الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة العربي التبسي - تبسة -
كلية الحقوق والعلوم السياسية
- قسم الحقوق -

مطبوعة مقدمة لطلبة السنة الأولى ماستر تخصص جريمة وأمن عمومي

- السداسي الأول -

محاضرات في مقياس
التحقيق في الجريمة الإلكترونية

إعداد الدكتور/ عزالدين عثماني

أستاذ محاضر قسم - أ -

2022/2021

مقدمة

في ظل الإنتشار السريع للتكنولوجيا خاصة خلال العقد الأخير، أصبحت معظم التعاملات الإجتماعية والتجارية والسياسية تتم عن طريق الشبكة المعلوماتية (الإنترنت)، وأصبح الإنسان أكثر عُرضة للوقوع ضحية لتلك الجرائم الإلكترونية أو المعلوماتية.

وتمثل الجريمة الإلكترونية اعتداء معلوماتيا يقوم فيه الجاني باستخدام وسائل إتصال حديثة بهدف ابتزاز الضحية أو تشويه سمعتها وما إلى ذلك من صور الإعتداء، سواء بغرض تحقيق مكاسب مادية أو أهداف سياسية، ويتحمل المستخدمون من المواطنين، والشركات والحكومات كل تلك المخاطر، وذلك بالنظر إلى أن الإنترنت أصبحت تستخدم في شتى التعاملات وبات من الصعب على مستخدميها تجنب التعامل بها.

وللجرائم الإلكترونية عدة أشكال وأنواع تستخدم من قبل قراصنة المعلومات أو أشخاص آخرين أهمها:

انتحال الشخصية: يعتبر انتحال شخصية غير الشخصية الحقيقية، جريمة يعاقب عليها القانون في أغلب دول العالم، لذلك فإن الدخول إلى عالم وسائل التواصل الاجتماعي باسم وحساب شخص آخر يمكن أن يعرض صاحبه للمسائلة القانونية، خاصة في حال كان انتحال الشخصية تم بهدف التشهير بها أو تسريب معلومات شخصية عنها.

التهديد: يعتبر التهديد من بين المخالفات التي يحاسب عليها القانون، حيث يشكل مساسًا بالحق الأساسي للإنسان في الحياة وسلامة الجسد.

ويُستخدم التهديد في الجرائم الالكترونية بهدف ترهيب الضحية وإخضاعها لطلبات المبتز، وذلك يأتي بعد الحصول على معلومات ومحتوى للشخص عن طريق عمليات اختراق إلكترونية، ومن الممكن أن تقدم لائحة اتهام رسمية ضد المهددين وملاحقة الحسابات الإلكترونية للوصول إلى المجرم حتى وإن كان الحساب مزيفًا وليس حساب المبتز الحقيقي ومن ثم معاقبته.

تشويه السمعة: هي أحد أوضح الجرائم الالكترونية وأكثرها انتشارًا، حيث يكون المجرم المسؤول عنها في غالبية الأمر على معرفة شخصية بالضحية وهدفه الرئيس هو إيذاء الضحية وإلحاق الأضرار بها عن طريق التشهير بها وتشويه سمعتها، ويتم تحقيق ذلك بعدة طرق ووسائل أهمها أن يصنع المجرم حسابا وهميا على وسيلة تواصل معينة مثل فيسبوك، باسم الشخص الذي يود إلحاق الأذى به، ويقوم بنشر صور أو محتويات خاصة بالضحية ونشرها مما قد يؤذي الضحية، ويستغل ذلك فيما بعد بتهديد الضحية بتقديم المال له مقابل التوقف عن نشر هذه الأمور.

التحريض على القيام بأعمال غير مشروعة: هذا النوع من الجرائم يأتي بعد أن يصل المجرم إلى معلومات الضحية والعديد من الأمور التي تساعده في التهديد، ويتواصل بعد ذلك المجرم مع الضحية ويعرض عليها أن تقدم له خدمات غير مشروعة أو غير مستحقة، مقابل التخلص من المعلومات المقرصنة التي يملكها.

وهذه أهم أنواع الجرائم الإلكترونية التي من الممكن أن يتعرض لها الأفراد، ولكن كما ذكرنا سابقا أن الجرائم الالكترونية قد تطال المؤسسات والمجموعات أيضا لاختلاف الأهداف من ابتزازهم عن الأهداف المتعلقة بابتزاز الأفراد.

وابتزاز المؤسسات من الممكن أن يحدث عن طريق قرصنة المعلومات المهمة الخاصة للمؤسسة بهدف نشرها ونزع سمعة المؤسسة في الشارع عن طريق إظهار معلوماتها السرية وإفقاد مصداقيتها أمام جمهورها.

ومن الممكن أن يصل المبتزين إلى مراكز التحكم الأصلية في الشركات وتعطيل كافة الأنظمة مما يعرض الشركات إلى خسارة كبيرة.

وهنالك أنواع عديدة وجهات مستهدفة كثيرة للابتزاز أو للجرائم الالكترونية مثل؛ أجهزة الأمن للدول ومراكز جمع المعلومات الاستخبارية، حيث تتعرض هذه المراكز لهجمات اختراق وتسريب معلومات مستمرة بسبب خصوصية وأهمية مكانتها في أماكن اتخاذ القرار والتحكم في حياة المواطنين حسب تصنيفهم.

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 الجرائم المعلوماتية بعناصرها ووسائل ارتكابها قد تدفع المشرع الجزائي إلى أن يعيد النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون.

ذلك أن الدليل الذي قد يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعتها التقنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية لاستخلاص الدليل قادرة على القيام به. مما يستوجب تدخل المشرع لتكريس قواعد إجرائية يمكن للجهات المكلفة بالبحث والتحري عن الجريمة المعلوماتية الاعتماد عليها في الوصول إلى الدليل المناسب لإثبات الجريمة المعلوماتية.

ولا شك أن هذا الدليل سيتم استخلاصه من البيئة الرقمية، التي تعتبر مسرح الجريمة المعلوماتية مما يجعله يتميز بخصائصها (خصائص البيئة الرقمية)، وهو الأمر الذي يقودنا إلى الحديث عن مسألة قبول هذا الدليل أمام القضاء و مدى كشفه للحقيقة نظرا لما يمكن أن يخضع له من التزييف والتحريف والأخطاء، بل وحتى مع ضمان مصداقية هذا الدليل وكذا مشروعيته فإن الأمر لا يتوقف عند هذا الحد، بل يتجاوزه إلى مسألة أكبر أهمية تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية للسلطة التقديرية للقاضي إعمالا لمبدأ الإقتناع الشخصي للقاضي الجزائي الذي يشكل جوهر أي حكم.

المبحث الأول: آليات التحقيق في الجرائم المعلوماتية

إن التحقيق القضائي من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء للحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة.

والثابت أن الدعوى الجزائية تمر بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بمرحلتين أيضا، مرحلة التحقيق الأولي ومرحلة التحقيق الإبتدائي.

فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق، وإننا نؤيد الرأي أو الاتجاه الذي يقسم التحقيق إلى:

- تحقيق أولي والذي يناط به رجال الضبطية القضائية.
- تحقيق قضائي ويناط به رجال القضاء، وهذا الأخير يقسم إلى تحقيق ابتدائي من اختصاص قاضي التحقيق والتحقيق النهائي ويكون في مرحلة المحاكمة من طرف قضاة الحكم.

وفي كل جميع أنواع التحقيق هذه، يكون للقائمين عليه من ضبطية قضائية وقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية، وهو الأمر الذي يفهم صراحة من خلال استقراء نص المادتين

12 و38 من قانون الإجراءات الجزائية الواردتين في الباب الأول من هذا القانون تحت عنوان "في البحث والتحري عن الجرائم" حيث تنص المادة 12 الفقرة الثالثة أنه "يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون"[1]

العقوبات"... وتنص في نفس الوقت المادة 38 من نفس القانون أنه "يناط بقاضي التحقيق إجراءات البحث والتحري ..."

وعليه فإنه يمكن القول أن إجراءات البحث والتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أم ابتدائيا، وبهذا المفهوم فإن إجراءات البحث والتحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولي، بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا ابتدائيا.

وإذا كان التحقيق عموما يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا تطويرا لأساليبه وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في هذه البيئة.

المطلب الأول: مميزات التحقيق في الجرائم الإلكترونية

لما كانت الجرائم الإلكترونية تتسم بحداثة أسالب ارتكابها وسرعة تنفيذها وسهولة إخفاء معالمها ودقة وسرعة محو آثارها، فقد ظهرت نتيجة عنها جملة من الصعوبات والإشكالات العملية التي تعرقل وتقف كحجر عائق أمام أجهزة العدالة في مواجهتهم لهذه الطائفة من الجرائم ولاسيما أجهزة البحث والتحري والتي تعمل من أجل استيفاء الدليل الإلكتروني، إذ أصبحت هذه الأخيرة تواجه مشاكل وصعوبات إجرائية أثناء مباشرة مهامها للكشف عن هذا النوع من الجرائم وملاحقة مرتكبيها وتقديمهم للعدالة.

أمام هذا الوضع ثار النقاش حول ما إذا كان بالإمكان الاكتفاء بالقواعد الإجرائية العادية للبحث عن الجريمة الإلكترونية، أم أن الأمر يتطلب وضع قواعد إجرائية خاصة بها تنسجم مع خصوصيتها وطبيعتها، حيث أشار بعض

[1] 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، الصفحة 102.

المهتمين إلى أن القواعد الإجرائية المتعلقة بالبحث والتحري عن الجرائم في شكلها التقليدي هي قواعد لا تخص جريمة معينة دون أخرى[2].

بل هي قواعد عامة يمكنها أن تنطبق على كافة الأفعال المخالفة للقانون الجنائي بما فيها الجريمة الإلكترونية والتي تبقى وتظل وإن اختلفت عن غيرها من الجرائم سواء من حيث طبيعتها أو خصائصها خاضعة من حيث المبدأ للقواعد العامة التي تسري على جميع الجرائم، كما أن البحث في الجرائم الإلكترونية يأخذ بجميع عناصر البحث ويمر بذات المراحل الفنية والشكلية المتبعة في الجرائم التقليدية لاحتمال ارتباطها بمختلف أنواع الجرائم الأخرى.

وبالتالي بوسع أجهزة العدالة أن تستعمل القواعد الإجرائية القائمة في تعاملها مع الجرائم الإلكترونية، فهذه القواعد القائمة لم تغيرها ولم تؤثر فيها الجرائم الإلكترونية، فقط ينبغي تطوير بعض المفاهيم وتناولها بطريقة قانونية.

كما سار البعض الآخر في نفس السياق واعتبر بأن القوانين الإجرائية الحالية تتضمن مجموعة من المقتضيات العامة التي يمكن أن تسري أو تنسحب على الجريمة الإلكترونية، فقط تحتاج إلى بعض التعديلات لتضفي على إجراءات البحث والتحري في هذا النوع من الجرائم نوعا من الخصوصية تلاءم طبيعة هذه الجريمة التي تتميز بخصوصية وذاتية متميزة عن باقي الجرائم.

إلا أن هذا الطرح أو الفرض— القواعد الإجرائية العادية قواعد عامة يمكنها أن تنطبق على الجريمة الإلكترونية – لا يمكن الأخذ بها على إطلاقها وذلك راجع بالتأكيد لطبيعة وخصوصية الجريمة الإلكترونية وصعوبة ضبطها والتي لا تنسجم مع البيئة التقليدية التي ترتكب فيها مختلف الجرائم الأخرى كما سنتولى تبيان ذلك[3].

فالقوانين الإجرائية بما تتضمنه من قواعد إجرائية تعتبر بمثابة الوثيقة الأساسية لحماية حقوق الأفراد و التي تؤكد على احترام المبادئ الأساسية المعترف بها دوليا وكذا تحقيق التوازن بين مصلحة الدولة في الوصول إلى الحقيقة و الحريات الفردية للمواطنين، فالقواعد الإجرائية تحتك باستمرار مع حقوق الفرد وحريته، وعليه فإن شرعية الإجراءات تقتضي أن تكون إجراءات البحث عن الأدلة و جمعها موافقة ومحددة وفق القانون و لا تخرج عن روح نصوصه، و بالتالي فإن التوسع في مباشرة الإجراءات أو في تفسير هذه الإجراءات المقررة فإنه يهدد حقوق وحريات الأفراد، لذلك فإن النصوص

---

[2] أيمن محمد عبد اللطيف، اشكالية اثبات 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

[3] أيمن محمد عبد اللطيف، المرجع نفسه.

الخاصة ببعض الإجراءات بمفهومها التقليدي لا ينبغي إعمالها بشأن الجريمة الإلكترونية مباشرة، باعتبار أن هذه النصوص تمثل قيدا على الحرية الفردية، ومن ثم يصبح القياس على الأشياء المادية محظورا لمنافاته الشرعية الإجرائية.

لذلك فإنه ينبغي الموازنة بين حقوق الفرد المتهم من جهة وحقوق المجتمع من جهة أخرى، وبين هذه الحقوق وضرورة احترام القواعد الشرعية والقانونية أثناء البحث عن الدليل في البحث الجنائي عموما وفي مجال الجريمة الإلكترونية على وجه الخصوص.

لذلك يمكن القول بأن القواعد الإجرائية العادية أبانت عن محدوديتها وقصورها لأن مباشرتها في بيئة لا تنسجم معها قد يشكل مساسا بالشرعية الإجرائية بصفة عامة وبحقوق الأفراد بصفة خاصة، لذلك بات من الضروري إفراد قواعد خاصة بالبحث عن هذا النوع من الجرائم تكفل في الوقت ذاته توازنا بين متطلبات الفعالية لأنشطة الأجهزة الجنائية الإجرائية في المجال المعلوماتي ومقتضيات حماية حريات الأفراد وحقهم في الخصوصية[4].

المطلب الثاني: الأجهزة المكلفة بالبحث والتحري عن الجريمة المعلوماتية

تتقدم الجرائم الالكترونية بسرعة هائلة توازي سرعة تقدم التقنية ذاتها، وحتى الآن فإن الحركة التشريعية أو الثقافة الأمنية والقانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التقدم أو التطور ينعكس سلبا على عملية جمع الاستدلالات والتحقيقات في الدعوى الجنائية عن الجريمة المعلوماتية، ومن هنا يأتي تقويم تأهيل سلطات الأمن وجهات التحقيق والإدعاء والحكم في شأن هذه الجرائم.

فالتعامل مع مثل هذه المعلومات يحتاج إلى جهود فريق من رجال الشرطة والعلوم الجنائية، والنيابة، والبرمجة وتحليل النظم، إذ ليس في مقدور واحد منهم أن يكون ملما بجميع المهارات اللازمة لكشف خزائن الجرائم ذات العلاقة بالتقنيات، فضابط الشرطة قد يكون ملما بالإجراءات الفنية والقانونية المعتمدة لربط الجرائم والتحقيق فيها وحماية حقوق الانسان، ولكن قد لا يكون ملما بعلوم الحاسب الآلي والحوسبة والاتصالات، ومن ثم لن يدرك تماما ماهية الأدلة الجنائية التي يسعى لها، كما أن محللو النظم والمبرمجين المهندسون الذين يفهمون كل شيء عن تقنية المعلومات وشبكات

[4] 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

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.[5]

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** بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة ووهران 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 لأجل تعميم هذا النشاط على كافة ربوع الوطن[6].

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» والتي تضم ثلاث أقسام هي:

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

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[7].

الفرع الثاني: مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية

---

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

[6] 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.

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

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 تشكيلة وتنظيم سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، 37 وتمارس هذه 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.
- القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني المشاركة في عمليات البحث والتحري عن الجرائم الإلكترونية[8].

المبحث الثاني: ضوابط التحقيق والتفتيش في جرائم تقنية المعلومات

إن أساليب التحري أو التحقيق التقليدية، قد لا تصلح لكشف الجريمة، وضبط مرتكبيها، والتحفظ على أدلتها، ويمكن إجراء بعض التحريات المبدئية قبل عملية التفتيش أو الضبط والتحقيق، توصلا لكشف غموض الجريمة تمهيدا لضبط مرتكبها، وجميع الأدلة المتعلقة بها.

ويمكن للمجني عليه في هذه الجرائم أن يقدم خدمات كبيرة لرجال الشرطة، أو لسلطة التحقيق، فما يقدمه لرجل الشرطة من معلومات، تحقق فائدة كبيرة في معرفة طبيعة الجريمة التي وقعت وأساليب ارتكابها، والأدوات المستخدمة في ارتكابها، والأشخاص المشتبه فيهم، وبواعث الجريمة، وما إذا كان هناك شهود أم لا، ذلك أن الجرائم ذات الصلة بالحاسب الآلي، تتسم بحداثة أساليب ارتكابها، وسرعة تنفيذها، وسهولة إخفائها، دقة وسرعة محو آثارها.

وهذه الخصائص العامة تقتضي أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وكيفية تشغيلها، وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي استخدمت في ارتكابها والتحفظ على البيانات أو الأجهزة التي استخدمت في ارتكابها أو تلك التي تكون محلا للجريمة[9].

المطلب الأول: جمع الإستدلالات في جرائم تقنية المعلومات

تسبق مرحلتي التحقيق الإبتدائي ومرحلة التحقيق النهائي (المحاكمة) ما يعرف "بمرحلة جمع الاستدلالات"، والتي تعتبر من أهم مراحل الإجراءات الجزائية، وهي المرحلة السابقة على تحريك الدعوى الجزائية والممهدة لمرحلة الخصومة

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

[9] 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.

الجزائية والأساس الذي تبنى عليه كافة الإجراءات الجزائية، فهي ليست مرحلة قضائية بالرغم من كونها الأساس الذي يبنى عليه التحقيق القضائي، فجمع الاستدلالات يعد مقدمة ضرورية في أغلب الجرائم، إذ كثيراً ما تحدث جرائم في الخفاء وتحتاج إلى كشفها وضبطها ومعرفة مسبباتها وملابساتها ودوافع ارتكابها لتسهيل مهمة التحقيق ولمنع المجرمين من الإفلات والهرب والتضييق عليهم تمهيداً لضبطها[10].

وتعد الاستدلالات مرحلة ممهدة للدعوى الجزائية، بالإضافة إلى اتصالها المباشر والوثيق بحرية الفرد وحقه في الحياة في أمان بعيدا عن أي اعتداءات من السلطات، كما تعد هذه المرحلة من أهم إجراءات العدالة الجنائية رهابا وأكثرها حساسية باعتبارها بداية الطريق إلى ساحة العدالة الجنائية وكفالة الحقوق، والسبيل إلى مواجهة الجرائم منعا وكشفا، كما أنها تعد- بحق- معيارا لقياس كفاءة الأجهزة الشرطية والأمنية وقدرتها على تحقيق الأمن بمنع وقوع الجرائم والحد منها، والكشف عنها، وضبط مرتكبيها عند وقوعها، وتقديمهم للمحاكمة العادلة.

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 عناصر الضبطية القضائية تلقي البلاغات التي ترد إليهم بشأن الجرائم، كما يجب عليهم قبول الشكاوى التي ترد إليهم بشأن الجرائم التي تطلب فيها المشرع تقديم شكوى من المجني عليه، وأن يثبتوها في محضر الاستدلال، ثم يرسلوها إلى النيابة العامة، وكذلك إجراء التحريات اللازمة لجمع كافة القرائن والأدلة التي تفيد في التوصل إلى الحقيقة إثباتا أو نفيا لوقوع الجريمة ونسبتها إلى فاعلها، وعليه سنتناول في هذا الفرع تلقي البلاغات والشكاوى وإجراءات البحث والتحري في جرائم تقنية المعلومات على النحو الآتي:

أولا: تلقي البلاغات والشكاوى في جرائم تقنية المعلومات

---

[10] 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.

البلاغ بصورة عامة، إخبار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع[11]، أو أن هناك اتفاقا جنائيا أو أدلة أو قرائن أو عزما على ارتكابها، أو وجود شك أو خوف من أنها ارتكبت، ويعرف بأنه "إبلاغ السلطات المختصة بوقوع جريمة ينص عليها القانون الجنائي".

وقد نصت المادة (12)من قانون الإجراءات الجزائية الجزائري[12] على أنه "يناط بالشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها مادام لم يبدأ فيها تحقيق قضائي"، كما نصت المادة (17) من قانون الإجراءات الجزائية على أن "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات"، كما نصت المادة (19) من القانون ذاته على أن "يقوم أعوان الضبط القضائي الذين ليست لهم 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 "يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم وأن يبادروا بغير تمهل إلى إخطار وكيل الجمهورية بالجنايات والجنح التي تصل إلى علمهم".

فقد نصت هذه المواد على ضرورة الإبلاغ عن الجرائم للسلطات العامة المختصة، سواء من أفراد المجتمع أم من الموظف العام والمكلف بخدمة عامة، وهذا يقتضي توافر العلم بالجريمة من المبلغ، ولا يشترط لذلك علم تام بالجريمة وظروفها ووقائعها، بل يكفي بأن يكون هناك جريمة ما تم ارتكابها، ثم يتدرج بعد ذلك مستوى العلم، وكلما أحاط المبلغ بمعلومات وتفصيلات عن الجريمة كان أفضل، وترتب عليه واجب ملزم بالإفصاح عنها دون أن يكتم شيئا.

ولقد رتب المشرع الجزائري المساءلة الجزائية عن كل من يمتنع على الإبلاغ عن الجرائم.

ومن هذا المنطلق؛ فبمجرد تلقي ضابط الشرطة القضائية أو جهة التحقيق المختصة بلاغا يشير إلى ممارسة شخص أنشطة تندرج ضمن جرائم تقنية المعلومات في مكان أو أجهزة محددة، ووفق لغات برمجية معلومة؛ كتلقيه مثلا بلاغا فيه معلومات عن نشر فيروسات تخريبية عبر الشبكة الإلكترونية، فإنه حينئذ يبدأ في ممارسة اختصاصاته.

---

[11] إيهاب محمد التاج، التحقيق وجمع الأدلة في الجرائم المعلوماتية، مجلة العدل، العدد 26، السنة الحادية عشرة، ص 392.

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

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:[13]

1. تحديد مكان وقوع الجريمة: على المبلغ تحديد المكان الذي وقعت فيه الأفعال غير المشروعة، ووصفها بما يسمح بالدلالة عليها كوصف موقع الشركة أو عنوانها أو البنك أو المنزل الذي تعرض للاعتداء.

2. تحديد نوع الجريمة: لا يكفي أن يقوم المبلغ بتحديد مكان وقوع الجريمة؛ بل ينبغي عليه أن يبين نوع الجريمة المرتكبة؛ ما إذا كانت اعتداء على مال أم تزوير بطاقة ائتمانية أو جرائم اختراق وتعطيل وإعاقة المواقع والإعتداء على البيانات والمعلومات الإلكترونية.

3. تحديد محل الجريمة: يجب على المبلغ أن يحدد لرجال الضبط القضائي المختصين الجهاز الذي وقعت عليه الجريمة، والموقع الذي استهدفه الاعتداء.

وعليه؛ تعد هذه العناصر مهمة وضرورة لمساعدة رجال الضبط القضائي في أي بلاغ يتعلق بجرائم تقنية المعلومات، بحيث تمكنهم من تحديد معالم الجريمة، ووضع خطة للتعامل معها من الناحيتين الفنية والقانونية.

والبلاغ هنا قد يتم عن طريق الإنترنت أي ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة إلكترونية إلى الجهات المختصة بالتحقيق والتحري لإبلاغها عن وجود صفحات أو مواقع غير مشروعة تمارس جرائم تقنية المعلومات، وقد تكون بلاغا مباشرا أمام أحد مقرات الأمن الوطني.

والمبلغ في جرائم تقنية المعلومات لابد وأن تكون لديه معرفة مقبولة بالجوانب الفنية للحاسوب الإلكتروني والشبكة الإلكترونية حتى يتمكن من تقديم معلومات تصف الحادث بشكل جيد، ويمكن لضابط الشرطة القضائية أو المحقق الوقوف على طبيعة الجريمة بشكل مقبول حتى يمكنه مباشرة التحقيق فيها، وبالتالي يفترض أن يكون لدى من يتلقى البلاغ المعرفة الكافية بالجوانب الفنية للحاسوب الإلكتروني والشبكة الإلكترونية حتى يستطيع مناقشة المبلغ في الكثير من الجوانب المتعلقة بالجريمة محل البلاغ.

ثانيا: البحث والتحري وكشف غموض جرائم تقنية المعلومات

[13] إيهاب محمد التاج، المرجع السابق، ص 392

يقصد بعملية التحري عبر الشبكة الإلكترونية: عمل أمني يقوم به رجل التحريات عبر شبكة الإنترنت بواسطة التكنولوجيا الإلكترونية الرقمية لتحقيق غرض محدد، وتخزين النتيجة في ملف رقمي أو إفراغها في وثيقة تفيد في إثبات حصول جريمة إلكترونية وإسنادها إلى شخص بعينه وهي أحد عناصر الإثبات الجنائي.

ولتحقيق ذلك يجب تدريب الكوادر التي تباشر التحريات والتحقيقات مع الإستعانة بذوي الخبرة الفنية المتميزة في هذا المجال، فضلا عن تطوير الإجراءات الجنائية، لتحقيق الغرض المطلوب[14].

وحددت المادة (17) من قانون الإجراءات الجزائية اختصاصات رجال الضبطية القضائية بالقول: "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات".

وعلى هذا الأساس؛ فإن التحري عبر الشبكة المعلوماتية يعد عملا أمنيا وقانونيا يقوم به رجل البحث الجنائي المختص عبر الشبكة بواسطة وسيلة تقنية المعلومات للحصول على بيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن أو الأشياء للحد من جرائم تقنية المعلومات، أو ضبطها؛ لتحقيق الأمن الإلكتروني، أو لأي غرض آخر.

ولرجال البحث الجنائي في هذا سلطة تقديرية واسعة في اختيار وسائل إجراءات التحري التي يرونها مناسبة ولازمة لإتمام عملهم بصورة إيجابية في جمع المعلومات التي سيستفيدون منها لضبط الجرائم الإلكترونية أو الحد منها، ولهم في ذلك مصادر عدة:

– **المراقبة الإلكترونية**: العمل الذي يقوم به المراقب– باستخدام التقنية الإلكترونية– لجمع بيانات بالزمن والتاريخ والوقت ومعلومات عن المشتبه فيه سواء أكان شخصا أم مكانا، أم شيئا حسب طبيعته لتحقيق غرض أمني أو لأي غرض آخر.

ولم يتصد المشرع الجزائري لضبط تعريف المراقبة الالكترونية لا في مواد قانون الإجراءات الجزائية ولا في مواد القانون 09-04 المتعّلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وإنما ترك ذلك للفقه الذي اختلف هو الأخر في ضبط تعريف دقيق وموحد لإجراء المراقبة الالكترونية، حيث عرفها بعض الفقه

[14] 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.

بأنّها إجراء يتعمد فيه الإنصات والتسجيل ومحّلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة أي سواء كانت ممّا يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكّية واللاسلكية[15].

وتعتبر المراقبة الإلكترونية من أهم مصادر البحث والتحري التي تتم باستخدام تقنية المعلومات، لجمع البيانات عن المشتبه فيهم في جرائم تقنية المعلومات، ومع ذلك فإن المراقبة تعد من الإجراءات التي تعتدي على حق الخصوصية (كمراقبة البريد الإلكتروني الخاص بالمشتبه فيهم) التي كفلها الدستور والقانون بالحماية، ومن ثم فهي تتطلب– قبل البدء بها – حصول مأمور الضبط القضائي على الإذن بها من السلطات القضائية المختصة.

ومن هذا المنطلق؛ فإن المراقبة الإلكترونية هي وسيلة من وسائل جمع البيانات والمعلومات عن جرائم تقنية المعلومات، ويقوم بها مراقب إلكتروني يتمثل في رجل الضبط القضائي الذي يتمتع بكفاءة تقنية عالية تتماشى مع نوعية جرائم تقنية المعلومات التي يتعامل معها، مستخدما في ذلك التقنية الإلكترونية وعبر الشبكة الإلكترونية؛ كأن يراقب أحد الهاكر ممن قام باختراق الحاسوب الآلي الخاص بالمجني عليه وبريده الإلكتروني، أو اختراقه للمواقع.

ويسمح القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لضباط الشرطة القضائية بالدخول ولو عن بعد لمنظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، بالإضافة إلى منظومة تخزين معلوماتية تفيد في عملية التحقيق[16].

فعندما يقوم الموظفون لدى مقدمي خدمة الاتصال بمراقبة الاتصالات لحماية حقوق مزودي الخدمة فيكتشفون الاختراقات التي ترتكب من المجرم الإلكتروني، ويكشفونها للسلطة؛ فلا يوجد حينئذ انتهاك للقانون؛ فمزودو الخدمة الذين يحققون في الاستخدامات غير المشروعة لنظم المعلومات لديهم سلطة موسعة للمراقبة، ولديهم الحق في الكشف عن دليل الاستخدام غير المشروع.

وعلى هذا الأساس؛ فإن ما يثير الإشكالية هنا هو أن القيام بالمراقبة السرية الإلكترونية في جرائم تقنية المعلومات التي تحدث عبر الشبكة الإلكترونية ووسائلها ليس بالأمر السهل؛ إذ ينبغي أن تتوافر لدى جهات الضبط القضائي القائمة بها المؤهلات العلمية والتقنية اللازمة لأداء هذه المهمة على أحسن وجه، وذلك لا يمكن إنجازه إلا من خلال

[15] 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.

[16] المادة 05 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.

إسناد مثل هذه المهمة لجهات ضبط قضائي خاصة مؤسسة ومعدة خصيصا لهذا الغرض ضمن جهاز شرطي مختص بمكافحة جرائم تقنية المعلومات والتحري عنها، كما أن أفراد هذه الجهات لا بد أن يكونوا على إلمام ودراية بالبيانات الإلكترونية التي ترتبط بمفهوم الحياة الخاصة للأفراد التي لا تجوز مراقبتها إلا بما يسمح به القانون.

وتحقيق مثل هذا الإلمام بدوره يقتضي- من جهة- تنظيم المشرع لإجراءات المراقبة التي تعد من الإجراءات التحقيقية، كما يقتضي- من جهة أخرى- إمداد أفراد تلك الجهات بالثقافة القانونية اللازمة لهذا الغرض عبر تنظيم دورات خاصة لهم.

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

أ- مزود الخدمة: الذي يمكنه رصد هذه التحركات من خلال اكتشاف العناوين التي تم الدخول 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[17]، وهو حاسوب يقوم بدور الوكيل، وذلك لاختصار الوقت اللازم للوصول إلى موضع معين على شبكة الإنترنت عند تكرار الدخول إلى الموقع نفسه.

هـ- مراقبة عمل الموظفين على الشبكة: ويعتبر من قبيل الرقابة الإدارية لمصلحة أصحاب العمل، للتأكد من أن العمال لا يبددون أوقات العمل لمصالحهم الشخصية، أو أنهم يعملون لمصلحة الغير.

و- التحري الإلكتروني: تقوم بعض الدول بتخصيص مأموري ضبط قضائي لإجراء التحريات عن جرائم تقنية المعلومات، وتتوافر لديهم الخبرة الفنية في التحقيق الجنائي، ومعالجة البيانات الإلكترونية.

- عملية توثيق وتحريز الأدلة الجنائية الرقمية

تعد الأدلة الجنائية الرقمية كمثلها من الأدلة المادية التي تحتاج إلى التوثيق والتأمين بالقدر الذي يكفل لها المصداقية ويبعد عنها العيوب، وذلك لأسباب عدة، منها:

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

1 . التوثيق الذي يحفظ الأدلة الرقمية في شكلها الأصلي، الذي يستعمل لعرض وتأكيد مصداقية الدليل وعدم تعرضه لتحريف أو تعديل الصورة المسجلة بالفيديو . مثلاً . يمكن الاستعانة بها في تأكيد مدى صحة المناقشة الحية بين طرفين عن طريق مطابقة النص الرقمي مع النص المصور على الشاشة[18].

2 . الأشخاص الذين يقومون بجمع الأدلة عليهم الإدلاء بشهاداتهم حول مطابقة الأدلة التي قاموا بجمعها مع تلك المقدمة أمام المحكمة، والتوثيق هو الأسلوب الوحيد الذيّ يمكن المحققين من القيام بهذا الدور أمام القضاء، ويعد فشل المحقق في التمييز بين أصل الدليل وصورته أمام القضاء سببا في بطلان الدليل.

3 . ينبغي توثيق مكان ضبط الدليل الرقمي في حالة إعادة تكوين الجريمة، فإذا تشابهت أجهزة الحاسب الآلي وملحقاتها يجعل من الصعب إعادة ترتيبها دون وجود توثيق سليم ومفصل يحدد الأجزاء والملحقات وأوضاعها الأصلية بدقة.

4 . يشكل التوثيق جزءا من عمليات حفظ الأدلة الرقمية حتى انتهاء إجراءات التحقيق والمحاكمة، إذ إن التوثيق يشمل تحديداً دقيقا للجهات التي تحتفظ بالأدلة وقنوات تداولها، التي ينبغي حصرها في نطاق محدود، قدر الإمكان. ويجب التأكد من . عند توثيق الدليل الرقمي . أين، كيف، متى، وبواسطة من تم ضبط الدليل وتأمينه، كما أنه من الضروري توثيق الأدلة الرقمية بعدة طرق، كالتصوير الفوتوغرافي، والتصوير بالفيديو والخرائط الكروكية، وطباعة نسخ من الملفات المخزنة في جهاز الحاسب الآلي، أو المحفوظة في الأقراص، وعند حفظها على الأقراص والشرائط ينبغي تدوين البيانات على كل منها، وذلك بحسب الآتي:

- التاريخ والوقت.
- توقيع الشخص الذي قام بإعداد النسخة.
- اسم أو نوع نظام التشغيل.
- اسم البرنامج أو الأوامر المستعملة لإعداد النسخ.
- المعلومات المضمنة في الملف المحفوظ[19].

الفرع الثاني: الإنتقال والمعاينة في جرائم تقنية المعلومات

---

[18] 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.

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

الإنتقال والمعاينة من أهم إجراءات مرحلة جمع الاستدلالات التي يقوم بها عناصر الضبط القضائي، وعصب التحقيق الجنائي ودعامته وعماده؛ فهي تعبر عن الوقائع والحقائق تعبيرا صادقا، لا تكذب ولا تحابي ولا تخدع؛ فتعطي رجل الشرطة صورة صحيحة واقعية لمكان الجريمة وما يتصل بها من ماديات وآثار، كما أنها تكشف غموض الجريمة التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبيها.

ففي جميع الأحوال عند تلقي بلاغ عن وقوع جريمة إلكترونية، وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، والمعاينة الإلكترونية إجراء يختلف طبعا عن الجريمة التقليدية، حيث تتضاءل الأدلة في الجريمة الإلكترونية، وذلك لندرة تخلف آثار مادية عقب ارتكاب هذه الجريمة، كما أن طول الفترة بين وقوع الجريمة وارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو محو أو تلف تلك الآثار[20] .

أولا: المقصود بالانتقال والمعاينة في مسرح جرائم تقنية المعلومات

يقصد بالانتقال: توجه المحقق إلى محل الواقعة أو إلى أي مكان آخر توجد به آثار أو أشياء تفيد في الكشف عن الجريمة، ويكون ذلك في أسرع وقت ممكن قبل أن تزول آثارها، وبغرض جمع الآثار المتعلقة بها، وكيفية وقوعها، وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة.

ويعرف الفقه الجنائي المعاينة بأنها: "رؤية بالعين لمكان أو شخص أو أشياء لإثبات حالته، وضبط كل ما يلزم لكشف الحقيقة ومعاينة مسرح الجريمة الإلكتروني يقصد به: معاينة الآثار التي يتركها مستخدم الشبكة الإلكترونية أو الإنترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها، وكل الاتصالات التي تمت من خلال الحاسوب الآلي والشبكة 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[21].

والانتقال فورا نحو مسرح الجريمة وإجراء المعاينة يهدف إلى ضمان عدم الشك في الدليل المستفاد منها، وذلك لأن انقضاء فترة ما بين وقوع الجريمة وإجراء المعاينة يمكن أن يسمح بأن يتمكن الجاني من إزالة العناصر المادية التي تفيد في كشف الحقيقة.

---

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

[21] 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.

فبعد تلقي البلاغ تأتي الخطوة التالية، وهي الانتقال لمعاينة مسرح الجريمة والتي غالبا ما يقوم بها رجال الضبط القضائي للكشف عن مكان وقوع الجريمة وفحصه والتحفظ على أي آثار أو مخلفات أو متعلقات مادية تمت بصلة إلى الجريمة ومرتكبيها، وكذلك تصوير الموقع ووضع السيناريوهات المقترحة لكيفية حدوثها وزمن ارتكابها والملابسات المحيطة بها وإثباتها على مرتكبها.

ثانيا: ضوابط المعاينة في جرائم تقنية المعلومات

تبدأ هذه العملية الإجرائية بنزول فريق متخصص مزود بكامل الإمكانات اللازمة للسيطرة على جميع الأجهزة والأشخاص العاملين عليها وحجزهم بعيدا عنها، مع ضبط الفلاشات والأقراص الصلبة والموبايلات الخاصة بهم.. الخ، ومن ثم الاتصال بالمبلغين؛ لكي يزودوا الفريق بكل المعلومات التي قد يحصلون عليها، ويتم العمل وفقا للإجراءات المبينة؛ حتى تكون جاهزة لتقديمها للقضاء كأدلة إثبات دون أن يشوبها أي قصور بالتنسيق مع النيابة والخبراء المتخصصين في هذا المجال[22]، وتتم هذه العملية بناء على النحو الآتي:

1 – مسرح الجريمة التقليدي: ويقع خارج بيئة الحاسوب، ويتكون- بشكل رئيسي- من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية، وقد يترك فيها الجاني آثار عدة كالبصمات وغيرها، وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه وفي هذه الحالة ليست هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات للمعاينة من قبل عناصر الضبط القضائي، والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبتها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل ما استعمل في ارتكاب الجريمة والتحفظ عليها، مع إخطار النيابة العامة بذلك، والسبب في سهولة المعاينة في هذه الحالة أنها تتم على عناصر مادية ملموسة كانت محلا للجريمة، أو تخلفت عنها عكس المعاينة التي تتم عقب وقوع الجريمة بواسطة مكونات غير مادية.

2 – مسرح الجريمة الإفتراضي: ويقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد وتتنقل داخل بيئة الحاسوب وشبكة الإنترنت، وفي ذاكرته وفي الأقراص الصلبة الموجودة بداخله. والتعامل مع الأدلة الموجودة في هذا المسرح يجب ألاّ يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع.

وفي هذه الجرائم تظهر صعوبات تحول دون فاعلية المعاينة أو فائدتها، ويمكن تلخيصها في الآتي:

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

أ- الصعوبة الأولى تتمثل في ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلوماتية بصفة عامة، وبرامج الحاسوب الآلي وبياناته بصفة خاصة.

ب- الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة نسبيا، ما بين وقوع الجريمة والكشف عنها، الأمر الذي يمنح فرصة لحدوث تغيير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها، وهو ما يلقي ظلا من الشك على الدليل المستمد من المعاينة.

وبخلاف ذلك فمن الممكن أن تكون الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الحاسوب الآلي ثرية جدا فيما تحتويه من معلومات مثل صفحات المواقع المختلفة والبريد الإلكتروني والفيديو الرقمي والصوت الرقمي وغرف الدردشة والمحادثة، والملفات المخزنة في الحاسوب الآلي الشخصي، والصورة المرئية، والدخول للخدمة والاتصال بالإنترنت والشبكة عن طريق مزود الخدمات.

ولذلك؛ فإنه يجب عند معاينة مسرح جرائم تقنية المعلومات مراعاة القواعد والإرشادات الفنية الآتية:

1- القيام بتصوير الحاسوب الآلي، وما قد يتصل به من أجهزة طرفية ومحتوياته وأوضاع المكان الذي يوجد به بصفة عامة، مع العناية بتصوير أجزائه الخلفية، وملحقاته الأخرى على أن يراعى تسجيل تاريخ المكان الذي تم التقاط الصورة فيه وزمانه.

2- ملاحظة طريقة إعداد نظام الحاسوب بعناية بالغة.

3- إثبات الحالة التي تكون عليها كابلات الحاسوب وتوصيلاته بمكونات النظام؛ حتى يسهل عليه القيام بعملية المقارنة والتحليل لها عند عرض الموضوع على المحكمة المختصة.

4- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة قبل إجراء الاختبارات اللازمة؛ للتيقن من عدم وجود أية مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة بسبب تداخل المجالات المغناطيسية مع بعضها البعض.

5- حفظ ما تحويه سلة المهملات من الأوراق الملقاة أو الممزقة، وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، ورفع البصمات التي قد تكون لها علاقة بالجريمة المرتكبة؛ لأن دليل الجريمة قد يكمن ضمن هذه القصاصات.

6-حفظ المستندات الخاصة بالإدخال، وكذلك مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع البصمات التي قد تكون موجودة عليها ومضاهاتها، ويجب قصر عملية المعاينة على عناصر الضبط القضائي سواء أكانوا من الباحثين أم المحققين الذين تلقوا التدريب الكافي والذين تتوافر فيهم الكفاءة العلمية والخبرة

الفنية في مجال الحاسبات واسترجاع المعلومات، ومواجهة هذه النوعية من الجرائم، والتعامل مع أدلتها التي قد تتخلف عنها على مسرح الجريمة التقليدي.

وقبل وصول المحققين والفنيين إلى مسرح الجريمة يجب إعداد خطة عمل بشكل شامل باتباع الخطوات التالية:

1. إعداد المواد والمغلفات الضرورية لأوعية الجريمة الرقمية مختلفة الحجوم والأشكال.
2. إعداد الشكل المبدئي للأوراق المطلوبة لتوثيق المعاينة.
3. التأكد من أن جميع المختصين والفنيين يدركون أشكال الأدلة بالإضافة إلى التعامل المناسب معها.
4. تقييم النتائج القانونية لتفتيش مسرح الجريمة الرقمية.
5. بحث المتوقع وجوده من الآثار المادية بمسرح الجريمة الرقمية.
6. تعيين شخص مسؤول قبل الوصول إلى مسرح الجريمة.
7. إعداد مهام الطاقم الأساسية قبل الوصول.
8. تقييم مهام الطاقم المطلوبة لمعالجة مسرح الجريمة بشكل ناجح.[23]

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 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

---

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

لم تحدد القوانين المقارنة المقصود بالتفتيش إلا أنه يمكن أن نعتبره أحد الإجراءات التي يقوم بها موظف مختص طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة والخصوصية، بهدف الوصول إلى أدلة مادية لجريمة تحقق وقوعها لإثبات نسبتها إلى شخص معين، والتفتيش كأصل عام تختص به سلطة التحقيق[24].

ويختلف التفتيش بحسب نوعية الجرائم، فالجرائم العادية يتعلق التفتيش بها على أشياء مادية، أما الجرائم المعلوماتية فهي تطرح العديد من الصعوبات لأنها تخص 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 كأن يكون النظام المعلوماتي داخل أحد المساكن مع وجود النهاية الطرفية له في مكان آخر بحيث يملك الجاني الفرصة لتدمير البيانات.

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

– رابعا: ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها ومعرفة السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الإتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار وبروتوكولات الإتصالات عبر الإنترنت وإن تعلقت الجريمة بهذه الشبكة والتي تعرف اختصارا ب (**ip**) [25].

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 فنية أخرى ضد الاختراق، وذلك لاتفاقهما في نفس العلة وهي رفض مسبق لعمليات الاطلاع الغير مصرح به، لكن يجب

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

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

أن يقابل ذلك رسم حدود للقاعدة العامة الموجودة في التشريعات العقابية وهي "إعفاء المتهم من تقديم ما من شأنه إثبات إدانته بطريقة مباشرة" 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 الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع جرائم الإنترنت، لأنه لا يقف أمام تنقل الملفات والرسائل الحاسوبية أي حدود جغرافية، كما أنه لا توجد معاهدات تسمح بالتعاون الدولي أو عدم كفايتها لمواجهة المتطلبات الخاصة بجرائم الكمبيوتر وديناميكية التحريات وكفالة السرعة للحصول على أدلة الإثبات[26].

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[27].

المطلب الثاني: إجراءات التحقيق الابتدائي في جرائم تقنية المعلومات

إن التحقيق الإبتدائي اختصاص أصيل وهام يباشره قضاء التحقيق بإجراءات متعددة تتسم بالحيدة التامة، وأعضاؤه هم الذين يضطلعون به أصلا ضد متهم معين، لبحث الجريمة ومدى ثبوتها أو عدم ثبوتها بأنفسهم توصلا إلى مدى توافر أركانها.

وعلى ذلك فإذ يباشر قضاة التحقيق عملهم لا يقصدون من ورائه سوى التوصل إلى كشف الحقيقة؛ سعيا إلى تطبيق موجبات القانون وتحقيق العدالة التي هي أسمى رسالة في الوجود، وللنيابة العامة أن تكلف أحد مأموري الضبط القضائي للقيام بعمل معين أو أكثر من أعمال التحقيق مثل التفتيش والضبط والانتقال والمعاينة فيما عدا استجواب المتهم.

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

---

[26] 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.

[27] سحتوت نادية، المرجع السابق، ص53.

الفرع الأول: التفتيش في جرائم تقنية المعلومات وجمع الأدلة وضبطها

التفتيش هو البحث عن شيء يتصل بجريمة وقعت و يفيد في كشف الحقيقة عنها وعن مرتكبيها وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة، وقد أحاط القانون التفتيش بضمانات وضوابط عديدة، ومحل التفتيش إما أن يكون مسكنا أو شخصا، وهو بنوعيه قد يكون متعلقا بالمتهم أو بغيره والغاية من التفتيش هي ضبط شيء يتعلق بالجريمة و يفيد في التحقيق الجاري بشأنها، سواء كان هذا الشيء أدوات استعملت في ارتكاب الجريمة، أو شيء نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة، ومحل التفتيش الخاص الحاسب الآلي هي كل مكونات الحاسوب سواء كانت مادية أو معنوية أو شبكات الإتصال الخاصة، والبيانات المسجلة في ذاكرة الحاسب أو في مخرجاته، والسجلات المثبتة باستخدام نظام المعالجة الآلية للبيانات، ودفتر يومية التشغيل، المعاملات الخاصة في عمليات الدخول إلى نظام المعالجة الآلية للبيانات، وما يتعلق بها من سجلات كلمات السر، مفاتيح الدخول، ومفاتيح فك الشفرة بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش، وتشمل المكونات المادية للحاسب ووحدة الذاكرة ووحدة الحاسب والمنطق ووحدات الإخراج وأخيرا وحدات التخزين الثانوي[28].

كما تنقسم المكونات المادية والمعنوية للحاسب الآلي إلى الكيانات المنطقية الأساسية أو برامج النظام والكيانات المنطقية التطبيقية أو برامج التطبيقات بنوعيها، برامج التطبيقات، وبرامج التطبيقات طبقا لاحتياجات العميل، ويستلزم الحاسب بمكوناته سالفة الذكر مجموعة من الأشخاص لديهم خبرة ومهارة في تقنية نظم المعلومات وهم مشغلو الحاسب وخبراء البرامج سواء كانوا مخططي برامج تطبيقات أم مهندسي الصيانة والاتصالات ومديري النظم المعلوماتية[29].

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 أوأثناءها.

ومن هذه الضوابط؛ الحصول على الإذن للقيام بعملية التفتيش، وتحديد الأشخاص المنوط بهم القيام بهذا الإجراء، والوقت المناسب لإجرائه، وغيرها من الضمانات[30].

---

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

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

[30] 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.

أولا: السلطة المختصة بالتفتيش في جرائم تقنية المعلومات:

التفتيش لا تملكه- بحسب الأصل- إلا سلطة التحقيق، ويخضع للخصائص العامة التي تخضع لها كل إجراءات التحقيق الابتدائي، وإذا كان القانون قد سمح لعناصر الضبط القضائي بالقبض على المتهمين وتفتيشهم وتفتيش مساكنهم في حالات معينة ووفقا لضوابط محددة، فهذا استثناء من القاعدة العامة، حيث أن القضاء غير مطالب بإجراء التفتيش بنفسه، فربما لا يتسع وقت قاضي التحقيق لتنفيذه، لا سيما إذا تعددت الأماكن أو الأشخاص أو الحاسبات المراد تفتيشها، لذا فقد جرى العمل- في غالب الأحيان- على ندب أحد ضباط الشرطة القضائية وبناء على إذن صادر عن السيد وكيل الجمهورية لإجرائه بإعطائه ما يسمى "بإذن أو بأمر التفتيش" الذي ينبغي أن تراعى في إصداره وتحريره جميع القيود الخاصة بالندب.

فالتفتيش الإلكتروني إجراء من إجراءات التحقيق يهدف إلى البحث في داخل نظام الحاسوب الآلي أو الإنترنت بإذن قضائي مسبق سواء أكان هذا النظام مكونا من حاسوب واحد أو عدة حواسيب مرتبطة فيما بينها بشبكة في محل له حرمة منحه إياها القانون، والغرض منه استخراج أدلة معلوماتية متمثلة في المعلومات أو البيانات التي تساعد على كشف الحقيقة في جريمة من نوع جناية أو جنحة وقعت، والتحقيق فيها جار[31].

ثانيا: محل التفتيش في جرائم تقنية المعلومات

إن تفتيش نظم المعالجة الآلية يعد من أخطر المراحل حال اتخاذ الإجراءات الجزائية ضد مرتكب الجريمة المعلوماتية، لكون 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[32]، حيث تتمثل في البرامج أو الكيانات المنطقية والبيانات المسجلة في ذاكرة الحاسوب الآلي أو في مخرجاته، والسجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات ودفتر يومية التشغيل وسجل المعاملات، والسجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات، وما يتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة، ويمكن رصد خضوع الحاسوب الآلي والشبكة المعلوماتية للتفتيش ،وذلك على النحو الآتي:

1 - الإحتمال الأول: أن يكون حاسوب المتهم متصلا بحاسب أو نهاية طرفية موجودة في مكان آخر داخل الدولة.

---

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

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

2- الإحتمال الثاني: هو اتصال حاسوب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة.

ومن المشكلات التي تواجه القائمين على جمع الأدلة والتحقيقات حالة امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها الإذن ودخوله في المجال الجغرافي لدولة أخرى وهو ما يسمى بالولوج أو التفتيش عبر الحدود، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها وحدودها الإقليمية.

3- الإحتمال الثالث: التنصت والمراقبة الإلكترونية لشبكات الحاسوب الآلي.

فمن خلال ما تقدم يتبين بجلاء أن جرائم تقنية المعلومات قد تقع في صورة كيانات مادية يسهل تفتيشها واكتشاف أمرها وضبطها، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حرمة فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبالضمانات نفسها والإجراءات المقررة قانونًا، أما الجرائم التي تقع على الكيان المعنوي فإنه يصعب اكتشافها إذا ظلت على صورتها المعنوية في شكل نبضات أو ذبذبات، أما إذا تحولت هذه الكيانات إلى مستخرجات أو مستندات أو سجلات فإنه يسهل الوصول إلى الجرائم التي ترتكب عليها[33].

الفرع الثاني: جمع الأدلة الإلكترونية وضبطها

إن الغرض من التفتيش هو ضبط الأدلة أو الأشياء التي تفيد في ظهور الحقيقة في الجريمة التي وقعت، فالضبط في معظم الأحوال هو غرض التفتيش، وإن لم يكن هو السبب الوحيد، فقد يتم الضبط استنادا لأسباب أخرى غير التفتيش من ذلك المعاينة وما قدمه المتهم والشهود أمام مراكز الضبط القضائي.

ويقصد بالضبط في قانون الإجراءات الجزائية وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق.

فالغاية من التفتيش هي ضبط كل ما يفيد في كشف الحقيقة سواء تعلق ذلك بأشخاص أو أماكن أو أشياء طالما كان لها اتصال بالجريمة، وتحصيل الأدلة في الجرائم الإلكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته، الأقراص الصلبة، الأقراص والأشرطة الممغنطة، الطباعة، البرامج اللينة، البطاقات الممغنطة وبطاقات الائتمان والمعدات المستعملة في شبكة الانترنت مثل المودم، ففي هذه الحالة لا يطرح ضبط هذه المكونات المادية أي إشكال قانوني أو عملي لإمكانية إخضاعها لإجراءات الضبط والتحريز التقليدية[34].

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

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

وبناء عليه، فإن الأشياء التي ينبغي إخضاعها لإجراء الضبط في جرائم تقنية المعلومات والتي تعد كيانات ذات قيمة يمكن الاستفادة منها في إثبات الجريمة أو نسبتها إلى الجاني هي:

1- ضبط المستندات والكيانات الورقية التي وقعت عليها العمليات الإلكترونية والتي يعتقد أن لها صلة بالجريمة أو مرتكبيها، وقد تكون محررات مزورة داخل نظام الحاسب الآلي أو في أي مكان خارجه، ويمكن أن تكون في سلة المهملات.

2 – وحدة المدخلات المكونة من مفردات لوحة المفاتيح والشاشة والفأرة والخادم ومجمع المعلومات والماسحة الضوئية وكذلك برنامج معالجة النصوص وبرنامج عرض الشرائح.

3- ضبط المراسلات الإلكترونية التي تستخدم البريد الإلكتروني عبر شبكة الإنترنت والتي يتم من خلالها نقل الرسائل ومحتوى المستندات الورقية حيث تتمتع هذه الوسيلة بنظام حماية تتكون من رموز وشفرات لا يمكن الطلاع عليها إلا إذا عرفت عليها الجهة المستقبلة، وهي تحتفظ بنسخ عن المواد المرسلة منها وإليها ويمكن استرجاعها والاطلاع عليها وضبطها[35].

4 – الشرائط الممغنطة وهي جميع الشرائط ووسائط النقل والتخزين التي يعتقد أنها تحتوي على مواد تفيد في كشف الحقيقية أو مرتكبيها.

5- ضبط الطابعات وأجهزة التصوير بكافة أنواعها، ولا سيما أن الأجهزة الحديثة يمكنها تخزين المستندات والمواد المطبوعة أو المنسوخة، حيث يمكن إعادة استخراجها والتعرف على محتوياتها.

6- ضبط وحدة الذاكرة الرئيسية، ووحدة التحكم، والمودم (وهي الوسيلة التي تتمكن من خلالها أجهزة الحاسوب من الاتصال فيما بينها بواسطة خطوط الهاتف).

الفرع الثالث: ندب الخبراء والاستجواب في جرائم تقنية المعلومات

الخبرة هي إجراء يتعلق بموضوع يتطلب إلماما بعلم أو فن معين لإمكان استخلاص الدليل منه لذلك فإن الخبرة تفترض وجود شيء مادي أو واقعة يستظهر منها الخبير رأيه[36].

فهي الوسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا عن الدليل القولي أو الدليل المادي، وإنما هي تقييم فني لهذا الدليل، والعنصر المميز للخبرة عن غيرها من

---

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

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

إجراءات الإثبات كالمعاينة والشهادة والتفتيش هو الرأي الفني للخبير في كشف الدليل أو تحديد قيمته التدليلية في الإثبات، حيث تفيد الخبرة في إثبات وقوع الجريمة أو نسبتها إلى المتهم أو في تحديد ملامح شخصيته الإجرامية.

أما الاستجواب فيعد من أهم إجراءات التحقيق المستخدمة في كشف الحقيقة، حيث يمكن الاستجواب ما السلطة المناط بها التحقيق من طرح الأسئلة الدقيقة والولوج في موضوع الدعوى، والتعرف إلى أدق التفصيلات فيما يتعلق بالجريمة، ويعرف الاستجواب بأنه "إجراء من إجراءات التحقيق تتم فيه مناقشة المتهم فيما هو منسوب إليه من جرم، وُيطلب منه الرد على الأدلة القائمة ضده إما بتفنيدها أو التسليم بها".

أولا: ندب الخبراء في جرائم تقنية المعلومات

لقد أدى التطور التقني في نظم المعالجة الآلية إلى تغيير كبير في المفاهيم السائدة حول الدليل، وقاد مثل هذا القول في الحقيقة إلى تعاظم دور الإثبات العلمي وإعلان انضمام الخبرة التقنية إلى عالم الخبرة القضائية، ذلك أن اشتقاق الأدلة الرقمية المطلوبة في إثبات الجرائم المعلوماتية وكشف أنماطها أمر يضطلع به الخبراء المتخصصون في هذا المجال[37].

ومن هذا المنطلق، فإنه من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع جرائم تقنية المعلومات، ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات، وكذلك إعداد البرمجيات وتشغيل الحاسوب الآلي وعلومه، وأن نجاح جمع الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء.

ويجب على المحقق الجنائي أن يحدد للخبير المعلوماتي دوره في المسألة المنتدب فيها على وجه الدقة، وهذا يعود بنا إلى ضرورة تأهيل رجال الضبط وسلطات التحقيق الابتدائي في الجرائم المعلوماتية لنجاح تحقيق مثل هذه الجرائم، ودرء لما ينادي به البعض من أنه يمكن للخبير نفسه أن يحدد إطار مهمته، إذ أن ذلك سوف يقوض دور المحقق والقاضي في الدعوى الجنائية المتعلقة بجرائم تقنية المعلومات[38].

والنيابة العامة وقضاء التحقيق يمتلكان سلطة تقديرية في ندب الخبراء من عدمه، وذلك تحت رقابة محكمة الموضوع.

وتجدر الإشارة إلى أنه يمكن القول بأن الاستعانة بالخبراء في مجال الجرائم التي تقع على تقنية المعلومات ضرورية، وخاصة عندما يعجز المحقق –أثناء التحقيق في جريمة ما– عن فهم الجوانب التقنية أو العلمية التي تحتاج إلى قدر متقدم

---

[37] سعيداني نعيم، المرجع السابق، ص165.

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

من التخصص لكشف غموضها أو فهم طبيعتها، وقد أجاز له القانون الاستعانة بأشخاص أو جهات فنية أو مخبرية أو مهنية متخصصة في المسألة موضوع الخبرة.

وتعد الاستعانة بالخبراء جزءا من عملية التحقيق، وذلك للمساعدة في كشف غموض الجريمة وإثبات أدلتها في مواجهة الجناة أو المشتبه فيهم أو نفيها عنهم.

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[39] .

ومباشرة الاستجواب في جرائم تقنية المعلومات تتم بواسطة سلطة التحقيق، فيجب على قاضي التحقيق عند حضور المتهم لأول مرة في التحقيق أن يدون جميع البيانات الخاصة بإثبات شخصيته، ويحيطه علما بالتهمة المنسوبة إليه، ويثبت في المحضر ما قد يبديه في شأنها من أقوال.

والاستجواب بهذا المعنى يحقق وظيفتين: أولهما، إثبات شخصية المتهم ومناقشته تفصيلا في الاتهام الموجه إليه، وثانيهما تحقيق دفاع المتهم، ذلك أن مناقشة المتهم في أدلة الاتهام قد تؤدي إلى اعترافه بارتكاب الجريمة، كما أنها في الوقت ذاته تفسح السبيل أمامه إذا كان بريئا، وذلك لتفنيد الأدلة القائمة ضده فتجنبه رفع الدعوى عليه، ومغبة الوقوف موقف الاتهام، علاوة على أنه قد تساعد العدالة على معرفة الحقيقة وكشف الفاعل الحقيقي[40].

على أن الاستجواب لا يخلو من خطورة، لأنه ينطوي بذاته على رغبة في تضييق الخناق على المتهم، وقد يدفعه تعدد الأسئلة التي توجه إليه بغية استدراجه إلى أن يقول صدقا أم كذبا، أو ما ليس في صالحه، أو إلى اعتراف غير مطابق للواقع ومضلل للعدالة.

وعليه يجب إلمام المحقق في مرحلة الاستجواب بجرائم تقنية المعلومات وطرق ارتكابها، و مبادئ الحاسوب والإنترنت والمصطلحات المتعلقة بها، ومبادئ وأسس أمن المعلومات بالشكل الذي يمكنه من التواصل الجيد مع الشهود والمتهمين من جهة ومع خبير الحاسوب في فريق التحقيق من جهة أخرى، وربما كان الأسلوب الأمثل في عملية الاستجواب هو الذي يقوم على ضرورة حضور خبير الحاسوب لعملية الاستجواب ،و تمكينه من الإشتراك فيها بتوجيه

---

[39] حاحة عبد العالي وقلات سمية، المكافحة الإجرائية للجرائم الالكترونية –دراسة حالة الجزائر –، مجلة المفكر، المجلد 13/ العدد 2 (جانفي 2018)، ص 233.

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

الأسئلة الفرعية للشاهد أو المتهم، وربما قام بكتابة السؤال على قطعة من الورق ووضعها أمام المحقق ليقوم الأخير بتحين الفرصة المناسبة لإلقاء السؤال بما يتناسب والأصول الفنية للاستجواب[41].

أما القواعد المتبعة في المناقشة والاستجواب فتكاد تكون واحدة فيما يتعلق بضرورة عزل الشهود والمتهمين حتى لا يتأثر أحدهم بأقوال الآخر فيؤثر عليه، وكذلك في الترتيب الذي يتم بموجبه أخذ الأقوال وأيضا في ضرورة أن يكون المحقق قادرا على قراءة لغة الجسد، ونبرة الصوت، اللتين يستطيع من خلالهما[42].

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

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

المحور الثاني: القيمة الثبوتية للدليل الإلكتروني أمام القضاء الجزائي

منذ ثمانينات القرن الماضي التي شهدت ثورة تقنية المعلومات برزت ظاهرة جرمية غير معتادة رافقت خط المسار التاريخي الذي مرت به تقنية المعلومات نشأة وتبلورا وتطورا، فتم توظيف تقنية المعلومات الحديثة في الاحتيال على المصارف واعتراض بطاقات الائتمان وسرقتها واستخدامها غير المشروع والابتزاز والسطو على البنوك إلكترونيا والتزييف والتزوير والاحتيال الإلكتروني وتدمير الحسابات البنكية، ووجد العابثون من ذوي النزعة الاجرامية ضالتهم في استغلال هذه التقنية وتحقيق مآربهم عن طريقها، بدءا من جرائم الاعتداء على حق الإنسان في شرفه وسمعته اعتباره، وحقه في حرمة حياته الخاصة، مرورا بالجرائم الأخلاقية والاخلال بالآداب العامة، انتهاء بالإرهاب والتجسس وتهديد أمن الدولة، فقد تحول الإنسان إلى هدف من أهداف مجرمي التقنية الحديثة بعد أن أتاحت الثورة الرقمية تحقيق أغلب صور الاعتداء على الأشخاص من جنح بسيطة إلى جنايات كبرى بأبسط الأساليب.

وهكذا توجهت الأنظار إلى طائفة من الأفعال في بيئة تكنولوجيا المعلومات الحديثة التي تقتضي العمل على خلق إطار قانوني لها يقوم على تصنيفها وضبطها وخلق العقوبات الرادعة اللازمة لحماية البشر من تأثير وحماية النشاطات بكافة أنواعها، ذلك أن التكنولوجيا والقانون متلازمان وكل منهما يخدم الآخر فجرائم تقنية المعلومات الحديثة تعني تأثير هذه التكنولوجيا وأدواتها على القوانين الجزائية.

والولايات المتحدة كانت من بين الدول الأوائل التي أقرت مشروعية الدليل الالكتروني عن طريق تشريع قوانين لمكافحة جرائم التقنية في مختلف الولايات، ويمثل الفصل 18 من قانون الولايات المتحدة التشريع الرئيس لجرائم التقنية الحديثة، وقد استجاب الكونجرس لمشكلة جرائم تقنية المعلومات من خلال سن العديد من القوانين الفيدرالية كان أولها قانون الاحتلال وإساءة استخدام الكمبيوتر لعام 1984 وتم تعديله عام 1986 من أجل التعامل مع مشكلة "**الشفرة الخبيثة**" وغيرها من البرامج التي تهدف إلى تغيير أو إتلاف أو تدمير البيانات على نظام الحاسب.

وينص القسم 1030 من الفصل 18 على عدة أفعال من قبيل الجريمة: كالتوصل غير المصرح به (الدخول) سواء إلى أحد أنظمة الحاسب للحصول على معلومات خاصة بأموال محمية، أو إلى نظام حاسوب خاص بالحكومة الفدرالية الأمريكية، أو الدخول بمعنى الاحتيال أو مع تعمد إلحاق أضرار، أو الاتجار الاحتيالي في كلمات السر الحاسوبية وغيرها من المعلومات، أو تهديد بارتكاب ضرر لأي نظام حاسب محمي عبر الولايات أو للتجارة الأجنبية.

والتجربة الفرنسية في مجال مكافحة جرائم تقنية المعلومات الحديثة، ليست أقل نضجا من التجربة الأمريكية بل أن فرنسا من أوائل الدول التي تعاملت مع ظاهرة جرائم تقنية المعلومات تعاملا واقعيا بحيث استجابت لها مبكرا، وبهذا

الخصوص جرم المشرع الفرنسي الهجمات على نظم معالجة البيانات وانتهاك حقوق الأشخاص الناشئة عن الملفات أو البيانات الشخصية المعالجة، وخرق قواعد التشفير كما نص المشرع الفرنسي على الجرائم الواقعة باستخدام تكنولوجيا المعلومات، والخاصة بالجرائم الواقعة على الأشخاص كالاعتداء على القصر، أو نشر أو تثبيت أو نقل الصور الإباحية للقاصرين كما جرم فعل القوادة المتعلقة بالقاصرين باستخدام وسائل تكنولوجيا المعلومات وجرم أيضا تعريضها للخطر عبر تصنيع أو نقل أو تثبيت أو تداول أي محتوى صفحة عنيفة أو إباحية أو ذو طبيعة تسبب ضررا خطيرا بكرامة الإنسان[43] .

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.

والمشرع الجزائري وكغيره من التشريعات قام بإرساء جملة من المقومات التشريعية لمكافحة الجريمة المعلوماتية من خلال ما جاء به القانون 06-22 المؤرخ في 20/12/2006 المعدل والمتمم لقانون الإجراءات الجزائية الأمر(66/155) من خلال إجرائي التسرب واعتراض المراسلات، وكذلك بموجب إصدار قانون إجرائي خاص به القانون 09-04 المتضمن القوّاعد الخاصة بالوقاية من الجرائم المتصلة 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 المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بعنوان مراقبة الاتصالات الإلكترونية –الحالات التي تسمح باللجوء إلى الرقابة الإلكترونية.

الفرع الأول: تعريف المراقبة الإلكترونية

[43] مليكة أبوديار، المرجع السابق، ص 110.

تعد المراقبة الإلكترونية من أهم مصادر التحري التي غالبا ما يستعان بها في البحث والتقصي عن الجرائم الإلكترونية، فهي جزء لا يستغنى عنه في أعمال رجال البحث والتحري.[44]

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 الإنصات والتسجيل ومحلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة، أي سواء كانت مما يتبادله الناس في موّاجهة 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 شفوي باستخدام أي جهاز آخر.[45]

الفرع الثاني: شروط وآليات المراقبة الإلكترونية

يمكن أن نستنتج شروط وآليات المراقبة الإلكترونية في التشريع الجزائري من خلال نص المادة 65 مكرر 5 ق.إ.ج على أنها:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع ترتيبات تقنية دون موافقة المعنيين من أجل بث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخصية أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص أما المادة 04 من القانون رقم 09-04 فهي تشير إلى الجرائم الماسة بأمن الدولة.
- في حالة توفر المعلومات عن احتمال الاعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحري والتحقيق القضائي، عندما كان يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

---

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

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

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 القضائية 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 من إجراءات البحث والتحقيق الجديدة التي أرستها معظم تشريعات العالم الحديثة لمواجهة الجرائم الإلكترونية، وقد كانت اتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية سباقة إلى احتواء هذا الإجراء بنصها في المادة (20) على أساليب التحري الخاصة بما فيها التسرب الذي عبرت عنه بـ «الأعمال المستترة."[46]

أما المشرع الجزائري فقد تبنى بدوره هذا الإجراء، مباشرة عقب تصديق الدولة الجزائرية على اتفاقية منظمة الأمم المتحدة أعلاه بموجب المرسوم الرئاسي رقم 05-02 المؤرخ في 02/02/ 2002 بتحفظ واتفاقية مكافحة الفساد لسنة 2003 بتاريخ 19/ 04/ 2004.

الفرع الأول: التسرب

وهو الإجراء المستحدث الذي تنص عليه المواد من 65 مكرر 11 إلى مكرر 18 من قانون الإجراءات الجزائرية.

أولا تعريفه:

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

---

[46] 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

– الحصول على إذن مكتوب ومسبق من طرف وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية يتضمن الإذن؛ الجريمة التي تبرر اللجوء للتسرب وهوية ضابط الشرطة المنسق للعملية وتحديد المدة إذ لا تتجاوز 4 أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق.

– أن تكون الجريمة ضمن الجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 05 من قانون الإجراءات الجزائية ومن ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ثالثا– مراقبة إجراءات التسرب:

يراقب التسرب وكيل الجمهورية 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 مستخدما في ذلك أسماء أو صفات وهيئات مستعارة وهمية سعيا منه للاستفادة منهم في كيفية اقتحام الهاكر للموقع، أو القيام بحلقات اتصال مع المشتبه فيهم عن طريق البريد الإلكتروني.

ولا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة والمتمثلة حسب أحكام المادة (65 مكرر 11 ق إ ج) في ووكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه، على أن تتم العملية تحت الرقابة المباشرة للجهة الصادرة للإذن حسب الحالة لتلافي حدوث تجاوزت وتعسف في استعمال هذا الحق[47].

الفرع الثاني: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

[47] براهيمي جمال، المرجع السابق، ص 85–86.

يتعلق الأمر بمسألة بالغة الأهمية كونها تشكل انتهاكا لحرمة المراسلات التي كفلها الدستور الجزائري، غير أن المشرع الجزائري قد سمح بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وذلك إذا اقتضت به ضرورة التحري في الجريمة المتلبس بها في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... إلخ، ويلاحظ من نص هذه المادة أن المشرع الجزائري قد يسمح بهذا الإجراء في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حتى تتمكن جهات التحقيق من استخلاص أدلة الإثبات والوصول إلى الحقيقة.

كما أشار إليه المشرع الجزائري في نص المادة 03 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على النحو التالي: "مع مراعاة القوانين التي تراعي سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحري أو التحقيقات القضائية حماية النظام العام وفق القواعد المنصوص عليها في الإجراءات الجزائية في هذا القانون ووضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة" ولقد كانت وسائل الاتصال في السابق تتمثل في الهاتف أما في الوقت الحاضر فانتقلت إلى البريد الإلكتروني وغرف الدردشة عبر الإنترنت، ونجد أن المشرع الجزائري قد عرف المراسلات في المادة 09 من القانون 03-2000 بأنها: "اتصال مجسد بشكل كتابي عبر مختلف الوسائل المادية التي يتم توصيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، وعرف وسائل الاتصال الإلكتروني بأنها الوسائل التي "ترسل أو إرسال أو استقبال أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية" ولهذا فإن مراقبة الاتصال على الإنترنت أو محتوى البريد الإلكتروني يعتبر جريمة يعاقب عليها القانون لاتصالها بحرّمة الحياة الخاصة وهذا ما أشار إليه المشرع في المادة 137من قانون 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

استقر الفقه والقانون الوضعي على أن للقاضي سلطة واسعة في تقدير الأدلة واستنباط القرائن وما تحمله الوقائع من دلالات، شريطة أن يكون الدليل ثابتا بيقين، مرتبطا بالوقائع الرئيسية منسجما مع التسلسل المنطقي للأحداث، وعليه ينبغي أن ينسجم هذا الرأي مع الأدلة الجنائية الرقمية باعتبارها أحد الأدلة المادية العلمية، بل أكثر منها حجية في الإثبات، لأنها محكمة بقواعد علمية وحسابية قاطعة لا تقبل التأويل، كما أنها معالجة بوسائل التقنية المعلوماتية التي أصبحت تستغل في الجرائم السيبرانية المستحدثة (والافتراضية، أي: الإلكترونية) ورغم عدم توفر التشريعات الموضوعية

والشكلية التي تنظم التعامل مع الحاسب الآلي وتقنية المعلوماتية، لم تواجه المحاكم مشكلة في تعاملها مع الأدلة الجنائية الرقمية، وذلك للأسباب الآتية:

1. الثقة التي اكتسبها الحاسب الآلي والكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف المجالات، وارتباط الأدلة الجنائية الرقمية وآثارها بالجريمة موضوع المحاكمة، ووضوح الأدلة الرقمية ودقتها في إثبات العلاقة بين الجاني والمجني عليه، أو بين الجاني والسلوك الإجرامي.

2. إمكانية تعقب آثار الأدلة الرقمية والوصول إلى مصادرها بدقة، وقيام الأدلة الرقمية على نظريات حسابية مؤكدة لا يتطرق إليها الشك، ما يقوى يقينية الأدلة الرقمية.

3. انتهاء العلم برأي قاطع إلى صحة النتائج التي توصلت إليها علوم الحاسب الآلي.

4. الأدلة الجنائية الرقمية يدعمها عادة رأي خبير، وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة وفحصها وتقييمها وعرضها أمام المحاكم وفق شروط وقواعد نظمها القانون وأقرها القضاء.

5. انتشار الجريمة الافتراضية **Cyber Crime** جرائم التقنية العالية **High – tech crime** كظاهرة مستحدثة لم يترك مجالا للبحث عن وسائل لتحقيق العدالة في سياق تلك الأنماط من السلوكيات إلا من خلال ذات التقنية الافتراضية.

وقد ظهرت بوادر الأخذ بالبيئة السمعية والمرئية عن بعد من خلال التحقيقات في أخذ أقوال الشهود وإيضاحات الصور والبيانات الموضحة لأية جرائم معلوماتية أو تقليدية بواسطة الوسائل الحديثة.

وبناء على تلك القواعد تعد التقارير والمعلومات والبيانات المحفوظة في أي شكل، وكذا الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بواسطة أشخاص ذوي معرفة وخبرة في نطاق الأنشطة والممارسات المنظمة بينة مقبولة أمام المحاكم الجنائية لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، والأدلة الجنائية الرقمية من هذا القبيل، لكونها معدة بعمليات حسابية دقيقة لا يدخل إليها الشك ويتم حفظها آليا بأسلوب علمي[48]

المطلب الأول: مفهوم الدليل الرقمي

يلعب الدليل الجنائي بشكل عام دورًا هامًا، في ظهور الحقيقة المتعلقة بالوقائع محل التحقيق أو المحاكمة، وهو حجر الأساس الذي تقوم عليه الدعوى في كثير من الأحيان، كما يلعب الدليل الجنائي دورًا محوريًا في تكوين عقيدة القاضي.

الفرع الأول: تعريف الدليل الرقمي:

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

هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون.

أو هو مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية[49].

الفرع الثاني: خصائص الدليل الرقمي

- يعتبر الدليل الرقمي دليلا غير ملموس أي هو ليس دليلا ماديا، فهو-أي الدليل الرقمي- تلك المجالات المغناطيسية أو الكهربائية، ومن ثم فإن ترجمة الدليل الرقمي وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل أن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيأة التي يمكن الاستدلال بها على معلومة معينة.

- يعتبر الدليل الرقمي من قبيل الأدلة الفنية أو العلمية، وهو من طائفة ما يعرف بالأدلة المستمدة في الآلة.
- إن فهم مضمون الدليل الرقمي يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه، ولذلك فكل ما لا يمكن تحديده وتحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلا رقميا، وذلك لعدم إمكانية الاستدلال به على معلومة معينة، ما يعدم قيمته التدليلية في إثبات الجريمة ونسبتها إلى الجاني.

الفرع الثالث: مميزات الدليل الرقمي

- يتميز الدليل الرقمي بصعوبة محوه أو تحطيمه، حتى في حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوي ذلك الدليل.
- إن محاولة الجاني محو الدليل الرقمي بذاتها تسجل عليه كدليل، حيث إن قيامه بذلك يتم تسجيله في ذاكرة الآلة وهو ما يمكن استخراجه واستخدامه كدليل ضده.
- إن الطبيعة الفنية للدليل الرقمي تمكِّن من إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للعبث والتحريف.

---

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

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[50]:

أ. أدلة أعدت لتكون وسيلة إثبات:

وهذا النوع من الأدلة الرقمية يمكن إجماله فيما يلي:

- السجلات التي تم إنشاؤها بواسطة الآلة تلقائيًا، وتعتبر هذه السجلات من مخرجات الآلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.

- السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة وتتمُّ معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.

ب. أدلة لم تعد لتكون وسيلة إثبات:

وهذا النوع من الأدلة الرقمية نشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغبا في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهي ما يمكن تسميه أيضاً بالآثار المعلوماتية الرقمية، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية.

والواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها، فالاتصالات التي تجري عبر الانترنت والمراسلات الصادر عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك.

الفرع الخامس: أشكال الدليل الرقمي

الأصل أن الدليل الرقمي غير مادي يتكون من بيانات ومعلومات ذات هيئة رقمية غير ملموسة وإخراجه في شكل مادي ملموس يتطلب الاستعانة بأجهزة الحاسب الآلي وأدواته واستخدام نظم برمجية حاسوبية، ويتميز بالسرعة والسهولة وصعوبة محوه أو تحطيمه، وإن حاول الجاني محو الدليل الرقمي، فإن هذه المحاولة بذاتها تسجل عليه كدليل[51].

---

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

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

أ. **الصور الرقمية**: وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة للصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطوراً ولكنها ليست بالصورة الأفضل من الصور التقليدية.

ب. **التسجيلات الصوتية**: وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الإنترنت والهاتف.... الخ.

ج- **النصوص المكتوبة**: وتشمل النصوص التي يتم كتابها بواسطة الآلة الرقمية، ومنها الرسائل عبر البريد الإلكتروني، والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسب الآلي، الخ...

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 قبول أو عدم قبول أي دليل بما في ذلك الدليل التقني[52].

ويقصد بمشروعية الوجود أن يكون الدليل معترف به، معنى أن يكون القانون يجيز للقاضي الإستناد إليه لتكوين عقيدته للحكم بالإدانة، ويمكن القول إن النظم القانونية تختلف في موقفها من الأدلة التي تُقبل كأساس للحكم بالإدانة بحسب الاتجاه الذي تتبناه، فهناك اتجاهان رئيسان؛ الأول نظام الأدلة القانونية، والثاني نظام الإثبات الحر.

أولا – نظام الأدلة القانونية:

يمتاز نظام الأدلة القانونية بالدور الرئيسي الذي يقوم به المشرع في عملية 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

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

الأخير على الحرص على تطبيق القانون من حيث توافر الدليل وشروطه، فدور القاضي إذا مجرد عملية حسابية بحتة يجب عليه تطبيقها[53].

فوفقا لهذا النظام فإن المشرع هو الذي يحدد حصرا الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات، كما يحدد القيمة الإقناعية لكل دليل، بحيث يقتصر دور القاضي على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون، فلا سبيل للاستناد إلى أي دليل لم ينص القانون عليه صراحة ضمن أدلة الإثبات، كما أنه لا دور للقاضي في تقدير القيمة الإقناعية للدليل، ولذا يسمى هذا النظام بنظام الإثبات القانوني أو المقيد، حيث إن القانون قيد القاضي بقائمة من الأدلة التي حددت قيمتها الاثباتية، وهذا النظام ينتمي للنظم ذات الثقافة الأنجلوسكسونية، مثل المملكة المتحدة "بريطانيا " والولايات المتحدة الأمريكية، ولذا فإن النظم التي تتبنى هذا النظام لا يمكن في ظلها الاعتراف للدليل الرقمي بأية قيمة إثباتية ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته الاثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لتكوين عقيدته.

وتطبيقا لهذا الفهم نص قانون الإثبات في المواد الجنائية البريطاني على قبول الدليل الرقمي وحدد قيمته الاثباتية اتفاقا وطبيعة النظام القانوني في بريطانيا.

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.[54]

ويمكن أن يعاب على نظام الإثبات القانوني أن من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون، ولذلك فإن هذا النظام بدأ ينحصر نطاقه حتى في الدول التي تعتبر الأكثر اعتناقا له، فنجد بريطانيا مثلاً قد بدأت تخفف من غلوائه، حيث ظهر فيها ما يعرف بقاعدة الإدانة

---

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

[54] يقاش فراس، المرجع نفسه، ص 382.

دون أدنى شك، والتي مفادها أن القاضي يستطيع أن يكوُّن عقيدته من أي دليل وإن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعا في دلالته.

ثانيا – نظام الإثبات الحر:

يسود الإثبات الحر في ظل الأنظمة اللاتينية، ووفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة بشأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للإستناد إليها في تكوين قناعته، فله أن يبنى هذه القناعة على أي دليل وإن لم يكن منصوصا عليه، بل إن المشرع في مثل هذا النظام لا يحفل بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، والقاضي هو الذي يختار من بين ما يُطرح عليه ما يراه صالحا للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يطمئن إليه، فالمشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، فعلى الرغم من توافر شروط الصحة في الدليل إلا أن القاضي يملك أن يرده تحت مبرر عدم الاقتناع، و لذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في مجال الإثبات في مقابل انحسار 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.[55]

وعليه فإنه في مثل هذا النظام لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود، على اعتبار أن المشرع لا يُعهد عنه سياسة النص على قائمة لأدلة الإثبات، ولذلك فمسألة قبول الدليل الرقمي لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي.

إذا وفقا لهذا النظام فإن الأصل في الأدلة مشروعية وجودها، فالدليل الرقمي سيكون مشروعاً من حيث الوجود استصحاباً للأصل.

ثالثا – حجية الدليل الرقمي أمام القضاء الجنائي الجزائري:

إن مجرد الحصول على الدليل الرقمي وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، فالطبيعة الفنية الخاصة للدليل الرقمي تُمكِّن من العبث بمضمونه على نحو يحرِّف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، فضلاً عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية

---

[55] يقاش فراس، المرجع السابق، ص 384.

في مثل هذا النوع من الأدلة، ولذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي، فهل من شان ذلك استبعاد الدليل الرقمي من دائرة أدلة الإثبات الجنائي لتعارضه وقرينة البراءة.

ففي ظل النظم القانونية التي تعتمد النظام اللاتيني في الإثبات فإن القاضي يملك سلطة واسعة في تقييم الدليل من حيث قيمته التدليلية، فللقاضي قبول الدليل أو رفضه وهو يعتمد في ذلك على مدى اقتناعه الشخصي بذلك الدليل.

ولم ينص المشرع الجزائري صراحة على قبول الدليل الإلكتروني ، وهذا على الأساس يمكن الاعتماد على نص 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؛ ما لم يرد نص مخالف يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناء على اقتناعه الشخصي، وفي المقابل ينص قانون الإجراءات بجواز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي نص فيها القانون على خلاف ذلك، وللقاضي أن يصدر حكمه وفقا لاقتناعه الخاص، ولا يصوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه.

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 الفيزيائي، والتخلي شيئا فشيئا عن عدة قيود تحد من الإثبات في البيئة التقنية 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[56].

المطلب الثاني: وسائل تقييم الدليل الرقمي

سوف نتناول وسائل تقييم الدليل الرقمي من حيث سلامته من العبث، ثم وسائل تقييمه من حيث سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية وذلك على النحو التالي:

الفرع الأول: تقييم الدليل الرقمي من حيث سلامته من العبث

يمكن التأكد من سلامة الدليل الرقمي من العبث بعدة طرق نذكر منها:

- لعب علم الكمبيوتر دوراً مهماً في تقديم المعلومات الفنية التي تساهم في فهم مضمون وهيئة الدليل الرقمي، وهذه العلوم يستعان بها في كشف مدى التلاعب بمضمون هذا الدليل، وتبدو فكرة التحليل التناظري الرقمي من الوسائل المهمة للكشف عن مصداقية الدليل الرقمي، ومن خلالها تتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا.

- حتى في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي أو في حالة أن العبث قد وقع على النسخة الأصلية، ففي الإمكان التأكد من سلامة الدليل الرقمي من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات.

- هناك نوع من الأدلة الرقمية يسمى بالدليل المحايد، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يساهم في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول تعديل أو تغيير في النظام (الكمبيوتري).

فمن خلال هذه الطرق يمكن التأكد من سلامة الدليل الرقمي ومطابقته للواقع.

الفرع الثاني: تقييم الدليل الرقمي من حيث السلامة الفنية للإجراءات المستخدمة في الحصول على الدليل الرقمي

عادة تتبع جملة من الإجراءات الفنية للحصول على الدليل الرقمي، وهذه الإجراءات من الممكن أن يعتريها خطأ قد يشكك في سلامة نتائجها، ولذا فإنه يمكن في هذا الشأن اعتماد ما يعرف باختبارات (داو بورت) كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الرقمي من حيث إنتاجها لدليل تتوافر فيه المصداقية

---

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

لقبوله كدليل إثبات، ولذا فإننا سنعرض باختصار للخطوات التي تتبع للتأكد من سلامة هذه الإجراءات من الناحية الفنية:

أ – إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المبتغاة، وذلك بإتباع اختبارين رئيسين هما:

– اختبار السلبيات الزائفة: ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي، وأنه لا يتم إغفال بيانات مهمة عنه.

– اختبار الايجابيات الزائفة: ومفاد ذلك أن تخضع الأداة المستخدمة في الحصول على الدليل الرقمي لاختبار فني يمكِّن من التأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة.

وبذلك يتم من خلال هذين الاختبارين التأكد من أن الأداة المستخدمة عرضت كل البيانات المتعلقة بالدليل الرقمي وفي ذات الوقت لم تضِف إليها أي بيان جديد، وهذا يعطي للنتائج المقدمة عن طريق تلك الآلة مصداقية في التدليل على الواقع.

ب– الإعتماد على الأدوات التي أثبتت البحوث العلمية كفاءتها في تقديم نتائج أفضل:

حيث تدل البحوث المنشورة في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل الرقمي، وفي المقابل تثبت تلك الدراسات الأدوات المشكوك في كفاءتها، وهذا يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات[57].

ومن خلال ما تقدم يمكن الوقوف على سلامة الدليل الرقمي، فإذا توافرت في الدليل الرقمي الشروط العامة لما يمكن أن يمثل أساسا لانبعاث الثقة فيه، فإنه قد يبدو من غير المقبول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على بساط البحث، فالدليل الرقمي بوصفه دليلاً علمياً فإن دلالته قاطعة بشأن الواقعة المستشهد به عنها، فإذا سلمنا سابقاً بإمكانية التشكيك في سلامة الدليل الرقمي بسبب قابليته للعبث و نسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنهما برأي حاسم وإن لم يقطع به أهل الاختصاص، ولذلك فإذا توافرت في الدليل الرقمي الشروط المذكورة سابقاً بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استناداً لسلطة القاضي التقديرية وفقاً للمادة، إذ سلطة القاضي في رد الدليل استناداً لفكرة الشك يلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك في الدليل، وهو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة، بحيث يقتصر دور القاضي على بحث صلة الدليل بالجريمة.

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

ولا شك أن الخبرة تحتل في هذه الحالة دروا مهما في التثبت من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، فبحث مصداقية هذا الدليل هي من صميم فن الخبير لا القاضي.

ويجب التنويه إلى أنه لا يمكن اعتبار هذه القيمة التي ندعيها للدليل الرقمي بمثابة خروج مستحدث عن القواعد العامة للإثبات الجنائي في القانون، حيث إن هناك من الأدلة ما لا يستطيع القاضي الجنائي تقديرها وفقاً لسلطته المقررة بالمادة (212) كمحاضر المخالفات مثلا.

وهنا ننوه إلى عدم الخلط بين الشك الذي يشوب الدليل الرقمي بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه وبين القيمة الإقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية فالقول فيها هو قول أهل الخبرة، فإن سلم الدليل الرقمي من العبث والخطأ، فإنه لن يكون للقاضي سوى القبول بهذا الدليل ولا يمكنه التشكيك في قيمته التدليلية.

لكونه وبحكم طبيعته الفنية يمثل إخبارا صادقاً عن الواقع، ما لم يثبت عدم صلة الدليل الجريمة المراد إثباتها[58].

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

يقصد بحجية الدليل الإلكتروني ما يتمتع به من القوة الاستدلالية في كشف الحقيقة وصدق نسبة الفعل الإجرامي إلى شخص معين أو كذبه، لذلك فبمجرد الحصول على الدليل وتقديمه إلى القضاء لا يكفي لاعتماده كدليل إدانة، إنما ينبغي تقديره وفحص قيمته في إثبات الواقعة الإجرامية، ومسألة تقييم الدليل هي مسألة موضوعية محضة تدخل في صميم سلطة القاضي التقديرية بحثا عن الحقيقة، فالسائد في الفقه أن سلطة القاضي الجزائي في تقدير الدليل يحكمها مبدأ حرية القاضي في تكوين قناعته، مما يستتبع ذلك حتما نتيجة مهمة ألا وهي "حرية القاضي في تقدير الأدلة"، وعملا بهذا المبدأ فالقاضي الجزائي كما يصح له أن يؤسس اقتناعه على أي دليل، له أن يهدره أيضا.

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.

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

ولا شك أن تطبيق ذلك على الدليل الإلكتروني قد يثير عدة صعوبات، فالقاضي الجزائي بثقافته القانونية وعدم كفاءته الفنية في مجال المعلوماتية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الإلكتروني، فضلا عن تمتع هذا الدليل في قوته التدليلية بقيمة إثباتية قد تصل إلى حد اليقين شأنه في ذلك شأن الأدلة العلمية عموما، ناهيك عن الطبيعة الفنية الخاصة بالدليل الإلكتروني والتي تمكن من العبث بمضمونه بسهولة على نحو يحرف الحقيقة دون أن يكون بمقدور غير المتخصص إدراك ذلك.

وبوجود هذه الصعوبات وغيرها يطرح تساؤل مهم عن مدى سلطة القاضي الجزائي في تقدير ومناقشة الدليل الإلكتروني في مصداقيته وبالتالي قبوله أو رفضه لعدم اقتناعه به؟

وعلى هدى ما سبق طرحه سوف نستعرض الشروط الواجب توفرها في الدليل الالكتروني حتى يعبر عن حقيقة علمية محققة الحجية (الفرع الأول) ثم نبرز دور ذلك في تكوين الاقتناع الشخصي للقاضي الجزائي (الفرع الثاني).

الفرع الأول: شروط اكتساب الدليل الإلكتروني 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.[59]

والدليل الالكتروني ما هو إلا تطبيق من تطبيقات الدليل العلمي الذي يعبر عن حقيقة علمية ثابتة، فهو يتمتع بحجية قوية في الإثبات، وذلك بما يتميز به من موضوعية وحياد، ولكونه محكما بقواعد علمية حسابية قاطعة لا تقبل التأويل مما يقوي يقينيته، ويساعد القاضي في التقليل من الأخطاء القضائية والاقتراب أكثر إلى تحقيق العدالة، والتوصل بدرجة أكبر من الحقيقة، لأن التقنية العلمية قد توفر طرقا دقيقة لجمع الأدلة ذات قوة علمية يصعب إثبات عكسها.

ومع هذا فرغم أن الدليل الإلكتروني بحكم طبيعته العلمية وموضوعيته وحياده يمثل إخبارا صادقا عن الواقع، إلا أن ذلك لا يستبعد أن يكون موضع شك في سلامته من العبث عن طريق التحريف أو التغيير من ناحية، وفي صحة الإجراءات المتبعة للحصول عليه من ناحية أخرى.

---

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

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 المستخرجة من الحاسوب والإنترنت أن تكون غير قابلة للظن، ولهذا اشترط قانون البوليس والإثبات في بريطانيا لسنة، 1984م "أنه لتحقيق يقينية الأدلة الإلكترونية أن تكون البيانات المستخرجة دقيقة وناتجة عن الحاسوب بصورة سليمة".

وأن الدليل الرقمي يتمتع من جهة قوته القانونية بقيمة إثباتية تصل إلى حد اليقين، وهذا لا يعني ألا يكون الدليل الرقمي موضع 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[60].

فالأدلة الجنائية الرقمية يدعمها عادة رأي خبير، وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة وفحصها وتقييمها وعرضها أمام المحاكم وفق شروط وقواعد نظمها القانون وأقرها القضاء[61].

ويعتمد القاضي الجزائي عادة لبلوغ اليقين والجزم في اقتناعه بالأدلة على نوعين من المعرفة، الأولى هي المعرفة الحسية التي تستنبط من الحواس بعد معاينته لهذه المخرجات وفحصها، أما الثانية فهي المعرفة العقلية التي يدركها القاضي عن طريق التحليلات، والاستقراءات والاستنتاجات التي يجريها على المخرجات الإلكترونية وربطها بالملابسات التي أحاطت بها.

فإن لم ينته القاضي إلى الجزم بنسبة الجريمة الإلكتروني إلى المتهم تعين عليه القضاء بالبراءة، لأن الشك يفسر لصالح المتهم.

وحتى يتحقق اليقين للأدلة الإلكترونية أكثر ينبغي إخضاعها للتقييم الفني بوسائل فنية من طبيعة هذا الدليل تمّكن من فحصه للتأكد من سلامته من العبث، وكذا صحة الإجراءات المتبعة في الحصول عليه، فمثلما يخضع الدليل الإلكتروني لقواعد وإجراءات معينة تحكم طرق الحصول عليه، فإنه يخضع كذلك لقواعد أخرى تحكم على قيمته التدليلية من الناحية العلمية، ولعل من أهم هذه الوسائل ما يلي:

---

[60] طارق عبد الرحيم الرdايدة، المرجع السابق، ص 172.

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

ـــ تقييم الدليل الإلكتروني في سلامته من العبث:

إن الطبيعة التقنية للدليل الالكتروني تجعله في الغالب عرضة للشك والظنون في سلامته، وذلك راجع إلى إمكانية تعرضه للعبث والخروج به على نحو يخالف الحقيقة، فقد يقدم هذا الدليل ليعبر عن واقعة معينة صنع خصيصا من أجل التعبير عنها خلافا للحقيقة، وذلك دون أن يكون بمقدور غير المتخصص إدراك ذلك العبث، على نحو يمكن القول معه أن ذلك قد أصبح هو الشأن في النظر لسائر الأدلة التقنية التي تقدم للقضاء، فالتقنية الحديثة تمكن من العبث بالدليل الإلكتروني التقني بسهولة و يسر ليظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة.

ولأجل التأكد من سلامة الدليل الإلكتروني من التغيير أو العبث تتم الاستعانة عادة بمجموعة من الآليات التالية:

أ ـ تقنية التحليل التناظري الرقمي: وهي تقنية يتم من خلالها مقارنة الدليل الرقمي المقّدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثمة يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا، ويستعان في ذلك بتكنولوجيا الإعلام الآلي التي أثبتت دورها الفعال في تقديم المعلومات الفنية التي تساهم في فهم مضمون وكينونة الدليل التقني، وكشف مدى التلاعب بمضمون هذا الدليل.

ب ـ استخدام عمليات حسابية خاصة تسمى بالخوارزميات[62]: ويتم اللجوء إلى هذه العملية عادة في حالة عدم الحصول على النسخة الأصلية للدليل الإلكتروني أو في حالة ما إذا كان هناك شك في أن العبث قد مّس النسخة الأصلية، فهنا تسمح هذه التقنية بالتأكد من مصداقية الدليل الالكتروني وسلامته من العبث بالتبديل أو التحريف.

ج ـ استخدام الدليل المحايد: وهو نوع من الأدلة الإلكترونية الرقمية المخزنة في البيئة الإفتراضية ولا علاقة له بموضوع الجريمة، ولكنه يساهم في التحقق من مدى سلامة الدليل الإلكتروني المقصود في عدم وقوع تعديل أو تغيير في نظام الحاسوب.

2 ـ تقييم الدليل الإلكتروني في السلامة الفنية لإجراءات تحصيله إذا كانت نسبة الخطأ الفني في الحصول على الدليل الإلكتروني ضئيلة جدا باعتباره تطبيقا من تطبيقات الدليل العلمي الدقيقة كما أسلفنا الذكر، فذلك لا يعني أنها منعدمة تماما، إنما يظل الوقوع في الخطأ ممكنا أثناء استخلاصه، ويكون ذلك إما بسبب الخطأ في استخدام الأداة المناسبة لاستخلاص الدليل، كالخلل في الشفرة المستخدمة، أو استعمال معلومات ومواصفات خاطئة.

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

وإما بسبب الخطأ في استخدام أداة تقل نسبة صوابها عن مائة بالمائة (100%)، مثل ما يحدث غالبا في وسائل اختزال المعطيات أو معالجتها بطريقة تختلف 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 يؤسس اقتناعه على العناصر الإثباتية التي طرحت أمامه في جلسات المحاكمة وخضعت لحرية المناقشة من طرف أطراف الدعوى جميعهم[63].

وتحقق شرط سلامة الدليل الإلكتروني من العبث وسلامته من الخطأ في إجراءات التحصيل وحده لا يكفي لاكتسابها حجة دامغة في الإثبات، بل لابد أيضا من مناقشة هذا الدليل بصفة علانية في جلسة المحاكمة وفقا لمبدأ أساسي في الإجراءات الجزائية هو مبدأ الشفوية والمواجهة، فلا يجوز للقاضي الجزائي أن يأخذ بدليل قدمه أحد أطراف الدعوى أو يبني حكمه على أساسه إلا إذا عرضه شفويا في جلسة المحاكمة ليعلم به سائر أطراف الدعوى، فتتاح لهم مناقشته والرد عليه وإبداء آرائهم في قيمته القانونية.

ويترتب عن 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 لا يجوز للقاضي الجزائي أن يبني اقتناعه على رأي الغير، إلا إذا كان من الخبراء والفنيين الذين استشارهم وفقا للقانون وارتاح ضميره لرأيهم فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه.

وعليه فإذا كان القاضي لا يمكنه أن يحكم في الجرائم الإلكترونية استنادا إلى علمه الشخصي، أو استنادا إلى أري الغير كما أسلفنا الذكر، فذلك يحتم عليه أن يعيد تحقيق و مناقشة كافة الأدلة المتولدة من الحاسبات الإلكترونية القائمة في ملف الدعوى لكي يتمكن من تكوين إقناع يقربه نحو الحقيقة الواقعية التي يصبو إليها كل قاض عادل، فمثلا بالنسبة لشهود الجرائم المعلوماتية الذين تم سماعهم من قبل في التحقيق الابتدائي فإنه يجب إعادة سماعهم مرة أخرى أمام محكمة الموضوع، كذلك بالنسبة لخبراء المعلوماتية على اختلاف تخصصاتهم ينبغي أن يمثلوا أمام المحكمة لمناقشة تقاريرهم التي

---

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

خلصوا إليها لأنه بهذا التصرف يكون القاضي قد حقق رقابة فعالة على جدية الأدلة التي تكون قد حصلت في مرحلة التحقيق فتعرض عليه مجددا، وهو ما يتيح له مراقبة التقدير الذي كانت سلطة التحقيق قد خلصت إليه بخصوص وقائع الجريمة الإلكترونية[64].

واعتبارا لذلك، أرست معظم تشريعات العالم هذه القاعدة وجعلتها عنصرا جوهريا لقبول أي دليل، فنجد الفقرة الثانية من المادة (427) من قانون الإجراءات الجنائية الفرنسي تنص على أنه "لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة و نوقشت أمامه في مواجهة الأطراف" وفي السياق نفسه نصت المادة (302) من قانون الإجراءات الجنائية المصري أنه "لا يجوز للقاضي أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة" أما المشرع الجزائري فقد تبنى شرط مناقشة الأدلة ضمن الفقرة الثانية من المادة (212) من قانون الإجراءات الجزائية بالصيغة التالية "لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

وتبدو المشكلة بالنسبة لمناقشة الأدلة الإلكترونية في كون معظم هذه الأخيرة تعتبر أدلة غير مرئية بالعين المجردة وتسجل على وسائل إلكترونية لا يمكن قراءتها أو استخراجها إلا باستعمال أجهزة إلكترونية، فضلا عن إمكانية التلاعب في المعلومات المسجلة بمسحها أو استبدال غيرها دون علم أحد، وهو ما يثير التساؤل عن إمكانية المناقشة العلنية لهذه الأدلة في أصالتها، ومدى تأثير ذلك على مبدأ قبوله من طرف القضاء، خاصة إذا تعلق الأمر بالدليل المستخرج بواسطة الطابعات، أو المسترجع بعدما تم حذفه باستخدام خاصية الإلغاء، أو عندما يقوم المتهم بإزالة الدليل الرقمي عن بعد، فيكون ما تبقى منه مجرد نسخة يتم التوصل إليها عن بعد بطريق المراقبة الإلكترونية، وفي هذه الحالة هل يمكن اعتبار الدليل المسترجع أو الناتج عن المراقبة الإلكترونية دليلا أصليا وبالتالي يقبل طرحه على القضاء ومناقشته ضمن أدلة الدعوى؟

ومن أجل الفصل في هذه المسألة من الناحية القانونية، عمدت بعض التشريعات المقارنة إلى اعتماد منطق افتراض أصالة الدليل الإلكتروني الرقمي، إذ نص قانون الإثبات الأمريكي في المادة (3/1001) على أنه " إذا كانت البيانات مخزنة في حاسب أو آلة مشابهة فإن أية مخرجات مطبوعة منها أو مخرجات مقروءة برؤية العين تبرز انعكاسا دقيقا للبيانات تعد بيانات أصلية" وتضيف المادة (5/1500) من قانون الإثبات لولاية كاليفورنيا لعام 1983 بأن "المعلومات المسجلة بواسطة الحاسب أو برامج الحاسب، أو نسخ أيهما، يجب ألا توصف أو تعامل على أنها غير

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

مقبولة بمقتضى قاعدة –أفضل دليل–" وقد ذهب المشرع الأمريكي إلى أبعد من ذلك، فاعترف للنسخة طبق الأصل بنفس القيمة الثبوتية للنسخة الأصلية، وكذلك فعل المشرع الانجليزي والياباني بقبوله ضمن أدلة الإثبات مخرجات الحاسب الآلي التي تم تحويلها إلى صور مرئية، سواء كانت هي الأصل أم كانت نسخا مستخرجة عن هذا الأصل، أما المشرع الألماني فقد جعل من خلال المادة (224) فقرة ثانية من قانون الإجراءات الجزائية مخرجات الحاسب الآلي بأنواعها المختلفة من بيانات أو مطبوعات أو نسخ من قبيل المصادر التي يجب على المحكمة قبولها في الإثبات[65].

وهو الشيء نفسه الذي تبناه المشرع اليوناني في المادة (364) من قانون الإجراءات الجزائية.

ولعل ما دفع هذه الدول إلى التسليم بمنطق افتراض الأصالة في الدليل الإلكتروني الرقمي على المستوى القانوني هو الطبيعة التقنية لهذا الدليل التي لا تعبر عن قيمة أصلية بمجرد رفع محتواه من النظام المعلوماتي إذ يظل متواجدا في المكان الذي تم استخلاصه واستدعاؤه منه.

ونخلص إلى أنه إذا كان القانون يشترط لاكتساب الدليل الإلكتروني حجية في الإثبات أن يخضع لمناقشة علانية في جلسة المحاكمة، فإن دور القاضي في ذلك يبقى محدودا جدا بسبب النقص الفادح في ثقافته المعلوماتية، وهو ما جعل البعض يعتقد أنه بمقدار اتساع مساحة الأدلة الإلكترونية يكون انكماش وتضاءل دور القاضي الجزائي في التقدير، مما يستتبع بالقول أن التطور العلمي من شأنه أن يطغى على نظام الاقتناع القضائي ولا يبقى للقاضي إلا الإذعان للخبراء المختصين دون أي تقدير من جانبه.

ومثل هذا الأمر يدفعنا إلى البحث في دور الطابع العلمي للدليل الإلكتروني في تكوين الاقتناع الشخصي للقاضي الجزائي[66].

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

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

المحور الثالث: عقبات التحقيق الجنائي في الجرائم الإلكترونية

لعل من أهم العناصر التي ترتبط بالجريمة هو مسرحها أو مكان وقوع أركانها، وهو العنصر الرئيسي لضبط وتحري الجريمة وملاحقة مرتكبيها، وهذا هو الحال نفسه فيما يتعلق بالجريمة الإلكترونية، حيث أن مسرحها متوفر وحتى إن كان مختلفا عن المسرح المادي للجريمة التقليدية كونه مسرحا معنويا، فتجول الشخص في الشبكة العنكبوتية يعني أن يترك آثار معنوية في الموقع الذي يزوره، إذ يتم تحديد عنوانه الإلكتروني الدائم له، ويتم تحديد نوع الجهاز الذي يستخدمه والمكان الذي يدخل منه.

ويمكن تتبع هذه العناصر بطرق بسيطة أحيانا وبعضها متوفر للمستخدمين العاديين والتي تكشف معلومات المستخدم ويجعلها متاحة لأي شخص يود تتبع تحركات المجرم، فضلا عن أن يقوم بذلك المتخصصون وحتى أن جهاز المجرم الشخصي نفسه يحتفظ بملفات الكوكيز للمواقع التي دخلها.

ولعل الأمر ليس بهذا القدر من البساطة، فيمكن اكتشاف المجرمين البسطاء ربما بمثل هذه الطرق، أما المجرمون المتخصصون بل وحتى الهواة منهم فيقومون بمحو اثارهم التي تم تسجيلها من خلال عدة طرق، منها: مسح ملفات الكوكيز الموجودة على أجهزتهم، وأيضا القيام بإخفاء عناوينهم الإلكترونية الخاصة بأجهزتهم بطرق مختلفة.

وتحاول مختلف الدول والشركات المقدمة لخدمات الإنترنت التغلب على هذه الاختراقات عبر برامج خاصة أحيانا وعبر رموز أخرى، وهذا يتطلب عند محاولة الاستفادة منه لغايات التحري تعاونا من مزودي الخدمة، لأن هذه الرموز تخص مزود الخدمة يتعرف من خلالها على هوية المتصلين عبر خطوطهم.

هذا ويعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة التي حدد المشرع وسائل إثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية، وتتمثل في وسائل الإثبات الرئيسية، وفي المعاينة، والتفتيش، وضبط الأشياء المتعلقة بالجريمة، أما غيرها من وسائل الإثبات كالاستجواب، والمواجهة، وسماع الشهود فهي مرحلة تالية من إجراءات التحقيق وجمع الأدلة[67].

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

---

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

المبحث الأول: صعوبات تتعلق بالدليل ذاته

بالرغم من وجود تشابه كبير بين التحقيق في جرائم الإنترنت وبين التحقيق في الجرائم الأخرى فهي جميعاً تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والشهادة والخبرة بالإضافة إلى جمع الأدلة، كما أنها تشترك في كونها تسعى إلى الإجابة على الأسئلة المشهورة لدي المحقق، ماذا حدث؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟

إلا أن الجرائم المتعلقة بشبكة الإنترنت تمتاز عن غيرها من الجرائم ببعض الخصائص وهذا بالطبع يستدعي تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن المحقق من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمين، فالتحقيق في هذا النوع من الجرائم يستدعي الرجوع إلى عدد كبير من السجلات التي يجب الاطلاع عليها مثل الكتيبات الخاصة بأجهزة الحاسب الآلي، وملفات تسجيل العمليات الحاسوبية، بالإضافة إلى الاطلاع على كم كبير من السجلات عن خلفية المنظمة وموظفيها، 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 العبث في بيانات الحاسب أو برامجه، في وقت قياسي وهذه البيانات التي يتم العبث بها يمكن محوها كذلك في وقت قياسي قبل أن تصل إلى يد العدالة. فالجريمة المعلوماتية عكس الجرائم العادية الأخرى تتم دون رؤية لدليل الإدانة وحتى في حالة وجود الدليل يمكن للجاني محو الدليل وفي حضور أجهزة العدالة غير المختصة بعد تنفيذه للجريمة، ولذلك فغالبية الجرائم المعلوماتية تكتشف مصادفة وليس بطريقة الإبلاغ عنها.

فقد دلت دراسة ميدانية قامت بها إدارة الصحة وخدمات الإنسان بالولايات المتحدة عام 1983 أن الحوادث المصادفة مثلا (الشكوى – الفضول – الانتقام) من المبلغ ضده أو النشاط غير العادي للجناة شكلت نسبة 49% من عوامل ساعدت 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 الجناة سرقة معلومات وبيانات وذلك باختراق نبضات إلكترونية عبر ألياف بصرية تنتقل ما بين البنك وأجهزة السحب الآلي للنقود.

ويقسم المجرمون بحسب خفاء الدليل إلى:

– المخادعون: لديهم مقدرة عالية على إخفاء دليل الجريمة المعلوماتية وتنصب جرائمهم على شبكات تحويل الأموال والتلاعب في حسابات المصارف.

فيعمد الجاني هنا إلى إعاقة وصول جهات التحقيق إلى الحيز المعنوي المشتمل على الدليل بوضع منظومات حماية تمنع أي دخول غير مشروع عن الأنظمة والبرمجيات والملفات، ومن ثم صعوبة نسخها، يستخدم الجاني لذلك كلمات سر معينة أو وضع تعليمات تعمل على إتلاف الدليل عند أي محاولة للدخول غير المصرح به إليه، 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[68].

– الجواسيس: وهؤلاء يسعون إلى جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها، فهم لديهم مقدرة فائقة على طمس الأدلة.

المطلب الثاني: فقدان الآثار التقليدية للجريمة

الجرائم المعلوماتية ليست كالجرائم التقليدية فهي لا تخلف آثارا مادية و يرجع السبب في افتقاد الآثار التقليدية حسب ما لاحظه جانب من الفقه، من أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسب الآلي دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها كما لو كان البرنامج معدا و مخزنا على جهاز الكمبيوتر، ويمكن هنا اقتراف بعض أنواع الجرائم كالاختلاس والتزوير، وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب الآلي أو تعديل البرنامج المخزن في جهاز الكومبيوتر وتكون النتيجة مخرجات على هوى مستعمل الجهاز دون استخدام وثائق أو مستندات ورقية، وبالتالي تفقد الجريمة آثارها التقليدية، كذلك من الأسباب التي تساهم في تعذر الحصول على آثار تقليدية تتمثل في كون الجاني بنفسه يملك محو الأدلة التي تدينه أو تدميرها في زمن قصير جدا، و حتى لو تم ضبطه فقد يرجع هذه الجريمة إلى خطأ في نظام الحاسب أو الشبكة.

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

ويتعين عند البحث عن آثار الجريمة المعلوماتية وأدلتها أن توجه التحريات إلى دائرة المتعاملين في نطاق المؤسسة التي وقعت بها الجريمة سواء أكانوا موظفين أو متعاملين معها، وذلك برصد حركة المعاملات التجارية ومراقبة المشبوهين داخل المؤسسات المالية وحولها، ويتعين على رجال الأمن جمع المعلومات السرية عن حركة السوق وتداول الأموال والممتلكات والتغيرات.

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[69].

ولما كان في الجريمة المرتكبة على الحاسب الآلي (إتلاف بيانات) أو بواسطته (سب، قدح) تتم بإشارات وأوامر معنوية تعطي من الجانب الحاسب الآلي المنفذ، فإن مسألة التخلص من تلك الأوامر أمر بغاية البساطة، خصوصا عندما تكون الجريمة واقعة بسلوك مجرم واحد يتمثل في الضغط على أحد أزرار لوحة التحكم في الحاسب الآلي ذاته، وهي مشكلة تؤدي إلى أخرى أعقد وأخطر، وهي صعوبة تحديد الفاعل وكشفه ما يجعل المصادفة المحضة الوسيلة الوحيدة لذلك[70].

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

على الرغم من قيام الجهات ذات الأنظمة المعلوماتية بحماية نظمها 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 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

---

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

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

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[71].

المبحث الثاني: صعوبات تتعلق بالأشخاص

طبيعة الجرائم ذات الصلة بالحاسب الآلي تقتضي معرفة متميزة بنظم الحاسبات، وكيفية تشغيلها، ووسائل إساءة إستعمالها من قبل مستخدميها، ولن تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري، والمباشرين للتحقيق في مجال الجرائم الإلكترونية، إلى الحد الذي دعا البعض إلى القول بضرورة وجود شرطة متخصصة، ونيابة متخصصة في هذا المجال.

المطلب الأول: طبيعة المجرم في الجرائم الإلكترونية

تتطلب الجرائم المعلوماتية على غرار الجرائم التقليدية حرفيه عالية سواء عند ارتكابها أو عند العمل على اكتشافها من الشخص الذي يرتكبها، أي يجب أن يكون ذلك الشخص خبيرا بالقدر اللازم والكافي بأمور الحوسبة والإنترنت ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي، وأن الشرطة تبحث أول ما تبحث عن خبراء الكمبيوتر عند ارتكاب هذا النوع من الجرائم.

لذلك يعمد الجاني إلى تشفير الملفات أو البيانات الإلكترونية التي تتضمن محتوى غير مشروع بغية منع الغير من الإطلا ع عليها واكتشافها، كما هو الحال في حالة نقل البيانات المتعلقة بجرائم غسيل الأموال عبر الإنترنت بعد تشفيرها.

ويحرص الجاني بعد ارتكابه لجريمته على محو آثارها التي تدل على وقوعها، وذلك من خلال التوصل بتقنيات معدة لهذا الغرض مع الأخذ بنظر الاعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الإلكترونية التي يمكن القيام بها في أزمان قياسية متناهية القصر تقاس باللحظات والثواني.

بناء على ذلك كثيرا ما يكون ضحايا الجرائم المعلوماتية هم السبب في تصعيب اكتشاف هذه الجرائم لعدة أسباب وهي:

- نقص الخبرة الفنية والتقنية.
- عدم اتخاذ الحيطة والحذر.
- الإمتناع عن الإخبار.

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

- عدم إدراك خطورة الجرائم المعلوماتية[72].

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 الجريمة المعلوماتية كوسيلة للحصول على الدليل

معاينة الجرائم التقليدية والإطلاع على مسرح الجريمة له أهمية متمثلة في تصور كيفية وقوع الجريمة وظروف ملابسات ارتكابها وتوفير الأدلة المادية التي يمكن تجميعها عن طريق المعاينة، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة المعلوماتية وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى مرتكبها ويرجع السبب في ذلك أن مسرح الجريمة يعطي المجال واسعا أمام سلطة الاستدلالات والتحقيق في الكشف عن الجريمة والأدلة والتحفظ على الآثار المادية التي خلفتها لكن مسرح الجريمة المعلوماتية يتضاءل دوره و ذلك لسببين:

الأول: أن الجريمة المعلوماتية قلما تخلف آثارا مادية.

الثاني: كثيرا من الأشخاص يردون إلى مسرح الجريمة خلال الفترة الممتدة من زمان وقوع الجريمة وحتى اكتشافها وهي فترة طويلة نسبيا الأمر الذي يعطي الفرصة للجاني أن يغير الآثار المادية إن وجدت مما يورث الشك في دلالة الأدلة المستقاة من المعاينة، والجريمة المعلوماتية قد تكون جريمة مستمرة كما في حالة الجرائم الإقتصادية السرقة والاحتيال وقد يكون مسرحها كالجرائم الأخرى كما في التزوير وإتلاف البرامج أو تفجير المباني، ففي النوع الأول من الجرائم تكون المعاينة هدفها المداهمة وضبط الأدلة على الطبيعة وفي الحالة الثانية التي تكون بعد وقوع الجريمة فالأمر متوقف على اعترافات المتهمين متى تم القبض عليهم و القرائن وفي كل الأحوال يتعين مراعاة الآتي قبل التحرك إلى مسرح الجريمة:

*وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها والخزائن والملفات أو خرائط توضح الموقع الذي ستتم معاينته وتفاصيل المبنى أو الطابق موضوع البلاغ.

* تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة سواء من حيث الضبط أو التأمين أو حفظ الأوراق والمستندات المتداولة.

*تأمين الأجهزة والمعدات التي ستتم الإستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج صلبة أو لينة[73].

---

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

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

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

*إعداد خطة معاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.

*تأمين عدم انقطاع التيار الكهربائي.

*إبطال مفعول أجهزة الهاتف التي قد تساعد عن طريق تقنية معينة في تدمير أدلة الجريمة المعلوماتية متى تم توصيلها بالأجهزة محل المعاينة، وعدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسب.

*التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقة وشرائط وأقراص ممغنطة ورفع البصمات وكذلك التحفظ على مستندات الإدخال والمخرجات الورقية لجهاز الحاسب الآلي والتي قد تكون ذات صلة بالجريمة.

الفرع الثاني: نقص المعرفة الفنية لدى سلطات التحقيق

من الصعوبات التي تواجه عملية استخلاص الدليل في الجريمة المعلوماتية نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي وكيفية التعامل معه، وذلك على وجه الخصوص في البلدان العربية، نظرا لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخرا عن أوروبا والولايات المتحدة الأمريكية[74].

ومن البديهي ونحن نتحدث عن جرائم تقع في بيئة حاسب الآلي أن تكون تلك الجرائم معتمدة بشكل أساسي على تقنية المعلومات ووسائل التقنية، الأمر الذي يظهر تطورا في وسائل ارتكاب الجريمة وفي نوع الدليل وطبيعته، وفي طريقه كشفه وضبطه، وهناك صعوبة أخرى في جمع الأدلة الرقمية من جداول الحالة التشغيلية في البروتوكولات والاتصالات، وتتمثل هذه الصعوبة في أن هذه الجداول تكون متاحة لفترات قصيرة ولا يمكن التغلب على هذه الصعوبة بالتحفظ الجنائي على أجهزة الهاردوير لحين الفحص، لأن هذه الجداول تزول تلقائيا بمجرد غلق أو انقطاع التيار الكهربائي عن تلك الأجهزة، لذلك مستحسن أن يتم استخدام أسلوب القص واللصق إلى ملف جديد خاص بجمع الأدلة وقبل غلق الأجهزة.

ورغم أن أسلوب القطع واللصق أسلوب ناجح لجمع الأدلة، إلا أن المشكلات القانونية المترتبة على قانونية هذا الأسلوب قد تثير بعض الشك في مدى سلامة جمع المعلومات وحجيتها أمام أجهزة العدالة الجنائية.[75]

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

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

الخاتمة:

إن التعرض لموضوع فن وأصول التحقيق الجنائي في الجرائم الإلكترونية يقتضي التعرض إلى المبادئ الأساسية للتحقيق في الجرائم المعلوماتية وهو ما يتطلب عرض العناصر الأساسية للتحقيق.

فيجب على المحقق أن يستظهر الركن المادي، والركن المعنوي للجريمة محل التحقيق، وتحديد وقت ومكان ارتكاب الجريمة المعلوماتية بالإضافة إلى علانية التحقيق.

ذلك أن النشاط أو السلوك المادي في جرائم الإنترنت يتطلب وجود بيئة رقمية واتصال بالإنترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلاً يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميل الكمبيوتر ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلي تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة وتحميلها علي الجهاز المضيف **Hosting Server**، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.

لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الإلكترونية فحتى ولو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق، وبرامج فيروسات، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

وتثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم **Server** أحد البنوك في الجزائر، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين، وهذا بالتالي يثير مشكلة أخرى وهي مكان ارتكاب الجريمة المعلوماتية، وتثور أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن، حيث أن هناك بعد دولي في هذا المجال ذلك أن الجريمة المعلوماتية جريمة عابرة للحدود.

وعلانية التحقيق من الضمانات اللازمة لتوافر العدالة، ولهذا قيل إن العلانية في مرحلة المحاكمة لا يقتصر فيها الأمر على وضع الاطمئنان في قلب المتهم، بل أن فيها بذاتها حماية لأحكام القاضي من أن تكون محلا للشك أو الخضوع تحت التأثير، كما أن فيها اطمئنانا للجمهور على أن الإجراءات تسير في طريق طبيعية.

والعلانية المقررة للتحقيق في الإجراءات الجنائية هي من بين الضمانات الخاصة بها، وهي تختلف في التحقيق الإبتدائي عنها في مرحلة المحاكمة.

– النتائج:

- ✓ في نطاق مفهوم الجرائم الالكترونية، امتازت التعريفات التي أوردها الفقه بالتعدد والاختلاف ضيقاً واتساعا تبعاً للمعايير والمنطلقات المستندة إليها، فمنها ما اعتمد أصحابها على معيار الوسيلة المستخدمة في ارتكاب الجريمة، ومنهم من اعتمد معيار موضوع الجريمة ذاتها، ومنهم من اعتمد معايير مختلطة جمعت بين المعيارين السابقين.
- ✓ إن عالم تقنية المعلومات عالم لا حدود له وفي تطور متسارع بشكل مذهل، ففي كل يوم يعرف ابتكارات جديدة.
- ✓ إن الوسائل الفنية التي قد تستخدم لتدمير مكونات الحاسوب كثيرة ومعقدة في الوقت الحاضر، ولا يُمكن التنبؤ بالوسائل التي قد تستحدثها التكنولوجيا في هذا الشأن.
- ✓ وجود العديد من المعوقات التي تعتري إثبات الجريمة الإلكترونية، منها ما هو متعلق بالجريمة ذاتها أو الجهات المتضررة من الجريمة أو الجهات التي تتولى التحقيق في هذه الجرائم بالإضافة إلى المعوقات التشريعية، وهذا الأمر يتطلب اتخاذ مجموعة من الخطوات الإصلاحية في هذا الصدد.
- ✓ للجرائم الإلكترونية طبيعة خاصة، إذ تمتاز بقدرتها على التحرك في مجال فضائي واسع لا توقفه حدود الدول وسيادتها الاقليمية، حيث يُمكن لجريمة تقنية المعلومات أن تقع في مكان وتُنتج آثارها في مكان أو أماكن أخرى خارج الدول.

قائمة المصادر والمراجع:

أولا: المصادر

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

2. 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.

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، 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: