلوماتية

لا يزيد من صعوبة القول بأنه يمكن الاستيلاء على الجرائم والأدلة، مثل سرقة الدعم المادي لبرنامج ما، أو نسخه بشكل غير قانوني، أوسرقة الوسائل المادية لتدميره بطريقة تقليدية، ولكن من الصعب إذا تعرضت للتلف باستخدام وسائل تقنية مثل الفيروسات وأحصنة طروادة.

تنشأ الصعوبة، بالطبع، أيضا من نقص خبرة الشرطة كدافع ضرائب بسبب نقص التدريب، وعملية الاستيلاء غير ممكنة في أنظمة المعلومات الكبيرة أو الشبكات الكبيرة.:

1–قد تتسبب التعديلات بمستخدمي النظام وقد تؤدي إلى فصل نظام المعلومات بالكامل على دائرته لفترة قصيرة من التحول أو الوقت.

---

[70] جاسم خريبط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، الجلد 2016، العدد 12، 2016، العراق، ص 14-15.

2–يعني أن مستخدم نظام المعلومات غير مستعد للتعاون بشكل كامل وفعال مع سلطات التحقيق، أي الاستيلاء على حقوق الآخرين.

أما فيما يخص بيانات الحاسب:

وتعترض المحقق صعوبات جمة التي تحول دون ضبطه للبيانات التي تعد دليلا على ارتكاب جريمة ما في بيئة المعالجة الآلية للبيانات ومنها:

. عدم وجود أدلة بصرية يمكن فهمها من خلال القراءة، مع الأخذ في الاعتبار أن بيانات الكمبيوتر التيار تكبت عليها الجريمة أو بيانات الكمبيوتر التيار تكبت عليها غير مرئية، وتمثل هذه المشكلة عقبة أما م جهاز الشرطة تمنعهم من القبض على هذه الجرائم و التعرف على أدلتها ومرتكبيها.

– تتميز الجرائم التي تم استبدالها ببيانات الكمبيوتر بعد متر كأي أثر يمكن استنتاجه منها، و هو ما يتجلى بوضوح في جرائم الاختلاس والتزوير التي تستخدم فيها أجهزة الكمبيوتر.

. حتى البيانات التي يمكن التوصل إليها فإنه يمكن للجاني محوها أو تدميرها في فترة زمنية قصيرة جدا لا تتعدى ثوان معدودة كما يمكن للجاني تبرير وجود هذه البيانات في حال التوصل إليها بوجود خطأ في نظام الحاسب وبالتالي يمكنه التنصل من المسؤولية[71].

[71]- حسين طاهري، المرجع السابق،ص417.

. الكم الهائل للبيانات الواجب فحصها من فبل المحقق ناهيك عن تطلب جانب كبير من الخبرة الفنية للتحديد البيانات المقبولة كأدلة أمام القضاء من عدمه الأمر الذي يعوق للوصول إليها في الكثير من الأحيان لا حزمة الأمنية المفروضة من قبل مستخدم النظام حول البيانات التي يحتويها هذا النظام مما يزيد من صعوبة الأمر على المحقق الجنائي عدم معرفته لكلمات السر وشيفرات المرور أو شفرات ترميز البيانات الأمر الذي يقضي تعاون مستخدم النظام معه أو الاستعانة بالغير ذوي الخبرة في هذا الصدد.

. تجنب المجنى عليهم بالإبلاغ على هذه الجرائم وخاصة في قطاع الأعمال تجنبا للأضرار على العلانية وقد تترتب عليها هؤلاء وعلى سمعتهم.

. صعوبة ضبط مراسلات البريد الالكتروني.

وفي صدد الكشف عن الجريمة والأدلة والمحافظة على الآثار المادية التي خلفتها لكن مسرح الجريمة المعلوماتية يضيق مجاله و ذلك لسببين:

الأول: أن الجريمة المعلوماتية قلما تخلف آثارا مادية.

الثاني: يتفاعل الكثيرون مع مسرح الجريمة في الفترة منوقت الجريمة إلى الاكتشاف. هذه هي فترة طويلة نسبيا من الزمن، وإعطاء الجاني الفرصة لتغيير التأثير المادي، و إعطاء شك في أهمية الأدلة التي تم الحصول عليها من التفتيش، وجريمة المعلوماتي مكن أن يكون جريمة مستمرة ، كما هو الحال في حالة الجريمة الاقتصادية و السرقة و الاحتيال، والمشهد هو مماثل لجرائم أخرى مثل التزوير، والضرر البرنامج، قصف المباني، في النوع 1 من الجريمة، ويهدف التفتيش إلى مداهمة والاستيلاء على

الأدلة الطبيعية.في الحالة 2 ،هو بعد الجريمة ويعتمد على اعتراف المتهم عندما يتم القبض عليه موال قرائن في كل شيء قبل الانتقال إلى مسرح الجريمة، ينبغي النظر في الشروط التالية:

* الوصول إلى مسرح الجريمة من حيث عدد الأجهزة التي يتم تفتيشها أو شبكاتها أو خزائنها وملفاتها أو خرائط توضح الموقع الذي يتم تفتيشه وتفاصيل المباني و الأرضيات المراد إبلاغها.

* يجب النظر في تحديد الأجهزة المحتملة المتورطة في الجرائم الإلكترونية سواء من حيث المضبوطات أو التأمين ، حيث يتم تحديد كيفية التعامل معها تقنيا قبل التفتيش.

*القيام بتأمين الأجهزة والمعدات المستخدمة في عملية الفحص، سواء كان جهازا أو برنامجا صلبا أولينا.[72].

*إعداد فريق متخصص يتولى المعاينة وتحديد اختصاصات المطلوبة من كل عضو على حدة.

*لضمان التنفيذ الكامل، قم بإعداد خطة معاينة موضحة في الرسم مع مراجعة كاملة.

* ضمان عدم انقطاع التيار الكهربائي.

[72]محمد حسن السراء، المرجع السابق، ص 41-42.

* يتم توصيلها بالجهاز قيد الفحص و يمكن أن تساعدها تقنيات معينة لتدمير أدلة جريمة المعلومات وتعطيل جهاز الهاتف والتحكم في الهاتف.

* ضبط محتويات القمامة، بما في ذلك ضبط مستندات إدخال الكمبيوتر وإخراج الورق، والتي قد تكون مرتبطة بالجريمة، وكذلك رفع الورق الممزق و الشريط والأقراص المغناطيسية وبصمات الأصابع.

الفرع الثاني: نقص المعرفة الفنية لدى سلطات التحقيق

من الصعوبات التي تواجه عملية استخراج الأدلة في الجرائم الإلكترونية حاجة الأجهزة القضائية و الأمنية بشكل عام، وكذلك النيابة العامة وسلطات التحقيق الجنائي، إلى ثقافة الكمبيوتر وكيفية التعامل معها، بالنظر إلى أن تجربة الاعتماد على أجهزة الكمبيوتر و تقنياتها و انتشارها في هذه البلدان قد تخلفت عن أوروبا وأمريكا وخاصة في الدول العربية. إنه نقص خبرة وكالات العدالة الجنائية الممثلة.[73].

ومن البديهي ونحن بصدد الحديث عن جرائم تقع في بيئة حاسب الآلي أن تكون تلك الجرائم تقوم بشكل كبير على تقنية المعلومات ووسائل التقنية، الأمر الذي يظهر يبرز مدى تطور وسائل ارتكاب الجريمة وفي نوع الأدلة وما يتعلق بها، وفي طريقه كشفها وضبطها، هناك صعوبات أخرى في عملية الحصول على الأدلة الرقمية من جداول الحالة التشغيلية للبروتوكول والاتصالات، ولكن هذه الصعوبة ترجع إلى حقيقة أن هذه الجداول متاحة لفترة قصيرة من الزمن، ويتم حذف هذه الجداول تلقائيا بمجرد انقطاعا

[73] جاسم خريبط خلف، المرجع السابق، ص 21.

لتيار الكهربائي عن تلك الأجهزة،ولا يمكن التغلب على هذه الصعوبة عن طريق الاستيلاء الجنائي على الأجهزة حتى الفحص. يوصى باستخدام طريقة القص واللصق في ملف جديد لإغلاق الجهاز واستخدامه قبل إغلاق الجهاز.

في حين أن قانون القص و اللصق هو طريقة ناجحة لجمع الأدلة ،فإن القضايا القانونية الناشئة عن شرعية هذه الطريقة تتعلق بسلامة و موثوقية جمع المعلومات أمام وكالات العدالة الجنائية[74].

الخاتمة:

أدى ظهور شبكة الانترنت بنقلة نوعية هائلة وقد كان الفضل لظهور هذه الشبكة في تسهيل ونقل المعلومات بين الأشخاص على الرغم من ذلك إلا أن سوء استخدام الانترنت أدت بظهور نوع جديد من الجرائم تسمى بالجرائم الالكترونية أو المعلوماتية، بسبب لجوء مستخدمي الانترنت تحت ستار المجهولين أو باسم مستعار أو إنتحالإسم الغير مما دفع الى ظهور علم جديد يطلق عليه التحقيق في الجرائم الالكترونية، موضحا بذلك أهم القواعد و الإجراءات التي نحوها يمارسها المحقق في مجال الكشف عن الجريمة و الحصول على الدليل الالكتروني للحد منها، ومن خلال دراستنا لهذه المطبوعة توصلنا الى مجموعة من النتائج و التوصيات:

- **النتائج:**

[74] محمد حسن السراء، المرجع السابق، ص 41-42.

- ✓ كشف الدراسة عن وجود قصور معرفي وتطبيقي واضح بهذا النوع من الجرائم لدى الكثير من المحققين سواء كانوا شرطة أو قضاة مما يصعب عليها التحقيق لكشف الحقيقة في سرعة وسرية.
- ✓ صعوبة التحقيق الجنائي في الجرائم الالكترونية وعبر شبكاتها المعلوماتية، لإتساع نطاقها خارج دود الدولة في ظل ظهور العالم الافتراضي وتطور تكنولوجيا الاتصالات والمعلومات والعلاقات الافتراضية.
- ✓ وجب على المشرع مسايرة حالات استخدام التكنولوجيا في مجال استخدام الأجهزة الحديثة للإثبات الجنائي، ووضع الضوابط القانونية التي تمنع إساءة استخدام.
- ✓ إن الوسائل التقنية المستخدمة لتدمير مكونات الكمبيوتر هي حاليا الكثير من التعقيد، ومن المهم التنبؤ بالوسائل التي يمكن أن تتطور بها التكنولوجيا في هذا الصدد.
- ✓ بالإضافة إلى العقبات التشريعية التي تحول دون إثبات الجريمة السيبرانية، هناك العديد من العقبات، بما في ذلك تلك المتعلقة بالجريمة نفسها، أو الأشخاص المتأثرين بالجريمة، أو الأشخاص الذين يحققون في هذه الجرائم، وهذا يتطلب سلسلة من الإجراءات الإصلاحية.
- ✓ للجريمة السيبرانية طبيعة خاصة، حيث تتميز بالقدرة على التحرك في مجال فضائي واسع، لا يمكن وقفها بحدود الدولة وسيادتها الإقليمية، حيث يمكن أن تحدث جريمة تكنولوجيا المعلومات في مكان واحد وتنتج تأثيرها في مكان واحد أو في أي مكان آخر خارج البلاد.

. التوصيات:

. الاهتمام بتلقى البلاغات من السلطات المختصة وتدوينها في محاضر، وسرعة الانتقال الى موقع الجريمة وانتداب الخبراء واستخدام أساليب التكنولوجيا الحديثة في التعامل مع الآثار المادية، وتطبيق سياسة الحوافز الايجابية والسلبية للقضاء على التباطؤ في تلقى البلاغات أو التهوين من شأنها، وذلك لمحاولة البعض الظهور بمظهر المسيطر على الأمن وذلك خلاف الحقيقة.

. عقد دورات تدريبة متخصصة في مجالات استخدام التكنولوجيا الحديثة بحضور ضباط الشرطة القضائية ونواب عامون، وذلك للتدريب على كيفية استخدام الأجهزة الحديثة في مجال الإثبات الجنائي.

. محاربة الجريمة المعلوماتية بكل صورها وأشكاله وملاحقة مرتكبيه مهما كانت مراكزهم وتشديد العقاب الردع العام والخاص.

. يجب إجراء الدراسات اللازمة لوضع الخطط على مستوى الدولة لتأمين حياة الشهود، وذلك على غرار ما هو متبع في بعض الدول المتقدمة كالولايات المتحدة الأمريكية .

قائمة المصادر والمراجع:

أولا: المصادر

1. الأمر رقم66 – 155 المؤرخ في 18 صفر عام 1386 الموافق 8 بونيو سنة 1966، التضمن فانون الإجراءات الجزائية الجزائري، المعدل والمتمم.

2. الفانون رقم09–04 المؤرخ في 14 شعبان عام 1430 المرافق لـ 5 غشت سنة 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتعلق بتكنولوجيا الإعلام والاتصال ومكافحتها، الصادر بالجريدة الرسمية الجزائرية، بالعدد رقم 47.

ثانيا: المراجع

3. إبراهيم رمضان إبراهيم عطايا، الجريمة الالكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، العدد 30، الجزء الثاني،2015.

4. إيهاب محمد التاج، التحقيق وجمع الأدلة في الجرائم المعلوماتية، مجلة العدل، العدد 26، السنة الحادية عشرة.

5. براهيمي جمال،التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه في القانون، جامعة تيزي وزو– الجزائر، نوقشت بتاريخ 2018/06/27.

6. بن بادة عبد الحليم، المراقبة الالكترونية كإجراء لاستخلاص الدليل الإلكتروني "بين الحق في الخصوصية ومشروعية الدليل الإلكتروني، المجلة الأكاديمية للبحث القانوني، المجلد 10، العدد 03–2019.

7. ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، مذكرة ماجستير تخصص السياسة الجنائية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض 2012.

8. جاسم خريبط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، الجلد 2016، العدد 12.

9. حاحة عبد العالي وقلات سمية، المكافحة الإجرائية للجرائم الالكترونية –دراسة حالة الجزائر –، مجلة المفكر، المجلد 13/ العدد 2 (جانفي).

10. سحتوت نادية، التنظيم القانوني للجريمة المعلوماتية (أدلة إثبات الجريمة المعلوماتية)، مجلة دراسات وأبحاث، المجلد 1، العدد 1، 2009.

11. سعيد سالم المزروعي وعزمان عبد الرحمان، إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقا للتشريع الإماراتي، مجلة العلوم الإقتصادية والإدارية والقانونية، المجلة العربية للعلوم ونشر الأبحاث، العدد 13، المجلد الثاني، أكتوبر 2018.

12. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة باتنة، كلية الحقوق والعلوم السياسية، الجزائر، 2012/ 2013.

13. طارق عبد الرحيم الردايدة، التفتيش الالكتروني في الجرائم الرقمية – دراسة وصفية مقارنة –، مذكرة ماجستير ضمن تخصص أمن نظم المعلومات والجرائم الرقمية، جامعة الأميرة سمية للتكنولوجيا، الأردن، 2017، ص 54.

14. طارق عبد الرحيم الردايدة، التفتيش الإلكتروني في الجرائم الرقمية – دراسة وصفية مقارنة –، مذكرة ماجستير ضمن تخصص أمن نظم المعلومات والجرائم الرقمية، جامعة الأميرة سمية للتكنولوجيا، الأردن، 2017.

15. طيبة جواد حمد المختار، صعوبات الملاحقة القضائية في الجرائم الحاسوبية، مجلات جامعة بابل، المجلد 14، العدد الأول، 2007.

16. عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية مجلة الفكر الشرطي، المجلد 22، العدد 86، 2013.

17. عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة– ، مذكرة ماجستير في القانون العام، جامعة الشرق الاوسط 2014.

18. عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة دكتوراه تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، 2018/2017.

19. عيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي آفلو – الأغواط، العدد 06، مارس 2021.

20. فلاح عبد القادر وآيت عبد المالك نادية، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019.

21. محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الالكترونية، مجلة الفكر الشرطي، المجلد 21، العدد 81.

22. محمد رضوان هلال وكاظم محمد عطيات، كيفية التعامل التقني والآمن مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص.

23. محمد قاسم أسعد الردفاني، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، المجلة العربية للدراسات الأمنية والتدريب المجلد 31، العدد (21) 157–192، 2014، الرياض.

24. مركز هردو لدعم التعبير الرقمي، الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، مصر، 2014.

25. مليكة أبوديار، الإثبات الجنائي في الجرائم الإلكترونية، المجلة الإلكترونية للأبحاث القانونية 2018، العدد 02.

26. يقاش فراس، أنظمة الإثبات الجنائي وخصائصها، مجلة الحضارة الإسلامية، المجلد رقم 10، العدد 13، الصفحات 381–396.

المواقع الإلكترونية:

1. أيمن محمد عبد اللطيف، اشكالية إثبات الجرائم الإلكترونية، وعقوبة اختراق المواقع الإلكترونية وما هي آليات إثبات الجرائم المعلوماتية طبقا للقانون، الجرائم الالكترونية في مصر ودستورية مبدأ الشرعية الجنائية، الجزء الثاني، ص 13–14، منشور على الانترنت على الموقع الآتي:
https://www.researchgate.net/publication/341281631

2. محمد أبو العلاء عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، مقال منشور على الموقع التالي: https://www.bibliotdroit.com/2021/12/blog-post_77.html تمت الزيارة بتاريخ 12–08–2022.

3. إسكندر إسلام،ماهية مرحلة جمع الاستدلالات، مقال منشور على الموقع التالي:http://lawpractice-iskandar.blogspot.com/2011/06/blog-post_7371.html تمت الزيارة بتاريخ 15-08-2022.

فهرس المحتويات:

مقدمة.....2

المحور الأول: إجراءات التحقيق في الجرائم الإلكترونية.....5

المبحث الأول: آليات التحقيق في الجرائم المعلوماتية.....5
المبحث الثاني: ضوابط التحقيق والتفتيش في الجرائم المعلوماتية 12
المطلب الأول: جمع الإستدلالات في جرائم تقنية المعلومات 13
المطلب الثاني: إجراءات التحقيق الابتدائي في جرائم تقنية المعلومات..... 35
المحور الثاني: القيمة الثبوتية للدليل الإلكتروني أمام القضاء الجزائي 48
المبحث الأول: الأحكام الاجرائية لاستخلاص الدليل الرقمي.....49
المطلب الأول: المراقبة الإلكترونية..... 50
المطلب الثاني: التسرب واعتراض المرسلات 53
المبحث الثاني: حجية الدليل الرقمي في الإثبات الجنائي 56
المطلب الأول: مفهوم الدليل الرقمي..... 58
المطلب الثاني: أساليب تقييم الدليل الرقمي 69
المطلب الثالث: مدى حجية الدليل الإلكتروني في الإثبات الجزائي أمام القضاء 72
المحور الثالث: عقبات التحقيق الجنائي في الجرائم الإلكترونية 83
المبحث الأول: صعوبات تتعلق بالدليل ذاته.....84
المطلب الأول: عدم ظهور الدليل المادي 85
المطلب الثاني: فقدان الآثار التقليدية للجريمة..... 87
المطلب الثالث: تعذر الحصول على الأدلة بسبب طريقة الحماية الفنية والقانونية وآثار ذلك إجرائيا88
المبحث الثاني: صعوبات تتعلق بالأشخاص 89
المطلب الأول: طبيعة المجرم في الجرائم الإلكترونية 90
المطلب الثاني: صعوبات تتعلق بعمل القائمين بالتحقيق في الجرائم الإلكترونية 91
الخاتمة: 96
فهرس المحتويات: 102