وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

المرجع: .....

قسم : قانون خاص

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجرائم الرقمية وطرق إثباتها

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق

التخصص: قانون قضائي

من إعداد الطالب(ة) :

- عاصف أسماء

تحت إشراف الأستاذ(ة):

- بوزيد خالد

أعضاء لجنة المناقشة

الأستاذ(ة).....زموش فاطمة الزهراء.....رئيسا

الأستاذ(ة) .....بوزيد خالد.....مشرفا مقررا

الأستاذ(ة).....بوكر رشيدة.....مناقشا

السنة الجامعية: 2024/2023

نوقشت يوم: 2024/06/19

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات
الرقم: 39 م.ت/

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
لإنجاز البحث

أنا الممضي أدناه،

السيد: عاطف أسماء الصفة: طالبة

الحامل لبطاقة التعريف الوطنية رقم: 406302623 والصادرة بتاريخ: 2023.07.04

المسجل بكلية: الحقوق والعلوم السياسية قسم: القانون الخاص

والمكلف بإنجاز مذكرة ماستر بعنوان:

الجرائم الرقمية وطرق إثباتها

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2024/06/03

إمضاء المعني

عن رئيس المجلس الشعبي البلدي
وبالتفويض
إمضاء: زعيطي خديجة

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها

الإهداء

ما الزمان وما المكان وما القديم وما الجديد سنكون يوما ما نريد لا الرحلة ابتدأت ولا الدرب انتهى وما توفيقي إلا بالله

اليوم سأعلن تخرجي وفرحتي وذلك الحلم الذي أتعبني، وشقت عمري في سبيل أن أحققه، ها هو قد تحقق واختلطت الدموع مع فرحة كنت انتظرها

أهدي تخرجي إلى حبيب القلب الذي سخر كل قواه كي أصل إلى ما أنا عليه

والدي الحبيب "عاصف مزيود"

وإلى الطاهرة الحبيبة على القلب التي صنعت مني امرأة

أمي الغالية "محي الدين فاطمة"

حفظهما الله

من الأعماق أهدي تخرجي إلى من تمنوا لي النجاح والتوفيق وإلى كل إخوتي الأعزاء

إلى كل من ساندني وإلى كل من تمنى لي الخير والنجاح أصدقائي وزملائي نلتقي في مناصب نعتز بها بإذن الرحمان

والشكر والامتنان لصديقة طفولتي ولأخت لم تلدها أمي "مقدمي خديجة"

انتهت هذه المرحلة بحياتي والتي قدمت لي أشخاصا اعتز وافتخر بمعرفتي لهم أساتذتي الكرام فهم أروع من صادفت في دراستي لكم مني كل الاحترام والتقدير على مجهوداتكم الجبارة

شكر وعرفان

قال الله تعالى: "ومن يشكر فإنما يشكر لنفسه"

وفي بداية كلمتي لابد من التوجه أولا بالشكر لله عز وجل الذي وفقني للوصول إلى هذه المرحلة العلمية العالية، ومهد لي الطريق لأن أكون بينكم اليوم لأناقش رسالتي في الماستر

كما أتوجه بالشكر والامتنان لأستاذي المشرف حفظه الله ورعاه وأطال في عمره، فقد كان لإشرافه ومنحه الكثير من الوقت لي اليد الأولى في خروج هذه الرسالة العلمية بالشكل الذي ظهرت عليه، كما كان لتوجيهاته ونصائحه دور أساسي في إتمام دراستي العلمية

والشكر موصول لأعضاء لجنة المناقشة الكرام على تفضلهم بقبول مناقشة رسالة الماستر

بالإضافة إلى شكري الكبير لجميع أفراد عينة الدراسة الذين منحوني الكثير من وقتهم، وبذلوا الكثير من الجهود في سبيل خروج الرسالة بأدق النتائج وأكثرها فعالية.

قائمة المختصرات

ص: صفحة

د د ن: دون دار النشر

د س ن: دون سنة النشر

د ب ن: دون بلد النشر

ق: قانون

ج ر: جريدة رسمية

ف: فقرة

مقدمة

مقدمة

الجريمة ظاهرة طبيعية في الحياة الاجتماعية للإنسان، فالتضارب والاختلاف بين مصالح الأفراد داخل المجتمع بصفة عامة، قد ينتج عنه نزاعات بين أفراد هذا المجتمع مما يؤدي في غالب الأحيان إلى ارتكاب جرائم متعددة الأشكال، وتطورت الجريمة بتطور نمط حياة الفرد داخل المجتمع، واختلفت أشكالها باختلاف مراحل حياته، الشيء الذي جعلها تطال مختلف مجالات حياته، وتتغير حسب أهدافه ودوافعه وظروفه الاجتماعية التي تخضع للزمان وللمكان.

تسارع إيقاع التقدم التكنولوجي والتقني الهائل، وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالفاكس والإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية استغله مرتكبو الجرائم الإلكترونية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية[1].

ولمكافحة الجريمة المعلوماتية أصبح من الضروري إيجاد وسائل جديدة تختلف جذريا عن ما يتم استعماله في مكافحة الجريمة العادية، وذلك بسبب عجز إجراءات التحقيق التقليدية في مجاراة نسق تطور هذه الجريمة، حيث عرفت الجرائم نقلة نوعية من حيث المسرح الذي ترتكب فيه، فمن الجرائم التقليدية الى الجرائم المعلوماتية والتي يختلف مسرح ارتكابها من وسط واقعي ملموس الى وسط افتراضي ومن أدلة اثبات مادية الى أدلة اثبات رقمية أو الكترونية تتماشى مع الوسط الذي ارتكبت فيه.

وفي عصرنا الحالي أصبحت العديد من النظم القانونية في الإثبات تدرج الدليل الإلكتروني كأداة إثبات لها قيمة قانونية وحجية في الإثبات وتساوي فيه في الإثبات ما بين الأدلة التقليدية والدليل الإلكتروني الذي يتميز بطبيعة خاصة لهذا النوع من الأدلة يطرح معه إشكالات عدة

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص 159.

نظرا لقابليته للتغيير في أية لحظة، فبضغطة زر واحدة وخلال ثواني يمكن محوها والغائها أو التلاعب في معطياتها مما يفتح الباب واسعا للطعن في مصداقيتها، وهي أدلة لا غنى عنها في الجرائم المعلوماتية، إلا أن الاستدلال بها مقيد باحترام الخصوصية المعلوماتية للأشخاص كأصل عام[1].

تكمن أهمية موضوع "الجرائم الرقمية وطرق إثباتها" في أنه يعالج نوعا جديدا من الأدلة الجنائية من الناحيتين الفنية والقانونية، ومن هنا تبرز قيمة هذا الموضوع من خلال أن له صلة وثيقة بطائفة جديدة من الجرائم ظهرت مع التطور التكنولوجي، وتتمثل في الجرائم الإلكترونية حيث ظهر بغرض التصدي لهذا النوع من الجرائم، فالقضاء الجنائي وجد نفسه في مواجهة هذا الدليل المستحدث، بما يفرض تحديات جديدة للقاضي الجنائي، ومن جهة أخرى تناول هذا الموضوع احد الوسائل العلمية الأكثر انتشارا في قضايا الإثبات الجنائي تلك الوسائل التي جاءت لتتلاءم مع الفكر الإجرامي والذي كان لزوما على المشرع ان يستحدث من التشريعات ما يتلاءم معه.

كما يعود اختياري لموضوع "الجرائم الرقمية وطرق إثباتها" الى موضوع الإثبات الجنائي بالأدلة رقمية هو رغبة مني في إثراء الدراسات الجامعية النظرية، وذلك بسبب ندرة الأبحاث والدراسات المتعلقة بتحديد ماهية الدليل الرقمي وحجيته أمام القضاء الجنائي، بحيث أن هذه الأدلة لم يتم دراستها بشكل علمي وقانوني معمق في الجزائر، وإنما تم التطرق إليها في مؤلفات عامة وبشكل مقتضب دون أن يتم الإحاطة بها.

وعليه يطرح الإشكال التالي:

ماهي طرق الإثبات الجنائي في الجرائم الالكترونية؟؟

[1] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجيستير، جامعة الحاج لخضر– باتنة–، كلية الحقوق والعلوم السياسية، 2013، ص 110.

وللإجابة عن هذا التساؤل سأقوم في هذه الدراسة بالاستعانة بالمنهج الوصفي، من خلال إعطاء وصف للدليل الرقمي من تعريفة وإبراز طبيعته ومختلف خصائص وكذا الإجراءات الحصول عليه، بالإضافة إلى المنهج التحليلي، بقصد مناقشة ما يحتاجه لجمع الحقائق والبيانات الإجرائية الخاصة بإحراز الدليل الرقمي.

وعلى هذا قسمت هذه المذكرة إلى فصلين كالتالي:

الفصل الأول: الإطار المفاهيمي للجريمة الرقمية

المبحث الأول: ضوابط الإثبات في الدليل الالكتروني

المبحث الثاني: ماهية الجريمة الرقمية

الفصل الثاني: معوقات الإثبات وحجيته في الجريمة الرقمية

المبحث الأول: معوقات إثبات الجريمة الرقمية

المبحث الثاني: حجية الدلائل الرقمية في الإثبات

ومن ثم خاتمة التي تشتمل على مجموعة النتائج المتوصل إليها، بالإضافة إلى جملة من الاقتراحات.

الفصل الأول

الفصل الأول: الإطار المفاهيمي للجريمة الرقمية

تعتبر الجريمة الالكترونية من الجرائم المستحدثة والخطيرة التي لم يكن المجتمع البشري يتوقعها، وذلك لارتباطها بالتطور التكنولوجي الهائل الذي يشهده عالم الكمبيوتر في الآونة الأخيرة وذلك توافقا مع انتقال المجتمعات إلى المجتمع الرقمي أي من الواقع الفعلي (المادي) إلى الواقع الافتراضي، فقد تنامت بسرعة فائقة في ظل الانفتاح العالمي وارتباط الأسواق الدولية ببعضها البعض، فأصبحت هذه الظاهرة الإجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم الخسائر والمخاطر التي تهدد الأفراد في ممتلكاتهم وخصوصياتهم والمؤسسات في كيانها المادي والاقتصادي وحتى المعلومات في أمنها وسيادتها خاصة أنها جرائم ذكية تنشأ في بيئة الإلكترونية (رقمية)، لهذا وجب الإلمام بالجريمة الإلكترونية من حيث مفهومها وخصائصها وتصنيفيها.

وعليه سنقسم الفصل الأول إلى مبحثين:

المبحث الأول: ضوابط الإثبات في الدليل الالكتروني

المبحث الثاني: ماهية الجريمة الرقمية

المبحث الأول: ضوابط الإثبات في الدليل الرقمي

ان ظهور أشكال مستحدثة من الجرائم المعلوماتية ادى بطبيعة الحال إلى ظهور ادلة مستحدثة وفي اثبات الجاني تختلف عن الادلة التقليدية وتعرف بالدليل الالكتروني (1) وهذا الاخير هو كل دليل مأخوذ من جهاز الكمبيوتر محل الجريمة أو يكون في شكل بيانات وملفات مخزنة بداخله وقد يكون عبارة عن ملفات ناجمة عن اتصالات بين الجاني والمجني عليه من خلال مواقع الانترنت، وهو ما يساعد القاضي على توضيح موقفه من القضية ومنها إصدار حكم آليات في القضية المعروضة أمامه.

وعلى هذا الأساس قسمنا هذا المبحث إلى مطلبين سنتطرق إلى الأدلة الرقمية (المطلب الأول) ثم إلى الأدلة الاجرائية المستخدمة في جميع الأدلة الرقمية (المطلب الثاني).

المطلب الأول: الدليل الرقمي

نتطرق من خلال هذا المطلب إلى تعريف الدليل الرقمي وخصائصه في الفرع الأول، وأنواعه في الفرع الثاني.

الفرع الأول: تعريف الدليل الرقمي وخصائصه

نتناول تعريف الدليل الرقمي أولا، ثم خصائصه ثانيا.

أولا: تعريف الدليل الرقمي

1- التعريف اللغوي:

الدليل في اللغة هو المرشد وما يستدل به وجمعه أدلة، كما يقصد به كذلك تأكيد الحق بالبينة، والبينة هي الدليل أو الحجة أو البرهان[1].

[1] جميل صليبا، المعجم الفلسفي المصطلحات القانونية، الجزء الأول، دار الكتاب اللبناني، بيروت، الطبعة الأولى1982، ص 564.

وقد جاء في القرآن الكريم معنى الدليل بقوله تعالى: "ألم تر إلى ربك كيف مد الظل ولو شاء لجعله ساكنا ثم جعلنا الشمس عليه دليلا"[1]

وبالنسبة لكلمة "الرقمي" فهي اسم منسوب للدليل وأصلها "رقم"، وهي علامات الأعداد المعروفة 1، 2، 3، ...، وينصب معناها أيضا إلى كلمة عدد، وجمعها أعداد[2].

2- التعريف الاصطلاحي القانوني:

لم يتعرض المشرع الجزائري إلى تعريف الدليل الرقمي ونفس الشيء بالنسبة للمشرع الفرنسي، ولهذا سأقوم بعرض بعض التعريفات التي أتى بها فقهاء القانون الجنائي، فقد عرفه البعض بأنه: "الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة أو الصور أو الأصوات أو الأشكال أو الرسوم وذلك من أجل اعتماده أمام أجهزة تنفيذ وتطبيق القانون[3]".

كما عرف أيضا: "الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الإلكترونية من معطيات الحاسوب وشبكة الأنترنت، والأجهزة الإلكترونية الملحقة والمتصلة به وشبكات الاتصال، من خلال إجراءات قانونية لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة[4]".

---

[1] الآية 45 من سورة الفرقان.

[2] طاهر عبد المطلب، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة مسيلة، 2015-2014، ص 02.

[3] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006، ص 88.

[4] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص 230.

وبأنه: "ذبذبات أو نبضات إلكترونية Impulses Electronic مسجلة على وسائط أو دعائم مادية[1]".

وهناك من يعرف الدليل الرقمي على أنه جميع المعلومات والبيانات الرقمية التي تقوم بإثبات أن هنالك جريمة قد ارتكبت، أو وجود علاقة بين الجريمة والجاني أو بين الجريمة والمتضرر منها، والبيانات الرقمية هي عبارة عن مجموعة من معلومات أو بيانات ذات قيمة في التحقيق، والتي جرى إرسالها أو تخزينها عبر جهاز إلكتروني.[2]

عند استقرائنا لأغلب التعريفات نجد أنها قد قدمت لنا وصفا للدليل الرقمي من حيث تكوينه، إلا أنه يعاب عليها أنها اعتمدت فقط على الأدلة المستخلصة من أجهزة الحاسب الآلي وشبكة الأنترنت[3]، وتجاهلت أنه يمكن الحصول على الأدلة الرقمية من الهواتف المحمولة الذكية، أو أجهزة تحديد المواقع GPS، أو أي جهاز آخر يتميز بخصائص معينة أهمها التخزين أو المعالجة.

وعليه يمكننا القول بأن الدليل الرقمي هو" الدليل المستخلص من أجهزة الحاسب الآلي وملحقاته، أو من شبكة الأنترنت أو أي جهاز آخر له خاصية معالجة وتخزين المعلومة، وهو عبارة عن نبضات مغناطيسية أو كهرومغناطيسية يمكن جمعها وتحليلها باستخدام برامج وتطبيقات خاصة، لتشكل لنا بيانات مختلفة يمكن اعتمادها في مرحلة التحقيق أو المحاكمة".[4]

ثانيا: خصائص الدليل الرقمي

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص 176.

[2] the technical working group for electrinic crime scence investigation, electronic crime investigation, the national instituteof justice,the united states of america,2001,page 6

[3] خالد عياد الحلبي، المرجع السابق، ص 230.

[4] Eoghan Casey, Digital Evidence and computer Crime, Third edition, Published by Elsevier Inc, London, 2011, page 07

على غرار خصائص ومميزات الجريمة المعلوماتية والمجرم المعلوماتي أيضا، يتميز الدليل الرقمي بعدة خصائص ينفرد بها عن الدليل التقليدي نذكر منها:

1- الدليل الرقمي دليل علمي:

وجب في استخلاص الدليل الرقمي وتحليله طرقا غير تقليدية، بحيث يتطلب إجراء تجارب تقنية وعلمية على جهاز الحاسب الآلي الذي تمت على مستواه جريمة معينة.[1]

فعند البحث عن الدليل الرقمي وجب أن تكون هذه العملية في إطار جغرافيا النظام الافتراضي System Information Geographicالخاضعة لقوانين الإعلام الآلي أو البيئة المعلوماتية ككل.[2]

وعليه يمكن أن يخلص القول إلى أنه لا يمكن الحصول على الدليل الرقمي أو الاطلاع عليه إلا باستخدام الوسائل والأساليب العلمية، وذلك راجع إلى المنشأ الذي تكون فيه هذا الدليل.

2- الدليل الرقمي ذو طبيعة تقنية:

ومفاد هذه الخاصية أن يتم التعامل مع الدليل الرقمي من قبل مختصين في العالم الافتراضي وفي الدليل الإلكتروني، لأن هذا الأخير ليس كالدليل، فهو عبارة عن ذبذبات إلكترونية تكمن قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب في أي شكل يكون عليه، وعلى إثر ذلك قام المشرع البلجيكي بتعديل قانون التحقيق الجنائي بمقتضى القانون 28 نوفمبر 2000 بإضافة المادة 39، والتي سمحت بضبط الأدلة الرقمية، كنسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية، كذلك بالنسبة للمشرع الأمريكي الذي قام بتدعيم تقنيات التحقيق الكاملة، وهو ما يستفاد من خلال الفصل بين الخبرة

[1] ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية – دراسة تأصيلية تطبيقية –، رسالة ماجيستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012، ص 74.

[2] عمر محمد بن يونس، الدليل الرقمي (Evidence Digita) ، دون دار نشر، مصر، 2006، ص 07.

وسلطات الاستدلال والتحقيق فيها يتعلق بالدليل الرقمي مع توافر هذه السلوكات على عناصر ذات خبرات عالية الكفاءة فيما يخص هذا الدليل[1].

3- الدليل الرقمي متنوع ومتطور:

مع توسع قاعدة الدليل الرقمي، يمكن لهذا الأخير أن يشمل أنواعا متعددة من المعلومات والبيانات الرقمية والتي بدورها تصلح أن تكون دليلا جنائيا بإدانة المتهم أو براءته، وأما ميزة التطور التي يختص بها الدليل الرقمي، فهي نتيجة تزايد استخدام تقنية المعلومات الرقمية، بعد أن أصبح كل من الحاسب الآلي وشبكة الأنترنت يشكلان موطئا هاما للبيانات والمعلومات الرقمية، ومن وجهة أخرى نجد أن تطورها اليومي جاء لتلبية احتياجات المستخدمين الشيء الذي أدى إلى ظهور أنواع جديدة من هذه الأدلة[2].

4- الدليل الرقمي يصعب التخلص منه:

من أهم ما يميز الدليل الرقمي أنه يصعب إتلافه أو التخلص منه، ففي حالة محاولة إزالة ذلك فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوي ذلك الدليل، بل مجرد محاولة محو الدليل تعد في حد ذاتها دليل لأنه في حال القيام بعملية المحو يتم تسجيلها في ذاكرة الآلة ويتم استخراجها كدليل ضد من قام بالفعل، كما يمكن أيضا عرض الدليل الرقمي على تطبيقات وبرامج لمعرفة ما إذا كان قد تعرض للعبث أو التحريف.[3]

5- الدليل الرقمي له سعة تخزين عالية:

---

[1] شهرزاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، مذكرة ماستر تخصص حقوق، كلية الحقوق والعلوم السياسية، جامعة أم البواقي، 2017، ص 14.

[2] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجيستير، جامعة الحاج لخضر– باتنة–، كلية الحقوق والعلوم السياسية، 2013، ص 124.

[3] أوشن حنان، وادي عماد الدين، الإثبات الجنائي والوسائل العلمية الحديثة، دار الخلدونية للنشر والتوزيع، الجزائر، 2015، ص 98 و 99.

يتميز الدليل الرقمي بالسعة التخزينية العالية حيث يمكن لآلة الفيديو الرقمية تخزين مئات الصور ويمكن لقرص صغير أن يقوم بتخزين مكتبة صغيرة، كما أن الدليل الرقمي يمكنه رصد معلومات عن الجاني وتحليلها في ذات الوقت حيث يمكنه تسجيل تحركات الفرد وتسجيل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لهذا فإن البحث الجنائي يجد غايته بسهولة أفضل من الدليل المادي التقليدي[1].

الفرع الثاني: أنواع الدلائل الرقمية

يتخذ الدليل الرقمي عدة أشكال وصور تشكل لنا العديد من البيانات والمعلومات المختلفة التي يمكن اعتمادها كوسيلة إثبات في الجرائم المعلوماتية وحتى التقليدية منها، لذا يأخذ الدليل الرقمي نوعين أساسيين، يتمثل الأول في الأدلة الرقمية التي أعدت لتكون وسيلة إثبات، أما النوع الثاني فيتمثل في تلك التي لم تعد لتكون وسيلة إثبات.

والدليل الرقمي (العلمي، الالكتروني) يقتصر على اجراء تجارب علمية وعملية على جهاز الحاسب الآلي التي استخدم في الاختراق أو التعدي، لتعزير دليل سبق تقديمه سواء بالنفي أو الإثبات الواقعة التي ثار الشك بشأنها.

أولا: الأدلة الرقمية التي أعدت لتكون وسيلة إثبات.

تنقسم الأدلة الرقمية إلى قسمين، يتمثل الأول في البيانات والمعلومات الناشئة تلقائيا من الحاسب الآلي، وأما القسم الثاني فيتمثل في البيانات والمعلومات ذات الطبيعة المختلطة.

– **البيانات والمعلومات الناشئة تلقائيا من الحاسب الآلي:** وهي مختلف المعلومات والبيانات الرقمية التي يتم إنشاؤها بواسطة الحاسب الآلي أو أي جهاز آخر ولا يكون للمستخدم دخل في

[1] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، 2010، ص 42.

إنشائها، أو السجلات التي تعد من مخرجات الحاسب الآلي كفواتير البطاقات البنكية المعدة آليا[1].

-**البيانات والمعلومات ذات الطبيعة المختلطة:** وهي تلك البيانات والمعلومات الرقمية التي يتم إنشاء جزء منها بواسطة الحاسب الآلي، وجزء آخر يتم حفظه بالإدخال، وأبرز مثال عن ذلك المعلومات و البيانات المدخلة والمعالجة من طرف برنامج Excel .[2]

ومنه فتكمن أهمية كلا النوعين في أنهما أعدا سلفا بغرض جعلهما وسيلة لإثبات بعض الوقائع التي تتضمنها، لهذا يتم حفظ هذه المعلومات والبيانات للاحتجاج بها لاحقا، كما يكون من السهل الحصول عليها عند الحاجة[3].

ثانيا: الأدلة الرقمية التي لم تعد لتكون وسيلة إثبات.

هي تلك الأدلة التي تنشأ دون إرادة الشخص ودون أن يكون راغبا في وجودها، بمعنى آخر هي أي أثر يتركه المستخدم عند استعماله لجهاز الحاسب الآلي أو شبكة الأنترنت بحيث تشمل الرسائل المرسلة منه أو الرسائل التي يستقبلها، ويسمى هذا النوع من الأدلة بالبصمة الرقمية أو الآثار المعلوماتية الرقمية ومثال ذلك البيانات والمعلومات المضمنة في ملفات الولوج Files Log، والتي تحتوي على معلومات كتاريخ ووقت التحميل أو إرسال ملفات المستخدم، أو الملفات الاحتياطية للنظام Backup FILES التي تستعمل في حالة انهيار النظام[4]، أو بيانات الكوكيز Cookies .[5]

---

[1] طاهر عبد المطلب، المرجع السابق، ص 12.

[2] عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية-دراسة تطبيقية مقارنة-، جامعة نايف العربية للعلوم الأمنية، السعودية، 2007، ص 14.

[3] نعيم سعيداني، المرجع السابق، ص 129.

[4] – Lynda volonino and ReynaldoAnazaldua, Computer Forensics For Dmmies, Wiley publishing, United states of America, 2008, page 85 .

[5] The Technical Working Group for Electronic Crime scence Investigation, Op .cit., page 11.

وتظهر أهمية هذا النوع من الأدلة في أنه قد يحمل معلومات تفيد في الكشف عن الجريمة ومرتكبها، بالإضافة إلى إمكانية ضبط هذه الأدلة ولو بعد مرور فترة زمنية طويلة، بواسطة تقنيات وبرامج خاصة لا تخلو من الصعوبة والتعقيد.

المطلب الثاني: القواعد الإجرائية

إن تطور التقني الذي لحق المعالجة الآلية، فضلا عن الطبيعة الخاصة للدليل الرقمي، أدى إلى تغيير الكثير من المفاهيم السائدة حول إجراءات وطرق الوصول إليها، وهو الأمر الذي فرض معه ضرورة إعادة تقسيم مناهج بعض الإجراءات المتبعة في استخلاص الدليل الالكتروني، والتي ثبتت عدم كفايتها نظرا الميزات التي تتسم بها، الأمر الذي فرض معه ضرورة استحداث قواعد إجرائية اخرى تتلاءم مع طبيعة البيئة التقنية، تستند هاته الأخيرة على طرق ومناهج بحث متخصصة ومتطورة[1].

فتطور الإثبات ووسائله أمر في غابة الأهمية لمواجهة هذا النوع الجديد من الجرائم، وهذا الأمر الذي سوف نعالجه من حيث بحث القواعد الاجرائية الحديثة في الوصول إلى الدليل الالكتروني وهذا ما سنتطرق إليه في النقاط التالية.

الفرع الأول: القواعد الاجرائية التقليدية لاستخلاص الدليل الالكتروني

تشترك الجريمة المعلوماتية مع باقي الجرائم في بعض الإجراءات التقليدية لجمع الدليل التي حافظت على وجودها رغم التطور الذي عرفته الجريمة في عصر التكنولوجيا، فهذه الإجراءات لا تزال صالحة للقيام بدورها في جميع الدليل وإثبات كل الجرائم بمختلف أنواعها ومنها الجريمة

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، الطبعة الأولى، الطبعة الأولى، منشورات الحلبي الحقوقية، الجزائر، 2012، ص 393.

الإلكترونية، وأهم هذه الإجراءات كما بينها القانون هي إجراءات مادية شخصية وهذا ما سنتطرق إليه في النقاط التالية:

سنتناول ثلاث إجراءات ذات طبيعة مادية تتم بنتائج مادية ملموسة، وسوف نبين في التالي دور كل إجراء في استنباط الدليل الإلكتروني:[1]

أولا: الإجراءات المادية

1- **المعاينة:** تعتبر المعاينة إجراء من إجراءات التحقيق تتطلب سرعة الانتقال إلى محل الواقعة الإجرامية لمباشرتها وذلك لإثبات حالته وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى فاعلها.[2]

ويمكن أن تقوم بها سلطة التحقيق بنفسها أو تندب ضباط الشرطة القضائية للقيام بها. كما يمكن المحكمة أن تقوم بإجراءات المعاينة إذا رأت.[3]

عند العلم بوقوع الجريمة فات أول خطورة يقوم بها امور ضبط القضائي هو الانتقال إلى مسرح الجريمة، لان هذا الأخير حجز الزاوية في التحقيق الجنائي ومكمن الآثار والأدلة المادية، وينبغي التعامل في الإطار مع مسرح الجريمة المعلوماتية على أنه مسرحان هما:

-**المسرح التقليدي:** يقع خارج بيئة الحاسوب والانترنت، ويتكون بشكل رئيسي من المكونات المادية المحسوسة المكان الذي وقعت فيه الجريمة، وهو أقرب إلى مسرح الجريمة التقليدية ويترك فيها الجاني عدة آثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزن رقمية.[4]

---

[1] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة للنشر، مصر، 2015، ص 135.

[2] انظر المادة 79 من الامر رقم 66155 المؤرخ في صفر عام 1386 الموافق 8 يونيو سنة 1966، الذي يتضمن قانون الإجراءات الجزائية، جريدة الرسمية الجمهورية الجزائرية، عدد 48 بتاريخ 11 جوان 1966، المعدل والمتمم.

[3] عائشة بن قارة مصطفى، المرجع السابق، ص84.

[4] أشرف عبد القادر قنديل، المرجع السابق، ص 138.

-**المسرح الافتراضي:** ويقع داخل البيئة المعلوماتية، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنت في ذاكرة الأقراص الصالة الموجودة بداخله.[1]

ومن الإجراءات التي يتعين اتباعها عند إجراء المعاينة ما يلي:

1. القيام بتصوير جهاز الحاسب الآلي الذي ترتكب عن طريق الجرائم.[2]

2. العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، وبوجه خاص السجلات الالكترونية التي تزود بها لمعرفة موقع الاتصال.

عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة وذلك قبل إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف البيانات المخزنة.[3]

2_ **التفتيش في البيئة الإلكترونية:** يمكن تعريف التفتيش بصفة عامة أنه إجراء من الإجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر، لذلك يعتبر من أهم الإجراءات التحقيق في كشف الحقيقة لأنه غالبا ما يسافر عن أداة مادية تؤيد نسبة الجريمة إلى المتهم.[4]

ولا يمكن أن يقوم به سوى النيابة العامة وقاضي التحقيق، الغرض منه هو البحث أدلة إثبات الجريمة المرتكبة محل التفتيش قد يكون مسكنا أو شخصا متعلقا بالمتهم أو غير المتهم[5].

---

[1] المرجع نفسه، ص 138.

[2] ممدوح عبد الحميد عبد المطلب، بحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية، مصر، 2006، ص 115.

[3] أشرف عبد القادر قنديل، المرجع السابق، ص 139.

[4] أشرف عبد القادر قنديل، المرجع نفسه، ص 140.

[5] عبد الفتاح البيومي الحجازي، المرجع السابق، ص 377.

عن يقصد بالشخص كمحل لتفتيش الوسائل الالكترونية، قد يكون من مستغلي أو مستخدمي الأجهزة الإلكترونية أو خبراء البرامج، سواء كانت برامج نظام أو برامج تطبيقات، أو من اي اشخاص اخرين يكون بحوزتهم اجهزة أو معدات معلوماتية أو اجهزة حاسب إلى محمولة أو هواتف متصلة بجهاز مودم أو مستندات.[1]

3**_الضبط:** إن النتيجة الطبيعة التي ينتهي إليها التفتيش هي ضبط الادلة المتحصل عليها أثناء تفتيش المنظومة المعلوماتية، وضبط يعني وضب على أي شيء يتصل بالجريمة المعلوماتية للكشف عن مرتكبيها.[2]

أما الضبط المعلوماتي فهو ينطبق على مكونات المادية والمعنوية للنظام المعلوماتي، كما أنه تعتليه عدة صعوبات بسبب ضخامة البيانات واجب فحصها من محقق المعلوماتي قدرة المجرم المعلوماتي على إخفاء ومحو آثار جريمته، وفي مقابل عاجز السلطات تحقيق عن كسر كلمات السر أو شفرات المرور، وضع المشرع الجزائري في قانون 09-04 المتعلقة بتكنولوجيات الاعلام والاتصال ومكافحتها طريقتين: أول تكون عن طريق نسخ المعطيات محل البحث وثاني باستخدام التقنيات المناسبة الشرف.

ثانيا: الإجراءات الشخصية

سنتطرق لمجموعة من الإجراءات الطبيعية ذات طبيعة الشخصية لأنه غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على الدليل.

1 – **الشهادة:**

[1] بن طالب ليندة، الدليل الرقمي ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2019، ص 49.

[2] خالد عياد الحلبي، المرجع السابق، ص 168.

الشهادة بصفة عامة هي إثبات حقيقة واقعة معينة علم بها الشاهد من خلال ما شاهده أو سمعه أو أدركه بحواسه الأخرى عن تلك الواقعة بطريقة مباشرة وشهادة على هذا الاساس تعد وسيلة إثبات اساسية في مسائل الجزائية.[1]

يطلق عليه اسم الشاهد المعلوماتي لأنه هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي والذي يكون لديه معلومات جوهرية لازمة الدخول لنظام المعالجة الآلية للبيانات فلذلك تجد أن شاهد المعلوماتي ينحصر في عدة طوائف تتمثل في مشاغلة الحاسب الآلي خبراء البرامج المحللون مهندسو الصيانة والاتصالات، مديرو النظام.

وللشاهد التزامات لابد التقيد بها مثل طبعا ملفات البيانات المخزنة في ذاكرة الحاسوب الآلي على أن يقوم بطبها وتسليمها إلى سلطان التحقيق والافصاح عن كلمات المرور السرية وكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة.[2]

2 – **الخبرة:**

لابد أن يكون الخبير صاحب مقدرة وامكانية علمية وفنية في مسألة الخبرة ويستطيع القيام بدوره وللقيام بهذا الاخير عليه أن يبين المكان المحتمل لدولة الإثبات وشكلها وهيئتها والآثار الاقتصادية والمالية المترتبة على التحقيق في جريمة المعلوماتية وكيفية عزل نظام المعلوماتي عند الحاجة دون إتلاف الادلة أو الأجهزة أو تدميرها[3].

[1] ابراهيم الغمار، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 1989، ص 30.

[2] بن زرت أسيا، اثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم 2019، ص 26.

[3] بن زرت آسيا، المرجع نفسه، ص 27.

الفرع الثاني: الادلة الاجرائية الحديثة للوصول للدليل الالكتروني

تبين من الإجراءات التقليدية أنها صعبة الاتباع للحصول على الدليل الإلكتروني، فكان من الضروري على التشريعات المختلفة خلق أدلة أو إجراءات حديثة تتماشى مع طبيعة الخاصة للدليل الالكتروني وهذا عن طريق الاعتماد على تكنولوجيا المعلومات. والمشرع الجزائري كغيره من التشريعات قام بإرسال جملة من مقومات التشريعية.

لمكافحة الجريمة المعلوماتية من خلال ما جاء به في القانون 06-222 المؤرخ في 20 2006-12 المعدل والمتمم للقانون الإجراءات الجزائية الامر (66-155) من خلال إجراءي التسرب واعتراض المراسلات السلكية واللاسلكية وكذلك بموجب إصدار قانون إجراء خاص به القانون 09-2004 المتضمن للقواعد الخاصة بالوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، وثاني باستخدام إجراء المراقبة التكنولوجية وسنتطرق إلى كل هذه الإجراءات المتحدثة في مجال المعلوماتية.[1]

أولا: التسرب

هو الإجراء المستحدث التي تنص عليه المواد من 64 مكرر 11 إلى مكرر 18 من ق إج ج عرفتها المادة 65 مكرر 12 من ق إ ج ج بأنه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضباط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه بارتكابهم جناية أو جنحة بإيهامهم أنه فاعل أو شريك لهم.[2]

وتكون عملية التسرب في الجريمة الالكترونية بدخول ضابط أو عون شرطة إلى العالم الافتراضي وذلك عن طريق اشتراكه في محادثات معرفة الدردشة، أو اختراق مواقع معينة

[1] عبير بعقيقي، فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09/04، مجلة العلوم القانونية والسياسية، جامعة محمد خيضر، بسكرة، المجلد 09، العدد 02، 2018، ص 41.

[2] بن طالب ليندا، المرجع السابق، ص 87.

مستخدما في ذلك أسماء أو صفات وهيئات مستعار وهمية سعيا منه للاستفادة المشتبه فيهم عن طريق منهم في كيفية اقتحام الهاكر الموقع، أو القيام بحلقات اتصال البريد الالكتروني.

ووكيل الجمهورية هو من يقوم بمراقبة التسرب أو قاضي التحقيق وفقا لنص المادة 65 مكرر 11 ق إ ج ج ويمكن لهما الامر يوقف التسرب في أي مرحلة وذلك من اجل تأمين متسلسل من الشبكة الإجرامية .

ثانيا: المراقبة الالكترونية

تناول المشرع الجزائري هذا الإجراء من المادة 04 من القانون رقم 09-04 المتعلق بالقواعد الخاصة بالرقابة من الجرائم المتصلة بتكنولوجيا لإعلام والاتصال ومكافحتها بعنوان مراقبة الاتصالات الالكترونية.[1]

والمشرع لم يعرف بإجراء المراقبة الالكترونية بل ترك أمر تعريفها للفقه ومنه تعرف بأنها "عمل أنني اساسي له نظام معلومات الكتروني، ويقوم فيه المراقب بمراقبة المراقب بواسطة الاجهزة الالكترونية أو عبر شبكة الانترنت، لتحقيق فرض محدد وافراغ النتيجة في الملف الإلكتروني، وتحديد التقارير بالنتيجة".[2]

والمراقبة الالكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، بحيث يقوم بها مراقب الكتروني يتمثل في ضابط من ضباط الشرطة القضائية ذي كفاءة تقنية عالية وباستخدام تقنيات وبرامج الكترونية فيها، وبالتالي ومن خلال القانون رقم 04-09 الذي سبق

[1] عبير بعقيقي، فيصل نسيغة، المرجع السابق، ص 41.

[2] مصطفى محمد موسى المراقبة الالكترونية عبر شبكة الانترنت (دراسة مقارنة بين المراقبة الامنية التقليدية والالكترونية)، دار الكتب القانونية، مصر، 2005، ص 192.

ذكره، نجد أن المشرع لم يعتبر هذا الإجراء طريقة من طرق الحصول على الدليل الرقمي فقط بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة المعلوماتية[1].

ويمكن استنتاج شروط وآليات المراقبة الالكترونية في التشريع الجزائري من خلال نص المادة 65 مكرر 5 ق إ ج ج وهي أن يتم تنفيذ هذه العملية تحت سلطة القضاء وبإذن منه، وهو ما نصت عليه المادة 4 من الق إ ج ج 09-04 المذكور، بحيث لا يجوز إجراء عمليات المقاربة إلا بإذن مكتوب من السلطة القضائية المختصة.[2]

ثالثا: اعتراض المراسلات السلكية واللاسلكية

نستشف من نص المادة (65) مكرر (5) من ق إ ج ج أن المقصود باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهاته المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين الاستقبال والعرض.[3]

وهي أيضا عملية مراقبة سوية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة.

بالرغم من أن عملية اعتراض المراسلات تشكل انتهاكا لحرمة حياة الخاصة للأفراد، واعتداء على سرية مراسلاتهم والتي كفلها في دستور 2020 المعدل بموجب القانون رقم 16-01 وذلك

[1] اوساسي فؤاد، دور الدليل الرقمي في الإثبات الجنائي مذكرة ماستر كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة 2019/20120، ص22-21.

[2] طاهري عبد المطلب، المرجع السابق، ص 24.

[3] أجازت الفقرة الأولى من المادة (65) مكرر (5) من ق اجج لوكيل الجمهورية أن بإذن بـ "اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية".

من خلال المادة 46 فقيرة 2 التي نصت « سرية المراسلات والاتصالات الخاصة بكل اشكالها مضمونة».[1]

إلا أن المشرع الجزائري قد وضع شروط قانونية تنص على منع التعسف في استعمالها وكذلك حماية الحرية الفردية وتتمثل هذه الشروط في الحصول على إذن من وكيل الجمهورية أو من قاضي التحقيق إذا تم فتح تحقيق قضائي.[2]

زيادة على ذلك يجب ان يكون الإذن مكتوب لمدة اقصاها أربعة أشهر قابلة للتجديد، وأيضا وجوب تضمنه على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوبة التقاطها والاماكن المقصودة.[3]

ويعتبر البريد الالكتروني اهم وسيلة تنفيذ في مجال التراسل الالكتروني ومن ثم فات عملية الاعتراض تنصب عليه والتي تمثل مصدرا غنيا الأدلة الرقمية للإثبات الجرائم الإلكترونية.

وكل رسالة الكترونية يظهر فيها معلومات عامة ولكن هذه المعلومات ليست كافية المعرفة المرسل، لأنه يمكن لهذا الأخير إرسال رسالة بأسماء وهمية، كما أن هناك وسائل تسمح للمرسل بإرسال رسالته دون أن يظهر فيها بريده الالكتروني، لذلك لابد من الحصول على المزيد من المعلومات التي يمكن العصور عليها في حاشية وسائل البريد (Email Leader) وهي أو خطوة للبدء في التحري عن المرسل الرسالة الالكترونية.[4]

---

[1] انظر المادة 46 / 2 من الدستور الجزائري، المؤرخ في 8 ديسمبر 1966 المعدل بالقانون رقم 1601 المؤرخ في 26 جمادى الأول عام 1437 المواقف ل 6 مارس 2016 المتضمن التعديل الدستوري، العدد 14.

[2] انظر المادة 65 مكرر 5 من الأمر 66-155 المؤرخ في 18 صفر 1386هـ المواقف ل 8 يونيو سنة 1966 م، المتضمن قانون الإجراءات الجزائية الجزائري ج ر ج ج عدد 48 صادر بتاريخ 11 جوان 1966، المعدل والمتمم.

[3] انظر المادة 65 مكرر ،7، المتضمن ق . ا . ج ، ج، السابق الذكر.

[4] مدربل كريم الإثبات بالدليل الرقمي في المسائل الجزائية، مذكرة الماستر كلية الحقوق، جامعة اكلي محند اولحاج البويرة 2019، ص 43 .

المبحث الثاني: ماهية الجريمة الرقمية

لقد عرف رواج الانترنت كوسيلة للاتصالات واستعمالها في جل المعاملات اليومية ظهور سلبيات عديدة، خاصة بعد استغلال الكثير من المجرمين هذا التغير في نمط المعاملات مما أدي إلى ظهور جرائم لم يكن يعرفها القانون من قبل ك الجريمة الإلكترونية بحيث أخذت هذه الظاهرة الإجرامية حيزا كبيرا من الدراسات من أجل تحديد مفهومها، ولهذا قسمنا هذا المبحث إلى مطلبين، خصصنا الأول لمفهوم الجريمة الرقمية، والثاني لتصنيفها.

المطلب الأول: مفهوم الجريمة الرقمية

نتطرق من خلال هذا المطلب إلى تعريف الجريمة الرقمية وأركانها من خلال الفرع الأول، وإلى خصائصها ودوافع ارتكابها من خلال الفرع الثاني.

الفرع الأول: تعريف الجريمة الرقمية وأركانها

- التعريف الضيق للجريمة الإلكترونية:

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وربطها بعناصر عديدة كالحاسوب أو مستخدمه أو بموضوع الجريمة حيث عرفها الفقيه ماروي (Merwe) على أنها: "الفعل غير مشروع الذي يستخدم في ارتكابه الحاسب الآلي." وهناك من عرفها على أنها: " فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"، وفي تعريف أخر هي: "الأفعال غير القانونية المرتكبة بواسطة العمليات الإلكترونية والتي تمس بالنظام المعلوماتي أو بالمعطيات التي يحتويها ومهما كان الهدف من ذلك.[1]

[1] يزيد بو حليط، الجرائم الالكترونية والوقاية منها في التشريع الجزائري (في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات –قانون الإجراءات الجزائية–قوانين خاصة)، دار الجامعة الجديدة للنشر، مصر، 2019، ص 48.

كما عرفت أيضا أنها مجموعة الأفعال غير القانونية التي تتم عبر شبكة الانترنت أو تبث عبر محتوياتها.[1]

كما عرفها الفقيه تديمان (Tiedement) بأنها كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي.[2]

كما عرفها الفقيه روز نبلات (Rosemblatt) بأنها نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه.[3]

ويعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف الحاسب بأنها: "الجرائم التي تلعب فيها البيانات الكومبيوترية والبرامج المعلوماتية دورا رئيسيا".[4]

وعليه يربط أنصار هذا الاتجاه تعريفهم لهذه الجرائم بضرورة وجود الحاسب الذي قد يكون أداة للجريمة أو هدفا لها، ناهيك عن وجود معارف مسبقة بتكنولوجيا الكومبيوتر ليس فقط من المجرم المعلوماتي، وإنما أيضا من القائمين على ملاحقة هذا النوع من الجرائم، وهذا يضيق على نحو كبير من الجريمة الإلكترونية التي هي في اتساع يوما بعد يوم تبعا لتطور تكنولوجيا المعلوماتية.[5]

- التعريف الموسع للجريمة الإلكترونية:

---

[1] هروال هبة نبيلة، جرائم الانترنيت، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة أبو بكر بالقايد، تلمسان، الجزائر، 2013-2014، ص 2.

[2] غانم مرصي الشمري، الجرائم المعلوماتية: ماهيتها، خصائصها، كيفية التصدي لها قانونا، ط 1، دار العلمية الدولية للنشر والتوزيع، الأردن، 2016، ص 25.

[3] حسن الطوالبة، الجرائم الالكترونية، ط 1، جامعة العلوم التطبيقية، مملكة البحرين، 2008، ص 48.

[4] أشرف عبد القادر قنديل، المرجع السابق، 93.

[5] يزيد أبو حليط، المرجع السابق، ص 49.

على عكس الاتجاه السابق يذهب فريق من الفقهاء لضرورة التوسيع من مفهوم الجريمة الإلكترونية أو المعلوماتية وعدم حصرها في الحاسوب وحده أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية.[1]

فعرفت على أنها كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال أو الأشياء المعنوية[2].

كما عرفها الأساتذة (Lestanc) و (Vivant) أنها "مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب"، كما أن الخبير الأمريكي (Parker) تبنى مفهوما واسعا للجريمة المعلوماتية على أنها كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل[3].

كما عرفتها منظمة التعاون الاقتصادي والتنمية (OCDE) بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"، كما تعرف أيضا تلك الجرائم المرتكبة ضد الأملاك باستعمال التقنية أو المعلوماتية ".

إن هذه التعريفات واسعة تتيح الإحاطة الشاملة قد الإمكان بظاهرة جرائم التقنية، كما أنها "تعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية، ويعرفها آخرون على أنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"، إذ يعتمد هذا التعريف على معيارين أولهما وصف السلوك، وثانيهما اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها، كما يجمع الفقه الفرنسي بصفة عامة على القول بأن فكرة الغش المعلوماتي (Fraude

[1] يزيد أبو حليط، المرجع نفسه، ص 50.

[2] بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري، دراسة مقارنة، مذكرة مكملة لمقتضيات نيل شهادة الماستر، كلية الحقوق، جامعة محمد خيضر، بسكرة، الجزائر، 2015-2016، ص 10.

[3] نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 1، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 49.

informatique) التي تعادل جرائم الحاسب الآلي تشمل العديد من الأفعال المتنوعة، حيث عرف كل من الفقيه ميشال (Michel) والفقيه ريدو (Redo) الجريمة المعلوماتية بأنها لسوء استخدام الحاسب ويشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، وكذا الاستخدام غير المشروع البطاقات الائتمان وانتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب وسرقة الحاسب الآلي في حد ذاته أو أي مكون من مكوناته.[1]

وبذلك تمثل هذه التعاريف المفهوم الموسع للجرائم الإلكترونية، والتي تتم بالحاسوب سواء كان هدفا لها أو وسيلة لارتكابها، أو عن طريق شبكة الإنترنت أو بأي وسيلة إلكترونية أخري تظهر مستقبلا كوسائل الاتصال الحديثة مثل الهاتف النقال وجهاز الفاكس وغيرها.[2]

- تعريف الجريمة الإلكترونية في التشريع الجزائري:

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب أحكام المادة 2 من القانون رقم 09-04 على أنها "جرائم" المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، أو أية جريمة أخري ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.[3]

ويلاحظ من هذا التعريف ما يلي:

أولا: أن المشرع الجزائري اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكترونية، وثانيها معيار موضوع الجريمة

[1] يزيد أبو حليط، المرجع السابق، ص 50-51.

[2] المرجع نفسه، ص 51.

[3] المادة 2 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430، الموافق ل 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47.

المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

ثانيا: كما حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الإلكترونية في القانون الجزائري.[1]

أما **أركانها:** إن للجريمة الإلكترونية أركان ثلاثة وتتمثل في الركن الشرعي وهو الصفة غير المشروعة للفعل، وتتمثل قاعدة التجريم والعقاب فيها من خلال ما ورد النص عليه في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أما الركن المادي يتمثل في ماديات الجريمة التي تبرز به إلى العالم الخارجي، وأخيرا الركن المعنوي وهو الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ.

كما أن للجريمة الإلكترونية كغيرها من الجرائم أطراف تتمثل في الجاني (المجرم الإلكتروني) وبهذا المعنى يكون الجاني شخصا طبيعيا ذا أهلية وقدرة على تحمل العقوبة أو شخص معنوي، أما الجاني عليه يكون في الغالب الأعم شخص معنوي، كالبنوك والشركات وغيرها من المنظمات والهيئات التي تعتمد في إنجاز أعمالها على الحاسب الآلي، علما أن للجريمة الإلكترونية محلا يتمثل في المعلومات، الأجهزة، الأشخاص أو الجهات.

الفرع الثاني: خصائص الجريمة الرقمية ودوافع ارتكابها

نتطرق أولا إلى خصائص الجريمة الرقمية وإلى دوافع ارتكابها ثانيا.

أولا: خصائص الجريمة الرقمية

[1] اسمهان بوضياف، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، مسيلة، 2008، ص 352-353.

تتميز الجريمة الإلكترونية بصفة عامة عن الجريمة التقليدية بجملة من الخصائص والسمات التي تجعلها تنفرد عن غيرها من الجرائم وسوف نحاول أن نبرز أهم هذه الخصائص من خلال ما يأتي.

- وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات:

يشترط لقيام الجريمة المعلوماتية أن يقع التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي، وذلك من أجل معالجتها إلكترونيا، بما يمكن المستخدم من إمكانية تصحيحها أو محوها أو تخزينها واسترجاعها أو طباعتها، وهذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية[1].

وعلى الرغم من ارتكاب جرائم المعلوماتية أثناء أية مرحلة من المراحل الأساسية التشغيل نظام المعالجة الآلية للبيانات في الحاسب الآلي (الإدخال المعالجة الإخراج).

فإن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن بالنظر إلى طبيعتها ارتكابها إلا في وقت محدد، ففي مرحلة الإدخال المعلوماتي يمكن إدخال معلومات غير صحيحة، أو عدم إدخال وثائق أساسية، وفي هذه المرحلة وفي مرحلة المعالجة الآلية للبيانات فإنه يمكن إجراء أي تعديلات تحقق الهدف الإجرامي عن طريق التلاعب في برامج الحاسب الآلي، أما في مرحلة المخرجات فقد يقع التلاعب في النتائج التي يخرجها الحاسوب بشأن بيانات صحيحة أدخل فيه وعالجها بطريقة صحيحة.

من المفيد الإشارة أن بعض التشريعات وسعت تعريف المعدات المستخدمة في مجال المعالجة الآلية إلى تلك التي تقوم بالتخزين أو نقل وتلقي بيانات الحاسوب أو المعلومات، ومن الشائع وصف بيانات الحاسوب مثلا كتمثيل للحقائق والمعلومات التي يمكن قراءتها ومعالجتها أو تخزينها بواسطة الحاسوب.[2]

---

[1] اسمهان بوضياف، المرجع السابق، ص 353.

[2] يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، ط 1، مطبعة الرمال، الجزائر، 2019، ص 26-27.

توضح بعض الاتجاهات أن هذا يشمل جهاز الحاسوب والبعض الآخر لم يحدد موقفه لكن من المرجح في الممارسة العلمية أن تتضمن تلك البيانات والمعلومات على وسائط التخزين المادية (مثل الأقراص الصلبة وبطاقات الفلاش للتخزين)، وكذا البيانات والمعلومات المخزنة في نظام بث المعلومات سواء السلكية أو البصرية أو تردد الراديو.[1]

- جريمة عابرة للحدود:

بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها ألاف الأميال[2]، بمعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا إذ إن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي تم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد آخر وهو بهذا السلوك قد يضر شخص أخر موجود في بلد ثالث.[3]

وعليه تعد جرائم المعلومات شكلا جديد من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية، وقد خلفت هاته الخاصية الكثير من الإشكالات القانونية في مسألة الاختصاص القضائي[4]، هل هي الدولة التي وقع فيها النشاط الإجرامي أم التي أضيرت مصالحها نتيجة هذا التلاعب بالإضافة إلى إشكالية مدي فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة مسألة جمع الأدلة وقبولها، إذ تتباين مواقف الدول فيما يتعلق بقبول الأدلة

---

[1] يعيش تمام شوقي، المرجع نفسه، ص 27-28.

[2] يوسف الصغير، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستر في القانون الخاص، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2013، ص 16.

[3] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستر، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2012-2013، ص 31.

[4] يعيش تمام شوقي، المرجع السابق، ص 29.

المستخلصة من أنظمة الحاسبات الآلية، وغيرها من المشاكل التي يمكن أن تثيرها الجرائم العابرة للوطنية بشكل عام.

لذلك فقد لفتت هذه المشكلات النظر إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجريمة المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم لمختلف الدول.

ومن أجل ذلك فقد تعالت الأصوات الداعية إلى التعاون الدولي المكثف من اجل التصدي لها بحزم، وأن يشمل هذا التعاون تبادل المعلومات وتسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى.[1]

-صعوبة اكتشافها وإثباتها:

تتميز الجريمة الالكترونية بصعوبة اكتشافها وإثباتها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء صعوبة في اكتشاف الجريمة الالكترونية وإثباتها إلى عدة عوامل منها[2]:

أولا: أن الجريمة الالكترونية لا تترك أثار مادية، فهي جريمة تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية ولا توجد مستندات ورقية، فهذه الجريمة عبارة عن أرقام تتغير في السجلات فالجريمة الالكترونية لا تترك شهودا يمكن استجوابهم ولا أدلة يمكن فحصها.

ثانيا: صعوبة الاحتفاظ بدليل الجريمة الالكترونية، إذ يستطيع المجرم في أقل من

[1] محمد بوعمرة، سيد علي بنيال، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر، كلية الحقوق، جامعة آكلي محند أولحاج، البويرة، 2018-2019، ص 8-9.

[2] ثنيان ناصر آل ثنيان، المرجع السابق، ص 24.

ثانية أن يمحو أو يحرف أو يغير المعلومات الموجودة في الكمبيوتر.[1]

ثالثا: تحتاج الجريمة الالكترونية لاكتشافها إلى خبرة فنية، حيث تتطلب جريمة الكمبيوتر إلمام ومعلومات واسعة سواء لارتكابها أو التحقيق فيها، كما أن رجال الضبطية القضائية يجدون صعوبة للتعامل مع الدليل الالكتروني، فقد يتسبب المحقق دون قصد في إتلاف الدليل الالكتروني أو تدميره كما في حالة محو البيانات الموجودة على الأسطوانة الصلبة أو قد لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو الطابعة أو الماسح الضوئي، لذلك أصبح من الضروري في وقتنا إجراء دورات تدريبية لرجال الضبطية القضائية ورجال القضاء والخبراء والفنين للتعاون فيما بينهم وصولا إلى أحسن الطرق لمكافحة الجريمة الالكترونية.

رابعا: تعتمد الجريمة الالكترونية على الخداع والذكاء في التعرف على مرتكبيها، إن الذي يساعد على عدم التعرف على مرتكبي الجرائم الالكترونية هو إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم تجنبا للإساءة إلى سمعتها وهز ثقة العملاء بها، وإخفاء أسلوب ارتكاب الجريمة خوفا من قيام الأخريين بتقليد هذا الأسلوب، وهو ما يدفع المجني عليه إلى الإحجام عن إبلاغ السلطات المختصة بها، كما أن الجريمة المعلوماتية تعتمد على الذكاء وهي جريمة فردية تعتمد على مهارات عالية وإلمام بتكنولوجيا النظم المعلوماتية.[2]

- السرعة في التنفيذ:

لا تتطلب جرائم الانترنت عنفا لتنفيذها أو مجهودا كبيرا، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة

[1] حسن فريجة، المرجع السابق، ص 3.

[2] حسن فريجة، المرجع السابق، ص 3.

العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة.[1]

تتميز جرائم الانترنت بأنها جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كب ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوي تقني يوظف في ارتكاب الأفعال غير المشروعة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل بالقاص مع الشبكة للقيام بجرائم مختلفة كالتجسس او اختراق خصوصيات الغير أو الغريرين، فمن هذا المنطلق تعد الجريمة المرتكبة عبر الانترنت من الجرائم النظيفة فلا آثار فيها لأية عنف أو دماء، وإنما مجرد أرقام وبيانات يتم تغيرها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي.[2]

ثانيا: دوافع ارتكاب الجريمة الرقمية

من خلال ما سبق يتضح لنا، أن الجريمة التقليدية والمجرم التقليدي يختلفان تماما عن الجريمة الإلكترونية والمجرم الإلكتروني، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع إلى ارتكاب الفعل غير المشروع، فالدافع(الباعث)، الغرض، الغاية، مفاهيم لكل منها دلالته في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا، ذلك أن القاعدة القضائية تقرر أن الباعث ليس عنصرا من عناصر القصد الجرمي، وأن الباعث لا أثر له في وجود القصد الجنائي، وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة تتمايز، فـالدافع هو العامل المحـرك للإرادة والذي يوجـه السلوك الإجرامي كـالمحبة والشفقة والبغضاء والانتقام، وهو إذن قوة نفسية تدفع الإرادة إلى ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى. أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي، ويتمثل بتحقيق النتيجة التي أصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه

[1] يوسف صغير، المرجع السابق، ص 16.

[2] يوسف صغير، المرجع نفسه، ص 16.

قانون العقوبات. وأما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام، أو سلب مال المجني عليه في جريمة القتل.

وبالنسبة للجريمة الإلكترونية، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنطوية تحت هذا المفهوم[1]، وأهم هذه الدوافع سيتم بيانها من خلال النقاط التالية:

- **الدوافع الشخصية لارتكاب الجريمة الإلكترونية:**

تصنف هذه الدوافع إلى دوافع مادية وأخرى ذهنية، وذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب الجريمة الإلكترونية، أو تأثير العنصر الذهني المعنوي على المجرم الإلكتروني ودفعه لارتكاب جريمته، هذا ما سيتم بيانه من خلال البندين المواليين:

البند الأول: الدوافع المادية.

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الإلكتروني إلى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الألية لها من خلال اكتشافه لفجواها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه، أو لحساب شركائه، أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة. كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب، وقد أشارت في هذا الإطار مجلة" informatique securite" وهي مجلة متخصصة في الأمن المعلوماتي، أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، و23% من أجل

[1] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة، ،2011/2012، ص 46-47.

سرقة معلومات، و19% أفعال إتلاف، و15% الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية. وفي حقيقة الأمر أن في حال نجاح المجرم الإلكتروني في ارتكاب جريمته فإن ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الإلكترونية، حيث تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة للأنظمة المعلوماتية، وأن 64% لحقتهم خسائر مادية جراء هذه الاعتداءات.[1]

البند الثاني: الدوافع الذهنية لارتكاب الجريمة الإلكترونية.

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات. وقد تكون هذه الدوافع مجرد شغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة هذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه، وعلى صعيد آخر قد يكون إقدام المجرم الإلكتروني على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي وإثبات المقدرة[2].

- **الدوافع الموضوعية لارتكاب الجريمة الإلكترونية:**

[1] ضاح محمود الحمود ونشأت مفضي المجالي، جرائم الأنترنت، دار المنار للنشر والتوزيع، 2005، ص 31.
[2] نعيم سعيداني، المرجع السابق، ص 61-62.

قد يتأثر المجرم الإلكتروني ببعض المواقف قد تكون دافعة له على اقتراف الإجرام الإلكتروني ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن إبراز أهم الدوافع من خلال البندين المواليين.

البند الأول: دافع الانتقام وإلحاق الضرر برب العمل.

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته[1]، كما يعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المجرم الإلكتروني الرغبة في الانتقام من رب العمل، ومثال ذلك أن الانتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

البند الثاني: دافع التعاون والتواطؤ.

هذا النوع يتكرر كثيرا في الجرائم الإلكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم.[2]

وإذا كانت هذه أبرز الدوافع لارتكاب الجريمة الإلكترونية، مع ذلك فهي ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لأن السلوك الإجرامي والدوافع لارتكاب الجريمة الإلكترونية قد تتغير

[1] يوسف صغير، المرجع السابق، ص 42.

[2] نعيم سعيداني، المرجع السابق، ص 62.

وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة، إلى تدميرها أو على الأقل حيازتها للقيام بعملية الابتزاز والحصول على الأموال، لذلك فإن هذه الدوافع قد لا تتوقف عند هذا الحد، إذ نجد في كل جريمة جديدة دوافع جديدة، بل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة.[1]

المطلب الثاني: تصنيف الجرائم الرقمية

تصنف الجريمة التقليدية من حيث خطورته إلى جناية وجنحة ومخالفة، ومن حيث طبيعتها تصنف إلى جريمة عادية وجريمة سياسية، جريمة عسكرية، على خلاف الجريمة الالكترونية التي تعددت تصنيفاتها وذلك لكونها من الجرائم المستحدثة، حيث عرفت اختلافا حول تقسيماتها نظرا للاختلاف في تسميتها، ولعل ما يميز هذه الجريمة عن غيرها من الجرائم كونها تنصب على معطيات الحاسوب (بيانات ومعلومات وبرامج....الخ).

والجرائم الالكترونية لا حصر لها ولذلك لا يمكننا أن نجملها بكل أصنافها فهي متشعبة وذلك راجع إلى سرعة تطورها فهناك من صنفها برجوع إلى وسيلة ارتكاب الجريمة أو على أساس محل الجريمة وعلى هذا الأساس قسمنا هذا المطلب إلى الفرعين المواليين.

الفرع الأول: الجرائم الموقعة بواسطة النظام المعلوماتية

يعد النظام المعلوماتية الوسيلة الأساسية لارتكاب هذا النوع من الجرائم ووسيلة لتسهيل النتيجة الإجرامية ومضاعفة لجسامتها وهي أنواع منها الجريمة الواقعة على الأشخاص أولا، ومنها ما هو واقع على الأموال ثانيا، والجريمة الأخيرة الواقعة على أمن الدولة ثالثا، وهذا ما سنوضحه في النقاط التالية:

أولا: الجرائم الواقعة على الأشخاص

[1] نعيم سعيداني، المرجع نفسه، ص 63.

إن للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، حيث أن الهدف الأول والاسمي من وضع القوانين هو حماية سلامة الأشخاص من مختلف الانتهاكات التي قد يتعرضون لها سواء في أبدانهم كالقتل أو الجرح أو الضرب أو إعطاء مواد ضارة، كما يمارس بعضها على الجنين في رحم أمه كجريمة الإجهاض ومنها ما يمس عرض الإنسان وحياءه كالاغتصاب.[1]

أما فيما يتعلق بالجريمة الالكترونية (المعلوماتية) فهناك العديد من الأفعال تدخل في نطاق هذا النوع من الجرائم والتي تستهدف الأشخاص في حياتهم وتشويه سمعتهم وكذلك التحريض عن القتل عبر الانترنت والتهديد والتحرش والمضايقة عبر وسائل الاتصال والملاحقة عبر وسائل تقنية وأنشطة اختلاس النظر والاطلاع على البيانات الشخصية.[2]

وهذا ما سنتطرق إليه في النقاط التالية:

1-جرائم القذف والسب:

عرف المشرع جريمة القذف في المادة 296 من قانون العقوبات الجزائري وعرف السب في المادة 297 من نفس القانون كما أن هذه المواد لم تشر إلى الوسيلة الالكترونية لنشر ذلك الادعاء أو الإسناد.[3]

تعتبر جريمة القذف والسب من أكثر الجرائم شيوعا عبر شبكة الانترنت حيث توجد هناك مواقع متخصصة تعمل على إبراز سلبيات الشخص المستهدف وإفشاء أسراره من أجل تشويه شرفه وسمعته.[4]

---

[1] محمود نجيب حسني، شرح قانون العقوبات (القسم الخاص)، ط 16، دار النهضة العربية، مصر، 1989، ص 317.

[2] لينا محمد الأسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، دار حامد، الأردن، د س ن، ص 35.

[3] راجع المادة 286 من قانون العقوبات الجزائري.

[4] حكيمة شريد، مايسة ربيع، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2016، ص 22.

وتعتبر شبكة الانترنت مسرحا غير محدود لارتكاب تلك الجرائم، وتتم وجاهيا عبر خطوط الاتصال المباشر أو يكون كتابيا، وذلك عبر المبادلات الالكترونية (بريد الكتروني، صفحات الويب غرف المحادثة).[1]

وهنا لابد من القول أن الجاني في مثل هذه الجرائم غالبا ما يستعمل البرامج التي تساعده على إخفاء هويته أثناء القيام بمثل هذه الأفعال عند إرسال البريد أو تصفح المواقع، الهدف من ذلك هو الخوف من تعرضهم للمساءلة القانونية أو الخجل من التصرفات الغير لائقة التي يقومون بها.

وفي المادة 144 مكرر والمادة 146 من قانون العقوبات نجد أن القذف والسب الموجه لرئيس الجمهورية أو الهيئات سواء قضائية أو أمنية أو أي هيئة أخري قد تكون بأية آلية لبث الصورة أو الصوت أو بأي وسيلة الكترونية أو معلوماتية أو إعلامية أخرى.

2-جرائم الاعتداء على حرمة الحياة الخاصة:

تعد فكرة الحياة الخاصة مسألة دقيقة جدا، وذلك لأنها تحكمها معايير المجتمع وعاداته وتقاليده.

وعلى هذا فإن جريمة الاعتداء على حرمة الحياة الخاصة في مجال المعلوماتية هي كل اعتداء على البيانات الاسمية عبر الانترنت وذلك عن طريق التمركز في موقع معين داخل شبكة الانترنت والعمل على تسجيل وحفظ البيانات المتبادلة فيما بين الأنظمة المعلوماتية[2].

3-جريمة التهديد:

[1] عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية الحاسب الآلي وشبكة المعلومات (الانترنت)، ط 1، دار الأوراق للطباعة والنشر والتوزيع، لبنان، 2004، ص 312.

[2] برمش مراد، خصوصية الجريمة الالكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر 1، 2020-2021، ص 72.

وهي التي يتم من خلالها إرسال بعض الصور أو الكتابات على الشخص المراد تهديده أو ابتزازه بغية حمله على القيام بفعل معين أو منعه من القيام به[1]، ويتم إرسال مثل هذه الكتابات إلى البريد الالكتروني أو في وسائل الحوارات الآنية المختلفة على شبكة الانترنت مثل الفايسبوك والواتساب .... الخ.

4- انتحال الشخصية:

تعني هذه الجريمة استخدام شخصية شخص أخر للاستفادة من سمعته أو ماله أو صلاحياته، وتتخذ جريمة انتحال الشخصية عبر الانترنت أحد الأسلوبين: إما انتحال شخصية الفرد أو انتحال شخصية المواقع، من أجل تحقيق أغراض ومصالح غالبا ما تكون الاستفادة منها بشكل مادي بطريقة ذكية تجعل من الصعب اكتشاف الفاعل.[2]

ثانيا: الجرائم الواقعة على الأموال

إذا كان قانون العقوبات الجزائري شأنه شأن كل القوانين العقوبات الأخرى قد جرم الاعتداء على الأموال في صورها التقليدية كالسرقة والنصب، خيانة الأمانة، واختلاس الأموال العامة، فقد كان ذلك في ظل عصر لا يعرف سوي النقود الورقية أو المعدنية وما يحل محلها من الصكوك والأوراق المالية كالسفتجة والشيك... إلخ.

ونظرا لتطور التقني والتكنولوجي في الوسائل المستخدمة في الاعتداءات عبر الانترنت، أصبحت معظم المعاملات التجارية تتم من خلالها مثل البيع والشراء، مما انجر عنه تطور وسائل الدفع والوفاء وأصبحت جزء لا يتجزأ من هذه المعاملات، في خصم هذا التداول المالي عبر الانترنت، حيث انتهز بعض المجرمين الفرصة من أجل السطو عليها، فابتكرت عدة طرق

[1] لينا محمد الأسدي، المرجع السابق، ص 45.

[2] حكيمة شريد، مايسة ربيع، المرجع السابق، ص 23.

من أجل ذلك كالسرقة والتحويل الالكتروني الغير المشروع للأموال والغسيل المعلوماتي[1]، وهناك عدة جرائم تندرج تحتها لعل أهمها:

- **جريمة غسيل الأموال عبر الانترنت:** إن جريمة غسيل الأموال هي من الجرائم المعاصرة وتعتبر من أخطر جرائم عصر الاقتصاد الرقمي[2]، فالسبب الذي أدي إلى ارتكاب مثل هذه الجريمة غسيل الأموال عبر هذه الوسائل المستحدثة هي السرعة وإغفال التوقيع وانعدام الحواجز الحدودية بين الدول، كما أن البطاقات الذكية والتي تشابه بطاقات البنوك التي تستخدم في مكان الصرف الآلية تساعد على تحويل الأموال بواسطة المودم أو الانترنت مع ضمان تشفير وأمان العملية.[3]

وهذا ما جعل عملية غسل الأموال عبر الوسائل التقنية خاصة عبر شبكة الويب العالمية، تتم بسرعة ودون أن تترك أي أثار في الغالب.[4]

- **جريمة الإتلاف المعلوماتي:** الإتلاف هو تخريب الشيء محل الجريمة وذلك بإتلافه أو التقليل من قيمته مما يجعله غير صالح للاستعمال أو تعطيله.[5]

وجريمة إتلاف المعلومات تتخذ إما صورة إجراء تعديلات غير مشروعة لها أو تدميرها أو الإدخال غير مشروع للمعلومات داخل أنظمة الحاسبات الآلية وهذا الجاني يكون على دراية وعلم بأن الأموال التي يتعدى عليها بالإتلاف ملك للغير وأن فعله من شأنه أن يتلف الشيء أو يجعله معطل أو يجعله غير صالح للاستعمال أو ينقص من قيمته.[6]

---

[1] اسمهان بوضياف، المرجع السابق، ص 358.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، مصر، 2018، ص 452.

[3] لينا محمد الأسدي، المرجع السابق، ص 51.

[4] عبد الفتاح بيومي حجازي، المرجع السابق، ص 17.

[5] خالد ممدوح إبراهيم، المرجع السابق، ص 416.

[6] خالد ممدوح إبراهيم، المرجع السابق، ص 420.

– **التلاعب بالبطاقة المالية:** لقد ظهرت أولي هذا النوع من الاحتيال بالتقاط الأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود إلى أن ظهرت الصرافة الآلية أما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الأرقام السرية الخاصة بها وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات وفي هذا النوع من الاعتداءات لا نجد صعوبة في تطبيق نصوص جرائم السرقة والنصب عليها سواء تم ذلك عن طريق سرقة البطاقة نفسها، أو عن طريق سرقة الرقم السري واستخدامه استخدام غير مشروع.[1]

– **جريمة الاحتيال الالكتروني:** الاحتيال المعلوماتي أو الغش المعلوماتي هي كل فعل أو مجموعة من الأفعال غير المشروعة والمعتمدة التي ترتكب بهدف الخداع أو التحريف للحصول على شي ذي قيمة ويكون نظام الحاسوب لازما لارتكابها أو إخفائها.[2]

وقد يسعي البعض إلى استغلال المعلومات للحصول على كسب مادي غير مشروع، من خلال الدخول إلى معطيات الحاسوب والتلاعب بها وتحويل الأموال إلى حسابه الخاص مما يسبب الضرر للآخرين.[3]

فجرائم الاحتيال تنصب على معطيات الحاسوب المخزنة فيه من أجل الحصول على الأموال أو الخدمات، حيث تتم بالتلاعب وفق الدلالة التقنية الواسعة بمعطيات الحاسوب المخزنة أو نظام المعالجة الآلية.[4]

---

[1] عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية (دراسة مقارنة)، مذكرة لنيل الماجستر، جامعة الشرق الأوسط، الأردن، 2014، ص 2.

[2] بشرى عواطة، حجة الدليل الالكتروني في الإثبات الجنائي، مذكرة ماستر، كلية الحقوق، جامعة 08 ماي 1945، قالمة، 2017-2018، ص 21.

[3] خالد عباد الحلبي، المرجع السابق، ص 99.

[4] خالد عباد الحلبي، المرجع نفسه، ص 101.

ثالثا: الجرائم الواقعة على أمن الدولة

إن التقدم الهائل في الوسائل الالكترونية واستخدام الانترنت وانتشارها الواسع سمحت لبعض الجماعات المتطرفة بنشر وبث معتقداتهم وأفكارهم، بل تعدي الأمر إلى ممارسات تهدد أمن الدولة خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا طريق أخر لاستخدام النظام المعلوماتي حيث سمحت لهم بارتكاب جرائم في غاية الخطورة بحق المجتمعات والدول، بل الأخطر من هذا سمح للكثير من الدول معرفة أسرار الدولة كأسرارها العسكرية والاقتصادية لممارسة ما يسمي بالتجسس[1]، وسنطرح بعض الجرائم التي تمس بأمن الدولة في النقاط التالية:

- **الإرهاب:** تعد جريمة الإرهاب من الجرائم البالغة الخطورة التي تواجه العالم بأسره، فهو يرتبط بعوامل اجتماعية وثقافية وسياسية وتكنولوجية، حيث أصبحت هذه الأخيرة أحد العوامل الإستراتيجية التي تمكن التنظيمات الإرهابية وأنصارها من استخدام الانترنت استخداما متزايدا في مجموعة واسعة ومتنوعة الأغراض تشمل التجنيد والتمويل، والدعاية والتحريض على ارتكاب أعمال إرهابية.[2]

حيث أصبح الإرهاب يستخدم الانترنت كثيرا لبث دعايتهم، وعادة ما تتخذ الدعاية شكل اتصالات عبر وسائط متعددة تحمل تعاليم إيديولوجية وإرشادات عملية، أو تقدم شروع للأنشطة الإرهابية أو تسوق المبررات لها أو تشجع على القيام بها، ومن بين ما يمكن أن تتضمنه هذه الاتصالات والرسائل الافتراضية والعروض الإيضاحية والمجلات والأطروحات وملفات صوتية ومرئية، وألعاب الفيديو التي تصممها التنظيمات الإرهابية أو يصممها المتعاطفون معها.[3]

- **جريمة التجسس:** تعتبر جريمة التجسس من أذكي الجرائم وأدهاها مقارنة بتلك الواقعة على أمن الدولة الخارجي، وازدادت ظاهرة التجسس خطورة في العصر الحالي نظرا لتزايد الوسائل

---

[1] اسمهان بوضياف، المرجع السابق، ص 358.

[2] مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC بفيينا، استخدام الانترنت في أغراض إرهابية، الأمم المتحدة، نيويورك، 2013، ص 3.

[3] مكتب الأمم المتحدة، المرجع السابق، ص 3.

وتطورها، فالتجسس هو الاطلاع على المعلومات الخاصة بالغير المؤمنة وليس مسموحا لغير المخولين بالاطلاع عليها.[1]

فالفاعل يسعي إلى كشف الأسرار أو معناها أو جهتها أو صاحبها أو قيمتها المهم أن تتمتع تلك المعلومات بخاصية الإخفاء.

فالتجسس المعلوماتي لا يشمل مجال واحد بل هو متعدد المجالات وأوجه النشطات المختلفة، حيث يمكننا القول عنه أنه أصبح يشمل الجوانب الصناعية والتجارية للمؤسسات الاقتصادية كما يشمل الجوانب المتعلقة بالجانب العسكري والأمني للدولة[2].

مارس العديد من الدول المعلوماتي حيث من قبل دولة دولة أخرى، أو من قبل دولة على مواطنيها، أو من قبل شركة على شركة منافسة.

-**الجريمة المنظمة:** تعرف الجريمة المنظمة بأنها تعبير عن المجتمع الإجرامي يعمل خارج إطار الشعب والتعقيد والحكومة ويضم بين طياته ألاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة. يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما، كما يخضع أفرادها لقواعد قانونية سنوها لأنفسهم وترفض أحكام بالغة القسوة على من يخرج من نظام الجماعة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة حيث يجنون من وراءها أموال طائلة. فالجريمة المنظمة. وبسبب تقدم وسائل الاتصال والتكنولوجيا، أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان، بل أصبح انتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود الجغرافية.[3]

[1] محمد عبد الرحيم، سلطان العلماء، جرائم الانترنت والاحتساب عليها، بحوث مؤتمر القانون والكمبيوتر والانترنت، المجلد 3، ط 3، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص 880.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 209.

[3] نهلا عبد القادر مومني، المرجع السابق، ص 87.

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتية والبرامج الالكترونية

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتية هناك نوع آخر من الجرائم المعلوماتية يمس النظام المعلوماتية ويستهدف إما المكونات المادية للنظام المعلوماتية أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتية[1].

وهذا ما سنتطرق إليه بشي من التفصيل في النقاط التالية:

أولا: الجرائم الواقعة على المكونات المادية للنظام المعلوماتية

يقصد بالمكونات المادية للنظام المعلوماتية الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات والشرائط والكابلات... الخ، ونتيجة للطبيعة المادية لهذه المكونات ف الاعتداء عليها يكون عن طريق جرائم عادية وتقليدية، كأن تكون محلا للسرقة أو خيانة الأمانة أو الإتلاف العمدي كإحراقها أو ضرب الآلات بشيء ثقيل أو حاد أو العبث بمفاتيح التشغيل أو خربشة الشريط وإفساد أسطوانات التشغيل مغناطيسيا بتعريضها إلى أي مجال مغناطيس متلف، ويترتب على هذا الإتلاف خسائر كبيرة.[2]

ثانيا: استغلال نظم المعلومات كمحور أساسي في الجريمة الالكترونية تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة حيث يتمثل هذا الأسلوب في تدمير البرامج من خلال التسلل إلى المواقع وبث الفيروسات أو البرامج المخربة التي تمحو البيانات وتعرقل سير العمل، وتؤدي إلى خسائر اقتصادية فادحة، ولعل أهمها الاختراق واستعمال البرامج الخبيثة (فيروس Virus)، والجرائم الواقعة على برامج التشغيل.[3]

أ-**الاختراق:** يتحقق هذا بولوج شخص غير مخول له الدخول إلى نظام الكومبيوتر والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية أو تدمير

[1] اسمهان بوضياف، المرجع السابق، ص 358.

[2] اسمهان بوضياف، المرجع السابق، ص 359.

[3] بن طالب ليندا، المرجع السابق، ص 24.

الملفات أو البرمجيات أو النظام أو لمجرد الاستخدام الغير مشروع، ويتحقق الاقتحام بشكل تقليدي من خلال أنشطة الاختراق والتخفي)، ويراد به تظاهر الشخص المخترق بأنه شخص آخر مصرح له بالدخول، أو من خلال استغلال نقاط ضعف في النظام إجراءات السيطرة والحماية أو من خلال المعلومات التي يجمعها الشخص المخترق من مصادر مادية ومعنوية، كالتنقيب في قمامة المنشأة للحصول على كلمة السر أو معلومات عن النظام[1]، حيث تنص المادة 394 مكرر من ق ع يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من المنظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة أذا ترتب على ذلك حذف أو تغير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام الاشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج.[2]

ومن أهم أساليب الاختراق ما يلي:

1- **الاختراق عن طريق استعمال نظام التشغيل:** لأن نظم التشغيل مليئة ب الثغرات، فإنه يتم استغلالها في عملية الاختراق ولكن الأهم هو القيام بذلك عن طريق البروتوكولات التي يستخدمها النظام للتعامل مع شبكة الانترنت أو الشبكات الداخلية بأنواعها.[3]

2- **الاختراق باستخدام البرامج:** لابد لقيام الاختراق بهذه الطريقة من وجود برنامجين، أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم server لأنه بمثابة الخادم الذي يتأثر ب أوامر المخترع وينفذ المهام الموكلة إليه داخل جهاز الضحية، وثانيهما برنامج يوجد بجهاز المخترق

[1] خالد عباد الحلبي، المرجع السابق، ص 51.

[2] انظر المادة 394 من الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386، الموافق ل 8 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم، ج ر، العدد 37.

[3] محمد خليفة، الحماية الجنائية لمعطيات الجانب الآلي، دار الجامعة الجديدة للنشر، مصر، 2007، ص 42.

ويسمى ببرنامج المستفيد العميل client، وأشهر مثال على هذه البرامج وأخطرها هو برنامج حصان طروادة.[1]

3- **المسح والنسخ:** هو أسلوب يستخدم فيه برنامج الماسح وهو برنامج احتمالات يقوم على فكرة تغير وتركيب أو تبديل احتمالات المعلومة، ويستخدم تحديثا بشأن احتمالات كلمة السر أو رقم الهاتف الموزع أو نحو ذلك، ومن جديد فإن هذا الاسلوب تقني يعتمد واسطة تقنية هي برنامج الماسح بدلا من اعتماد على التخمين البشري.[2]

-**البرامج الخبيثة (Les virus):** تعد الفيروسات بمثابة المرض المعدي الذي يصيب المعطيات فيقضي عليها أو يشوهها فتذهب في كلتا الحالتين بفائدتها، وفيروس الحاسب الآلي يشبه إلى حد كبير الفيروس الذي يصيب الإنسان لقدرته على الانتقال من حاسب إلى آخر فهو برنامج مثل أي برنامج أخر موجود على جهاز الحاسب الآلي يصمم بشكل يجعل منه قادر على نسخ نفسه إلى نسخ كثيرة والانتشار من نظام لأخر عبر شبكات الاتصال والقدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافه، كما انه قد يكون مصمما لتدمير برامج أخري أو تغير معلومات ثم يقوم بتدمير نفسه ذاتيا دون أن يترك أي أثر يدل عليه، فبمجرد فتح البرنامج الحامل للفيروس أو الرسائل البريدية المرسل معها الفيروس يصاب الجهاز به ومن ثم يبدأ الفيروس بالعمل وفقا للأسلوب الذي صمم لأجله[3]، والفيروسات أنواع لعل أهمها:

1 - **فيروس الحب:** يتمثل هذا الفيروس في شكل رسالة أو صورة مثيرة للإغراء، ترسل إلى البريد الالكتروني للمستخدم لحثه على فتحها وتكون ملحقة برسالة عادية، ويتذكر الفيروس في شكل رسالة بريدية آمنة وبمجرد فتح الرسالة، يقوم الفيروس بنسخ نفسه مرات عديدة، مما يضاعف قدرته على الانتشار لحذف الملفات أو إخفائها ويستبدلها بنسخ منه، ويقوم أيضا

[1] محمد خليفة، المرجع السابق، ص 42.

[2] محمد خليفة، المرجع السابق، ص 44.

[3] بن طالب ليندا، المرجع السابق، ص 25-26.

بإرسال رسالة بريد الكتروني لكافة العناوين الالكترونية الموجودة في سجل العناوين الالكترونية.[1]

2-**دودة الانترنت:** هي فيروس تنتقل عبر شبكة الانترنت، ويعتمد على استخدام برنامج Outlook express بشكل أساسي للقيام بعملية الانتشار وإصابة أكبر عدد ممكن من الأجهزة، ويقوم مصممه بزرعه داخل رسالة بريد الكتروني، ويرسلها إلى عدد كبير من مستخدمي الشبكة وبمجرد قيامهم بفتحها يبدأ الفيروس في الحصول على دفتر العناوين Address book الخاص بكل واحد منهم ثم إرسال هذه الرسالة للعديد من أصدقائهم فيفتحونها دون أدني شك لمعرفتهم للمرسل فيقع ضحية هذا الفيروس، وهذا ما أدي إلى انتشاره بنسبة كبيرة في العالم.[2]

ثالثا: جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتية

للمعلومة المعالجة آليا أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتية ولما لها من قيمة اقتصادية، وبهذا تعد هدفا للجرائم المعلوماتية من خلال التلاعب فيها أو إتلافها أو حذفها أو تغييرها.[3]

- **إتلاف المعلومات:** إن مكونات الحاسوب سواء مادية أو معنوية يمكن أن تتعرض لجريمة الإتلاف التي تعني تخريب وتغير المعلومات والبيانات المخزنة على الحاسوب ومحوها وتعديلها بهدف الاستفادة منها أو مجرد تخريبها والهدف من تدمير نظم المعلومات هو إتلاف أو محو تعليمات البرامج أو البيانات ذاتها، ولا يهدف إلى مجرد الحصول على منفعة الحاسوب أيا كان شكلها ولكن يريد ببساطة إحداث ضرر بنظام المعلوماتية وإعاقته على أداء وظائفه.

[1] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، مصر، 1994، ص 145.

[2] عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق، جامعة أبو بكر بالقايد، تلمسان، 2017-2018، ص 123.

[3] اسمهان بوضياف، المرجع السابق، ص 360.

ويتخذ الإتلاف عدة صور فقد يتم عن طريق طرق الإتلاف العادية كالحريق أو السرقة أو عن طريق استبدال أو محو المعلومات، ويشكل استبدال المعلومات نوع من جرائم الغش أو التزوير المعلومات وأما محو المعلومات فهو أسهل طرق الإتلاف كونه من خصائص الجرائم الالكترونية، وقدرة الجاني على محو أثار الجريمة في فترة وجيزة جدا لا تتعدي الضغط على زر بسيط في لوحة المفاتيح عن طريق الفأرة[1].

- **التلاعب بمعطيات الحاسوب:** إن التلاعب بمعطيات الحاسوب، يعني التلاعب بالبرامج والبيانات والمعلومات المخزنة فيه بقصد الاستلاء على المال دون وجد حق وهو أخطر طرق الاحتيال لصعوبة اكتشافه وللأضرار الجسيمة التي يسببها للآخرين.

والتلاعب بالبيانات والمعلومات يعني تغير مضمونها أو تعديلها أو تحريفها أو وضع بيانات خاطئة وغير صحيحة أو التوصل إلى منع إدخال بيانات جديدة، وهذه من صور الغش المعلوماتي الذي يهدف إلى الحصول على الأموال بطرق غير مشروعة.

أما فيما يتعلق بالبرامج فهي تعني إدخال أوامر الحاسوب من أجل الاستيلاء على أموال الآخرين بطريقة الغش والتحايل، حيث يقوم المحتال وغالبا ما يكون موظفا في البنك بفتح حساب خاص بيه وتحويل مبالغ من حسابات الآخرين لحسابه.[2]

رابعا: الجرائم الواقعة على البرامج الالكترونية

وتنقسم هذه الجرائم إلى جرائم واقعة على البرامج التطبيقية وبرامج التشغيل وسنتطرق لهاتين الصورتين:

أ-الجرائم المعلوماتية الواقعة على البرامج التطبيقية:

[1] خالد عباد الحلبي، المرجع السابق، ص 68.

[2] خالد عباد الحلبي، المرجع نفسه، ص 106.

يقوم الجاني في هذه الصورة بتحديد البرنامج أولا ثم التلاعب فيه لتحقيق أكبر قدر من الاستفادة المادية.

1- **تعديل البرنامج:** الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود وتكثر هذه البرامج في مجال الحسابات[1].

ومن أمثلة ذلك قيام أحد المبرمجين بالبنوك الأمريكية بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بتقيد المصاريف الزائدة في الحساب الخاص به أطلق عليه اسم Zawick وحصل على إثر ذلك على مئات الدولارات كل شهر[2].

2- **التلاعب في البرنامج:** يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية، أو عن طريق قيام أحد المبرمجين بزرع برنامج فرعي غير مسموح به بالبرنامج الأصلي يسمح له بالدخول الغير مشروع في العناصر الضرورية لأي نظام معلوماتي.[3]

ب-الجرائم المعلوماتية الواقعة على برامج التشغيل:

وهي البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم وضبط ترتيب التعليمات الخاصة بالنظام، ويتحقق هذا النوع من الجرائم المعلوماتية في شكلين:

1-**المصيدة:** تتمثل في إعداد برنامج به أخطاء وعيوب عمدا، لا يكتشف بعضها عند استخدام البرنامج، إذ يترك المبرمج ممرات خيالية وفواصل وتفرعات في البرنامج حتى يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال تفرعات إضافية أو إحداث مخارج وسيطة للولوج داخل نظام معلوماتية، وبهذه التقنية يمكن للمبرمج استخدام البرنامج في أي وقت وفق أهوائه.[4]

---

[1] أحمد خليفة الملط، الجرائم المعلوماتية، ط 2، دار الفكر الجامعي، مصر، 2006، ص 174.

[2] اسمهان بوضياف، المرجع السابق، ص 361.

[3] أحمد خليفة الملط، المرجع نفسه، ص 545.

[4] محمد سامي الشوا، المرجع السابق، ص 82.

2-**تصميم برنامج وهمي:** وتقوم هذه الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه مخصص خصيصا لارتكاب الجريمة ومراقبة تنفيذها، ومن أمثلة ذلك قيام إحدى شركات التأمين الأمريكية في مدينة لوس انجلوس بواسطة مبرمجيها تصميم برنامج وهمي يقوم بتصنيع وثائق تأمين الأشخاص وهمين بلغ عددهم 46.000 بهدف تقاضي هذه الشركة من اتحاد شركات التأمين عمولات من نظيراتها.[1]

[1] اسمهان بوضياف، المرجع السابق، ص 361.

الفصل الثاني

الفصل الثاني: معوقات الإثبات وحجيته في الجريمة الرقمية

يعتبر الإثبات الجنائي الأساس الذي تتحقق به براءة المتهم أو إدانته، كما يعد من أهم مواضيع الإجراءات الجنائية ذلك أن هدف هذه الأخيرة هو إظهار الحقيقة كما وقعت، وبالنسبة للإثبات الجنائي فهدفه هو إقامة الدليل من أجل الكشف عن الحقيقة التي وقعت بشأن الجرائم التي ارتكبت، وذلك بغية تحقيق العدالة المرجوة، وذلك عن طريق الاستعانة بكافة وسائل الإثبات ومنح القاضي الحرية في تقدير الأدلة المطروحة عليه، عملا بمبدأ الاقتناع القضائي القائم على حرية الإثبات، على عكس الإثبات في المواد المدنية الذي يقوم على نظام الأدلة القانونية أو بمصطلح آخر مبدأ الإثبات المقيد.

بالرغم من الجهود المبذولة في مكافحة الجريمة المعلوماتية إضافة إلى الدور البارز الذي يلعبه الدليل الرقمي في إثبات مختلف الجرائم المعلوماتية، إلا أن الواقع العملي والقانوني كشف عن الكثير من الصعوبات التي تثيرها عملية الإثبات بتلك الأدلة الرقمية الحديثة.

وعليه يقسم هذا الفصل إلى:

المبحث الأول: معوقات إثبات الجريمة الرقمية

المبحث الثاني: حجية الدلائل الرقمية في الإثبات

المبحث الأول: معوقات إثبات الجريمة الرقمية

سنتطرق في هذا المبحث إلى القيمة الثبوتية للدليل الرقمي، وذلك من خلال تبيان إجراءات استخلاص الدليل الرقمي وذلك في المطلب الأول، لفهم الطرق والأساليب المستخدمة في استخلاص الدليل الرقمي، أما المطلب الثاني فخصصته لصعوبات استخلاص الدليل الرقمي.

المطلب الأول: إجراءات استخلاص الدليل الرقمي

إن الإثبات من الناحية الجنائية هو تلك النتيجة التي تتحقق باستعمال مختلف الوسائل والطرق والإجراءات للتوصل إلى الدليل، والذي بدوره يستعين به القاضي لاستخلاص حقيقة الوقائع المعروضة عليه وفقا لأحكام القانون، وبمعنى آخر إقامة الدليل على الجريمة الواقعة ونسبها إلى المتهم.

وعليه سنتطرق من خلال هذا المطلب إلى الإجراءات التقليدية في الفرع الأول، والإجراءات الحديثة في الفرع الثاني.

الفرع الأول: الإجراءات التقليدية لجمع الأدلة الرقمية

سأقوم بدراسة الإجراءات التقليدية والمتمثلة في التفتيش والمعاينة والخبرة، وذلك لعلاقتها المباشرة بالدليل الرقمي، وسأستبعد الشهادة والاعتراف والاستجواب باعتبارها لا تثير أي صعوبة في اتخاذها نظرا لخضوعها للقواعد العامة المقررة لها قانونا.

أولا: التفتيش

يعد التفتيش من أهم إجراءات التحقيق لأنه في الغالب ما يكشف عن أدلة مادية تؤيد في نسب الجريمة إلى المتهم، فعرف التفتيش بصفة عامة بأنه: "البحث في مكنون سر الأفراد على دليل للجريمة المرتكبة، أو هو البحث عن الدليل..."[1]

[1] عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، الطبعة الرابعة، دار هومة، الجزائر، 2013، ص 266.

وبالنسبة للفقه الفرنسي فقد عرفه بأنه:" البحث الدقيق لكل عناصر الأدلة التي يمكن استخدمها في الدعوى الجزائية والتي تجري على مسكن المتهم"، ومنه يتضح لنا أن التفتيش ما هو إلا وسيلة إجرائية تستهدف ضبط أشياء مادية تتعلق بالجريمة وتفيد في كشف حقيقتها إلا أن ذلك يتعارض مع الطبيعة غير المادية للدليل الرقمي.[1]

أ-مدى خضوع أنظمة الحاسب الآلي للتفتيش: إن نظام المعالجة الآلية للمعطيات يتكون من مكونات مادية وأخرى معنوية، وبناءا على ذلك يمكن القول بأن تفتيش أنظمة الحاسب الآلي يكون بإحدى الصورتين:

- **الصورة الأولى:** تتمثل هذه الصورة في تفتيش مكونات الحاسب الآلي المادية ويتوقف حكم تفتيش هذه المكونات على طبيعة المكان الموجودة فيه سواء في الأماكن العامة أو الخاصة، ذلك أن المكونات المادية تتمثل في وحدات الإدخال التي بواسطتها يتم إدخال البيانات والمعلومات كلوحة المفاتيح، الفأرة، مشغل الأقراص الممغنطة، الماسح الضوئي...، ووحدات المعالجة المركزية والمتمثلة في وحدة الذاكرة المركزية...، ووحدات الإخراج التي تتمثل في الشاشة، الطابعة، وجميع التجهيزات التي تصنف كتجهيزات اتصال المودم.
- وبناءا على هذه الصورة فليس هناك صعوبة عند معاينة القائمين على التفتيش لمسرح الجريمة الواقعة على المكونات المادية للحاسب الآلي، نظرا لعدم التنافي بين تفتيش المكون المادي لجهاز الحاسب الآلي، مع مفهوم التفتيش التقليدي، بالتالي كل ما يتطلبه إجراء التفتيش في هذه الحالة هو أن يتم وفقا للقواعد القانونية التي تحكم التفتيش[2].

---

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، مصر، 2007، ص 223.

[2] بكرى يوسف بكرى، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011، ص 68.

- **الصورة الثانية:** وتتمثل في تفتيش مكونات الحاسب الآلي المعنوية حيث تعتبر المعطيات المعنوية تلك المعلومات التي يتم تنظيمها ومعالجتها داخل نظام المعالجة الآلية للمعطيات وتخزينها بغية استرجاعها عند طلبها، وهي نبضات إلكترونية لا يمكن لمسها، واختلف الفقه حول إمكانية تفتيشها، إذ رأى جانب من الفقه أنه متى كان الهدف من التفتيش ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة، فإن هذا المفهوم يمتد حتى يشمل جميع، أما من جانب آخر فذهب البيانات والمعلومات الرقمية بمختلف أشكالها[1] رأي آخر إلى تعارض المفهوم المادي مع بيانات الحاسب الآلي المعنوية، لذلك فإنه يقترح بالنص صراحة على أن تفتيش الحاسب الآلي لا بد أن يشمل المواد المعالجة عن طريق الحاسب الآلي أو بياناته[2].

ومن خلال هذا تبين لنا موقف المشرع الجزائري من خلال نص المادة 05 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إذ نص صراحة من خلال المادة السابقة الذكر على تفتيش أنظمة الحاسب الآلي، بحيث يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، وأيضا منظومة تخزين معلوماتية.

ب- مدى خضوع شبكات الحاسب الآلي للتفتيش: إن شبكات الحاسب الآلي مهمة لربط الحواسيب مع بعضها البعض سواء كان ذلك على المستوى المحلي أم على المستوى العالمي، ومن خلال ما نصت عليه المادة 05 من القانون 09- 04 فإن هناك احتمالين:

---

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006، ص 378.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص 197.

- **الاحتمال الأول:** في حالة اتصال نظام المتهم بنظام آخر موجود في مكان آخر داخل الدولة حيث نص المشرع في الفقرة الثانية من المادة 05 من القانون 09- 04 على أنه في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكانت هناك أسباب تدعو للظن بأن المعطيات المرجوة مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة، أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.[1]

- **الاحتمال الثاني:** في حالة اتصال نظام المتهم بنظام موجود في مكان آخر خارج الدولة أجاز المشرع الجزائري في الفقرة الثالثة من المادة 05 السابقة الذكر تفتيش الأنظمة المتصلة حتى ولو كانت خارج إقليم الدولة وذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.[2]

ج-مدى صلاحية ضبط الدليل الرقمي: يعد حجز المعطيات المعلوماتية النتيجة الطبيعية التي تترتب عن التفتيش، أي وضع اليد على المكونات المادية والمعنوية للأنظمة المعلوماتية، وهناك طريقتين لضبط المعلومات والأدلة الرقمية التي كانت محل التفتيش:

- **الطريقة الأولى:** وتتحقق عن طريق نسخ وتحميل البيانات والمعطيات محل البحث على دعامة تخزين مادية (الأقراص الممغنطة، بطاقات الذاكرة، المودم) تكون قابلة للضبط والوضع في أحراز مختومة وهذا ما نص عليه المشرع الجزائري بالقول: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية

[1] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجيستير، جامعة الحاج لخضر- باتنة-، كلية الحقوق والعلوم السياسية، 2013، ص 149.

[2] خالد ممدوح ابراهيم، المرجع السابق، صفحة 205.

قابلة للحجز، والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية"[1]، كما أن المشرع عالج إشكالية صعوبة ضبط النظام كله لا سيما إذا ما كان الحاسوب ليس حاسوبا شخصيا وإنما جزء من شبكة معقدة إذ سمح بنسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية قابلة للحجز.

- **الطريقة الثانية:** وتتحقق من خلال استعمال تقنيات وتدابير الحماية الفنية كالتشفير والترميز، وبرامج منع الكتابة، في حالة استحالة ضبط المعلومات لأسباب تقنية، كما يتم اللجوء إلى تعطيل تشغيل المعطيات أو محوها بعد أخذ نسخة منها في حالة ما إذا كانت المعطيات تتضمن خطرا على النظام العام والآداب العامة كالبرامج التي تحتوي على فيروسات.[2]

ثانيا: المعاينة.

تعتبر المعاينة من أهم الوسائل لتكوين أول فكرة عن كيفية ارتكاب الجريمة بالإضافة إلى أنها من أهم مصادر الأدلة الجنائية المادية، ويقصد بالمعاينة:

"مشاهدة العين لمكان أو شخص أو أي شيء لإثبات حالته التي تركها عليه الجاني وضبط كل ما يلزم لكشف الحقيقة[3]".

وتظهر أهمية المعاينة في الجرائم التقليدية في مساهمتها في تصوير كيفية وقوع الجريمة وتحديد ملابساتها وظروف ارتكابها، إلا أن دورها قد يتضاءل في الكشف عن الدليل الرقمي لأسباب منها:

- ندرة الآثار المادية التي يتركها مرتكب الجرائم الإلكترونية.

---

[1] المادة 06 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] المادة 07 من القانون 09-04 السالف الذكر.

[3] خالد ممدوح ابراهيم، المرجع السابق، ص 149.

- حدوث تغيير أو تلفيق أو زوال بعض آثار الجريمة خلال الفترة الممتدة بين اقتراف الجريمة والكشف عنها والتي تكون طويلة نسبيا، نظرا لكثرة الأشخاص المترددين على مسرح الجريمة[1].

وعليه يمكن تجاوز هذا الإشكال من خلال تعامل الفنيين القائمين على عملية المعاينة مع مسرح الجريمة المعلوماتية على أنه مسرحان:

1-**مسرح تقليدي:** ويشمل مختلف المكونات المادية للحاسب الآلي، ويمكن أن يحتوي على آثار مادية مثل بصمات الجاني أو وسائط تخزين رقمية، أو أوراق.

2-**مسرح رقمي:** ويوجد داخل العالم الافتراضي لجهاز الحاسب الآلي، ويحتوي على جميع البيانات والمعلومات الرقمية المخزنة فيه والتي تفيد في التحقيق[2].

وأمام الأسباب السابقة الذكر قام المشرع الجزائري بفرض عقوبة من خلال نص المادة 43 من قانون الإجراءات الجزائية.

ثالثا: الخبرة.

تعرف الخبرة بأنها تلك الاستشارة التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة[3]، إذن هي في مجملها تقرير أو رأي فني صادر عن الخبير في أمر من الأمور المتعلقة بالجريمة.[4]

---

[1] بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي: دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2019، ص 47-48.

[2] فاطمة زهرة بوعناد، "مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانونية، العدد الأول، دون دار نشر، الجزائر، 2013، ص 68.

[3] فاطمة زهرة بوعناد، المرجع السابق، ص 71.

[4] محمد زروق، إشكالية الحصول على الدليل الإلكتروني في الجريمة المعلوماتية، منتدى استشارات قانونية، تاريخ الزيارة: 15-05-2024، الساعة 14:22: متوفر على الرابط law/net.mohamah.www://htt :

1- أهمية الخبرة في كشف وتحليل الدليل الرقمي:

يعد الخبير شخص مختص فنيا في مجال من المجالات الفنية أو العلمية أو غيرها من المجالات الأخرى والاستعانة به في مجال الجريمة المعلوماتية ضروري جدا لأن عملية استخلاص الدليل الرقمي تتطلب مهارة ودراية كبيرة في مجال الحاسب الآلي.

ونظرا لطبيعة عمل الخبير في هذا المجال، اهتم المشرع الجزائري بتنظيم أعمال الخبرة وكيفية اللجوء إليها وذلك من خلال المواد من 143 إلى المادة 156من قانون الإجراءات الجزائية الجزائري، بالإضافة إلى المادة 05 في فقرتها الأخيرة من القانون رقم 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وعليه نظرا لهذا نرى أنه دائما هناك حاجة ماسة إلى خبراء وفنيين من أجل القيام بالعديد من المهام التقنية كالكشف عن الأدلة الرقمية وتحليلها، أو التأكد من عدم العبث بالدليل، أو إعادة تجميع الدليل من المكونات المادية للحاسب الآلي وإصلاحه[1].

2-الضوابط التي تحكم عمل الخبير في الجريمة المعلوماتية:

لقيام الخبير بمزاولة مهامه، وجب توفر مجموعة من الضوابط القانونية والفنية:

- **الضوابط القانونية:** هي أن يتم اختياره من قائمة الخبراء المعدة سلفا حسب نص المادة 144 من قانون الإجراءات الجزائية، بحيث يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة... واستثناء يجوز للجهات القضائية أن تختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول، كما يجب على الخبير أيضا أن يكون قد أدى اليمين القانونية وذلك لكي لا يترتب على عمله البطلان، وهو ما أدلت به المادة 145من

[1] خالد ممدوح ابراهيم، المرجع السابق، ص 302.

نفس القانون، و ذلك بأن يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس[1].

-**الضوابط الفنية:** وهنا يجب على الخبير أن يكون ملما بكل ما يتعلق بالحاسب الآلي وملحقاته، وأن يكون قادرا على أداء المهام الموكلة إليه دون أن ينتج عن ذلك ضررا بالدليل الرقمي المراد استخلاصه.[2]

الفرع الثاني: الإجراءات الحديثة لجمع الدليل الرقمي.

إن الأدلة الرقمية صعبة الوصول إليها، وللحصول على هذا النوع من الأدلة يجب اتباع طرق ووسائل فنية معقدة جرى تقسيمها إلى وسائل مادية وأخرى إجرائية.

أولا: الوسائل المادية الحديثة لجمع الأدلة الرقمية

تعد الوسائل المادية عبارة عن أدوات أو برامج ذات طبيعة تقنية يتم استخدامها في التحقيق بغرض إثبات وقوع الجريمة وتحديد مرتكبها، ومن بين هذه الوسائل نجد:

-استخدام البروتوكول:

يعتبر عنوان الأنترنت المسؤول عن تراسل حزم البيانات عبر شبكة الأنترنت وتوجيهها إلى أهدافها وهو يتواجد بكل جهاز مرتبط بالأنترنت، ويتكون من أربعة أجزاء حيث أن الجزء الرابع يحدد جهاز الحاسوب الذي تم منه الاتصال، وعليه في حالة اقتراف إحدى الجرائم يكون من السهل التعرف على رقم الجهاز الذي تم من خلاله ارتكاب العملية وبالتالي تحديد الجاني[3].

-استخدام معلومات الكوكيز:

[1] براهيم بلعليات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، 2012، ص 304.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 330-331.

[3] خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2009، ص 304.

تعد الكوكيز أداة يتم من خلالها جمع البيانات التعريفية الخاصة بالمستخدم عن طريق الاتصال بين الخادم والقرص الصلب لحاسب المستخدم[1]، ومنه فهو يسجل العديد من المعلومات التي يمكن أن تساعد في التحقيق من بينها تاريخ زيارة الموقع الإلكتروني، أو تاريخ إجراءات التعديلات عليه أو الانتهاء منها، وإضافة إلى ذلك الاحتفاظ بكلمات السر الخاصة بالمستخدم عند زيارته للموقع.[2]

-استخدام معلومات البروكسي:

يعمل البروكسي كوسيط بين المستخدم و الشبكة، و تقوم فكرته على أساس تلقيه طلبا من المستخدم للبحث عن صفحة ما ضمن ذاكرة المحلية المتوفرة لديه، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم بإرسالها دون الرجوع إلى الشبكة، أما في حالة عدم تنزيلها من قبل فإنه يعمل كمزود زبون ويقوم بإرسال الطلب إلى الشبكة العالمية حيث يستخدم أحد عناوين، ومن أهم مزاياه أن الذاكرة المتوفرة لديه تحفظ تلك المعلومات التي تم تنزيلها، وفي حالة وجود أي إشكال يتم فحص تلك العمليات المحفوظة والتي تخص المتهم والموجودة عند مزود الخدمة.[3]

-استخدام برامج التتبع وكشف الاختراق

تقوم برامج التتبع بالتعرف على محاولات الاختراق وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ومثاله برنامج tracer Hack وهو مصمم للعمل في الأجهزة المكتبية، وعندما

---

[1] سيدي محمد البشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية – دراسة تحليلية تطبيقية –، رسالة ماجيستير، جامعة نايف العربية للعلوم الأمنية، السعودية، 2010، ص 73.

[2] –Steve Bunting and William Wei, Encase Computer forensic, Wiley publishing(inc), United States of America , 2006, page 371.

[3] خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص 304.

يرصد محاولة للاختراق يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ بعملية مطاردة تستهدف اقتفاء أثر مرتكب عملية الاختراق، حتى الوصول إلى الجهاز المرتكب منه العملية[1].

أما برامج كشف الاختراق فهي تقوم بمراقبة بعض العمليات التي تتم على مستوى الشبكة أو الحاسب، مع تحليلها بحثا عن وجود أي إشارة تدل على وجود تهديد، وفي حالة اكتشافه لإحدى الاعتداءات يقوم بإنذار مدير النظام ويسجل البيانات الخاصة بذلك الاعتداء.[2]

ثانيا: الوسائل الإجرائية الحديثة لجمع الأدلة الرقمية

هي عبارة عن أساليب محددة قانونا تهدف إلى إثبات وقوع الجريمة وتحدد شخصية مرتكبها، وقد استحدث المشرع الجزائري وسائل إجرائية تتمثل في: اعتراض المراسلات والتسرب والذي جاء بهما القانون رقم 06- 22 المؤرخ في 20/ 12/ 2006 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية الجزائري.[3]

ومن جهة أخرى تم استحداث إجراء المراقبة الإلكترونية الذي أتى بها القانون رقم 09- 04 المؤرخ في 05/ 08/ 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[4]

-التسرب:

يعرف التسرب بموجب المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري بأنه القيام بمراقبة الأشخاص أو المشتبه في ارتكابهم الجريمة من خلال ضابط عون الشرطة القضائية

---

[1] خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع نفسه، ص 306.

[2] خالد ممدوح ابراهيم، الجرائم المعلوماتية، ص 306-308.

[3] قانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم ،84 الصادرة بتاريخ 12/24/ 2006، ص 04.

[4] قانون رقم 04-09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، الصادرة بتاريخ 2009/08/16، ص 05.

تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بإيهامهم أنه فاعل معهم أو شريك أو خاف للجريمة، وقد حددت شروط القيام بعملية التسرب كالآتي:

- الحصول على إذن من وكيل الجمهورية أو من قاضي التحقيق إذا تم فتح تحقيق قضائي.
- أن يكون الإذن الصادر عن وكيل الجمهورية أو قاضي التحقيق مكتوبا ومسببا لمدة أقصاها 4 أشهر، قابلة للتجديد مرة واحدة.
- وجوب تضمنه على هوية ضابط الشرطة القضائية التي تتم عملية التسرب تحت مسؤوليته أو عون الشرطة باعتباره مساعدا له.
- أن يكون هذا الإجراء في جرائم محددة والتي نصت عليها المادة 65 مكرر 05 والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

وعليه يمكن القول أن عملية التسرب في نطاق الجريمة الإلكترونية تتمثل في دخول ضابط أو عون الشرطة القضائية إلى العالم الرقمي، من خلال اختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو اشتراكه في محادثات غرف الدردشة والظهور كما لو كان فاعلا مثلهم، مستعملا أسماء أو صفات وهمية بغية الحصول على معلومات هامة تفيد التحقيق.[2]

- اعتراض المراسلات:

لم يقم المشرع الجزائري بتعريف إجراء اعتراض المراسلات وترك أملا تعريفه للفقه، لذا من خلال نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري، نجد أن عملية اعتراض المراسلات يقصد بها "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات عبارة عن بيانات قابلة للإنتاج

[1] عبد الله أوهابية، المرجع السابق، ص 281.

[2] نعيم سعيداني، المرجع السابق، ص 177.

والتوزيع، التخزين، الاستقبال، والعرض"، إلى أن جاءت المادة 20 الفقرة "و" من القانون رقم 09- 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي وسعت من المفهوم التقليدي للمراسلات، وأدخلت الاتصالات الإلكترونية في مفهومها تماشيا مع التطور التكنولوجي، إذ أنها:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية."

وعليه فقد وضع المشرع الجزائري شروطا للقيام بإجراء اعتراض المراسلات وتتمثل هذه الشروط في:

- الحصول على إذن من وكيل الجمهورية، أو من قاضي التحقيق إذا تم فتح تحقيق قضائي.[1]
- أن يكون الإذن الصادر عن وكيل الجمهورية أو قاضي التحقيق مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات البحث والتحري.
- وجوب تضمنه على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة.[2]
- أن يكون هذا الإجراء في الجرائم المحددة بموجب المادة 65 مكرر 05، من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

أما في الجريمة الإلكترونية فيمكن اعتراض المراسلات من خلال المعلومات التي تحتويها حاشية رسالة البريد الإلكتروني Header mail-E حيث تتضمن على عنوان IP لمرسل الرسالة، وطبقا لهمل تم دراسته من قبل، فعنوان IP يحتوي على معلومات تتمثل في الكمبيوتر

[1] المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري

[2] المادة 65 مكرر 07 من قانون الإجراءات الجزائية الجزائري.

الذي تم إرسال منه الرسالة، وأيضا الموقع الجغرافي الذي أرسلت منه، وفي الأخير معلومات مزود الخدمة الذي يتعامل معه مرسل الرسالة.[1]

- المراقبة الإلكترونية:

هنا نجد أن المشرع الجزائري لم يعرفها، وعرفها الفقه بأنها "العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لاسما مراقبة شبكة الاتصالات، لجمع بيانات ومعلومات عن المشتبه به سواء كان شخصا أو مكانا، أو شيئا حسب طبيعته مرتبط بالزمن، التاريخ أو الوقت لتحقيق غرض أمني أو لأي غرض آخر"، وعليه يمكن القول أن المراقبة الإلكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه[2].

لذا وبالرجوع إلى القانون رقم 09- 04 الذي سبق ذكره، نجد أن المشرع الجزائري لم يعتبر هذا الإجراء طريقة من طرق الحصول على الدليل الرقمي فقط، بل أدرجه ضمن التدابير الوقائية من الجريمة المعلوماتية بداعي حماية النظام العام، وهذا وفقا لنص المادة 04من نفس القانون.

وعليه فقد حدد المشرع الجزائري شروطا للجوء إلى تقنية المراقبة الإلكترونية وهي كالتالي:

- أن يتم تنفيذ هذه التقنية تحت سلطة القضاء وبإذن منه، بحيث لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة.[3]

---

[1] أوساسي فؤاد، دور الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور – الجلفة–، 2020–2019، ص 20.

[2] نبيلة هبة هروال، المرجع السابق، ص 199.

[3] المادة 04 من القانون 09–04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- أن تكون هناك ضرورة تتطلب هذا الإجراء، وذلك عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات البحث أو التحقيق دون اللجوء إلى المراقبة الإلكترونية، وهو ما نصت عليه المادة 04 الفقرة "ج" من القانون 09-04 السالف الذكر[1].

المطلب الثاني: صعوبات إثبات الجريمة الرقمية

نتطرق من خلال هذا المطلب إلى الصعوبات التي تتعلق بالدليل الرقمي في حد ذاته في الفرع الأول، والصعوبات التي تتعلق بجهات التحقيق والتشريع في الفرع الثاني.

الفرع الأول: الصعوبات المتعلقة بالدليل الرقمي

إن من أبرز خصائص الجريمة المعلوماتية هو وقوعها في بيئة الكترونية وهذه الخاصية تترتب عليها جمله نتائج تصعب من مهمة اكتشاف هذه الجرائم لا بل وحتى التحقيق فيها.

وهذا عكس الجرائم التقليدية فرجل الشرطة الذي يقوم بجمع التحريات في واقعة سرقة حتى يصل المتهم، ويستصدر أمرا بالقبض عليه وتتولى جهات التحقيق استجوابه وأحالتها إلى محكمة الموضوع، فكل هذه وقائع خاضعة السيطرة أجهزة العدالة، والدليل فيها مرئي ومقروء، عكس الجريمة المعلوماتية التي تتم دون رؤية لدليل الإدانة، وحتى وجود الدليل يمكن للجاني طمس الدليل او محوه وفي حضور أجهزة العدالة غير المتخصصة، ولذلك فغالبية الجرائم المعلوماتية تكتشف مصادفة وليس بطريق حالة الإبلاغ عنها.[2]

لأنها لا تخلف في الغالب أية أثار مادية كتلك التي تخلفها الجرائم التقليدية، حيث أنها لا تخلف لا سكينة ولا سلاحا ولا ظروفا فارغة لطلقات نارية ولا بقعة دموية أو غير ذلك من الآثار المادية.

[1] طاهر عبد المطلب، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة مسيلة، 2015-2014، ص 24.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 78.

كما أن أغلب الآثار المتخلفة عن هذه الجرائم هي أثار الكترونية وهذه الآثار بدورها وإنما هي عبارة عن نبضات الكترونية غير مرئية بالعين المجردة، فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة بحيث انه لا يمكن رؤيتها إلا خلال الاستعانة بأجهزة ووسائل تقنية تظهرها للعيان إن ضخامة حجم وكم البيانات والملفات المعلوماتية التي تتواجد في البيئة المعلوماتية تصعب من أمكانية تحديد الملفات والبيانات المعلوماتية المجرمة من بين ذلك الكم الهائل لفصلها عن تلك البريئة منها، وتؤدي في الغالب إلى اصطدام مهمة الاكتشاف بحق الأفراد في الخصوصية الشخصية.[1]

كما أن البيئة المعلوماتية غالبا ما تكون مؤلفة من شبكات منتشرة في كافة أرجاء المعمورة ومرتبطة ببعضها البعض عن طريق شبكة الانترنيت، بحيث تتيح الفرصة أمام مجرمي المعلوماتية للولوج عن بعد إلى البيانات المعلوماتية المخزونة في آية بقعة من بقاع العالم، وعلى العكس من ذلك فأن سلطات الضبط القضائي والسلطات التحقيقية لا يكون بإمكانها الولوج إلى تلك البيانات كونها تقع في الغالب خارج حدود اختصاص دولها، بحيث تصطدم بسيادة الدول الأخرى.[2]

ولصعوبة استخلاص الدليل في مثل هذه الجريمة يرى المختصين في جرائم الحاسب الآلي، أن هذا الجهاز وما يقع عليه من جرائم معلوماتية يعد تحديا هائلا لرجال الأمن، ذلك أن رجل الأمن غير المتخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادرة على التعامل مع الجريمة المعلوماتية التي تقع بطريقة تقنية عالية.[3]

---

[1] المرجع نفسه، ص 79.

[2] بن مالك أحمد، الخال ابراهيم، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، جامعة تمنراست، المجلد 05، العدد 01، أفريل 2021، ص 114-113.

[3] عبد الفتاح بيومي حجازي، المرجع السابق، ص 89.

وبعد انتحال الشخصية، وكذلك التسلل الإلكتروني من أبرز أمثلة السلوك الإجرامي في الجرائم المعلوماتية، وذلك كدليل على عدم رؤية دليل الجريمة، فكلاهما يستخدم أساليب عالية التقنية في الدخول إلى المناطق المؤمنة والمحمية إلكترونية أو الوصول إلى مراكز الحاسب الآلي والدخول إلى قواعد المعلومات، ويكون الدخول شخصية أو إلكترونية، فالدخول أو التسلل الإلكتروني، يتم عن طريق قيام الجاني بتوصيل جهازه إلى جهاز آخر له حق الدخول وذلك عن طريق خط هاتفي، وعندما يفتح الجهاز المتصل بمركز المعلومات والمسموح له بذلك، نجد أن جهاز الجاني يمارس نشاطه ويحصل على ذات المعلومات دون أن يراه أحد إلى أن يغلق الجهاز الأصلي صاحب الحق في الدخول، وهذه الجريمة وإن أمكن السيطرة عليها بوسائل متطورة وحراسة شخصية ومراقبة إلكترونية، فإن محاولات القراصنة والمحتالين في الجرائم المعلوماتية تتجاوز هذه الحراسات، ويتضح من خلال ما سبق، أنه عند كشف وتجميع الأدلة في الجرائم المعلوماتية عن طريق الحاسب الآلي تواجهه صعوبة بالغة سببها عدم رؤية الدليل أو عدم القدرة على استظهاره.

بينما في الجرائم المعلوماتية تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي مما تجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة.

لذلك يرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسؤولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم، وهذا يقتضي توفير الإمكانيات التقنية اللازمة لتحقيق الجرائم المعلوماتية، وبمعنى آخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال.[1]

وللاستعانة بها في تحقيق هذه الجرائم، ويتعين عدم التذرع بالميزانيات المالية كسبب يحول دون قيام الدولة بواجباتها نحو تحقيق العدالة الجنائية، وحتى يتم ذلك يرى هذا الجانب ضرورة

[1] سعيداني نعيم، المرجع نفسه، ص 189.

الاستعانة بالنبضة المتخصصة في الحاسب الآلي حال تحقيق الجرائم المعلوماتية وذلك لضبط هذه الجرائم واكتشافها، وتقديم أدلة الإدانة فيها وشرح هذه الأدلة وإبعادها أمام المحاكم، ويجب أن يتم ذلك في أطار القانون الجنائي وخصوصا قواعد الخبرة أمام المحاكم الجنائية والتي ينظمها قانون الإجراءات الجنائية.[1]

الفرع الثاني: فقدان آثار الجريمة

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

ويمكن في الفروض السابقة ارتكاب بعض أنواع الجرائم كالاختلاس أو التزوير وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب أو تعديل البرنامج المخزن في جهاز الكومبيوتر، وتكون النتيجة مخرجات على هوى مستعمل الجهاز الذي ادخل البيانات أو عدل البرنامج دون استخدام وثائق أو مستندات ورقية، وبالتالي تفقد الجريمة أثارها التقليدية.

---

[1] ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية – دراسة تأصيلية تطبيقية –، رسالة ماجيستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012، ص 131.

[2] ثنيان ناصر آل ثنيان، المرجع السابق، ص 132.

ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل المعلوماتية انه يمكن محو الدليل في زمن قصير، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جدا.

بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بها فأنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده، لذلك يجد أعضاء الضبط القضائي، أحيانا أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم فضلا عن صعوبة أجراء التحريات السرية وتتبع مسار العمليات المعلوماتية العابرة للحدود.

ومن المسائل التي أثيرت كذلك بمناسبة تعذر الحصول على الدليل في الجريمة المعلوماتية بطرق تقليدية نظرا لخصوصية هذا النوع من الجرائم، هو مدى سريان الحماية المعول بها للاطلاع غير المصرح به على الأوراق المختومة أو المغلقة، لتمتد إلى نظام المعالجة الآلية للبيانات والمحمي فنية ضد الاختراق، حيث يجب عدم المساس بمبدأ المشروعية.

إن السبب في حظر الاطلاع على الأوراق المغلقة، والمغلقة والمختومة هو رغبة صاحبها في عدم اطلاع الغير عليها، بدليل انه اتخذ سبل الحماية الممكنة ضد محاولة الاطلاع غير المصرح بها ، بدليل إغلاق هذه الأوراق أو تغليفها بأي طريقة وذات العلة تتوافر في البيانات المعالجة آليا، حيث لا يمكن بدون الحصول على مفتاح الشفرة أو الكود أو كلمة المرور الدخول إلى نظام هذه البيانات، وبذلك يكون صاحب ذلك النظام قد رفض مسبقا عمليات الاطلاع غير المصرح به ما لم يكن الراغب في الاطلاع مصرح له عن طريق إعطائه مفتاح المرور إلى هذه البيانات وذلك لا يتوافر في حالة عضو الضبط القضائي القائم بالتفتيش موضوع ،الحديث إن هذا التوجه يهدف أولا وأخيرا إلى إيجاد مظلة حماية قانونية لنظام البيانات المعالجة أليا والتي لا يصرح للغير بالاطلاع عليها.[1]

[1] نعيم سعيداني، المرجع السابق، ص 190.

ولا يفوتنا أن نتطرق إلى المعاينة في الجريمة المعلوماتية كوسيلة للحصول على الدليل، فالمعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة حيث يقوم عضو الضبط القضائي بمعاينة الأثار المادية للجريمة ويعمل في المحافظة عليها.

وعلى أي حال فإنه عند معاينة مسرح الجريمة المعلوماتية يجب مراعاة عدة ضوابط وهي:[1]

1-تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملف، وذلك لتعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها، ويراعى تصوير الأجهزة الموجودة، خاصة الأجزاء الخلفية منها.

2-وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخل مسرح الجريمة بل ورصد الاتصالات الهاتفية من وإلى مكان مسرح الجريمة.

3-ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها، ومعرفة السجلات المعلوماتية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار.

4-عدم نقل المواد المعلوماتية خارج مسرح الجريمة ألا بعد التأكد من خلو المحيط الخارجي للحاسب من مجالات الممرات المغناطيسية التي قد تتسبب في محو البيانات.

5-التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقه وشرائط وأقراص ممغنطة وغير سليمة أو محطمة ورفع البصمات التي قد تكون عليها.

6-قصر المعاينة على الباحثين والمحققين الذين لديهم كفاءة علمية وخبرة فنية في مجال الحاسبات والشبكات واسترجاع المعلومات وان يكونوا قد تلقوا تدريبا جيدة على ذلك.[2]

---

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص 90.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 92.

وبالتالي تظل الجريمة المعلوماتية عن طريق الحاسب الآلي مجهولة ما لم يبلغ عنها الجهات الخاصة بالاستدلالات أو التحقيق الجنائي، والمشكلة التي تواجه أجهزة العدالة الجنائية أن هذه الجرائم لا تصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية، لا تخلف آثاره مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة وجثة المجني عليه في القتل، واختلاس المال من المجني عليه في السرقة إلى آخره، ويرجع ذلك إلى صعوبة اكتشاف الجريمة المعلوماتية عن طريق الحاسب الآلي، ذلك أن الجهات التي تتعامل بالحاسب الآلي في معاملاتها اليومية كالشركات التجارية أو المؤسسات لا تراجع أعمالها يوميا، وحتى تلك التي تقوم بالمراجعة اليومية أو الأسبوعية أو الشهرية، قد لا تكتشف الجريمة وتبدو لها وكأنها خسائر عادية على أثر ممارسة نشاطها وحتى في حال اكتشافها فإن بعض الجهات المجني عليها لا تقدم على الإبلاغ خوفا من الأثر السلبي الذي ينعكس عليها من جراء هذا البلاغ.[1]

وقد يرجع السبب في افتقاد الآثار التقليدية للجريمة المعلوماتية عن طريق الحاسب الآلي ما يلاحظ 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 معدة ومخزنة على جهاز الحاسب ويتوافر أمام المتعامل عدة اختيارات وليس له سوى أن ينقر أو يضغط على الخيار الذي يريد فتكتمل حلقة الأمر المطلوب تنفيذه، كما في المعاملات المالية في البنوك، أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى حيث يتم ترصيد الأشياء المخزنة أو حسابات العملاء، أو نقلها من مكان لآخر بطريقة آلية وحسب الأوامر المعطاة لجهاز الحاسب الآلي، ويمكن ارتكاب بعض أنواع الجرائم المعلوماتية كالاختلاس أو التزوير، وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب أو تعديل البرنامج المخزن في جهاز الكمبيوتر، وتكون النتيجة مخرجات على حسب متطلبات مستخدم الجهاز

[1] نعيم سعيداني، المرجع السابق، ص 90-91.

الذي أدخل البيانات أو عدل البرنامج دون استخدام وثائق أو مستندات ورقية، وبالتالي تفقد الجريمة آثارها التقليدية.[1]

ولذلك يتعين عند البحث عن آثار الجريمة المعلوماتية عن طريق الحاسب الآلي وأدلتها بمعرفة سلطات الاستدلال والتحقيق أن توجه تحرياتها إلى دائرة المتعاملين في نطاق المؤسسة أو الجهة التي وقعت بها الجريمة سواء كانوا موظفين بتلك الجهة أو من المتعاملين معها، وذلك برصد حركة المعاملات المعلوماتية ومراقبة المشبوهين داخل المؤسسات وحولها.[2]

ويتضح من خلال ذلك ضرورة حصر البحث الجنائي عن آثار الجريمة المعلوماتية عن طريق الحاسب الآلي في دائرة المهتمين والمتعاملين بجهاز الحاسب الآلي، حيث إنه يتعين تطوير ثقافة الحاسب الآلي وسط رجال الأمن، وربط تلك الثقافة بالثقافة الأمنية التقليدية بحيث يكفل للأجهزة الأمنية نجاحا في مواكبة الظاهرة للتعامل مع الجريمة المعلوماتية وذلك من حيث القدرة على الملاحظة، ومراعاة تصرفات الأشخاص العاملين في مجال الحاسب بدقة أو المهتمين ببرامجه أو هواة صناعة الأنظمة المعلوماتية وتقليدها فدراسة تصرفات هؤلاء ومراقبتها، تعد مدخلا جيدة للسيطرة الأمنية على نشاط مرتكبي الجريمة المعلوماتية عن طريق الحاسب الآلي ووسيلة لضبطها، ذلك أن الفئات التي يجب وضعها تحت المراقبة والملاحظة الدائمة هم في الغالب من المتعلمين والذين تدل مظاهرهم على الوقار والمكانة الاجتماعية المرموقة، وللتعامل مع هؤلاء يتعين الانتقال بالحس الأمني الرجل البحث الجنائي من اهتمامه بالعاطلين والمتشردين والطبقات الفقيرة إلى مراقبة طبقات اجتماعية حديثة تتسلح بالعلم والخبرة والذكاء والثقافات المتنوعة، ولن يأتي ذلك إلا إذا كان قادرا على فهم عبارات ومفردات لغة الحاسب الآلي، التي تمكنه من جمع المعلومات المناسبة ومتابعتها.[3]

---

[1] طاهر عبد المطلب، المرجع السابق، ص 27.

[2] نبيلة هبة هروال، المرجع السابق، ص 200.

[3] أوساسي فؤاد، المرجع السابق، ص 25.

وفضلا عن رفع المستوى الثقافي لرجال الضبط في الجريمة المعلوماتية عن طريق الحاسب الآلي وأجهزة التحقيق، وربطهم بثقافة الحاسب الآلي، وذلك كوسيلة للسيطرة على آثار الجريمة المعلوماتية عن طريق الحاسب الآلي وضبط أدلتها، لأنها في النهاية ستؤول إلى الجناة بوصفها ثمرة الجريمة، وحينئذ يمكن ضبط مرتكبي الجريمة. ومن الأسباب التي تساعد في تعذر الحصول على آثار تقليدية تخلف الجريمة المعلوماتية عن طريق الحاسب الآلي أن الجاني نفسه يملك محو الأدلة التي تدينه أو تدميرها في زمن قصير جدا وحتى لو تم ضبطه فقد يرجع هذه الجريمة إلى خطأ في نظام الحاسب أو الشبكة أو الأجهزة.[1]

المطلب الثاني: الصعوبات المتعلقة بجهات التحقيق

إن اكتشاف الجرائم عموماً ومن ضمنها الجرائم المعلوماتية بعد وقوعها يدخل ضمن المفهوم العام للتحريات التي بدورها من إجراءات الاستدلال، التي تدخل ضمن مهام أعضاء الضبط القضائي المكلفون قانوناً بعدة واجبات من ضمنها التحري عن الجرائم والكشف عنها، بكافة الوسائل المتاحة والمشروعة وهذا الواجب يشمل أيضا محاولة اكتشاف أية جريمة يمكن أن تكون قد وقعت.

فهم عين العدالة وإذنها في التنقيب عن الجرائم عموما، ووضع مرتكبها تحت تصرف القضاء، ألا أن مهمتهم هذه ليست بالسهلة وإنما تكتنفها صعوبات عدة كنقص المعرفة الفنية لدى سلطات التحقيق والخبرة في الجرائم المعلوماتية، وضعف التعاون الدولي في مواجهة الجريمة المعلوماتية.

الفرع الأول: دور الضبط الإداري في الإثبات

فمن 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

[1] المرجع نفسه، ص 26.

معها، وذلك على الأقل في البلدان العربية، نظرا لان تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخرة عن أوربا والولايات المتحدة، فقد اثبت الوقائع بان بعض من أعضاء الضبط القضائي قد أعانوا مجرمي المعلوماتية على ارتكاب جرائمهم عن جهل ومن دون قصد، بدلا من ضبطهم وذلك بالنظر لعدم امتلاكهم المعرفة اللازمة للتعرف على مثل هذه الجرائم ووسائل ارتكابها.[1]

وبالتالي فإن الصعوبات التي تواجه عملية استخلاص الدليل في الجريمة المعلوماتية تتمثل في نقص الخبرة لدى المحقق، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة المعلوماتية عن طريق الحاسب الآلي وكيفية التعامل معها، وذلك على الأقل في البلدان العربية نظرا لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخرة عن أوربا وكندا والولايات المتحدة، وأن أجهزة العدالة المقاومة الجرائم المرتبطة بهذه التقنية تبدأ في التكوين والتشكيل عقب ظهور هذه الجرائم، وهو أمر يستغرق وقتا أبطأ من وقت انتشار الجريمة لان هذه الجريمة تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها، وحتى الآن فإن الحركة التشريعية، أو الثقافية الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التقدم أو التطور ينعكس سلبا على فنية إجراء الاستدلالات والتحقيقات في الدعوى الجنائية عن الجريمة المعلوماتية عن طريق الحاسب الآلي، ومن هنا تأتي الدعوة إلى وجوب تأهيل المختصين في جهات التحقيق والادعاء تأهيلا مناسبا في شأن هذه الجرائم.

إن جهات الضبط القضائي التقليدية تعاني عموماً من ضعف الثقافة القانونية اللازمة للتعرف على الجرائم المعلوماتية وتقدير خطورتها ومثل هذه الإشكالية تتضاعف أضعافا مضاعفة في الدول التي لا تملك قانون خاص بمكافحة الجرائم المعلوماتية، فوجود الأخير ضرورة لا غنى

[1] نعيم سعيداني، المرجع السابق، ص 94.

عنها لتعريف المجتمع عموماً وجهات الضبط القضائي خصوصا بخطورة هذه الجرائم، وكذا لتحديد الأفعال التي تشكل هذه الجرائم من عدمها.[1]

وهذا ما لاحظه جانب كبير من الفقه الجنائي، ذلك أن البحث والتحقيق في الجريمة المعلوماتية هي مسألة في غاية الأهمية، والصعوبة، ولاسيما بالنظر لاعتبارات التكوين العلمي والتدريبي، والخبرات المكتسبة لرجال الضبط القضائي وسلطات التحقيق الجنائي، ذلك أن حداثة هذه الجرائم وتقنياتها العالية تتطلب من القائمين على البحث الجنائي والتحقيق إلمام كاف بها، فلا يكفي أن يكون لديهم الخلفية القانونية أو أركان العمل الشرطي فقط، ولكن لا بد من الإلمام بخبرة فنية في مجال الجريمة المعلوماتية عن طريق الحاسب الآلي.[2]

ويزيد من التحدي الذي تواجهه أجهزة العدالة الجنائية في جرائم الحاسب الآلي وجرائم الانترنت، أن الجناة في هذه الجرائم لهم المفردات والمصطلحات الخاصة، لدرجة أنهم يطلقون على أنفسهم اسم (النخبة) بدعوى أنهم الأكثر معرفة بأسرار الحاسب الآلي ولغاته المتميزة، ويطلق على رجال الشرطة والنيابة والقضاء صفة الضعفاء.

يبدو لنا أن هذا القصور الفني والمعرفي لدى سلطات التحقيق يتطلب ابتداء تفعيل عدة أمور لمكافحة الجرائم المعلوماتية وإمكانية ضبط الأدلة الجنائية أن وجدت ويمكن أن نورد أهمها:

أ-تفعيل دور الضبط الإداري:

يعد الضبط الإداري أو البوليس الإداري من أهم وظائف الإدارة، ويهدف إلى المحافظة على النظام العام في الأماكن العامة عن طريق إصدار القرارات اللائحية والفردية واستخدام القوة المادية مع ما يتبع ذلك من فرض قيود على الحريات الفردية، يستلزمها انتظام أمر الحياة في المجتمع.

[1] نعيم سعيداني، المرجع السابق، ص 95.

[2] طاهر عبد المطلب، المرجع السابق، ص 29.

إن بعض العاملين في بيئة الانترنت يتمتعون بصفة الضبطية الإدارية، كمزودي الدخول وخدمات الانترنت، إذ تبعا لأعمالهم ووفقا للقانون فهم يمنحون الصلاحية في الرقابة عبر المزود عن سير حركة العمل ومدى الخضوع للنظام والقانون من قبل العاملين والمتعاملين مع الانترنت، حيث إذ حدث ووجدت الجريمة باكتشافها بهذا الأسلوب، فانه ليس الرجل الضبط الإداري سوى التحفظ على أدلة الجريمة إلى حين حضور رجال الضبط القضائي.[1]

والى جانب الإجراءات التي يتخذها رجال الضبط الإداري لمواجهة جرائم الانترنت مبكرة، وبالتالي منع وقوعها، هناك إجراءات يقوم بها العاملون بالمنشآت الحيوية، يطلق عليها، امن المعلومات وهي عبارة عن احتياطات وإجراءات تتخذها الإدارات الحديثة لمنع وقوع الجريمة، وذلك من خلال تحديد المعلومات الهامة، ثم تحليل المخاطر والتهديدات والقابلية للعدوان، ثم تطبق الإجراءات المضادة لتصل إلى مرحلة التقييم.[2]

ب-التدريب التخصصي لجهات التحقيق:

ان التحقيق في الجرائم المعلوماتية في حاجة إلى خبرة ومهارات خاصة لا تتأتى دون تدريب تخصصي يراعى فيه عدة عناصر تتعلق بشخص المتدرب ومنهج التدريب وصفته ما أن كان رسمية ام غير رسمي وكذلك أسلوب التدريب وجهة التدريب فبخصوص المتدرب لابد أن يكون الشخص مؤهلا لذلك سواء من رجال الشرطة أو سلطات التحقيق الجنائي، وهذا يتطلب قدرات ذهنية ونفسية خاصة لتلقي هذا التدريب، ألا أن تدريب المتخصصين في معالجة البيانات ونظم التشغيل يؤتي ثماره وبسرعة عن أولئك المنتمين لأجهزة العدالة كما في الشرطة والتحقيق الجنائي، ويتعين توافر الخبرة لدى متلقي برنامج التدريب.

والتدرب قد يكون بصفة رسمية أو غير ذلك، والتدريب غير الرسمي يكون بتكليف المتدرب بالعمل مع شخص لديه خبرة في تحقيق الجرائم المعلوماتية، أما التدريب الرسمي فيكون من

[1] عائشة بن قارة مصطفى، المرجع السابق، ص 268.

[2] نعيم سعيداني، المرجع السابق، ص 97.

خلال حلقات دراسية أو حلقات نقاش وهو ما يسمى (بورش العمل)، وذلك حول جرائم الحاسب الآلي وشبكات المعلومات وإساءة استخدامها.[1]

الفرع الثاني: ضخامة البيانات المتعين فحصها

إن الجريمة المعلوماتية عبارة عن حرب ما بين المجني عليه وهو ربما يكون فرد أو مؤسسة أو شركة وتكون هدفا للاعتداء على نظامها المعلوماتي ومن ثم الإضرار بها، وما بين المجرم المعلوماتي أو الجناة في حال تعددهم، لذلك فإن الهيئات والجهات التي تتبنى في نشاطها نظام معلوماتية لتسيير حركتها سواء كانت جهات خدمية أو أمنية أو مؤسسات اقتصادية تحاول دائما الحفاظ على معلوماتها وبياناتها عن طريق تخزين هذه البيانات والمعلومات بعيدة عن أيدي محترفي الجريمة المعلوماتية عن طريق الحاسب الآلي، ويظهر ذلك واضحا في مجال التجارة المعلوماتية، ومنها التعاقد بطريقة الإنترنت، ولذلك تحاول الجهات المعنية بالتجارة المعلوماتية المحافظة على عمليات الدفع الإليكتروني– أي السداد بطريقة آلية فضلا عن تواصل المعلومات والبيانات بينها وبين الأطراف الأخرى، وكذلك حماية عملية التحويلات المالية، ويتبع في ذلك طريقتين هما استخدام أسلوب التشفير والتحقيق عن شخصية المتعاقدين. وفيما يتعلق بالشفرة فهي متفق عليها بين الطرفين، ويعرف كلاهما مفتاح هذه الشفرة لضمان عدم قراءة الرسالة إلا لمن هو مصرح له بذلك.[2]

أما التحقق من شخصية المتعاقدين فيتم عن طريق استخدام الشفرة المفتاح العام" حيث يمكن للطرفين المتعاقدين أن يوقعا على المستندات بطريقة رقمية، ويتأكد كل طرف من توقيع الطرف الآخر باستخدام المفتاح العام للشفرة.[3]

وعلى الرغم من قيام الجهات ذات الأنظمة المعلوماتية بحماية نظمها عن طريق الترميز والتشفير وغيرها من طرق الحماية المعلوماتية، فإن قراصنة الحاسب الآلي والعاملين في ذات

[1] نعيم سعيداني، المرجع نفسه، ص 98.

[2] طاهر عبد المطلب، المرجع السابق، ص 30.

[3] طاهر عبد المطلب، المرجع نفسه، ص 31.

المؤسسات يستطيعون اختراق هذه الأنظمة ومن ثم يجعلون حمايتها عديمة الجدوى، لا سيما لو كانوا من العاملين داخل المؤسسة، وذلك بالدخول إلى المعلومات السرية أو الأسرار التجارية بغرض بيعها أو استخدامها في مؤسسات جديدة يسعون إلى إنشائها أو يكون هدفهم فقط تغيير الأرقام والبيانات أي تخريب المعلومات، كما أن الأمور لا تقف عند هذا الحد، بل إن هؤلاء يقومون بفرض تدابير أمنية لمنع التفتيش المتوقع بحثا عن أدلة إدانة ضدهم، وذلك كاستخدام كلمات سر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة الاطلاع على أي دليل يخلفه نشاطهم الإجرامي، الأمر الذي يعوق الرقابة على البيانات المخزنة أو المنقولة عبر حدود الدولة، حيث إنه بعد تقدم شبكة الإنترنت الدولية، لم تعد الحدود الجغرافية عائقا في الاختراق بل أكثر من هذا يلجأ الجاني إلى أسلوب حماية لمنع ضبطه أو الإيقاع به، الأمر الذي يشكل تهديدا لحرمة البيانات الشخصية المخزنة، وكذلك أسرار التجارة المعلوماتية وكذلك تدابير الدفاع والأمن.[1]

والحقيقة فإن مسألة استخلاص الدليل في الجريمة المعلوماتية، وبغير الطرق التقليدية، يثير ما يسمى "بالدليل العلمي في مسألة الإثبات الجنائي، والدليل العلمي يقصد به النتيجة التي تسفر عنها التجارب العلمية والمعملية لتعزيز دليل سبق تقديمه سواء الإثبات أو لنفي الواقعة التي يثار الشك بشأنها، وبطبيعة الحال فإن إجراء هذه التجارب والوسائل لا تكون سوى من مختص فنية وهو بهذه المثابة لا يعدو إلا إن يكون رأيا فنيا وهذا الدليل العلمي، يعد شكلا استثنائية للأدلة المقدمة في الدعوى الجنائية، ويكون طلبه بناء على طلب القاضي أو أحد الخصوم في الدعوى، وطلب القاضي للدليل العلمي، هو من المسائل الفنية التي لا يجوز للمحكمة أن تحل نفسها فيها محل الخبير، لأنها مسألة فنية في حاجة إلى خبير فني، ومع ذلك لو كان طلب ندب الخبير من جانب الخصوم فإن المحكمة غير ملزمة بإجابة طلبهم طالما أن الواقعة قد وضحت لديها، وفي مقدورها أن تشق طريقها في المسألة المطروحة عليها.[2]

[1] نعيم سعيداني، المرجع السابق، ص 99.

[2] نعيم سعيداني، المرجع نفسه، ص 99.

والقاعدة العامة أن الدليل العلمي والمستفاد من الخبرة الفنية لا بد وأن يكون مشروعة ومع ذلك ورغم مشروعية الدليل العلمي والحاجة إليه، فإن ذلك لا يعني سلب المحكمة حقها في أن تأخذ أو لا تأخذ بتقرير الخبير الذي نديته، إن هي رأت لأي ، من الأسباب ألا تأخذ بتقرير الخبير فلا يصح رميها بالتناقض، وتفسير ذلك أن الدليل العلمي يخضع لوزن وتقدير القاضي في ضوء الأدلة التي قدمت في الدعوى من خلال بحث مشروعية الأساليب التي يمكن من خلالها الحصول على هذا الدليل وإن كان هذا الدليل هو الوحيد في الدعوى فلا يمكن عده قاطعة في الإثبات أو النفي، ومن ثم يفسر الشك لمصلحة المتهم. وهناك جانبا من الفقه القانوني يرى أن الوسائل العلمية في أغلب حالاتها ليست دليلا مستقلا في ذاته وإنما هي قرائن يتم دراستها واستخلاص دلالتها، وهي غير مستقلة عن القرائن ويرجع ذلك إلى أنها لا تصلح في ذاتها كدليل وحيد في الإثبات الجنائي.[1]

ولو تم التسليم بالقواعد التقليدية في الإثبات في شأن وزن الدليل العلمي في الجريمة المعلوماتية عن طريق الحاسب الآلي وعدم اعتماده وحده كدليل في الإثبات بوصفه قرينة ما لم تؤازره أدلة أخرى فسوف يؤدي ذلك إلى إفلات الجناة في هذه القضايا، كما أن عدم وجود كوادر فنية مدربة من رجال أجهزة العدالة في شأن ضبط هذه الجرائم، فيؤدي ذلك إلى أن تقوم هذه الأجهزة بندب الفنيين والخبراء في مجال الحاسب الآلي لضبط هذه الجرائم، وهؤلاء الفنيين والخبراء يقومون بالمعاينة، والمشاركة في الضبط وفحص الأدوات وتحليل الأجهزة والتوصل للمعلومات ووضعها تحت يد أجهزة العدالة وتحت إشرافهم، والقول بأن عمل هؤلاء الخبراء ليس سوى قرينة يتعين أن تؤازر بأدلة أخرى.

لعل من الصعوبات الكبيرة التي تواجه رجال الضبط وسلطات التحقيق الجنائي في الجرائم المعلوماتية عن طريق الحاسب الآلي كمية المعلومات والبيانات الضخمة والتي هي في حاجة إلى فحص ودراسة كي يستخلص منها دليل هذه الجريمة، ففضلا عن ضرورة توافر الخبرة الفنية في مجال الحاسب الآلي والمعلوماتية لدى رجل الضبط أو المحقق، يتعين كذلك أن

[1] عائشة بن قارة مصطفى، المرجع السابق، ص 270.

يتوافر لديه القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة على الحاسب الآلي أو على ديسكات أو اسطوانات منفصلة.[1]

ولذلك يمكن القول أن ضخامة هذه البيانات والمعلومات، تعد عائقا في تحقيق الجرائم المعلوماتية عن طريق الحاسب الآلي، ذلك أن طباعة كل ما هو موجود على الدعامات الممغنطة لحاسب متوسط العمر، يتطلب مئات الآلاف من الصفحات، في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئا مفيدة للتحقيق. وهذا عكس ضخامة أو وفرة المعلومات في الجرائم التقليدية كالقتل أو السرقة، ذلك أن وفرة المعلومات في مثل هذه الجرائم هو أمر يساعد العدالة ويساعد رجل الضبط أو المحقق على السواء في استخلاص الدليل الجنائي في هذه الجريمة.[2]

ومن خلال ما سبق، وفي ظل تواضع المستوى الفني لرجل الضبط والمحقق الجنائي فيما يتعلق بفنون الحاسب الآلي واستخداماته، فإنه يكون الملائم وجوب ندب خبراء فنيين في مثل هذه الجرائم حتى يمكن فرز المعلومات التي يحتاجها التحقيق عن تلك التي لا حاجة لها، وإلا دخل رجل الضبط والمحقق في دائرة مغلقة من المعلومات لن يخرج منها، وهذا يتطلب أن يكون ندب هؤلاء الخبراء وجوبية، ومن ثم تعديل التشريعات الجنائية القائمة التي تجعل ندب خبير في الدعوى أمر جوازي للمحقق إن شاء أمر به أو رفضه؛ وذلك لأن طبيعة الجريمة تستلزم التعامل معها بطريقة حرفية أو فنية تفوق قدرات رجل الضبط أو المحقق؛ إلا إذا كان مؤهلا لذلك، فيمكنه الاعتماد على قدراته الشخصية في ضبط وتحقيق هذه الجرائم، بشرط ألا يخرج عمله عن الأصول الفنية المتعارف عليها.

---

[1] طاهر عبد المطلب، المرجع السابق، ص 34.

[2] أوساسي فؤاد، المرجع السابق، ص 29.

المبحث الثاني: حجية الدلائل الرقمية في الإثبات

يعد مبدأ الإثبات من أهم وأدق المسائل التي تواجه القاضي على وجه الخصوص، بسبب أن الإثبات ينصب ويتعلق بوقائع مادية ونفسية يتعذر إثباتها في المسائل الجنائية، على عكس المسائل المدنية التي يكون محل الإثبات فيها وقائع قانونية يسهل إعداد دليلها سلفا.[1]

المطلب الأول: مفهوم الإثبات الجنائي

تعرف الغاية من الإثبات الجنائي هو إظهار ومعرفة الحقيقة وثبوت وقوع الجريمة بجميع عناصرها، وبالتالي قيام الدليل الذي يصدر بفضله القاضي الحكم بإدانة أو براءة المتهم.

الفرع الأول: تعريف الإثبات الجنائي

يعرف الإثبات في المواد الجنائية بأنه كل ما يظهر لنا الحقيقة، ولا يمكن الحكم على المتهم في المسائل الجنائية إلا إذا ثبت وقوع الجريمة بذاتها وبجميع عناصرها هذا من جهة، ومن جهة أخرى قيام الدليل على أن المتهم هو مرتكبها، أو بعبارة أخرى وقوع الجريمة بوجه عام ونسبتها إلى المتهم بوجه خاص، وعليه نجد أن الإثبات الجنائي يتضمن النقاط الآتية[2]:

- ضرورة تحديد وفحص ومشروعية الدليل الجنائي، وتقدير أثره في جميع المراحل التي تمر بها الدعوى العمومية.
- الدليل في الإثبات الجنائي يشمل أدلة الدعوى بالثبوت أو بالنفي.

الفرع الثاني: المبادئ التي يقوم عليها الإثبات

يحكم نظام الإثبات الجنائي ثلاثة مبادئ رئيسية تتمثل في:

أولا: مبدأ البراءة.

---

[1] محمد مروان، نظم الإثبات في المواد الجنائية، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 463.

[2] بيراز جمال، الدليل العلمي في الإثبات الجنائي، مذكرة ماجيستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الحاج لخضر-باتنة-، 2013، ص 11.

إن مبدأ البراءة يجد موضعه في أحكام الدستور، حيث أن المتهم بريء حتى يقوم الدليل القاطع والمقنع على إدانته امتثالا للمبدأ العام "إن المتهم بريء حتى تثبت إدانته "، وعليه فلا يجوز المساس بالحرية الفردية في أي مرحلة من مراحل الدعوى ولا توقيع الجزاء بعد صدور حكم نهائي وبات من الجهة القضائية.

وتجدر الإشارة إلى أن الأصل في المتهم البراءة وهي قرينة قانونية بسيطة تقبل إثبات العكس، وتبقى قائمة هذه القرينة إلى أن يصدر حكم نهائي يكون عنوانا للحقيقة القضائية.[1]

وتترتب على هذا المبدأ عدة نتائج نذكر منها[2]:

- يفسر الشك لصالح المتهم ويعد دليلا إيجابيا على عدم مسؤوليته، ذلك أن الأحكام الجزائية يجب أن تبنى على الجزم واليقين لا على الظن والاحتمال.
- إعطاء سلطة الاتهام جميع الوسائل الضرورية التي تؤدي إلى الكشف عن الحقيقة وعلة ذلك إلقاء عبئ الإثبات الكامل على عاتقها.
- دور القاضي الإيجابي في تقصي الحقائق وذلك من خلال المهمة الموكلة إليه وهي سد النقص في الأدلة.
- لا يعد امتناع المتهم عن الكلام قرينة ضده فهو أهم نتيجة تترتب على مبدأ الأصل في الإنسان البراءة[3].

ثانيا: مبدأ حرية الإثبات

إن الإثبات الجنائي هو الوصول بالدليل المقدم في الدعوى الجنائية في مراحلها المختلفة سواء بالنفي أو الإثبات بطريقة مشروعة إلى مبلغ اليقين القضائي.

---

[1] بيراز جمال، المرجع نفسه، ص 34.

[2] المرجع نفسه، ص 35.

[3] بيراز جمال، المرجع السابق، ص 35-36.

وعليه فعندما نرجع إلى التشريع الجزائري نجد أن نظام الإثبات المعمول به والذي نص عليه المشرع هو نظام الإثبات الحر، وذلك من خلال ما جاءت به المادة 212 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم والتي تنص على أنه: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص.

ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه."

وعلى إثر ذلك نلاحظ من خلال هذه المادة أن المشرع الجزائري تبنى مبدأ الإثبات الحر، وهو بهذا قد اتبع خطى معظم التشريعات الحديثة الأخرى، وهذا راجع إلى أن متطلبات العصر الحالي إلزامية العمل بنظام الإثبات الحر في المحاكم الجزائرية، وعلة ذلك نوعية الجرائم التي تعرض على القضاء الجزائري والذي يتفاجئ بدوره بتطور العقليات والذهنيات التي تقف خلف هذه الجرائم، فكان من اللزوم الأخذ بنظام الإثبات الحر الذي يواكب جميع الظروف المستخدمة[1].

ثالثا: مبدأ الاقتناع الذاتي للقاضي.

يعتبر مبدأ الاقتناع الشخصي للقاضي الجزائي من أهم المبادئ التي تحكم المادة الجزائية، فقد قام المشرع الجزائري بتكريسه من خلال المادة 212 من قانون الإجراءات الجزائية بقولها"...وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص[2]."

وعليه فإن القاضي في المواد الجنائية يبني حكمه على اقتناعه الشخصي القائم على الترجيح بين الأدلة المقامة أمامه في الدعوى، دون أن يكون مقيدا في تكوين اقتناعه بدليل معين أو يكون مراقبا من طرف المحكمة العليا أمام محكمة الجنح والمخالفات، ما دام أن الوقائع التي تم

[1] طاهر عبد المطلب، المرجع السابق، ص 27.

[2] انظر المادة 212 من قانون الإجراءات الجزائية الجزائري.

إثباتها في حكمه لا تتعارض مع الرأي الذي خلص له القاضي، وكذلك ما دام الدليل المسند إليه متفقا مع الأدلة المقدمة في الدعوى.[1]

ويخلص القول إلى أنه لا يجوز للقاضي أن يحكم وفقا لهواه أو أن يكون حكمه القضائي بمحض عاطفته، وإنما هو ملزم أن يحكم بالمنطق الدقيق في تفكيره والذي قاده إلى الاقتناع، ولهذا دائما يقترن وصف الاقتناع القضائي بالحرية أو بالذاتية.

المطلب الثاني: سلطة القاضي في الإثبات الجنائي.

انطلاقا من مبدأ حرية الإثبات والاقتناع القضائي، فإن القاضي الجزائي يملك السلطة المطلقة في اللجوء إلى مختلف وسائل الإثبات المقررة قانون وتقدير مدى حجيتها وصحتها، إذ أن القاضي يصدر حكمه القضائي وفقا لاقتناعه الخاص، وذلك على عكس ما هو معروف في مجال الإثبات المدني، والذي يتقيد بموجبه القاضي من خلال النصوص القانونية الواردة في القانون المدني والذي يحدد بها قيمة كل دليل دون أن يملك الحق في الخروج عن ذلك، وسبب ذلك أن الأدلة الواردة في القانون المدني مرتبة حسب قوتها الإثباتية، وسلطته فيها مقيدة.

الفرع الأول: سلطة القاضي الجنائي في تقدير الدليل

مع رواج الأنترنت وانتشار النظم المعلوماتية، ظهرت تحديات لم يكن لها وجود أمام القانون الجنائي بمختلف شقيه الموضوعي ولإجرائي، بالنسبة للشق الموضوعي فقد ظهرت ما يسمى بالجرائم المعلوماتية، أما على المستوى الإجرائي فلإثبات هذه الجرائم ظهر ما أطلق عليه بالدليل الرقمي.

[1] خميس رياض، تأثير أدلة الإثبات الجزائية على الاقتناع الشخصي للقاضي في مادة الجنايات، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، 2017-2016، ص 05.

فإن الدليل الرقمي يتميز بعدة مزايا تتمثل أهمها في أنه دليل علمي ذو طبيعة تقنية، يصعب التخلص منه وقابلا للنسخ، أما من حيث حجية هذا الدليل فإن للقاضي السلطة الواسعة والكاملة في تقدير الدليل الرقمي حيث أنه لقبوله ينبغي توافر عدة شروط وهي:

أولا: مشروعية الدليل الرقمي

وهو شرط أساسي لقبول الدليل الرقمي كدليل إثبات، حيث يقصد بمشروعية الدليل الجنائي أن يكون الإجراء الذي تحصل منه القاضي على الدليل يتفق مع القواعد القانونية التي تحطمه، أو بمعنى آخر ضرورة اتفاق الإجراء الذي تم الحصول من خلاله على الدليل الرقمي مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر.[1]

واما كان الدليل الرقمي مختلف في البحث عنه عن الدليل التقليدي، وجب أن يتوفر فيه شرطان، الأول هو مشروعية الحصول على الدليل ومعناه أن تكون وسائل وأدوات الاستدلال والتفتيش بأنظمة الحاسب الآلي أو شبكة الأنترنت تمت بشكل مشروع، والشرط الثاني هو ضمانة الحفاظ عليه من التلاعب وهذا هذا يكون من خلال الخبراء واستخلاص الدليل دون إكراه والحفاظ عليه من التلاعب وإلا كان غير مشروع وعليه لا يصلح لتكوين قناعة القاضي

ثانيا: بلوغ اقتناع القاضي درجة اليقين.

ومعناه أن يكون اقتناع القاضي مبني على الجزم واليقين لا على الشك والظن والتخمين، وذلك بسبب أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عند وصول القاضي درجة الجزم واليقين والذي لا يشترط فيه أن يكون مطلقا بل بصفة نسبية يتحقق معها تكوين القاضي لعقيدته التي يبني عليها حكمه القضائي، ولكن ليس المطلوب هنا الاقتناع الشخصي للقاضي

[1] روابح إلهام شهرزاد، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة –2–، المجلد 05، العدد 10، جوان 2016، ص 194.

وفقط بل أيضا اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل في ذاتها معالم القوة في الاقناع.[1]

ثالثا: مناقشة الدليل الرقمي

حتى يتمكن القاضي من بناء قناعته يجب أن يتم شرط مناقشة الدليل أو ما يطلق عليه بشرط "وضعية الدليل"، ومعناه أن يكون للدليل أصل ثابت في أوراق الدعوى ثم يطرح للمناقشة بعد اطلاع الخصوم عليه وهذا ما نصت عليه المادة 212 في فقرتها الثانية من قانون الإجراءات الجزائية الجزائري بقولها:" ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه[2]"، والحكمة من ذلك هي تكوين القاضي لقناعته القائمة على مناقشة كل الأدلة.[3]

وما نستنتجه أخيرا أن استبعاد الأدلة أو قبولها راجع إلى الاقتناع الذاتي للقاضي بها، فهو وحده الذي يقدر الدليل إذا كان منتجا في الدعوى أو غير منتج، أو كان يدل على الحقيقة بعينها أو لا يدل، فالقاضي الجنائي لا يأخذ بالدليل في حالة ما إذا كان الدليل ضعيفا أو يكون متناقضا مع أدلة أخرى قائمة في الدعوى.

الفرع الثاني: سلطة القاضي الجنائي في قبول الدليل

تعد حرية القاضي في تقدير وسائل الإثبات المطروحة أمامه في الدعوى نتيجة حتمية ومنطقية لمبدأ القناعة الوجدانية للقاضي الجزائي، فإن اقتناعه وجب أن يكون منطقيا وغير مبني على

---

[1] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، 2010، ص 278.

[2] الأمر رقم 66- 155 المعدل والمتمم المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 48 لسنة 1966.

[3] سارة مساعدي، مشروعية الوسائط الرقمية في الإثبات الجنائي، المجلة الجزائرية للأمن الإنساني، جامعة الجزائر -1-، المجلد 05، العدد 01، جانفي 2020، ص 748.

التصورات الشخصية للقاضي، حيث أنه إذا اعتمد في تفكيره على أساليب ينكرها المنطق السليم، فإنه يعرض حكمه للنقض.

وعليه فقيمة الدليل الإلكتروني يمكن حصرها في نقطتين تتمثل الأولى في أن يكون هذا الدليل معترف به أو بمعنى آخر أن القانون يجيز للقاضي الاستناد إليه في تكوين عقيدته، أما النقطة الثانية فهي أن يتوفر على مجموعة من الشروط التي تضفي عليه المشروعية.

وأخيرا فإن مبدأ حرية القاضي في إقناع نفسه بالدليل العلمي هو أساس التبرير بالوسائل العلمية، بحيث يحق له قبول أي دليل مشروع يكتسب يقينا، حتى ولو كان هذا الدليل مستمدا من الوسائل العلمية الحديثة ، وبالرغم من أن القاضي حر في اختيار أي دليل، فإن هذا لا يعني أنه قادر على إصدار أحكام مطلقة، وعم ذلك هناك حدود يجب احترامها والضمانات التي يمنحها القانون للإدانة الشخصية هي :مراجعة المحكمة العليا للأحكام الصادرة عن المحكمة ، بحيث تعتمد سلطة المحكمة العليا المذكورة على التحكم فب التطبيق الصحيح للقانون على الخلاصة الجيدة للوقائع من قبل القاضي الذي تم ضبطه وفقا للمنطق القضائي، وبالتالي تعتبر العلاقة السببية المنطقية أداة فعالة تبرز الأحكام وأصالتها.[1]

[1] عمر خوري وعقيلة بتلاغة، الرقابة على سلطة القاضي الجنائي في تقدير الدليل العلمي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجزائر –1–، المجلد 03، العدد 11، سبتمبر 2018، ص 545.

خاتمة

خاتمة

من خلال دراستنا لموضوع إثبات الجرائم الإلكترونية فلا ريب أن هذه الجرائم من أكثر وأخطر الجرائم في الآونة الأخيرة وبلغت حد الغزو وتهديد للمجتمعات، نظرا لكون الإثبات فيها صعب المنال، لاعتبار أدلتها رقمية خفية وغير مرئية، ومن أبرز ما توصلنا إليه هو أن الجريمة الإلكترونية أحدثت تغييرا جذريا في النظرة العامة للجريمة وما زالت محل خلاف فقهي والقضائي بالنظر إلى قيمة المعلومات وطبيعتها غير المادية وكذلك من حيث إجراءات التحقيق من التفتيش الذي قد يكون حتى عن بعد، وطبيعة الأدلة الناتجة عنها وتعديها للحدود الجغرافية ومدى شرعية الحصول على الأدلة الناتجة عنها والعمل بها وتحديد نطاق الاختصاص المكاني المحلي والدولي والقانون الواجب التطبيق، ومدى كفاية النصوص التقليدية الموضوعية والإجرائية لمواجهتها، خاصة في ظل الدول التي لا زالت لم تعدل بعد قوانينها ولم تصدر بعد قوانين حديثة لمواجهتها.

وعليه نستنتج النتائج والاقتراحات التالية:

أولا: النتائج

- فإن الإثبات في الجرائد الإلكترونية يتطلب من رجال الضبط القضائي والقضاة ان يكونوا ملمين التدابير والإجراءات اللازمة لتأمين مسرح الجريمة الإلكترونية.
- ضبط وتحرير الآثار الجنائية الرقمية ونقلها بالطريقة العلمية الصحيحة وهذا ما يستلزم التعاون الكامل بين كل من رجال الضبط القضائي وقاضي التحقيق والخبير من أجل نجاح عملية ضبط الجريمة.
- تحرير ونقل الأدلة إلى المخبر وتحليلها ثم تقديمها في شكل ينفي أو يثبت إدانة المتهم ويؤدي إلى إقناع القاضي بالحكم الذي أصدره.
- كون التعامل مع الدليل الجنائي الرقمي يحتاج إلى معرفة بأصله وإلى مختبرات رقمية مجهزة بأحدث أنواع الأجهزة اللازمة.

- أما التشريع الجزائري فإن الإثبات الجنائي في مجال الجرائم الإلكترونية لا يزال في مرحلة التطور، بحيث لم يتضمن الاستثناء الخاص بوقت التفتيش والأشخاص المطلوب حضورهم ضمن قانون رقم (09-04 لسنة 2009) إلى كل الاعتراف والشهادة والاستجواب في مجال الجريمة المعلوماتية.

ثانيا: التوصيات

- على المشرع الجزائري الإشارة إلى الاستثناء الخاص بوقت التفتيش والأشخاص المطلوب حضورهم ضمن القانون رقم (09-04) طالما ان المشرع قد وسع هذا القانون من صلاحيات سلطات الاستدلال والتحقيق حيال مكافحة الجرائم الإلكترونية.
- كما ان من الأولى النص على صدور إذن بالتفتيش مقتصرا على تفتيش الحاسوب فان كان هذا الأخير متواجدا في أحد المساكن يتعين توافر شروط تفتيش المساكن أما اذا كان الحاسوب في حيازة شخص خارج مسكنه أو كان في سيارته في الخارج مثلا فانه يكفى توافر شروط التفتيش الأشخاص، وهو ما يفتح الباب أيضا للتذكير انه على المشرع إدراج تفتيش الأشخاص وتحديد كيفية وشروط إجرائه ضمن قانون الاجراءات الجزائية.
- كذلك عليه إدراج كل من إجراء الاعتراف والشهادة والاستجواب ضمن القانون رقم (04-09) من أجل وضعا مكانية للقاضي الاعتماد عليها للفصل في الدعوى، بالرغم من أن لهذه الاجراءات دور ضئيل في مجال المعلوماتية.
- وجوب الاهتمام بتكوين الخبراء والمحققين والقضاة على التعامل مع الجرائم الإلكترونية.
- دعوة المشرع الجزائري إلى إعادة صياغة المادة 81 من قانون الاجراءات الجزائية بإضافة معطيات المعلوماتية لتصبح على النحو "يباشر التفتيش في جميع الأماكن التي يمكن العشور فيها على أشياء أو معطيات معلوماتية، يكون كشفها مفيدا لإظهار الحقيقة".

- التركيز على تطوير الوسائل التقنية باستمرار للتمكن من التحليل الجيد والنسخ المناسب للمحتويات من الأقراص وتخزين البيانات.
- الاستثمار في التوعية بمخاطر الجرائم الإلكترونية والتنويه بأساليب المجرمين في ارتكابها عن طريق استغلال وسائل الإعلام المختلفة.
- تطوير النظرة الاستشرافية في مكافحة الجريمة الإلكترونية من خلال تفعيل التعاون الدولي لمواجهة هذه الجرائم بالأخص من خلال ربط الاتفاقيات والمعاهدات الدولية التي تجرم صور هذه الجرائم وبصفة موحدة ليسهل اتخاذ موقف موحد منها.
- مسابقة الزمن في تكوين وإنشاء فرق متخصصة في مكافحة الجرائم وضبطها على غرار ما قامت المديرية العامة للأمن الوطني باستثناء أول فرق مكافحة الجرائم السيانية في سنة 2004 موزعة على القطر الوطني بمديريات الأمن.
- الاستفادة من تجارب وخبرات الدول المتطورة في مجال مكافحة الجرائم الإلكترونية أو العمل على استعمال الآليات الوقائية قبل وقوع الجريمة، خاصة عند ما يتعلق الأمر ببعض الجرائم الإلكترونية التي تهدد أمن الدولة مثل الإرهاب الإلكتروني أو التجسس الإلكتروني.

قائمة المراجع

قائمة المراجع

أولا: القوانين

1-الامر رقم 66-155 المؤرخ في صفر عام 1386 الموافق 8 يونيو سنة 1966، الذي يتضمن قانون الإجراءات الجزائية، جريدة الرسمية الجمهورية الجزائرية، عدد 48 بتاريخ 11 جوان 1966، المعدل والمتمم.

2-قانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم ،84 الصادرة بتاريخ 12/24/ 2006.

3-قانون رقم 04-09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، الصادرة بتاريخ 2009/08/16.

ثانيا: الكتب

1-ابراهيم بلعليات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، 2012

2-أحمد خليفة الملط، الجرائم المعلوماتية، ط 2، دار الفكر الجامعي، مصر، 2006،

3-أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة للنشر، مصر، 2015

4-أوشن حنان، وادي عماد الدين، الإثبات الجنائي والوسائل العلمية الحديثة، دار الخلدونية للنشر والتوزيع، الجزائر، 2015.

5-بكرى يوسف بكرى، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011

6-حسن الطوالبة، الجرائم الالكترونية، ط 1، جامعة العلوم التطبيقية، مملكة البحرين، 2008،

7-جميل صليبا، المعجم الفلسفي المصطلحات القانونية، الجزء الأول، دار الكتاب اللبناني، بيروت، الطبعة الأولى1982
8-خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011.
9-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009.
10-خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2009
11-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، 2010
12-عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، الطبعة الرابعة، دار هومة، الجزائر، 2013.
13-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006
14-عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية الحاسب الآلي وشبكة المعلومات (الانترنت)، ط 1، دار الأوراق للطباعة والنشر والتوزيع، لبنان، 2004
15-عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية-دراسة تطبيقية مقارنة-، جامعة نايف العربية للعلوم الأمنية، السعودية، 2007
16-عمر محمد بن يونس، الدليل الرقمي (Evidence Digita) ، دون دار نشر، مصر، 2006،
17-ضاح محمود الحمود ونشأت مفضي المجالي، جرائم الأنترنت، دار المنار للنشر والتوزيع، 2005

18-رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، الطبعة الأولى، الطبعة الأولى، منشورات الحلبي الحقوقية، الجزائر، 2012
19-محمد عبد الرحيم، سلطان العلماء، جرائم الانترنت والاحتساب عليها، بحوث مؤتمر القانون والكمبيوتر والانترنت، المجلد 3، ط 3، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004،
20-محمد مروان، نظم الإثبات في المواد الجنائية، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999
21-محمود نجيب حسني، شرح قانون العقوبات (القسم الخاص)، ط 16، دار النهضة العربية، مصر، 1989.
22-مصطفى محمد موسى المراقبة الالكترونية عبر شبكة الانترنت (دراسة مقارنة بين المراقبة الامنية التقليدية والالكترونية)، دار الكتب القانونية، مصر، 2005،
23-ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006.
24-نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 1، دار الثقافة للنشر والتوزيع، عمان، 2008
25-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، مصر، 2007
26-لينا محمد الأسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، دار حامد، الأردن، د س ن.
27-يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، ط 1، مطبعة الرمال، الجزائر، 2019

ثالثا: المذكرات والرسائل

1-ابراهيم الغمار، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 1989.
2-اوساسي فؤاد، دور الدليل الرقمي في الإثبات الجنائي مذكرة ماستر كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة 2019/20120
3-بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري، دراسة مقارنة، مذكرة مكملة لمقتضيات نيل شهادة الماستر، كلية الحقوق، جامعة محمد خيضر، بسكرة، الجزائر، 2016-2015
4-بن طالب ليندة، الدليل الرقمي ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2019
5-بن زرت أسيا، اثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم 2019.
6-بشرى عواطة، حجة الدليل الالكتروني في الإثبات الجنائي، مذكرة ماستر، كلية الحقوق، جامعة 08 ماي 1945، قالمة، 2017-2018
7-برمش مراد، خصوصية الجريمة الالكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر 1، 2020-2021
8-بيراز جمال، الدليل العلمي في الإثبات الجنائي، مذكرة ماجيستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الحاج لخضر-باتنة-، 2013
9-ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية - دراسة تأصيلية تطبيقية -، رسالة ماجيستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012
10- حكيمة شريد، مايسة ربيع، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2016

11- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة، 2011/2012،

12- خميس رياض، تأثير أدلة الإثبات الجزائية على الاقتناع الشخصي للقاضي في مادة الجنايات، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، 2017-2016

13- عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية (دراسة مقارنة)، مذكرة لنيل الماجستر، جامعة الشرق الأوسط، الأردن، 2014

14- طاهر عبد المطلب، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة مسيلة، 2015-2014

15- سيدي محمد البشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية – دراسة تحليلية تطبيقية –، رسالة ماجيستير، جامعة نايف العربية للعلوم الأمنية، السعودية، 2010،

16- شهرزاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، مذكرة ماستر تخصص حقوق، كلية الحقوق والعلوم السياسية، جامعة أم البواقي، 2017

17- مدربل كريم الإثبات بالدليل الرقمي في المسائل الجزائية، مذكرة الماستر كلية الحقوق، جامعة اكلي محند اولحاج البويرة 2019

18- محمد بوعمرة، سيد علي بنيال، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر، كلية الحقوق، جامعة آكلي محند أولحاج، البويرة، 2019-2018

19- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجيستير، جامعة الحاج لخضر –باتنة–، كلية الحقوق والعلوم السياسية، 2013

20- هروال هبة نبيلة، جرائم الانترنيت، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة أبو بكر بالقايد، تلمسان، الجزائر، 2013
21- يوسف الصغير، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستر في القانون الخاص، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2013

رابعا: المجلات

1-اسمهان بوضياف، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، مسيلة، 2008
2-بن مالك أحمد، الخال ابراهيم، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، جامعة تمنراست، المجلد 05، العدد 01، أفريل 2021
3-عبير بعقيقي، فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09/04، مجلة العلوم القانونية والسياسية، جامعة محمد خيضر، بسكرة، المجلد 09، العدد 02، 2018،
4-عمر خوري وعقيلة بتلاغة، الرقابة على سلطة القاضي الجنائي في تقدير الدليل العلمي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجزائر -1-، المجلد 03، العدد 11، سبتمبر 2018
5-فاطمة زهرة بوعناد، "مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانونية، العدد الأول، دون دار نشر، الجزائر، 2013
6-سارة مساعدي، مشروعية الوسائط الرقمية في الإثبات الجنائي، المجلة الجزائرية للأمن الإنساني، جامعة الجزائر -1-، المجلد 05، العدد 01، جانفي 2020
7-روابح إلهام شهرزاد، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة -2-، المجلد 05، العدد 10، جوان 2016

خامسا: المواقع

1-محمد زروق، إشكالية الحصول على الدليل الإلكتروني في الجريمة المعلوماتية، منتدى استشارات قانونية، تاريخ الزيارة: 15-05-2024، الساعة 14:22: متوفر على الرابط :www.mohamah.net/law :

سادسا: المراجع باللغة الأجنبية

-Eoghan Casey, Digital Evidence and computer Crime, Third edition, Published by Elsevier Inc, London, 2011,

- Lynda volonino and ReynaldoAnazaldua, Computer Forensics For Dmmies, Wiley publishing, United states of America, 2008.

-Steve Bunting and William Wei, Encase Computer forensic, Wiley publishing(inc), United States of America.

the technical working group for electrinic crime scence investigation, electronic crime investigation, the national instituteof justice,the united states of america,2001

الفهرس

الفهرس

الملخص

الجرائم الرقمية وطرق إثباتها

ملخص:

تقتضي الجريمة الالكترونية على غرار بقية الجرائم التقليدية أساليب خاصة للبحث والتحري عنها لطبيعتها الخاصة، الأمر الذي أدى بالمشرع إلى استحداث إجراءات وأساليب استثنائية لإثبات هاته الأخيرة. بالإضافة إلى أنه يتوجب مع انتهاج هذه السياسة المغايرة في الاثبات معرفة مدى حجية هذا الدليل في اثبات وتكوين قناعة القضاة لأن هذا الدليل يواجه صعوبات أثناء تقييمه كونه مستحدث.

الكلمات المفتاحية:

1-الجريمة الالكترونية. 2-دليل رقمي. 3-الإثبات الالكتروني.

4-ضخامة البيانات. 5-نظام المعلوماتية. 6-برامج الكترونية.

Abstract:

Electronic crime, like other traditional crimes, requires special methods to search and investigate it due to its special nature, which led the legislator to develop exceptional procedures and methods to prove the latter. In addition, while adopting this different policy of proof, it is necessary to know the extent of the authority of this evidence in proving and forming the conviction of judges, because this evidence faces difficulties during its evaluation because it is new.

***Key words*:**

1- Electronic crime 2- Digital guide 3- Electronic proof

4- Data enormity 5- Informatics system 6- Electronic programs