الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم قانون عام

المرجع:.....

مذكرة نهاية الدراسة لنيل شهادة الماستر

حجية الدليل الإلكتروني في الإثبات الجنائي

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق

التخصص: قانون جنائي وعلوم جنائية

من إعداد الطالب(ة)

حمري ميليسة

تحت إشراف الأستاذ(ة):

بن قارة مصطفى عائشة

أعضاء لجنة المناقشة

الأستاذ(ة)	بصايفي مزيود	رئيسا
الأستاذ(ة)	بن قارة مصطفى عائشة	مشرفا مقررا
الأستاذ(ة)	بن عودة نبيل	مناقشا

السنة الجامعية: 2020/2019

تاريخ المناقشة : 2020/09/22

شكر وتقدير

الشكر لله أولا وأخيرا وأحمده حمدا كثيرا على توفيقه لنا في إتمام هذا العمل المتواضع وعلى كل النعم التي أنعمها علينا .

أتقدم بجزيل الشكر و العرفان للأستاذ الفاضل الأستاذ المشرف

" بن عودة نبيل "

خالص التقدير و الاحترام على قبوله الإشراف على هذا العمل و الذي لم يبخل علي بالتوجيهات و الرأي السديد

كما يشرفني أن أتقدم بخالص الشكر و العرفان للأساتذة الأفاضل لجنة المناقشة لتحمهم عناء قراءة هذه المذكرة

فلهم ني أرقى عبارات الشمر و الامتنان وجزاهم الله خير الجزاء

إهداء

الحمد لله رب العالمين و الصلاة و السلام على خاتم الأنبياء و المرسلين

أهدي هذا العمل إلى :

من ربتني وأنارت دربي وأعانتني بالصلوات و الدعوات،إلى أغلى إنسان في الوجود

أمي الحبيبة أدامها الله لي

إلى من عمل بكد في سبيلي و أوصلني إلى ما أنا عليه قدوتي في الحياة

أبي العزيز أطال الله في عمره

إلى من عملوا معي بكد بغية إتمام هذا العمل

أختي الغالية وأخي الغالي وكل عائلتي

وفي الأخير أرجو من الله تعالى أن يجعل عملي هذا نافعا يستفيد منه جميع الطلبة المقبلين على التخرج

فهرس المحتويات

فهرس المحتويات

المقدمة

نظرا لتطور الكبير وغير المسبوق الذي عرفه العالم في مجالات الإعلام والاتصال خلال السنواتالأخير ة مما أسهم إلى حد كبير في انتشارها واعتمادها من خلال الأشخاص الطبيعية والاعتبارية في جميع نواحي حياتها العامة والخاصة على الابتكارات الجديدة في مجال المعلوماتية كالانترنت والرقمية وغيرها من التقنيات الالكترونية المستحدثة ومن هنا تطور فكر المجرم كتسلسل وكيفية استخدام المجرم لتقنية المعلومات والتكنولوجيا الحديثة استغلالها لأحد سريعة الإجرامية وأعمال المخالفة للقانون وبالتالي الاستفادة من هذه لمواجه طريقة ارتكابه جرائم أن الطبيعة الفنية والتقنية الناجمة عن الجرائم الالكترونية نتج عنها نوع جديد من الأدلة في مجال الإثبات الجنائي يطلق عليه الدليل الالكتروني أو الدليل الرقمي وهو الأمر الذي أدى إلى تدخل المشرع الجزائري بنصوص قانونية إجرائية تساعد الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم ووسائل ارتكابها .

أما عن إشكالية هذا الموضوع فاعتبار أن صعوبة كشف وضبط الدليل الالكتروني المستخلص من الجرائم الالكترونية وما يصاحب إجراءات الحصول عليه من خطوات معقدة واتساع مصرح الجريمة الذي يتخطى غالبا حدود الدولة الواحدة وعليه ارتأينا أن تكون إشكالية الدراسة كالأتي : ما المقصود بالجريمة الالكترونية والدليل الالكتروني؟ فيما تتمثل الإجراءات المتبعة للحصول على الدليل الالكتروني في التحقيق الجنائي؟ إلى أي مدى يمكن الاعتماد على الدليل الالكتروني في الإثبات الجنائي؟أما السؤال الرئيسي فهو ما حجية الدليل الالكتروني على اقتناع القاضي الجنائي به؟

وللإجابة على هذه الإشكالية اتبعنا كل من المنهج الوصفي التحليلي لمختلف العناصر وتبيان الخصائص المميزة في هذا البحث، وأدرجنا المنهج الوصفي وذلك النماذج لوصف النماذج المستخدمة في الإجرام المعلوماتي واستخراجها .ومن خلال إعداد بحثنا والوصول إلى الإشكاليات المطروحة قمنا بتقسيم البحث إلى فصلين حيث نتعرض من خلال الفصل الأول إلى ماهية الجريمة الالكترونية و الدليل الالكتروني وذلك من خلال تناولنا إلى مفهومها ,براز

الخصائص التي تتميز بها كل من الجريمة الالكترونية، وهذا ما تعرضنا له في المبحث الأول وأما بخصوص المبحث الثاني قد تطرقنا للإطار المفاهيمي للدليل الالكتروني ومدى اقتناع القاضي الجنائي به .

لذا خصصنا مبحثين كما حاولنا إبراز الدليل الالكتروني وكيفية جمعه هذا بالنسبة للمبحث الأول وجاء في المبحث الثاني مدى تأثير القاضي الجنائي بالدليل الالكتروني.

الفصل الأول

ماهية الجريمة الإلكترونية و الدليل الإلكتروني

تمهيد :

إن الوسط الذي ترتكب فيه الجريمة الالكترونية يختلف من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الافتراضي وعلى ضوء ذلك فإن الدليل المناسب لإثبات الجريمة الإلكترونية هو الدليل الالكتروني كما عبرت عنه الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية، فطبيعة الدليل تتشكل من طبيعة الجريمة التي يولد منها، وبإسقاط هذا على الجريمة الإلكترونية، فإنه يمكن أن تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها أو من خلالها .

وعلى ضوء ما سبق طرحه سنتطرق في دراستنا إلى محل الدليل الإلكتروني أي الجريمة الإلكترونية في (المبحث الأول)، ثم سنتعرض في المبحث الثاني إلى الإطار المفاهيمي للدليل الإلكتروني.

المبحث الأول: محل الدليل الإلكتروني (الجريمة الإلكترونية)

إن تزايد سوء استخدام الحاسب الآلي وشبكة الانترنت أدى إلى تنامي معدلات الجريمة المعلوماتية، والتي يطلق عليها أيضا الجريمة الإلكترونية أو جرائم الحاسب الآلي والانترنت أو جرائم التقنية العالية أو جريمة الغش المعلوماتي، أو جرائم تكنولوجيات الإعلام والاتصال أو جرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات وغيرها[1]

من خلال هذا المبحث سنتطرق إلى مفهوم الجريمة الالكترونية في (المطلب الأول)، وأنواعها في(المطلب الثاني)، ثم نتعرف على دوافع ارتكاب هذه الجريمة الالكترونية في (المطلب الثالث)

المطلب الأول: تعريف الجريمة الالكترونية وخصائصها

نظرا للطبيعة الخاصة للجرائم الالكترونية اختلف الفقه في وضع تعريف مانع وجامع لها فأحيانا يكون الحاسوب وسيلة لارتكابها بواسطة الانترنت وأحيانا أخرى يكون هدف لها، سنتناول هذا المطلب تعريف الجريمة الالكترونية في(الفرع الأول) ثم نتطرق إلى خصائص الجريمة الالكترونية في (الفرع الثاني).

الفرع الأول: تعريف الجريمة الالكترونية

استقطب مفهوم الجريمة المعلوماتية اهتمام الفقهاء والقانونيين والمختصين في مجال المعلوماتية من أجل وضع تعريف شامل للجريمة المعلوماتية، فحاول كل منهم حسب اختصاصه وضع تعريف ملائم فمنهم من عرفها تعريفا ضيقا وقال بأنها " الجرائم المرتبطة بالحاسوب والتي تشكل انتهاكا للقانون الجنائي" ومنهم من قال بأنها " تلك الجريمة التي يستخدم فيها الحاسوب " وهو تعريف واسع جدا[2].

---

[1] اخترنا اصطلاح الجريمة المعلوماتية دون غيره من التسميات الأخرى لكونه مفهوم عام يشمل مختلف التقنيات المستخدمة في التعامل مع المعلومات بما فيها الحاسوب وشبكة الإنترنت.

[2] عمر بن محمد العتبي، الأمن المعلوماتي ومدى توافقة مع المعايير المحلية والدولية - رسالة مقدمة لأجل نيل شهادة الدكتوراه - قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2010، ص 21 .

أما من الناحية القانونية فلا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن سوء استغلال النظم المعلوماتية أو إساءة استخدامها فهناك من يطلق عليها وصف جريمة الغش المعلوماتى وهناك من يطلق عليها وصف جريمة الاختلاس المعلوماتي، وهناك من يصفها بجرائم الاحتيال المعلوماتي،غير أن المصطلح الأكثر شيوعا هو مصطلح الجريمة المعلوماتية أو الإلكترونية[1].

وقد تعددت التعاريف الواردة بشأن الجريمة المعلوماتية بتعدد النظم والتشريعات والاتجاهات الفقهية وعليه تناولنا التعريف الفقهي في (الفقرة الأولى)، ثم تطرقنا إلى التعريف القانوني في (الفقرة الثانية).

الفقرة الأولى: التعريف الفقهي

مما يلاحظ في هذا الشأن هو عدم وجود اتفاق سواء على المستوى التشريعي أو الفقهي على استعمال مصطلح معين للدلالة على هذه الظاهرة الجرمية الناشئة في بيئة الكمبيوتر والانترنت، وهو اختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات، فهناك من يطلق عليها مصطلح جرائم الغش المعلوماتي أو الجرائم المعلوماتية، أو الجرئم الالكترونية، أو جرائم الحاسب الآلي، أو جرائم تقنية المعلومات، أو الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أو جرائم التكنولوجيا الحديثة، أو جرائم الكمبيوتر والانترنت

.ويرجع السبب في ذلك إلى عدة عوامل منها التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات، مما نتج عنه جرائم مستحدثة اختلفت التشريعات حول وضع مفاهيم موحدة لها[2]. وقد يكون السبب أيضا ترك المجال أمام المشرع لاحتواء التقنيات المتلاحقة في هذا الميدان، ولعدم حصر قاعدة التجريم في نطاق أفعال معينة تتبدل في المستقبل. ويشير

[1] تركي بن عبد الرحمان المويشير - بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليته - رسالة مقدمة لأجل نيل شهادة الدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2009 ، ص15

[2] Nidal EL chaer la criminalité informatique devant la justice pénale édition juridique sader, beyrouth liban .2014. pp. 18-19

هذا الإشكال العديد من التحديات أهمها صعوبة مواجهتها وتعذر الحلول المناسبة لمكافحتها سواء على المستوى الداخلي أو الدولي[1]. ورغم هذه الصعوبات حاول الفقهاء جاهدين وضع مفهوم لهذه الجرائم المستحدثة أين برز اتجاهان هما :

أولا : الاتجاه الضيق لمفهوم الجرائم الالكترونية :

تزعم هذا الاتجاه الفقيه **(ميروي) Merwe** خلال وضعه تعريفا مضمونه " أن الجريمة المعلوماتية هي ذلك الفعل غير المشروع الذي يتورط في ارتكابه بأنها" نشاط غير مشروع موجه لنسخ أو تغيير أو حذف Rosblat الحاسب [2]،كما عرفها (روز بلات - فعرفها Solerezأو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه " أما (سولريز بأنها " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات[3] .الملاحظ أن هذه التعاريف تستند إلى موضوع الجريمة ونمط السلوك محل التجريم، دون أن نأخذ بعين الاعتبار المجرم وهو ما أدى ببعض من الفقهاء إلى وضع تعاريف أخرى ذات طابع موسع تستند إلى الفاعل بدل موضوع الجريمة .

ثانيا : الاتجاه الموسع لمفهوم الجرائم الالكترونية :

حاول هذا الاتجاه إعطاء تعريف موسع للجريمة المعلوماتية لهدف تفادي النقص الظاهر على التعاريف السابقة، فعرفت بأنها "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية بهدف الاعتداء على الأموال المادية أو المعنوية "، كما عرفت بأنها " كل سلوك سلبي كان أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأي صورة كانت"[4]

---

[1] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2009، ص 73

[(2)] محمد أمين الشوابكة - جرائم الحاسوب والانترنت (الجريمة المعلوماتية) - دار الثقافة للنشر والتوزيع، عمان، الأردن 2009 ،ص 06 .

[3] تركى بن عبد الرحمان المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليته، المرجع السابق، ص 17

[4] محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية، دار ناشري للنشر الالكتروني الكويت، سنة 2012 ، ص 62

كما عرفت أيضا بأنها "كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسوب المادية و المعنوية وشبكات الاتصال الخاصة، باعتبار من المصالح و القيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها[1]

وفي ذات الاتجاه يرى الفقيهان **(ميشال و كريدو) Michel & Caredo** أن سوء استخدام الحاسوب يشمل استخدام الحاسوب كأداة لارتكاب الجريمة، بإضافة إلى الحالات المتعلقة بالولوج غير المصرح به الحاسوب المجني عليه أو بياناته، كما تمتد هذه الجريمة لتشمل الاعتداءات المادية الماسة بالحاسوب ذاته، أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وتزييف المكونات المادية والمعنوية للحاسوب بل وسرقة جهاز الحاسوب في حد ذاته أو مكون من مكوناته[2]

ونستخلص مما سبق أن اختلاف الفقه في وضع تعريف للجريمة المعلوماتية أو الإلكترونية مرده الاختلاف في المعيار المعتمد عليه والزاوية التي ينظر إليها كل اتجاه إلى هاته الجريمة المستحدثة، إلا أنه يمكن إعطاء تعريف ملخص تبعا لهذه الاتجاهات فهي : سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الكمبيوتر، فالسلوك يشمل الفعل الايجابي والامتناع عن الفعل وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية ومعاقب عليه قانونا، لأن إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك، ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة، بيانات ومعلومات معالجة ومخزنة، البرامج بأنواعها الأنظمة المعلوماتية...الخ). وأما الكمبيوتر فهو النظام التقني بمفهومه

[1] محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، المرجع السابق، ص09

[2] محمد علي العريان - الجرائم المعلوماتية - دار الجامعة الجديدة، الإسكندرية، مصر، 2004، ص 45.

المعلومات المستخرجة، والمتبادلة بين الشامل الذي يزاوج بين تقنيات الحوسبة والاتصال بما في ذلك شبكات المعلومات[1]

الفقرة الثانية : التعريف القانوني

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 02 / أمن القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته [2] بالقول بأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ."فمن خلال استعمال المشرع الجزائري لهذا المصطلح"الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" للدلالة على الجرائم الالكترونية فهو يزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة فالحوسبة تقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات"، أما الاتصال فهو قائم على وسائل تقنية النقل المعلومات بجميع إذن وعملا بالتعاريف المقترحة للجريمة المعلوماتية، فإنه يمكننا اقتراح تعريف خاص يشمل كافة الجوانب المتعلقة بالجريمة هذه فنعرفها بأنها" كل السلوكات المجرمة التي يشكل الحاسوب وشبكات الاتصال الخاصة به وسيلة لارتكابها أو محلا لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الالكترونية ."دلالاتها[3]

[1]يونس عرب، صور الجرائم الالكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، يومي 2 و 4 أفريل 2006، ص 7

[2]القانون رقم: 09-04 مؤرخ في: 5 أوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (جر) رقم 47 المؤرخة في: 16/08/2009

[3]يونس عرب، صور الجرائم الالكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، يومي 2 و 4 أفريل 2006. ص 1.

الفرع الثاني: خصائص الجريمة الالكترونية

إن تعريف الجريمة الالكترونية كما سبق والتطرق إليه، والقاضي بأنها ذلك النشاط الإجرامي المتصل باستعمال تقنية الحاسوب وشبكات الاتصال، يجعل من هذه الجرائم ذات طبيعة خاصة تختلف والمفهوم التقليدي المرتبط بتجريم السلوكات ذات الطبيعة المادية والتي تترك أثرا ملموسا في العالم الخارجي، ذلك لأن هذا النوع من الجرائم يتخذ من العالم الافتراضي ملجأ له بحيث لا تكاد تظهر سلوكات إجرامية نظرا لما تتميز به هذه الجرائم من خصوصيات، تجعل من أمر اكتشافها أمرا غاية في الصعوبة وهي الإشكاليات والمسائل التي سنحاول جاهدين معالجتها في هذا الفرع، من خلال تقسيمه إلى أربع فقرات، تناولنا الجريمة الالكترونية متعدية الحدود أو جريمة عابرة للحدود في (الفقرة الأولى)، وصعوبة اكتشاف الجريمة الإلكترونية في (الفقرة الثانية)، الجريمة الإلكترونية جريمة ناعمة في (الفقرة الثالثة) وأخيرا الجريمة الإلكترونية حديثة في (الفقرة الرابعة).

الفقرة الأولى: الجريمة الالكترونية متعدية الحدود أو جريمة عابرة للحدود

إن ارتباط كل دول العالم بشبكة الاتصالات الدولية، من خلال الأقمار الصناعية، وشبكة الإنترنت الجريمة لا تعترف بمفهوم الحدود الإقليمية للدول جعل أمر عولمة الجريمة أمرا ممكنا وشائعا فأصبحت واكتسحت الساحة العالمية[1]

فأصبح من الممكن أن يرتكب الجاني جريمة في دولة ويكون المجني عليه في دولة أخرى، وقد يترتب الضرر على أماكن متعددة في العالم بسبب الجريمة الواحدة.

ونتيجة للخسائر الكبيرة التي تتسبب فيها هذه الجرائم، تعالت الأصوات الداعية إلى التعاون الدولي المكثف للتصدي لها عن طريق إبرام الاتفاقيات والمعاهدات وتسهيل إجراءات التعاون والمساعدة القضائية بين الدول، فقد تتأثر دول عدة بجريمة إلكترونية واحدة تخلق مشكلات كثيرة مثل: تحديد الدولة صاحبة الاختصاص القضائي وحول القانون الواجب التطبيق

[1] عبد العال الدريبي - الجرائم الالكترونية - دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012، ص 55

وا ٍجراءات الملاحقة القضائية، فعولمة الجريمة المنظمة[1]، تقتضي عولمة مكافحتها أيضا بواسطة التعاون الدولي في صوره المتعددة .

في هذا الشأن سارع المشرع الجزائري إلى التصديق على نصوص الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية[2]، حيث نصت في مادتها الأولى: " تهدف هذه الاتفاقية إلى تعزيز التعاون العربي لمنع ومكافحة الجرائم المنظمة عبر الحدود الوطنية"، كما نصت بموجب المادة (21) منها على تجريم ارتكاب أو المشاركة في ارتكاب الأفعال التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع التقنية أنظمة المعلومات[3]، وتدخل مكافحة الجرائم الالكترونية ضمن هذا الإطار لأنها تتميز بأنها جرائم عابرة للحدود.

وفي السياق نفسه قام المشرع أيضا بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[4] والتي تنص في مادتها الأولى على:" تهدف هذه الاتفاقية إلى تعزيز التعاون

---

[1] يقصد بالجريمة المنظمة :مشروع إجرامي له نوع من الديمومة يمارس عدة أنشطة إجرامية، ويقوم عليه عدد من الأشخاص متفقون أو متعاونون على استثمار المخطط والحصول على الربح من خلال السوق غير المشروعة، يوسف گور ان، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، منشورات مركز كردستان الدراسات الإستراتيجية السليمانية، مصر، 2007، ص 72 .

[2] الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم-251 : 14 المؤرخ في: 2014/09/08، (ج، ر) رقم56: المؤرخة في: 2014/09/25

[3] تنص المادة (21) من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية على :" تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال الآتية التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع التقنية أنظمة المعلومات:

الاختراق غير المشروع أو تسهيل الاختراق غير المشروع على نحو كلي أو جزئي لأحد نظم المعلومات - تعطيل أو تحريف تشغيل أحد نظم المعلومات - إدخال بيانات بطرق غير مشروعة في أحد نظم المعلومات أو مسح وتعديل أو نسخ أو نشر البيانات التي يحتويها هذا النظام بطريق غير مشروع - استيراد أو حيازة أو عرض أو ترك أو إتاحة إحدى المعدات أو الأدوات أو برامج تقنية المعلومات بدون سبب مشروع بهدف ارتكاب إحدى الجرائم المنصوص عليها في الفقرات الثلاث السابقة - أي جريمة من الجرائم التقليدية ترتكب بإحدى وسائل تقنية أنظمة المعلومات.

[4] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ: 21 / 12 /2010، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم : 14- 252 المؤرخ في: 08 / 09 / 2014 ، (ج ، ر) رقم: 57 المؤرخة في: 28 / 09 / 2014

وتدعيمه بين الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها"، والتي ستشكل إضافة جديدة في مجال مكافحة الجرائم الإلكترونية في الجزائر .

الفقرة الثانية: صعوبة اكتشاف الجريمة الالكترونية

تتسم الجرائم الالكترونية المعلوماتية بأنها خفية ومستترة في أغلبها لأن الضحية لا يلحظها رغم أنها قد تقع أثناء وجوده على الشبكة لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة كإرسال الفيروسات والتجسس على البيانات المخزنة ولعل أن ما يزيد من خصوصية صعوبة اكتشافها[1] هي :

أولا: سرعة التنفيذ :

لا يتطلب أمر تنفيذ الجريمة الالكترونية أكثر من وقت الضغط على لوحة المفاتيح، و زر الفأرة أو ملامسة الشاشة الرقمية غير أن هذا لا يعني أنها لا تتطلب إعداد مسبقا من خلال توفير المعدات اللازمة والبرامج الضرورية لذلك .

ثانيا: التنفيذ عن بعد:

لا تتطلب الجرائم المعلوماتية في أغلبها وباستثناء جرائم سرقة معدات الحاسوب، وجود الفاعل في مكان الجريمة، فيمكن له إتيان جريمته وهو في مكان بعيد أو في دولة أخرى.

ثالثا: إخفاء معالم الجريمة

عادة ما تكتسي الجرائم المعلوماتية طابعا خفيا فلا يمكن ملاحظة أثارها إلا بعد التدقيق والتمعن من قبل أهل الاختصاص. [2]

المشتركة بين الشرطة الإسبانية ومعهد باندا للأمن المعلوماتي **(Mariposa)** وهذا ما كشفت عنه عملية في 03 مارس 2010، والتي أفضت إلى اكتشاف شبكة عالمية من الحواسيب بلغ عددها ثلاثة عشر (13) مليون حاسوب موزعة على 190 دولة كانت خاضعة للتحكم

[1] عبد المؤمن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والمقارن بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16 و17 نوفمبر 2015، كلية الحقوق جامعة بسكرة الجزائر، ص 08.

[2] عبد العال الدريبي، الجرائم الالكترونية، المرجع السابق, ص 2.

من قبل مجموعة من المجرمين، في شكل شبكة (BOT)، وقد كانوا يستعملون برنامجا خفيا في شكل فيروس يعرف باسم**(Botnet)** خاصة خفية تعرف باسم يهدف إلى اعتراض أرقام البطاقات البنكية والأشخاص المرتبطين بالشبكة بما في ذلك عدد كبير من المؤسسات المالية والبنكية، وقد استولى هؤلاء على ما يقارب 800.000 معلومة بنكية خاصة بالأفراد وقدر عدد الشركات التي مسها الاختراق بأكثر من 50% من الشركات على المستوى العالمي وبلغت الخسائر ملايين الدولارات[1]

الفقرة الثالثة: الجريمة الالكترونية جريمة ناعمة

تختلف الجرائم الالكترونية عن الجرائم التقليدية التي تتطلب أحيانا استخدام العنف، كما في جرائم القتل والضرب والجرح والسرقة، وجرائم الإرهاب ...الخ، إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، بل تتطلب مواصفات خاصة كالذكاء و امتلاك الوسائل المناسبة و قدرة على التعامل مع شبكة الانترنت فنقل البيانات من كمبيوتر إلى أخر أو المساس بأنظمة المعالجة الآلية للمعطيات أو الدخول غير مشروع للحاسوب أو القرصنة والسطو الإلكتروني على الأرصدة وبيانات بطاقات الائتمان، لا يتطلب أي عنف سواء مادي أو معنوي ولا يبذل فيه الجاني أي جهد عضلي، فهي جرائم هادئة بطبيعتها[2] ، فلا يحتاج المجرم الإلكتروني إلى العنف وا ٍنما يحتاج إلى مهارة وفن ودقة في استعمال تقنية المعلومات مثل: استخدام ما يعرف بالقنابل المنطقية والفيروسات المعلوماتية...الخ، كما أن معظم هؤلاء من الشباب المثقفين ذوي الاختصاصات العالية في مجال الحاسوب مما يخلق صعوبات إضافية للأجهزة القضائية المتخصصة لملاحقتهم[3]

[1] Myriam Quéméner. Yves Charpenel. La cybercriminalité. Edition Economica. Paris, France. 2010. p10.

[2] نهلا عبد القادر المومنى، جرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2008، ص 58.

[3] نعيم مغبغب، حماية برامج الكمبيوتر، منشورات الحلبي الحقوقية، لبنان، ط2، 2009، ص 141.

الفقرة الرابعة: الجريمة الالكترونية من الجرائم الحديثة

إن وجود الجريمة الإلكترونية جاء نتيجة لتطور تكنولوجيا تقنية المعلومات، إذ أن الجريمة الالكترونية لا تقع على أشياء مادية ولا يكون موضوعها إلحاق الضرر بالموجودات الفيزيائية إنما تعتبر البرامج الالكترونية وأنظمة المعلومات والبرامج الحاسوبية وشبكة الانترنت هي مسرح هذه الجرائم، كما أنها جرائم متنوعة عديدة لا يمكن حصرها وا ٍن كانت بعض التشريعات قد أدرجت تسميات لبعض الجرائم الالكترونية، إلا أنه لا يمكن في الواقع حصر هذه الجرائم والسبب في ذلك كما ذكرنا يعود إلى ارتباط هذه الجرائم بتكنولوجيا المعلومات وتطور الاتصالات التي لا يكاد يمر بعض الزمن حتى نسمع بتكنولوجيا حديثة ظهرت للبشرية[1]

المطلب الثاني: أنواع الجرائم المعلوماتية الالكترونية

تصنف الجرائم الالكترونية إلى فئات متعددة، تتباين تبعا للأساس المعتمد في ذلك فهناك عدة تقسيمات منها ما تقسم حسب دور الحاسب الآلي في الجريمة إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته (فقد يكون النظام المعلوماتي هدفا للاعتداء، أو وسيلة لارتكاب جريمة أخرى)[2] ومنها ما تصنف الجريمة الالكترونية على أساس الغاية من ارتكاب الجريمة التي قد تكون الاعتداء على نظام المعالجة الآلية للمعطيات أو الأموال أو الأشخاص.

[1] عبد الخالق صالح عبد الله مغرب، الأدلة المستخدمة في ارتكاب الجريمة الالكترونية، مجلة العدل، العدد السابع والثلاثون، السنة الرابعة عشر، ص 58.

[2] أمير فرج يوسف، الجريمة الالكترونية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، مصر، 2011، ص 97

وعلى غرار المشرع الجزائري[1] ،اهتم المشرع المقارن بتجريم صور الاعتداء الناجمة عن المعالجة الآلية للبيانات، نتيجة ظهور العديد من الصور المستحدثة التي لا تنفك أخطارها في أخذ أبعاد محلية، إقليمية وعالمية، وتكبد الدول والأشخاص خسائر لا يستهان بقيمتها، حيث تعذر على النصوص الجزائية التقليدية توفير الحماية القانونية للنظام المعلوماتي، لذلك تم إصدار نصوص عقابية عدة تطبيقا لمبدأ الشرعية الجزائية المواجهة الجرائم المعلوماتية الماسة بالنظم المعلوماتية والتي سنتطرق إليها في هذا المطلب من خلال (الفرع الأول)، بالإضافة إلى الجرائم المعلوماتية الماسة بالأموال والتي تناولناها في (الفرع الثاني)، وتلك الماسة بالأشخاص في (الفرع الثالث).

الفرع الأول: الجرائم الماسة بالنظم المعلوماتية

عالج المشرع الجزائري [2] العديد من صور الاعتداء على النظام المعلوماتي وقرر لها عقوبات بمقتضى المواد من 394 إلى 394 مكرر 7، وتشمل هذه الجرائم كل فعل أو امتناع عن فعل غير مشروع يقع على نظام المعالجة الآلية للمعطيات[3]، سواء كان ذلك بالتغيير أو التدمير أو إعاقة عملها أو الدخول إليها، أو استعمالها على نحو مخالف للقانون، وسنتناول في هذا الصدد جريمتين، حيث تطرقنا في الفقرة الأولى (إلى جريمة الدخول والبقاء غير المشروع للنظم المعلوماتية، في حين تناولنا في الفقرة الثانية) جريمة إتلاف وتعديل المعطيات.

الفقرة الأولى: جريمة الدخول والبقاء غير المشروع في نظام المعلوماتية (جرائم الاختراق)

---

[1] وذلك بإضافة نوع جديد من الجرائم في القسم السابع مكرر تحت مسمى المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04_15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66_155 المتضمن قانون العقوبات، الصادر في الجريدة الرسمية عدد : 71 بتاريخ 12 نوفمبر 2004، ومن ثمة إصدار القانون رقم 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

[2] القانون 04-15 المؤرخ في 10 نوفمبر 2004، المعدل و المتمم للأمر 66-156 المؤرخ في 05 جوان 1966 المتضمن قانون العقوبات والصادر في الجريدة الرسمية عدد 76 بتاريخ 10 نوفمبر 2004

[3] نشناش مينة، الإطار المفاهيمي للجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني حول الجريمة المعلوماتية، بين الوقاية و المكافحة، يومي 16 و 17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر ،2015 ، ص 12.

تعتبر جريمة الدخول و البقاء غير المشروع، أو جرائم الاختراق بشكل عام بأنها :القدرة على الوصول لهدف معين بطريقة غير مشروعة (بطريقة الغش)، عن طريق ثغرات في نظام الحماية الخاص بالهدف، وهي سمة سيئة يتسم بها المخترق، لقدرته على دخول أنظمة الأخرين دون رغبة منهم ودون علمهم بغض النظر عن الأضرار التي قد تحدثها، وتعد هذه الأنشطة الجريمة الأكثر انتشارا[1].

وقد نص عليها المشرع الجزائري بموجب المادة 394 مكرر من القانون 04-15[2] .

الفقرة الثانية: جريمة إتلاف وتعديل المعطيات

قد يعقب جريمة الدخول والبقاء غير المشروع، أفعال أخرى غير مشروعة تتمثل في جريمة إتلاف وتعديل المعطيات، حيث شملت الحماية الجنائية التي تدخل في نظام المعالجة الآلية من كل إدخال أو تعديل أو إزالة بطريق الغش .

" إضافة معطيات جديدة على الدعامة الخاصة بها، ويقصد ب: الإدخالL'intrusion سواء كان خالية أم تحمل معطيات من قبل، ونكون أمام فعل الإدخال في حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة والتزوير"[3]

- المحو أو الإزالة :(Leffacement) يقصد به إزالة جزء من المعطيات المسجلة داخل النظام وتحطيم تلك الدعامة أو نقل أو تخزين جزء من معطيات في ذاكرة مختلفة.
- التعديل :(La Modification) عبارة عن تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، سواء تم ذلك بصفة جزئية أو كلية، ويكون عن طريق برامج

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع 30) عمان، الأردن، 2011، ص 51 .

[2] تنص المادة 394 مكرر من (ق.ع. ج) على "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك

[3] أمال قارة، الحمايةالجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومه، الجزائر، 2007، ص 121 .

الفيروسات بصفة عامة[1].وقد نص عليها المشرع الجزائري بموجب المادة 394 مكرر أمن القانون 04-15[2].

الفرع الثاني: الجرائم المعلوماتية الواقعة على الأموال

أن كانت الجريمة المعلوماتية تستهدف النظم المعلوماتية بدافع الفضول أو الانتقام، توسعت الغاية منها لتشمل اكتساب المال بطريق غير مشروع وتحقيق مصلحة مالية عن طريق الاعتداء على المال والمالية عبر شبكة الانترنت واعتماد البنوك والمصارف على المعلوماتي تزامنا مع ازدياد المعاملات التجارية استخدام الأنظمة المعلوماتية ومن بين هذه الجرائم، تناولنا جرائم الاحتيال الالكتروني في (الفقرة الأولى)، والاعتداء على بطاقات الائتمان من خلال (الفقرة الثانية).

ويمكن تعريف المال المعلوماتي المشمول بالحماية القانونية بأنه: " كل مال الكتروني قابل النقل والتملك" أو بأنه: "المال الموجود على الحاسوب سواء في صورة معلومات أو بيانات الكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أو دعامات تخزين خارجية، فهو بذلك كل المدخلات الإلكترونية التي لها من قيمة المادية مما يجعلها قابلة للتملك وتكتسي الحماية القانونية "[3]

الفقرة الأولى: جرائم الاحتيال المعلوماتي

الاحتيال المعلوماتي أو الغش المعلوماتي أو غش الحاسوب كما يطلق عليها البعض[4]، هي كل فعل أو مجموعة من الأفعال غير المشروعة والمعتمدة التي ترتكب بهدف الخداع أو التحريف للحصول على شيء ذي قيمة ويكون نظام الحاسوب لازما لارتكابها أو إخفائها".

---

[1] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص ص 121-122

[2] تنص المادة 394 مكرر1 من قانون العقوبات الجزائري على: يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو زال أو عدل بطريق الغش المعطيات التي يتضمنها.

[3] تاير نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2012 ص .32

[4] نهلا عبد القادر المومني، جرائم المعلوماتية، المرجع السابق، ص188 .

الفقرة الثانية: جرائم الاعتداء على بطاقات الائتمان

تستخدم بطاقة الائتمان من قبل حاملها كوسيلة وفاء لالتزاماته بدلا من الدفع الفوري بالنقد، وذلك وفقا الشروط البنك مصدر البطاقة، وتختلف أنواع هذه البطاقات ونطاق استخدامها، فمنها ما هو محلي لا يتجاوز حدود الدولة التي صدر فيها ومنها ما يستخدم في كل دول العالم[1] .

إن جرائم إساءة استخدام بطاقة الائتمان قد ترتكب من طرف الغير، ويكون ذلك في حالة سرقة بيانات بطاقة الائتمان، أو في حالة استخدام بطاقة الائتمان مزورة و قد ترتكب من قبل حاملها الشرعي لدفع ثمن السلع والخدمات من خلال شبكة الانترنت، رغم علمه بعدم كفاية رصيده في البنك مصدر البطاقة، أو بعد انتهاء مدة صلاحيتها أو إلغائها كل بطاقة ائتمان مدة صلاحية محددة، عادة ما تقدر نسبة يقوم العمل بعد انتهائها بإعادتها إلى بنك لأن بطاقة الائتمان بمثابة محرر يتم تسليمها للعمل الأداء وظيفة معينة، واستخدامها بعد انتهاء صلاحيتها وعدم إعادتها إلى مصدرها بعد جريمة خيانة أمانة[2] .

الفرع الثالث: الجرائم الماسة بالأشخاص

إن تسخير البيئة المعلوماتية لارتكاب مختلف صور الاعتداء على نظم المعالجة الآلية للمعطيات وكذا تلك الجرائم الماسة بالأموال، سمح كذلك للمجرم بتحقيق أغلب صور الاعتداء على الأشخاص سواء نجم عنه أذي معنوي أو أدى إلى حدود ضرر مادي، وتعدد صور الجرائم المعلوماتية المتعلقة بالأشخاص، لذا سنأخذ على سبيل المثال جريمة القذف والتشهير عبر الإنترنت من خلال (الفقرة الأولى) وجرائم الاعتداء على البيانات الشخصية في (الفقرة الثانية).

الفقرة الأولى : جريمة القذف والتشهير عبر الإنترنت

[1] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الأول، نظام التجارة الالكترونية وحمايتها مدنيا، دار الفكر الجامعي، الإسكندرية، مصر، 2002، ص 108 .

[2] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، المرجع السابق، ص 125.

تعتبر هذه الجرائم من أكثر الجرائم شيوعا عبر شبكة الإنترنت، أين يعتقد العابثون أن لهم حرية التصرف في نشر وبث رسائل تحمل عبارات ذم وقدح وتحقير لأشخاص مستهدفين بذاتهم أو مجموعة من الأفراد، بصفة غيابية أو وجاهية عبر مختلف الوسائط الإلكترونية[1].

إن غياب نصوص تشريعية تتماشى مع هذه الصورة لجريمة القذف والتشهير، يجعلها تقع تحت أحكام النصوص العقابية لهذه الجريمة بصورها التقليدية، مما يطرح صعوبات في مجال إثباتها، وهو ما ينطبق على المشرع العقابي الجزائري، حيث تبقى المواد من 296 إلى 299 من القانون 06_23 المؤرخ في 20 ديسمبر 2006، مجرد توضيح للفعل المادي لجريمة القذف والسب والتحقير، دون ربطها مع تقنية المعلومات .

عكس المشرع السعودي الذي قام بإيضاح هذا النوع من الجرائم في قانون مكافحة الجرائم المعلوماتية حيث تناول في الفقرة 05 من المادة 03 وذلك تفسيرا لما ورد في نص المادة 14[2]. من الاتفاقية العربية المكافحة الجرائم المعلوماتية، ويمكن حصر هذه الجرائم في السلوكات التالية :

1-استهداف شخص معين بذاته بالذم والقدح والتشهير:

حيث يعمد الجاني باستخدام البريد الالكتروني إلى إسناد مادة معينة إلى شخص ما ينال فيها من شرفه أو كرامته ويعرضه إلى بعض الناس واحتقارهم، لا سيما إذا ما عمد الجاني في ذلك على توزيع فحوى الرسالة الالكترونية إلى عدد غير محدد من المتعاملين عبر شبكة الإنترنت . العالمية في إسناد مادة كتابية أو رسومية أو مرئي من (WEB) كما قد يستعمل الجاني شبكة

[1] محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، المرجع السابق، ص 31 .

[2] عرفت المادة 14 من الاتفاقية العربية لمكافحة الجرائم المعلوماتية المذكورة سابقا، جريمة الاعتداء على حرمة الحياة الخاصة باعتبارها جريمة معلوماتية بأنها :" الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات ."

الويب شأنها الإساءة لشخص معين فتطال شرفه وكرامته وتضعه موضع احتقار وذم من قبل الغير[1].

كما أن غرف قد تستخدم أيضا (TWITER) وتويتر (FACEBOOK) الدردشة والمحادثة ومواقع التواصل الاجتماعي، منها الارتكاب هذه الأفعال التي قد تتم وجاهيا باستعمال تقنيات الاتصال السمعي البصري عن طريق خدمة السكايب مثلا (SKYPE).

2-استهداف مجموعة من الأفراد وحث الغير على كراهيتهم :يكون ذلك بالنسبة لمجموعة من الأفراد لهم نفس الانتماءات الدينية أو العقائدية أو العرقية، وهو الموضوع الذي تناوله البروتوكول الإضافي الاتفاقية الجريمة الالكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية، التي تحرض على كراهية الأجانب، والتي ترتكب عن طريق أنظمة الكمبيوتر بتاريخ 28 جانفي2008 في ستراسبورغ - فرنسا حيث تضمن الفصل الثاني هذه الجرائم المعلوماتية، والتي تم حصرها في السلوكات التالية :

نشر المواد التي تتعلق بالعنصرية وكراهية الأجانب عبر أنظمة الكمبيوتر.

التهديد الذي تحركه دوافع التمييز العنصري وكراهية الأجانب؟

الإهانة التي تحركها دوافع التمييز العنصري وكراهية الأجانب.

الإنكار أو التقليل أو الموافقة أو تبرير جرائم الإبادة الجماعية وجرائم ضد الإنسانية[2].

تجدر الإشارة إلى أن هذه الصور تكاد تكون نفسها تلك التي جرمتها الفقرة المعاد 4/15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية .

إن سرعة وسهولة النشر التي توفرها المعلوماتية زادت من تفشي جرائم القذف والتشهير على نطاق واسع تصعب السيطرة عليه.

[1] محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، المرجع السابق، ص 33.

[2] المرجع نفسه، ص 37

الفقرة الثانية: جرائم التعدي على البيانات الشخصية

للإنسان بطبيعته حياة خاصة يحفظها ويهيئ سبل البقاء لها، وتقتضي حرمة هذه الحياة أن يكون له الحق في إضفاء السرية على مظاهرها، لكن التهديد المعلوماتي بهذا الصدد يبرز أساسا في إساءة استخدام المعلومات والبيانات المتعلقة بالأفراد.

ومن صور جرائم التعديعلى البيانات الشخصية، انتهاك السرية والخصوصية، وا ٍفشاء البيانات بما يضر بصاحبها، وكذلك الإطلاع على المراسلات الالكترونية، والإدلاء ببيانات كاذبة في إطار العمليات والمعاملات الالكترونية[1].

المطلب الثالث: دوافع ارتكاب الجريمة الإلكترونية

مما لا شك فيه أن السلوك الإنساني أيا كان، شرا أم خيرا له ما يغيره وما يبعث على ارتكابه وهو الذي يطلق عليه الدافع[2]، إلا أن صورة الدافع في قانون العقوبات فكرة تشوبها بعض الغموض وعدم إتفاق من جانب الفقه، ولذلك تعددت الاتجاهات واختلفت فمنهم من أطلق عليه الغاية، ومنهم النية ومنهم الغرض ومنهم الباعث، ولهذه التسميات المختلفة فائدة تذكر كلها تؤدي إلى معنى واحد وهو الدافع، وعليه ارتأينا إلى تقسيم هذا المطلب إلى فرعين، تناولنا في الفرع الأول) الدوافع الشخصية والسعي إلى تحقيق الربح، وفي (الفرع الثاني) تطرقنا إلى الإثارة والمتعة و التحدي.

الفرع الأول: الدوافع الشخصية والسعي إلى تحقيق الربح

تطرقنا في هذا الفرع إلى الدوافع الشخصية لارتكاب الجريمة الإلكترونية من خلال (الفقرة الأولى)، ثم تناولنا عنصر السعي إلى تحقيق الربح من خلال ارتكاب هذا النوع من الجرائم وذلك في (الفقرة الثانية).

---

[1] نهلا عبد القادر المومني، جرائم المعلوماتية، المرجع السابق، ص ص 173 - 174

[2] الدافع عرفه الدكتور محمد مصطفى زيدان بأنه " حالة فسيولوجية وسيولوجية داخل الفرد تجعله ينزع إلى القيام بأنواع معينة من السلوكات في اتجاه معين، وتهدف الدوافع إلى خفض حالة التوتر لدى الكائن الحي وتخليصه من حالة عدم التوازن...

الفقرة الأولى: الدوافع الشخصية

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبوا جرائم نظم المعلومات إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبوا هذه الجرائم لديهم شغف الآلة يحاولون إيجاد وغالبا ما يجدون _ الوسيلة إلى تحطيمها بل والتفوق عليها.

ويتزايد شيوع هذا الدافع لدى فئات صغار السن الذين يمضون وقتا طويلا أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن الأنظمة الكمبيوتر وشبكات المعلومات وا ٍظهار تفوقهم على وسائل التكنولوجيا، الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مسالة مرتكبي جرائم الحاسب الآلي الذي يتمثل باعثهم في إظهار تفوقهم، واعتبار أعمالهم غير منطوية على نوايا آثمة[1].

الفقرة الثانية: السعي إلى تحقيق الربح

يعتبر السعي إلى تحقيق الربح في المرتبة الأولى، من دوافع ارتكاب جرائم الحاسب الآلي، وفي دراسة فإن 13 % من حالات الغش المعلن عنها قد بوشرت من أجل الحصول على المال، ووفقا للدراسات فإن القطاع المالي يعد أكثر القطاعات استهدافا من جرائم الحاسب الآلي، مثال أن البنوك تعتمد وبشكل أساسي على أنظمة التمويل الإلكتروني[2].

الفرع الثاني : الإثارة والمتعة والتحدي

يدرك القراصنة شيئا عن أساسيات الكمبيوتر وأن هذا الأمر يمكن أن يكون ممتعا، حيث جاء على لسان أحد القراصنة ما يأتي " كانت القرصنة هي النداء الأخير الذي يبعثه دماغي فقد

---

[1] http://hrdoegypt.org/wp-content/uploads/2014/12/_ الإلكترونية-الجريمة-تقرير-2_ pdf:18 على الساعة 05 : 20 /05/ 2020.يوم

[2] التمويل الإلكتروني يعرف بصورة رئيسية على انه خدمات مالية تقدم بواسطة شبكة الإنترنت وبما أن التمويل صناعة كثيفة الاستخدام للمعلومات فانه يتأثر تأثرا بالغا بالانخفاض الشديد الذي شهدته تكلفة توليد المعلومات ومعالجتها ونقلها الذي تحقق بفضل تكنولوجيا المعلومات والاتصال والإنترنت ومن زاوية تطوير البنية الأساسية المالية خصوصا تمويل المشاريع الصغيرة والمتوسطة الحجم. أنظر الرابط التالي:

يوم : 2020/05/20 على الساعة : 19.20 http://www.alyaum.cm/article/1091233

كنت أعود إلى البيت بعد يوم ممل آخر في المدرسة، وأدير تشغيل جهاز الكمبيوتر، وأصبح عضوا في نخبة قراصنة الأنظمة، كان الأمر مختلفا برمته حيث لا وجود لعطف الكبار، وحيث الحكم هو موهبتك فقط، في البدء كنت أسجل أسمي الخاصة حيث يقوم الأشخاص الآخرين الذين يفعلون مثلي بالتردد علىBulletin Borard في لوحة النشرات هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد .وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة وأنسى جسدي تماما بينما أتنقل من جهاز كمبيوتر إلى آخر محاولا العثور على سبيل للوصول إلى هدفي، لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لأعداد ضخمة من المعلومات."

وكان يرافق تزايد سرعة الأدرينالين الإثارة المحظورة بفعل شئ غير قانوني. وكل خطوة أخطوها كان يمكن أن تسقطني بيد السلطات، كنت على حافة التكنولوجيا واكتشاف ما وراءها، واكتشاف الكهوف الإلكترونية التي لم يكن من المفترض وجودي بها[1].

المبحث الثاني: الإطار المفاهيمي للدليل الإلكتروني

نظرا للطابع الخاص الذي تتميز به الجريمة المعلوماتية، فإن عملية إثباتها تحيط بها الكثير من الصعوبات، ومما لاشك فيه أن كشف هذا النوع من الجرائم يحتاج إلى أدلة ذات طبيعة خاصة، تختلف عن الأدلة التقليدية، بحيث تكون من ذات الطبيعة التقنية الناجمة عن النظم المعلوماتية الناتجة عنها،فما هو إذا الدليل الأنسب لإثبات الجرائم المعلوماتية؟

وما هي صعوبات الحصول عليه؟.

[1] دورثي إي، قراصنة أنظمة الكمبيوتر، دينغ ورقة مقدمة للمؤتمر القومي الثالث عشر من الكمبيوتر، واشنطن ترجمة : آمنة علي يوسف، ديسمبر 1998، ص 11.

للإجابة على هذا التساؤل سنحدد (مفهوم الدليل الإلكتروني) في (المطلب الأول) ثم (مصادر الحصول على هذا الأخير) في (المطلب الثاني)، و (تقسيمات الدليل الإلكتروني) وذلك في مطلب مستقل (المطلب الثالث).

المطلب الأول: مفهوم الدليل الإلكتروني

يشمل مفهوم الدليل الإلكتروني على عدة عناصر ينبغي بيانها حتى يتضح هذا المفهوم بشكل جيد، لذلك سنتناول في هذا المطلب تعريف الدليل الإلكتروني في (الفرع الأول) ثم طبيعة الخاصة للدليل الإلكتروني في (الفرع الثاني) وفي الأخير شروط صحة هذا الدليل في (الفرع الثالث)

الفرع الأول: تعريف الدليل الإلكتروني

لتعريف الدليل الإلكتروني، لا بد من دراسة الأصل العام المتمثل في الدليل بصفة عامة، ثم التطرق إلى الفرع المتمثل في الدليل الإلكتروني .

وعليه سنتناول في هذا الفرع معنى الدليل الجنائي في (الفقرة الأولى)، من خلال التكلم عنه لغة وكذا إيراد المعنى الاصطلاحي، ثم سيكون التكلم عن معنى الدليل الإلكتروني من الجاني الفقهي في (الفقرة الثانية).

الفقرة الأولى: معنى الدليل الجنائي

لغة : يعرف على أنه "المرشد"، والدليل هو ما يستدل به، ويقال أدل فأمل والاسم الدالة بتشديد اللام وفلان يدل بفلان أي يثق به [1]. فهو المرشد وما به الإرشاد، وما يستدل به، والدليل الدال والجمع أدلة ودلالات .

منه نقول أن التعريف اللغوي للدليل الجنائي يعني بصفة عامة "الإرشاد"، وكذلك يأخذ معنى ما يتم الاستدلال به في إطار الإثبات .

[1] ابن منظور: لسان العرب، دار صادر، الطبعة الثالثة، المجلد الحادي عشر، لبنان، 1414هـ ، 1994م ، ص ص 248-249

اصطلاحا : يعرف على أنه :" ما يلزم من العلم به شئ آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة المنشودة [1]وبالنظر إلى غالبية التشريعات نجد أنها لم تعرف الدليل، وا ٍنما اكتفت بتعداد الأدلة ، سواء كان هذا التعداد على سبيل الحصر، أو المثال، إلا أن هناك بعض القوانين التي عرفته مثل قانون أسس الإجراءات الجنائية السوفيتية، إذ عرف الأدلة بأنها : " المعلومات الحقيقية التي على ضوئها يحدد المحقق, أو المحكمة طبقا للطرق المقررة قانونا توافر، أو تلف فعل خطر اجتماعيا وتأثيم الشخص الذي ارتكب الفعل[2].

فقد تعددت وجهات نظر القانونيين في معنى الدليل، ومن التعاريف ما جاء به الخبراء الذين عرفوه بأنه "البرهان القائم على المنطق والعقل في إطار من الشرعية الإجرائية لعثات صحة افتراض أو لرفع درجة اليقين الإقناعي في واقعة محل خلاف [3].

ومن خلال ما سبق نقول أن أغلب هذه التعريفات تتمحور حول الوصول للحقيقة، باستعمال المنطق السليم، سواء كان المنطق القانوني، أو العقلي، فهو وسيلة القاضي التي يصل من خلالها للحقيقة، ويكون بها اقتناعه، فالدليل الجنائي عبارة عن معلومة يثبت من خلالها ارتكاب الشخص للجريمة، أو عدم ارتكابه لها، فهو عنوان الحقيقة التي من خلالها يثبت الأمر أو يدحض، من خلال النظر في الواقع من جهة، وكذا النظر في القانون من جهة أخرى .

الفقرة الثانية : معنى الدليل الإلكتروني : هناك عدة تعريفات من أهمها

عرفه البعض على أنه :" الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا،

[1]عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2010 ص 51.

[2]سامي جلال قي حسين : الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر 2011، ص 16

[3]أحمد مسعود مريم : (آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09-04)، ماجستير منشورة، جامعة قاصدي مرباح، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2013 ، ص 81.

وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل : النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ القانون[1] "

وعرفه آخرون على أنه :" كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما"[2]

وأيضا هناك من يعرفه بأنه : معلومات يقبلها المنطق، والعقل، ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية، وعلمية، بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلى، وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق، أو المحاكمة الإثبات حقيقة فعل أو أي شئ له علاقة بجريمة، أو جان، أو مجني عليه [3]"

بمعنى أن الدليل الإلكتروني يستخلص من البرامج المعلوماتية الموجودة في الحاسوب، وكذا ما يمكن استخلاصه من معدات، وأدوات الحاسوب الآلي، وهذا مربوط بأن يكون هذا الدليل قد استخرج بطريقة قانونية، هذا بهدف تحليلها، وتقديمها للقضاء في شكلها النهائي .

الأدلة الرقمية بأنها: "تشمل جميع البيانات كما نجد التعريف الذي قال به الأستاذ كيسي (Casey) الرقمية التي يمكن أن تثبت أن هنالك جريمة ارتكبت أو توجد علاقة بين الجريمة والجاني بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الصور، الصوت و الفيديو[4].أما التعريف المقترح الدليل الالكتروني (IOCE) من قبل المنظمة الدولية لأدلة الحاسوب أنه "المعلومات المخزنة أو المثقلة

[1] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية مصر، 2006، ص 77 .

[2] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 53

[3] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 53

[4] digital evidence encompasses any andall digital data that ran rstablish that a crime has been this digital data is a combination of numbers that represent information of various kinds including trext, images, audio,and vidéo, by eogham casey, Digital Evidence And Computer Crime, Forensic Science Computer And The Internet, Second Edition, Academic Press An Imprint Of Elservier, London; 2004, p 260.

في شكل ثنائي، (International Organization Of Computer Evidence) ويمكن أن تعتمد عليها المحكمة"[1]

من خلال جملة التعاريف السابقة فضلا عن كونها متقاربة يتبين لنا ما يلي :

-وقوع تداخل بين تعريف الدليل الالكتروني من جهة ومفهوم برامج الحاسب الآلي من جهة أخرى حيث أن الوظيفة التي يؤديها كل منهما تفرق أحدهما عن الآخر، فدور برنامج الحاسوب يتمثل في تشغيله وتوجيهه إلى حل المشاكل ووضع الخطط المناسبة، أما الدليل الإلكتروني فله دور أساسي في معرفة كيفية حدوث الجريمة المعلوماتية بهدف إثباتها ونسبتها إلى مرتكبها في البيئة الافتراضية غير المحسوسة، إذ يمكن تفتيش الفرص الصلب لمعرفة ما مر به المجرم لتحقيق هدفه الإجرامي .

وما لا ينبغي إغفاله فيما يخص الفرق بين كل من الدليل الإلكتروني، وبرامج الحاسوب الآلي، أن الدليل الالكتروني لا يقتصر دوره في إثبات الجرائم الالكترونية فقط، كسرقة الملكية الفكرية، وا ٍنما يمتد أيضا إلى الجرائم التقليدية، كالقتل، والاختطاف، أيضا الاتجار بالمخدرات، وغيرها من الجرائم التي تستخدم فيها التقنية الإلكترونية للتسهيل فيها هذا من جهة .

من جهة أخرى نجد أن هذه التعريفات قد حصرت مصادر الأدلة الإلكترونية في أجهزة الحاسب الآلي ملحقاتها، دون العديد من النظم الأخرى المدمجة بحواسب التي قد تحتوي على العديد من الأدلة الرقمية و البطاقات الذكية **Smart Cards** و غيرها كالهواتف المحمولة **Mobile Telephone** وبالرجوع إلى الملاحظات السابقة نجد أن التعريف الأنسب للدليل الإلكتروني هو الذي يعرف بأنه :معلومات مخزنة في أجهزة الحاسوب وملحقاتها أو متنقلة عبر شبكات الاتصال، والتي يتم تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبها"[2]

[1] أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09-04، المرجع السابق، ص82

[2] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 60

الفرع الثاني: طبيعة الدليل الإلكتروني

إن الأدلة الجنائية متنوعة، وبالنسبة لطبيعتها فهي لا تخرج عن إما أن تكون ذات طبيعة مادية أو طبيعة معنوية، وفيما يخص الأدلة المادية فالمقصود بها تلك الأدلة التي يمكن إدراكها بالحواس، أي تتميز بطبيعة مادية محسوسة، كوجود الشئ المسروق في حيازة الجاني، أو ضبط الجاني حاملا لسلاح استعمل في ارتكاب الجريمة، بمعنى آخر الأدلة المادية هي تلك التي تخرج عن عناصر مادية معبرة عن نفسها، ولها تأثير في اقتناع القاضي بطريقة مباشرة وفيما يخص الأدلة المعنوية فهي عكس الأدلة المادية، أي ليس لها وجود مادي ملموس يعبر عنها، سواء كان هذا الأمر بالقول، أو الإيحاء، أو الكتابة، فهذه الأدلة يطلق عليها تعبير الأدلة الناطقة وهذا راجع إلى أن هذه الأدلة تصل للقاضي عن طريق لسان الغير، كاعتراف المتهم، وشهادة الشهود وبقول آخر هي تلك الأدلة الصادرة من إرادة شخصية، والمتجسدة في أقوال الغير، وتؤثر في اقتناع القاضي بطريقة غير مباشرة[1] .

إذا فإن الإشكال المثار هنا هو حول طبيعة الدليل الإلكتروني، سواء كانت مادية أو معنوية .

إن الدليل الإلكتروني بأنواعه هو ذو طبيعة مادية، مهما كان شكله، وسواء كان في شكل مخرجات ورقية، أو غير ورقية، وغيرها، باعتبار أنه حتى وا ٍن كانت غير ذلك فسيتم إخراجها في شكل دعامات، عبارة عن أشرطة ممغنطة، أو أقراص مغناطيسية، إلى غير ذلك، وبالتالي فهي ستصبح ذات طبيعة مادية[2] .

ومنه نقول أن الأدلة الإلكترونية لها طبيعة مادية وهذا الأمر لا يمكن إنكاره، باعتبار أن التطور التكنولوجي في الوقت الحالي يسمح باستخراج مختلف المعلومات من جهاز الحاسوب الآلي أو التقنيات المرتبطة به، في شكل أشياء مادية ملموسة لتصبح دليلا يعتمد عليه في قضية ما وتثبت به

[1] سامى جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، المرجع السابق، ص 65 .

[2] المرجع نفسه، ص 65

الفرع الثالث: خصائص الدليل الإلكتروني

للدليل الإلكتروني خصائص تميزه عن باقي الأدلة الجنائية التقليدية، وهذا يعود للبيئة التي يستخلص منها هذا النوع من الأدلة المتمثلة في البيئة الافتراضية، وما يمكن أن يقال عن هذه البيئة أنها متطورة بطبيعتها، بحيث تتوافر على أنواع متعددة من البيانات الرقمية التي قد تكون منفردة، أو مجتمعة حتى تكون دليلا، ومنه فإن هذه البيئة انعكست على هذا الدليل و أضفت عليه خصائص لا تتوافر في باقي الأدلة الجنائية.

وهذا ما سنوضحه من خلال تقسيم هذه الخصائص إلى أربع فقرات، حيث تطرقنا إلى أن الدليل الإلكتروني هو دليل علمي غير مرئي وهذا من خلال (الفقرة الأولى)، دليل يصعب التخلص منه في (الفقرة الثانية)، الدليل الإلكتروني قابل للنسخ (الفقرة الثالثة)، صعوبة طمس أو حذف الأدلة الإلكترونية (الفقرة الرابعة) .

الفقرة الأولى: دليل علمي غير مرئي

يتكون هذا الدليل الإلكتروني من بيانات ومعلومات ذات صفة إلكترونية غير ملموسة ولا تدرك بالحواس العادية، بل يتطلب لإدراكها الاستعانة بالبرامج والوسائل الخاصة بذلك[1]، والدليل الإلكتروني كالدليل العلمي يخضع لقاعدة لزوم التجاوب مع الحقيقة كاملة وفق قاعدة (إن القانون مسعاه العدالة، أما العلم فمسعاه الحقيقة).

إذن فبحكم الطبيعة الخاصة للدليل الإلكتروني فإنه لا يجب أن يخرج عما توصل إليه العلم الرقميوا ٍلا فقد معناه[2].

الفقرة الثانية: يصعب التخلص منه

تعتبر هذه الخاصية من أهم خصائص الدليل الرقمي و التي تميزه عن غير من الأدلة التقليدية فيمكن للجاني أن يتخلص بكل سهولة من الأوراق التي تحمل دليل إدانته بحرقها، أو بمسح بصماته من موضعها أو التخلص من الشهود، أما بالنسبة للأدلة الر قمية فإن الحال غير

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، المرجع السابق، ص 231.

[2] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 62 .

ذلك حيث يمكن استرجاعها بعد محوها أو سواء إتلافها وذلك عن طريق العديد من البرامج الخاصة مثل(Rescue Box أو Recover Lost) وهذا ما يشكل (Format) أو قام بإعادة تشكيل القرص عن طريق تقنية استخدام الجاني أمر المحوDelete على الجاني صعوبة في إخفاء جريمة والتخفي منها عن أعين العدالة والأمن[1].

الفقرة الثالث: قابل للنسخ

تتيح التقنية المعلوماتية استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها القيمة العلمية نفسها، وهذه الخاصية لا تتوافر في الأدلة الجنائية التقليدية، مما يشكل ضمانة فعالة لعدم إتلاف الدليل أو فقده أو تلفه[2] .

الفقرة الرابعة : صعوبة طمس أو حذف الأدلة الإلكترونية

الأدلة الإلكترونية يمكن استرجاعها بعد محوها، وا صلاحها بعد إتلافها وا ظهارها بعد إخفائها مما يؤدي إلى صعوبة التخلص منها وهي من أهم خصائص الدليل الإلكتروني بالمقارنة مع الدليل التقليدي فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغاؤها سواء تم ذلك بالأمر باستخدام الأمرHard Disk، أو حتى لو تم عمل إعادة التهيئة أو التشكيل القرص الصلب Delete والبرامج التي تم إتلافها أو إخفاؤها سواء كانت صورا أو رسوما أو كتابات أو غيرها مما يعني Format صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة طالما وصل علم رجال البحث والتحقيق الجنائي بوقوع الجريمة[3]، بل أن محاولة الجاني محو الدليل الإلكتروني بذاتها تسجل عليه كدليل، حيث أن قيامه بذلك يتم

[1] سامية بلجراف، سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي، ورقة بحثية مقدمة إلى أعمال الملتقى الوطني حول) الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر بسكرة، الجزائر، يومي 16 و17 نوفمبر 2015 ص ص 4-5

[2] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 64.

[3] عبد الناصر محمد محمود فرغلي، د محمد عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث من ضمن أعمال المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية الرياض، 2007، ص 15 .

تسجيله في ذاكرة الآلة وهو ما يمكن استخراجه واستخدامه كدليل ضده[1] ويزيد من صعوبة التخلص من الأدلة الإلكترونية أنه يمكن استخراج نسخ مطابقة للأصل ولها ذات القيمة والحجية الثبوتية،الشيء الذي لا يتوافر في أنواع الأدلة الأخرى(التقليدية) مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد أو التلف أو التغيير عن عمل نسخ طبق الأصل من الدليل[2] .

الفرع الرابع : شروط صحة الدليل الإلكتروني

هناك عدة شروط يجب توافرها في الدليل الإلكتروني لقبوله كأساس تقوم عليه الحقيقة في الدعاوى الجنائية سواء كان الحكم الصادر فيها بالبراءة أو الإدانة، وهذه الشروط تم تقسيمها إلى ثلاث فقرات

وهي : يجب أن يكون الدليل الإلكتروني غير قابل للشك (الفقرة الأولى)، يجب الحصول على هذا الدليل بصورة مشروعة (الفقرة الثانية ، وفي الأخير يجب أن يكون الدليل الإلكتروني قابلا للمناقشة (الفقرة الثالثة) الفقرة الأولى : يجب أن يكون الدليل الإلكتروني غير قابل للشك أي يقيني يشترط في الأدلة المستخرجة من الحاسوب والإنترنت أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا مجال لدحض قرينة البراءة أو افتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم و اليقين [3]، ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الإلكترونية، والمصغرات الفيلمية، وغيرها من الأشكال الإلكترونية، وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية وما ينطبع في ذهنه من تصورات

[1]طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول للمعلوماتية والقانون المنعقد في الفترة (28-29 /10 /2009)تنظمه أكاديمية الدراسات العليا ، طرابلس، ص 6

[2]عبد الناصر محمد محمود فرغلى، عبيد سيف المسماري، المرجع السابق، ص 15.

[3]في هذا السياق يشترط قانون البوليس والإثبات البريطاني لسنة 1984 حتى تتحقق يقينية الأدلة الرقمية أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة، وقد نصت بعض القوانين في الولايات المتحدة الأمريكية أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد من أفضل الأدلة المتاحة للإثبات وبالتالي يتحقق مبدأ اليقين لهذه الأدلة .

واحتمالات بالنسبة لها، أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه .[1]

الفقرة الثانية : يجب الحصول على الدليل بصورة مشروعة

يعرف بعض الفقه المشروعية بأنها: " التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام فهي تهدف إلى تقرير ضمانة أساسية وجدية لأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة والتطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الاجتماعي تحقيق حماية مماثلة للفرد ذاته.

فطبقا لهذا المبدأ ينبغي على القاضي أن يستقي قناعته في الحكم من خلال أدلة مشروعة، أما الأدلة التي جاءت وليدة إجراءات غير قانونية أو باطلة فلا يجوز الاعتماد عليها، ويجب طرحها نهائيا لأن ما بني على باطل فهو باطل، كما يجب على المحكمة استبعاد كل دليل معيب من بين الأدلة،وا ٍلاكان حكمها باطلا حتى وا ٍن استندت في إصدارها إلى أدلة أخرى مشروعة إلى جانب الدليل الباطل.[2]

الفقرة الثالثة : يجب أن يكون الدليل الإلكتروني قابلا للمناقشة

ويعني هذا المبدأ أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى[3]، وهذا يعني أن الأدلة المتحصلة من جرائم الحاسوب والإنترنت سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب، أم كانت بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية كل هذه ستكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا

[1] علي حسن الطوالبه، أستاذ القانون الجنائي المساعد، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي " دراسة مقارنة ، جامعة العلوم التطبيقية، البحرين، 2009، ص 8.

[2] سامية بلجراف، سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي، المرجع السابق، ص 7

[3] قرار محكمة النقض المصرية في 11/20 /1986- رقم 179- المبادئ القانونية- ص 943

المعلومات، يجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات[1].

المطلب الثاني : مصادر الحصول على الدليل الإلكتروني

من أجل تحصيل الدليل الرقمي، تعتمد جهات التحقيق على العديد من المصادر في عمليات البحث والتحري لجمع المعلومات بشأن الجرائم بصفة عامة والجريمة المعلوماتية بصفة خاصة، ومن بين المصادر التي سمح بها القانون هناك ما يعرف بإجراء الإرشاد وهذا ما سنتطرق إليه من خلال (الفرع الأول)، و إجراء الوضع تحت المراقبة الإلكترونية في (الفرع الثاني)، وفي الأخير تناولنا تعاون مقدمي خدمات الإنترنت مع السلطات القضائية في (الفرع الثالث).

الفرع الأول: إجراء الإرشاد الجنائي

من بين أهم الأساليب المعتمدة لكشف الجرائم المعلوماتية وتعقب المجرمين، نجد ما هو معروف بإجراء الإرشاد الجنائي، الذي يقوم بمقتضاه ضباط الشرطة القضائية بتجنيد أحد عناصرها لولوج العالم الافتراضي وبالأخص عبر حلقات النقاش وقاعات الدردشة والاتصال المباشر، مستعملين في ذلك أسماء وصفات هيئات وهمية من أجل البحث عن هذه الجرائم وكشف المجرمين[2].

[1] علي حسن الطوالبه، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي "دراسة مقارنة"، المرجع السابق، ص 10

[2] في هذا الصدد يقوم المرشد L'indicateur بعد حصوله على إذن رسمي بمباشرة مهامه، بالدخول في نقاشات مع الغير عبر الشبكة لمعلوماتية، وبمجرد إبراز هذا الشخص لنيته الإجرامية كأن يذكر أنه ينوي الاستيلاء على بطاقات ائتمان بصورة احتيالية، يقوم المرشد باستدراجه من أجل الحصول على كافة المعلومات، ثم يقوم بتوصيلها إلى الضبطية القضائية والتي تقوم بإلقاء القبض على المجرم، عن طريق برمجيات تقودها إلى مسار مزود الإنترنت الذي يستعمله مرتكب الجريمة ، أنظر : هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي الجديد، الإسكندرية، مصر، 2007، ص 197

وما يميز هذا الإجراء أنه لا يتطلب بذل جهد مادي كبير، حيث يقوم به ضابط الشرطة القضائية أو يكلف غيره من ذوي الاختصاص، وهذا بعد الحصول على إذن رسمي للقيام بمهام البحث والتحري عن الجرائم وضبط مرتكبيها[1].

وقد أتاح المشرع الجزائري إمكانية اللجوء إلى هذا الأسلوب تحت إسم " التسرب" من خلال نصوص المواد من 65 مكرر 05 إلى غاية المادة 65 مكرر 18 (ق إ ج ج)، وذلك في العديد من الجرائم بما فيها الجريمة المعلوماتية، بعد الحصول على إذن مسبب من وكيل الجمهورية أو قاضي التحقيق وتحت رقابة الأول المدة 4 أشهر قابلة للتجديد.

الفرع الثاني: إجراء الوضع تحت المراقبة الإلكترونية

تعتبر المراقبة من بين أهم مصادر البحث والتحري سواء في الجرائم التقليدية أو المستحدثة ومنها ، ويقصد بها مراقبة شبكة الجرائم المعلوماتية،

(Cyber surveillance)وتسمى حينئذ بالمراقبة الإلكترونية الاتصالات فتعرف بأنها : " العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع بيانات ومعلومات عن المشتبه سواء أكان شخصا أو مكانا، أو شيئا حسب طبيعته، من أجل تحقيق غرض أمني أو أي غرض آخر، وهي مرتبطة بالزمن[2].

و أجاز المشرع الجزائري المراقبة الإلكترونية في الجرائم المعلوماتية وهذا عن طريق اعتراض المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية، كما أجاز كل الترتيبات التقنية لها دون علم المعنيين ولا موافقتهم، بغية الحصول تسجيلات الكلام الصادر عنهم بصفة سرية أو خاصة، وذلك بإذن من وكيل الجمهورية[3]

وهناك العديد من الأساليب التقنية لإجراء المراقبة الإلكترونية من بينها[4]:

---

[1] المرجع نفسه، ص 196

[2] نبيلة هبة هروال،الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 105

[3] المادة 65 مكرر 5من قانون الإجراءات الجزائية الجزائري المعدل والمتمم .

[4] نبيلة هبة هروال، المرجع نفسه، ص ص 201 – 203

- تقنية برنامج كارنيفور
- تقنية كشف وجمع الأدلة والقرائن من رسائل البريد الإلكتروني .
- تقنية مراقبة البريد الإلكتروني .
- تقنية تعقب المواقع الإباحة

سنتطرق لعنصر إجراء الوضع تحت المراقبة الإلكترونية بالتفصيل في الفصل الثاني من هذه الدراسة، في المطلب الثاني من المبحث الأول تحت عنوان الإجراءات الحديثة لجمع الدليل الإلكتروني .

الفرع الثالث :تعاون مقدمي خدمات الإنترنت مع السلطات القضائية

يقصد بمزود الخدمة كل شخص يقدم خدمته إلى الجمهور بوجه عام في مجال الاتصالات الإلكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بعقد من العقود[1]، وقد عرف المشرع الجزائري "مقدم الخدمة " بموجب المادة 02/ د في القانون 04/09 بأنه:

1) أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و أو نظام للإثبات.
2) وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها .

ونظرا لضلوع الشبكة المعلوماتية في أغلب جرائم العالم الافتراضي، فإن المشرع الجزائري قد فرض على مقدمي خدمات الإنترنت مجموعة من الالتزامات من اجل مساعدة السلطات القضائية في أعمال التحقيق وذلك من خلال القانون رقم 09-04 في فصل الرابع تحت عنوان: " التزامات مقدمي الخدمات"، ومن بين الالتزامات الواردة نجد : الالتزام بمساعدة السلطات و الالتزام بحفظ المعطيات المتعلقة بحركة السير .

[1] شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، 2007، ص 209.

المطلب الثالث: تقسيمات الدليل الإلكتروني

تختلف الجريمة الإلكترونية عن الجريمة التقليدية في كون الأولى تتم في بيئة غير مادية عبر نظام حاسب ألي أو شبكة المعلومات الدولية الانترنت، حيث يمكن للجاني عن طريق نبضات إلكترونية رقمية لا ترى أن يعبث في بيانات الحاسوب أو برامجه، و ذلك في وقت قياسي كما يمكن محوها في زمن قياسي مما يصعب الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على الدليل المتوافر، إلا أن لهذا الأخير ميزة التنوع فلا يأتي على صورة واحدة، بل يوجد له العديد من الصور والأشكال، وفي هذا الصدد نجد نوعين من التقسيمات للأدلة الإلكترونية بالإضافة إلى تقسيمات أخرى ومنه ارتأينا إلى تقسيم هذا المطلب إلى ثلاث فروع رئيسية، تناولنا في الفرع الأول) التقسيمات الفقهية للدليل الإلكتروني، في حين خصصنا (الفرع الثاني) للتقسيمات التشريعية للدليل الإلكتروني، أما (الفرع الثالث) تطرقنا من خلاله إلى بعض من التقسيمات الأخرى لهذا الدليل.

الفرع الأول: التقسيمات الفقهية للدليل الإلكتروني

إن فقهاء القانون الجنائي لم يتوسعوا في دراسة الدليل الإلكتروني، ومرد ذلك للحداثة النسبية لهذا الدليل من جهة، وتطوره بصفة دائمة من جهة أخرى، ومن المحاولات الفقهية أنه تم تقسيم الدليل الإلكتروني لأربعة أقسام[1]، والتي قسمناها إلى أربع فقرات كالآتي: الأدلة الإلكترونية المتعلقة بجهاز الكمبيوتر وشبكاته في(الفقرة الأولى)، الأدلة الإلكترونية المتعلقة بالانترنت في (الفقرة الثانية)، الأدلة الإلكترونية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات في (الفقرة الثالثة)، والأدلة الإلكترونية المتعلقة بالشبكة العالمية للمعلومات في (الفقرة الرابعة).

[1] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 88.

الفقرة الأولى: الأدلة الإلكترونية المتعلقة بجهاز الكمبيوتر و شبكاته

وهي تتماشى مع جرائم الكمبيوتر الواقعة على أجهزة الكمبيوتر بسلوك غير مشروع، سواء كان هذا الأمر على المكونات المادية له[1]، أو المكونات المعنوية[2]، أو قواعد البيانات الرئيسية مثل تخريب مكونات الكمبيوتر كالشاشات .

الفقرة الثانية: الأدلة الإلكترونية المتعلقة بالانترنت وهي تتطابق مع جرائم الانترنت وهي أيضا سلوك غير مشروع يقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات مثل الدخول غير المشروع لمواقع يمنع الدخول إليها واستخدام عناوين غير دقيقة للدخول لشبكة العالمية للمعلومات وغيرها.

الفقرة الثالثة: الأدلة الإلكترونية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات

وهي متعلقة بالجرائم التي ترتكب باستخدام الكمبيوتر، حيث أنه لا يعتبر استعمال الكمبيوتر أو الشبكة العالمية للمعلومات أو انترنت، في هذه الجرائم من طبيعة الفعل الجرمي، وا ٍنما تعتبر كوسيلة مساعدة لارتكاب الجريمة، مثل غسيل الأموال أو نقل المخدرات من مكان لأخر وغيره، وجهاز الكمبيوتر في هذه الحال يحتفظ بآثار الكترونية قد ترشد للفاعل[3]

الفقرة الرابعة: الأدلة الإلكترونية المتعلقة بالشبكة العالمية للمعلومات

وهي متماشية مع الجرائم المتعلقة بهذه الشبكة، وهي فعل غير مشروع قانونا يقع على أي وثيقة أو نص موجود بالشبكة، مثل قرصنة المعلومات وسرقة بطاقات الائتمان وانتهاك الملكية الفكرية للبرامج وغيرها، فهذا النوع من الجرائم يتطلب الاتصال بالانترنت[4] .

---

[1]يقصد بالمكونات المادية للحاسوب: هي المكونات الفعلية لجهاز الكمبيوتر التي يمكن مشاهدتها ولمسها. يشتمل ذلك على وحدة النظام وكل شئ متصل بها، مثل الشاشة، لوحة المفاتيح، الفأرة (Hardware)... وغيرها .

[2]يقصد بالمكونات المعنوية للحاسوب: هي التي لا يمكن مشاهدتها ولكن يمكن أن نرى تأثير عملها مثل البرامج (Software)

[3]ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 95 .

[4]عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 73 .

الفرع الثاني: التقسيمات التشريعية والقضائية للدليل الالكتروني

برزت عدة تشريعات حول تقسيم الدليل الالكتروني وا ٍحاطة كل ما يتعلق به، وكان للقضاء أيضا دور في معالجة موضوع الدليل الالكتروني وكذا العمل على إعطاء تقسيمات، إلا أن تشريع الولايات المتحدة الأمريكية كان من السابقين الذين تطرقوا لهذا الموضوع أي الدليل الالكتروني، ولهذا ستكون كنموذج لدراستنا مع إبراز تقسيم المعتمد من قبلها لهذا الدليل، سواء كان هذا الأمر على مستوى التشريع أو القضاء .

فهي تعتبر ثاني دولة بعد السويد في إصدار القوانين الخاصة بها التي تجرم عن طريقها نوع مستحدثا ورافقتها من الجرائم وهي الجرائم الالكترونية(ICOE)، كما أنها قامت بإنشاء المنظمة الدولية لأدلة الحاسوب (SWGDE)وهذا بغرض توحيد الجهود التي تقوم بها هذه بالفريق العامل على مستوى الأدلة الالكترونية المنظمة[1].

ومنه ستبرز من خلال ما يلي تقسيمات وزارة العدل الأمريكية للدليل الإلكتروني لسنة 2002 والتي حصرناها في ثلاث فقرات، حيث تطرقنا في الفقرة الأولى إلى السجلات المحفوظة في الحاسوب وفي (الفقرة الثانية)، السجلات المحفوظة جزئيا في الحاسوب، أما في (الفقرة الثالثة) فتناولنا السجلات المحفوظة للإدخال والمنشأة بواسطة الحاسوب .

الفقرة الأولى: السجلات المحفوظة في الحاسوب

عبارة عن وثائق مكتوبة ومحفوظة والمقصودة بالكتابة الإلكترونية أيضا كل الحروف أو الأرقام أو الرموز أو أي علامات أخرى، تثبت على عامة إلكترونية أو رقمية أو ضوئية أو أي وسيلة أخرى وتعطي دلالة قابلة للإدراك[2] من أمثلتها البريد الإلكتروني الذي عرف على أنه: "لطريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات[3] فهو عبارة عن صندوق

[1]عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص ص 73 74

[2]محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، مصر، 2006، ص 272

[3]خالد ممدوح إبراهيم، التقاضي الإلكتروني، دار الفكر الجامعي، الطبعة الأولى، مصر، 2007، ص ص 101-102

تتواجد به كل الرسائل المرسلة إلى صاحب البريد والتي سبق له إرسالها و الملفات وغيرها من الأمور التي يحتوي عليها البريد الإلكتروني.

الفقرة الثانية: السجلات المحفوظة جزئيا في الحاسوب

هذا النوع من السجلات يتم إنشاؤها بواسطة الحاسوب، أي هي عبارة عن مخرجات برامج الحاسوب، بالإضافة لسجلات الهاتف وكذا فواتير أجهزة(Log Files) معنى ذلك أنه لم يتم لمسها من الأشخاص مثل(ATM) السحب الآلي .

الفقرة الثالثة: السجلات المحفوظة للإدخال والمنشأة بواسطة الحاسوب

ومن أمثلة هذا النوع من الأدلة الإلكترونية أوراق العمل المالية التي تحتوي على مدخلات يتم تحويلها ثم تتم معالجتها بإجراء العمليات الحسابية لبرامج عمل مثل EXCEL. وهذا التقسيم هو نفسه الذي أخذ به القضاء الأمر فسجلات الحاسوب المقبولة أمام القضاء الأمريكي هي التي تكون في شكل نصوص، وهذا إما في هيئة سجلات الحاسوب المتوالدة، أو سجلات الحاسوب المخزنة، ويكمن الفرق بينهما فيما إذا كان الشخص هو المنشى لمحتوي هذه السجلات أو الآلة، فسجلات الحاسوب المخزنة تحتوي على كتابات شخص أو بعض الأشخاص في شكل إلكتروني مثل: البريد الإلكتروني، أما ما يخص سجلات الحاسوب المتوالدة فالكمبيوتر هو الذي يصدرها، فهي عبارة عن مخرجات برامج الحاسوب مثل سجلات الدخول على الإنترنت التي يكون مصدرها مزود خدمة الإنترنت، كما أن هناك نوعا ثالثا من السجلات الذي يجمع بين التدخل الإنساني ومعالجة الكمبيوتر مثلا كأن يدخل متهم معين بيانات ويطلب من الكمبيوتر معالجتها للوصول إلى نتائج يمسح بها هذا البرنامج المستخدم، كالشخص الذي يتهرب من الضرائب فيسجل بيانات غير صحيحة تتعلق بدخله وربحه ويطلب من الكمبيوتر حساب الضريبة المستحقة[1].

[1] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص ص 74-76 .

إلا أن ما يؤخذ على هذه التقسيمات أنها لا تشمل الدليل الإلكتروني، فهي حصرته في نوع واحد وهو سجلات الحاسوب المحتواة على نص، رغم أن الدليل الإلكتروني يتعلق بكافة البيانات الإلكترونية التي يمكن تداولها إلكترونيا، كالصور والأصوات والرسوم وغيرها، فنجد في الوقت الراهن بروتوكولات الاتصالات (IP/TCP) والتطبيقات المعلوماتية التي تستعمل في التحقيق فيما يخص الجرائم الإلكترونية، حيث يعتبر نظام من أكثر البروتوكولات المستعملة في شبكات الإنترنت، فهي تعتبر جزءا مهما منه فهي تدل بصفة يقينية عن مصدر الجهاز الذي استخدم في الجريمة، كما تقوم بتحديد الأجهزة التي أصابها الضرر من هذا الفعل الإجرامي[1].

ومنه نقول أن التقسيم الذي جاء به كل من التشريع الأمريكي، وكذا القضاء الأمريكي فيه جانب من الصحة، باعتبار أنه تحدث عن نوع مهم من الأدلة الإلكترونية والتي تعتبر أدلة قوية.

إلا أن هذا التقسيم ناقص ولا يشمل كل الأدلة الإلكترونية، حيث نستطيع أن نقول أنه حصر تقسيمه في الأدلة الإلكترونية المكتوبة فقط في حين أن هناك أدلة إلكترونية أخرى، فهو لم يخرج في تقسيمه هذا عن السجلات المتعلقة بالحاسوب فقط

الفرع الثالث : تقسيمات أخرى للدليل الإلكتروني

هناك تقسيمات فقهية أخرى للدليل الإلكتروني، فقد أعطى الفقهاء احتمالات عديدة للدليل الإلكتروني وهذا ما سنحاول إيضاحه من خلال تقسيمنا هذا الفرع إلى فقرتين، لمحاولة الإلمام بجميع الأنواع المقترحة للدليل الإلكتروني، حيث تطرقنا في (الفقرة الأولى) إلى تقسيم الدليل الإلكتروني تبعا لمكوناته، أما (الفقرة الثانية) فقد تناولنا فيها تقسيم الأدلة الإلكترونية بحسب مكان وجودها.

[1] خالد ممدوح إبراهيم، التقاضي الإلكتروني، المرجع السابق، ص 76.

الفقرة الأولى : تقسيم الدليل الإلكتروني تبعا لمكوناته

أولا: الأشرطة المغناطيسية

وهذا الشريط هو عبارة عن شريط بلاستيكي مغطى بمادة قابلة للمغنطة ويكون ملفوفا على بكرة مثل التي تستخدم في أجهزة التسجيل الصوتي. يستعمل هذا الشريط في تخزين البرامج والملفات المتتالية أي اللازمة القراءة البيانات فيها قراءة الشريط من بدايته، والمعلومات الموجودة فيه تنظم على شكل وحدات خاصة.

ثانيا : الأقراص المغناطيسية

إن الأقراص المغناطيسية تعد من أفضل وسائط التخزين، التي يمكن استخدامها للتخزين المباشر وهذا راجع لقدرتها الاستيعابية الكبيرة، ولها خاصية مهمة هي إمكانية القراءة أو التسجيل، وكذا إمكانية تغيير أو تعديل أي ملف عليها دون الحاجة إلى إنشاء ملف جديد حيث يتم تعديل التسجيل وهو في موضعه، وهناك عدة أنواع نذكر منها : القرص المرن، القرص الصلب، قرص الخرطوش أو قرص الكارتريدج، المصغرات الفيلمية[1] .

الفقرة الثانية : تقسيم الأدلة الإلكترونية بحسب مكان وجودها

أولا : أدلة ورقية : مثل مخرجات الحاسوب والتقارير والرسوم البيانية .

ثانيا : أجهزة الحسابات : وهي التي تحتوي على ملحقات الحاسوب من شاشات وغير ذلك .

ثالثا : الأقراص المرنة والصلبة : تعتبر من أهم الأدلة لاحتوائها على بيانات وكلمات مرور و صور وتقارير وخطط ارتكاب الجريمة وغيرها.

رابعا : أشرطة تخزين المعلومات : تستخدم لحفظ النسخ الاحتياطية .

خامسا : القطع الإلكترونية : مثالها أجهزة الإرسال التي يجب أن تفحص للتأكد من طبيعتها خاصة في قضايا التجسس.

سادسا : أجهزة المودم : والتي تستخدم في نقل المعلومات.

[1] سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، المرجع السابق، ص 75

ويمتاز بعضها بإمكانية أن يعمل كجهاز الرد على رسائل الهاتف, ويجب تسجيل الكابلات المتصلة به عند ضبطه .

سابعا : البرامج : وهي التي تمثل الأدوات الرئيسية التي يستغلها المجرم في ارتكاب جريمة نظم المعلومات .

ثامنا : الطابعات والأجهزة الخاصة بتصوير المستندات ك وما قد تحتويه من أوراق مطبوعة و مصورة أو ما هو مخزن في ذاكرتها من معلومات[1].

يمكن القول أن هذه التقسيمات قد ألمت بجانب كبير ومهم من الأدلة الإلكترونية التي تعتبر من الأدلة القاطعة، ففي تقسيم الدليل الإلكتروني لا بد من الأخذ في عين الاعتبار التطور المستمر الذي يطرأ على هذا النوع من الأدلة من جهة، وعلى البيئة الافتراضية أو الإلكترونية من جهة أخرى. فهي أدلة متطورة بطبيعتها، كما تتطور وسائل الحصول عليها والتي يجب مراعاتها قانونيا حتى يكون من الإمكان الاعتماد عليها كدليل إثبات في مختلف القضايا .

[1] على جبار الحسيناوي : جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع ، الأردن، 2009، ص 143.

خلاصة الفصل

تطرقنا في هذا الفصل إلى الجريمة الإلكترونية باعتبارها مصدر للدليل الإلكتروني من خلال مناقشة تعريف هذه الجريمة وخصائصها، فلا يوجد اتفاق على المستوى التشريعي أو الفقهي على استعمال مصطلح محدد للدلالة على هذه الظاهرة الجرمية، وهذا بسبب طبيعتها الأصلية، فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود .

غير أن المشرع الجزائري وفق في اعتماد مصطلح " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال "وعرفها بموجب أحكام المادة (02 /أ) من القانون رقم 09-04 المؤرخ في 5 أوت 2009 والمتضمن القواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي يتوافق مع مصطلح " الجرائم الإلكترونية."

بعد ذلك عالجنا مختلف جوانب الدليل الإلكتروني كأثر ناتج عن الجريمة الإلكترونية من خلال تحديد مفهومه وخصائصه بالإضافة إلى شروط صحة ومصادر الحصول عليه مع إبراز أهم التقسيمات التي جاء بها.

الفصل الثانـي

إجراءات جمع الدليل الإلكتروني ومدى اقتناع القاضي الجنائي به

تمهيد :

لقد تناولنا في الفصل الأول مفهوما عاما وشاملا للجريمة الإلكترونية كمصدر للدليل الإلكتروني باعتبارها جريمة فريدة من نوعها حيث أن مسرحها فضاء افتراضي، كما عرفنا الدليل الإلكتروني كأثر ناتج عنها باعتباره الوسيلة الوحيدة أو الرئيسية لإثبات هذه الجرائم، وعليه فإنه يجب علينا أن نبين في هذا الفصل (المبحث الأول)، بينما نخصص (المبحث الثاني) المسألة مدة الإجراءات الخاصة لجمع الدليل الإلكتروني اقتناع القاضي الجنائي بهذا الدليل.

المبحث الأول: الإجراءات الخاصة بجمع الدليل الإلكتروني

مما لاشك فيه أنه لا يوجد ما يسمى بالجريمة الكاملة مهما حاول الجاني إخفاءها وذلك استنادا إلى قاعدة الوكارد لتبادل المواد التي تنص على أنه عند احتكاك جسمين بعضهما ببعض فإنه لابد وأن ينتقل جزء من الجسم الأول إلى الثاني وبالعكس، وبالتالي ينتج عن هذا الاحتكاك ما يعرف بالدليل الإلكتروني، وفي مجال الجريمة الالكترونية لدينا الدليل الالكتروني، وحتى يتحقق هذا الدليل الإثبات هذا النوع المستحدث من الجرائم فإنه لابد من جمع عناصر التحقيق والدعوى، و تقديم هذه العناصر إلى سلطة التحقيق الابتدائي، فإذا أسفر هذا التحقيق عن دليل أو ترجح معها إدانة المته، قدمته إلى المحكمة، ومرحلة المحاكمة هي أهم المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي لإدانة المتهم ٍلا قضي ببراعته[1] .

إلا أن خصوصية الجريمة الإلكترونية وذاتية الدليل الإلكتروني سيقودان دون شك إلى تغيير كبير إن لم يكن كليا في المفاهيم السائدة حول إجراءات الحصول على هذا الدليل وذلك نتيجة لضآلة دور بعض الإجراءات التقليدية في بيئة تكنولوجيا المعلومات كالمعاينة أو الشهادة مثلا، و بالتالي يقودنا إلى إتباع الإجراءات التقليدية لجمع الدليل الإلكتروني في (المطلب الأول)، ثم يليه الإجراءات الحديثة لجمع هذا الدليل في (المطلب الثاني)

المطلب الأول: الإجراءات التقليدية لجمع الدليل الإلكتروني

نظم المشرع كيفية استنباط الدليل عن طريق إجراءات تتبع وصولا إلى هذه الغاية. وعليه قسمنا المطلب إلى ثلاث فروع أساسية، فقد خصصناه تناولنا في إلى هذا التفتيش الفرع الثاني المعاينة والخبرة التقنية، وفي الفرع الأول سماع الشهود، وهذه الإجراءات تستخدم بصفة عامة الفرع الثالث (وضبط الأشياء، أما في

[1] خالد حمد محمد الهادي، الثورة البيولوجية ودورها في الكشف عن الجريمةDNA ، دار الجامعة الجديدة ، 2005 ،ص 19.

اجمع الدليل في جميع الجرائم التقليدية منها والمستحدثة، إلا أن دورها يكون بين المد في الجرائم الأولى والجزر في الثانية

الفرع الأول: المعاينة والخبرة التقنية

إن التعامل في الجريمة المعلوماتية يتطلب إجراءات روتينية متفق عليها وذلك من أجل حماية الدليل، غير أن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة المعلوماتية الرقمية، ذلك لأن البرامج والبيانات عنصران أساسيان يتحتم على أجهزة تنفيذ القانون وخبراء الأدلة الجنائية جمعها واستخلاصها، وتعد المعاينة والخبرة من بين إجراءات التحقيق، والتي تؤدي للوصول إلى الدليل المستمد من الواقعة الإجرامية، وسوف نتعرض في هذا الفرع لمفهوم الانتقال والمعاينة في (الفقرة الأولى)، وكذا الخبرة التقنية في العالم الافتراضي في (الفقرة الثانية) .

الفقرة الأولى: مفهوم الانتقال والمعاينة

لم تحدد أغلب التشريعات المقصود بالانتقال والمعاينة ومنها المشرع الجزائري الأمر الذي دعا بالفقه للتصدي لتعريفهما، حيث يعتبر الانتقال عملا هاما من أعمال التحقيق يتم بقصد جمعا الأدلة وفحصها لكشف حقيقة الجريمة ويتطلب ذلك أن ينتقل المحقق من مقر عمله إلى مكان آخر قد يكون مسرح الجريمة الإجراء عمل من أعمال التحقيق، حيث يتم الانتقال بهدف إجراء معاينة أو بهدف القيام بعمل آخر كالتفتيش والضبط وسماع أقوال الشهود في بعض الأحوال [1]، أما فيما يخص المعاينة فهناك عدة تعاريف لها، فيقصد بها" :رؤية بالعين المكان أو شخص أو شيء لإثبات حالته ومعرفة كل ما يلزم لكشف الحقيقة[2] في حين عرفها جانب أخر من الفقه

[1] خالد ممدوح إبراهيم، التقاضي الإلكتروني، المرجع السابق، ص 156

[2] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة منشورات الحلبي الحقوقية، بيروت، لبنان، (دس، ت)، ص303.

تعريف أكثر دقة بأنها: مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها أو محوها أو تعديلها[1].

الأصل في المعاينة أنها إجراء من إجراءات التحقيق، ولهذا في غير حالات التلبس المنصوص عليها في القانون يجب أن تقوم بها سلطة التحقيق بنفسها، أو تنتدب مأمور الضبط للقيام بذلك [2]تحرير محضر بها عن طريق كاتب، لأنها من الإجراءات التي تستلزم من المحقق تفرغا ذهنيا، وتتبع في شانها أيضا جميع القواعد التي تحكم إجراءات المحاكمة، من إخطار الخصوم بمكان المعاينة وزمانها ليتمكنوا من ويقتضي ذلك الحضور أثناء إجراءها[3]. كما يمكن للمحكمة أن تقوم بإجراء المعاينة إذا ما رأت في ذلك سبيلا في كشف الحقيقة، سواء كان ذلك من تلقاء نفسها أو بناء على طلب الخصوم[4].

هذا فيما يخص بالأحكام العامة للمعاينة، وسنتناول فيما يلي المعاينة في الجريمة الالكترونية ومدى أهميتها مقارنة بالجريمة التقليدية .

للمعاينة أهمية كبيرة في كشف غموض العديد الجرائم التقليدية، إلا أن دورها في كشف غموض الجرائم الإلكترونية، وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها لمرتكبها ليس بالدرجة نفسها من الأهمية مقارنة بالجريمة الإلكترونية وذلك لأسباب عدة منها :

أن الجرائم الواقعة على نظم المعلومات أي الجرائم الالكترونية، من النادر ما يتخلف عنها آثار مادية .

---

[1]علي عدنن الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، طا المكتب) الجامعي الحديث، مصر، 2012، ص22

[2]محمد علي الجمال، التقاط الدليل المادي من مسرح الجريمة، مجلة الدراسات العليا، العدد الثاني، يناير 2000 ص 190.

[3]جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالانترنت، دار الفكر العربي، القاهرة، 2001، ص 27 .

[4]جلال ثروت، نظم الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، 1997، ص 456.

إن عن عدد كبير من الأفراد يكونوا قد ترددوا على مسرح الجريمة خلال الفترة التي تتوسط عادة بين ارتكاب الجريمة واكتشافها، و هذا ما يفتح المجال لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو محو بعضها، وهو ما يثير الشك على الدليل المستنبط من المعاينة[1].

استطاعة الجاني من التلاعب في البيانات عن بعد أو محوها عن طريق قيامه بالتدخل من خلال وحدة طرفية، لذلك نص كل من المشرع الجزائري في المادة 43 من قانون الإجراءات الجزائية الجزائري[2] ، والمشرع الفرنسي من خلال المادة 55 /1 من قانون الإجراءات الجنائية الفرنسي[3]،أن تقرر جزاءات جنائية على كل من يقوم بإجراء أي تغيير أو تعديل في المعلومات المسجلة في ذاكرة الحاسوب أو وسائط التخزين أو في بنك المعلومات أو قاعدة البيانات قبل قيام سلطة التحقيق بإجراء المعاينة وذلك حرصا منهما على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي، والملاحظ و إن كانت أحكام هذه النصوص تنصرف إلى أغلب الجرائم التقليدية، إلا أنه يمكن تطبيقها عند معاينة مكونات الحاسوب ذات الطابع المادي على خلاف معاينة المكونات غير المادية لأنها تتطلب إجراءات خاصة[4].

أولا: الانتقال والمعاينة على مسرح الجريمة الإلكترونية

تتم معاينة الجريمة الإلكترونية بالانتقال إلى مسرح الجريمة الإلكترونية وينبغي التعامل مع هذا المسرح على أنه مسرحان هما :

---

[1]عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2001 ص ص 365- 366

[2]تنص المادة 43من قانون الإجراءات الجزائية الجزائري، يحظر في مكان ارتكاب جناية على كل شخص لا صفة له أن يقوم القضائي، بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق وا ٍلا عوقب بغرامة 200 إلى 1000دج، غير انه يستثنى من هذا الحظر حالة ما إذا كانت التغيرات أو نزع الأشياء للسلامة و الصحة العمومية أو تستلزمها معالجة المجني عليه

[3] Article 55 DU (cppf)

= dans les lieux ou un crime à été commis, il est interdit, sous peine le l'amende prévue pour les contraventions de la quatrieme classe, à toute personne non habilitée, de modifie avant les premieres opérations de l'enquete judiciaire l'état des lieux et d'y effettuer des prélèvement quelconques....

[4]عائشة بن قارة مصطفى،، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 82.

مسرح تقليدي: يقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية للحاسوب وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية، فقد يترك الجاني آثارا كالبصمات وبعض المتعلقات الشخصية أو وسائط تخزين رقمية.

مسرح افتراضي: يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنت وفي ذاكرة الأقراص الصلبة للحاسوب غير أن الانتقال لا يتم بالضرورة عبر العالم المادي وا ٍنما عبر العالم الافتراضي (cuber space) ، وعليه يستطيع ضابط الشرطة القضائية الانتقال إلى العالم الافتراضي لمعاينة الجريمة الإلكترونية كما يأتي[1]

- يستطيع ضابط الشرطة القضائية الانتقال إلى العالم الافتراضي لمعاينة مسرح الجريمة من خلال حاسويه الموجود بمكتبه .
- يمكن لضابط الشرطة القضائية اللجوء إلى مقهى الانترنت.
- يمكن لضابط الشرطة القضائية اللجوء على مزود خدمة الانترنت internet server provide الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة.

ونتيجة لاختلاف مسرح الجريمة الإلكترونية عن غيره من الجرائم لكون هذا النوع من الجرائم يتميز بوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية، لذلك ينبغي تعاملا خاصا معه ويكون ذلك من خلال إتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة الإلكترونية أبرزها :

-توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة وشبكات الاتصال الخاصة بها قصد تحديد إمكانية التعامل معها فني[2].

-إعداد خريطة الموقع المتوقع الإغارة عليه والتأكيد من تأمين وصلاحية الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة.[3]

---

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 218

[2] هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية، دار الكتب القانونية، القاهرة، مصر، 2015، ص186.

[3] نبيلة هبة هروال، المرجع نفسه، ص 219.

-إعداد فريق متخصص من الخبراء ورجال الأمن والضباط واعطائهم الوقت الكافي للاستعداد فنيا عن طريق وضع خطة عملية لضبط أدلة الجريمة وقت معاينتها[1] .

-الحصول على الاحتياجات الضرورية من أجهزة و برامج للاستعانة بها في الفحص والتشغيل مثل :

برامج معالجة الملفات (xtreeprogold) وبرامج النسخ (laplink) وبرامج إنتاج صور مطابقة عن القرص الصلب(encase) ، والذي تستخدمه المباحث الفدرالية الأمريكية في التحقيقات الجنائية ويطلق عليه الخبراء (حقيبة الأدلة الرقمية)[2]

-تأمين عدم انقطاع التيار الكهربائي المفاجئ لأن ذلك يتسبب في محور المعلومات من الذاكرة وبالتالي ضياع كافة العمليات التي تم تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة[3] .

ثانيا: الإجراءات التي يتعين إتباعها عند إجراء المعاينة

-تصوير الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجهزة الخلفية للحاسوب وملحقاته مع مراعاة تسجيل وقت و تاريخ ومكان التقاط كل صورة[4] .

-عدم نقل أي مادة معلوماتية من مكان وقوع الجريمة إلا بعد إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي قد تؤدي إلى فقد البيانات المخزنة[5].

---

[1] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية، ط1، دار النهضة العربية الإسكندرية مصر، 2009، ص 216.

[2] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 85

[3] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية المرجع السابق، ص217

[4] خالد ممدوح إبراهيم، التقاضي الإلكتروني، المرجع السابق، ص172.

[5] عبد العال الدريبي،محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، مصر 2012 ،ص 296 .

-القيام بحفظ المستندات الخاصة بالإدخال وكذا مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة وذلك من أجل رفع مضاهاة البصمات التي قد تكون موجودة عليها[1].

-التحفظ على محتويات سلة المهملات، وكذا القيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطمة المتواجدة فيها[2] .

-ربط الأقراص الكومبيوترية التي ربما تحمل الأدلة، مع جهاز يمنع الكتابة أو التسجيل عليها، مما يتيح للمحققين قراءة بياناتها من دون تغييرها.

-قصر مباشرة المعاينة على المحققين الذين تتوافر الكفاءة العملية والخبرة التقنية في مجال المعلوماتية واسترجاع المعلومات، و الذين تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يمكن أن يحتويها مسرح الجريمة الإلكترونية[3].

وعلى ضوء ما تقدم يمكن القول بعدم كفاية المعاينة كإجراء تقليدي للإحاطة بكافة جوانب مسرح الجريمة الإلكترونية نظرا لمميزات الدليل الإلكتروني، فهو غير مرئى كما يسهل على المجرم محوه أو بتعديله بضغطة زر وفي جزء من الثانية وهو جالس وراء حاسوبه، لذا لنجاح المعاينة لابد من توفير فريق متخصص من ضباط الشرطة القضائية لديهم معرفة متميزة بالمعلوماتية عموما وبنظمها خصوصا وكيفية تشغيلها ووسائلها، وتقنيات إساءة استعمالها من قبل مستخدميها. ولا يتأتى ذلك إلا بتكوينهم وتدريبهم وتجديد معارفهم قصد حصولهم على المهارات اللازمة في مجال الكشف عن الجرائم المستحدثة[4].

---

[1] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، المرجع السابق، ص 307.

[2] عائشة بن قارة مصطفى، المرجع نفسه، ص ص 86-87.

[3] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتب الآلات الحديثة، مصر، 1994.

[4] يزيد بوحليط، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر، أطروحة لنيل شهادة دكتوراه العلوم تخصص قانون خاص، جامعة باجي مختار، عنابة، 2016، ص 226

الفقرة الثانية: الخبرة التقنية في العالم الافتراضي

الخبرة القضائية عموما هي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه [1] فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية والفنية والتي لا تتوافر سواء لدى المحقق أو القاضي، وفي هذا المجال نتطرق أولا إلى دراسة القواعد القانونية التي تحكم الخبرة القضائية بصفة عامة، ثم نتناول ثانيا الجوانب الفنية التي تحكم إنجاز الخبرة التقنية المتعلقة بإثبات الجريمة الإلكترونية .

أولا: القواعد القانونية التي تحكم الخبرة القضائية

وسنتناول من خلالها مفهوم الخبرة القضائية، طرق اختيار الخبراء، وواجبات الخبير التقني وذلك من خلال النقاط التالية:

1-مفهوم الخبرة القضائية

أ- تعريف الخبرة

يقصد بالخبرة: مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرها إلى معرفة فنية أو دراية علمية لا تتوافر لديه"[2] فهي بحث في المسائل المادية أو الفنية التي يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات .كما يعرف الخبير الإلكتروني بأنه الشخص الذي تكمن له دراية بمسألة من المسائل وله كفاءة فنية وعلمية خاصة [1]

[1]أنظر: أمال عثمان، الخبرة في المسالة الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964، ص 68 وما بعدها.

أيضا: عادل حافظ غائم، الخبرة في مجال الإثبات الجنائي، بحث بمجلة الأمن العام، العدد 43، سنة 1968 ص 19 وما بعدها.

[2]صغير يوسف، الجريمة المرتكبة عبر الانترنت، ماجستير، منشورة، جامعة مولود معمري، كلية الحقوق والعلوم السياسية،الجزائر، 2013، ص88

ب- طرق اختيار الخبراء

إذا كانت الاستعانة بالخبير في الجرائم التقليدية أمر بالغ الأهمية في إثبات الجريمة، فإن الاستعانة به في مجال إثبات الجرائم الإلكترونية يعد أمرا متطلبا و ضروريا بسبب التطور التقني السريع في مجال تقنية المعلومات، إذ لا يكشف غموض الجريمة إلا من طرف شخص على درجة كبيرة من العلم والدراية في مجال تخصصه [2]، حيث يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة كما تحدد الأوضاع التي يجري فيها قيد الخبراء أو شطبهم بقرار من وزير العدل [3]

وقد ترك المشرع القاضي التحقيق حرية ندب خبير واحد أو خبراء متعددين بحسب المادة 147 من قانون الإجراءات الجزائية الجزائري، التي جاء فحواها بصفة عامة أنه في إمكان القاضي الجنائي أن يندب أكثر من خبير، بغرض حل الدعوى المطروحة أمامه، فقد لا يطمئن القاضي الجنائي الرأي خبير فني وتقني واحد فيلجأ لرأي عدة خبراء .

وكذلك لم يحدد المشرع طبيعة من يقوم بالخبرة سواء كان شخصا طبيعيا، أو معنويا كمؤسسة متخصصة تعمل في مجال الحاسوب الذين يتم اللجوء إليهم خاصة في مجال الدليل الإلكتروني باعتبار أن هذا النوع من المؤسسات يملك موارد مادية من برامج و أجهزة حديثة وموارد بشرية من مهندسين متخصصين في الحاسوب و الانترنت[4].

ج- واجبات الخبير التقني:

له عدة واجبات تتمثل في :

---

[1]عبد الناصر محمد محمود فرغلى، محمد عبيد سيف سعيد السماري، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة)، المؤتمر العربي الأول للعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 24.

[2] David forest et gautier kaufman, droit de l'informatique gualino éditeur extenso édition, France, 2010, p79, 80

[3]نصت المادة 144 من (ق... ج. ج) على:يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة، وتحدد الأوضاع التي يجري بها قيد الخبراء أو شطب أسمائهم بقرار من وزير العدل..

[4]عائشة بن قارة مصطفى، المرجع السابق، ص ص 141 - 142.

حلف اليمين: أوجب المشرع الجزائري لضمان صحة تقرير الخبير ونيل ثقة أطراف الدعوى، أن يحلف اليمين[1] قبل البدء في انجاز الخبرة .

-إنجاز الخبير الأعمال الخبرة بنفسه: لابد على الخبير أن يقوم بأعمال الخبرة بنفسه وفي حدود ما نص عليه أمر أو حكم الندب، وأن يستجيب للطلبات التي يقدمها أطراف الخصومة مثل: سماع أي شخص قادر على إعطاء معلومات فنية[2].

-الخضوع للرقابة القضائية: يتعين على الخبير أن يتولى مهمته تحت رقابة القاضي الذي عينه وأن يبقى على اتصال دائم به لأجل إحاطته علما بتطورات الأعمال التي يقوم بها، فالخبير هو مساعد للقاضي ومعاون فني لا أكثر[3]

إيداع الخبرة التقنية: بعد انتهاء الخير من أعماله التي كلف بها يقوم بإيداع الخبرة التقنية خلال المدة المحددة في أمر أو حكم الندب، وأن يقدم نتائج ما قام به من أبحاث فإن خال ذلك جاز للقاضي استبداله بغيره، كما يمكن أن يتخذ في حق الخبير الذي ثبت وقوع إهمال منه إجراءات تأديبية قد تصل إلى شطب اسمه من جداول الخبراء بقرار من الوزير[4] .

---

[1] حيث تنص المادة 145 من قانون الإجراءات الجزائية على: يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الأتية بيانها، أقسم بالله العظيم أن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص و أن أيدي رأي بكل نزاهة و استقلال. ولا يجدد هذا القسم ما دام الخبير مقيدا في الجدول "...

[2] المادة 152 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[3] Michaud le juge d'instruction et l'expert, R. S.C, 1975.p791.

[4] حيث تنص المادة 148 من قانون الإجراءات الجزائية على: "كل قرار يصدر بندب خبراء يجب أن تحدد فيه مهلة لإنجاز مهمته ويجوز أن تمتد هذه المهلة بناء على طلب الخبراء إذا اقتضت ذلك أسباب خاصة ويكون ذلك بقرار مسبب يصدره القاضي أو الجهةالتي تديتهم، وإذا لم يودع الخبراء تقاريرهم في الميعاد المحدد لهم جاز في الحال أن يستبدل بهم غيرهم وعليهم إذ ذلك أن يقدموا نتائج ما قاموا به من أبحاث. كما عليهم أيضا أن يردوا في ظرف ثمان وأربعين ساعة جميع الأشياء والأوراق والوثائق التي تكون قد عهد بها إليهم على ذمة إنجاز مهمتهم...ويجوز دائما لقاضي التحقيق أثناء إجراءاته أن يستعين بالخبراء إذا رأى لزوما لذلك."

الفرع الثاني: التفتيش والضبط في البيئة الإلكترونية

يعتبر التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر والغرض منه هو ضبط كل ما يفيد في كشف الحقيقة عن الجريمة التي يجري التحقيق أو جمع الاستدلالات بشأنها، ومعنى ضبطها هو ضعها تحت يد السلطة العامة للتحفظ عليها إلى حين انتهاء الإجراءات في الدعوى الجنائية[1].

ومنه سنتعرف في هذا الفرع على التفتيش في (الفقرة الأولى) والضبط في (الفقرة الثانية)

الفقرة الأولى: التفتيش

يختلف التفتيش في الجرائم المعلوماتية عن التفتيش المعروف في الجرائم التقليدية، ويرجع ذلك لعدة اعتبارات .

أولا: تعريف التفتيش

يجمع الفقه الجنائي على أن التفتيش هو إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في مكان يتمتع بحرمة، وذلك وفقا للضمانات والقيود القانونية المقررة[2]

والتفتيش هو "التنقيب في وعاء السر بقصد ضبط ما يفيد من معلومات في كشف الحقيقة، وهو كشف نقاب السرية عما تحويه نظم الحاسوب من خفايا ونوايا إجرامية، وبالتالي إزاحة ستار الكتمان عنها للاستفادة منها في معرفة الحقيقة"، وهذا المعنى لا يتقيد بالكيان المادي للحاسوب والأجهزة الملحقة به بل يشمل كذلك كيانه المنطقي من شبكات أو أنظمة و برمجيات[3] .

---

[1] فرج علواني هليل، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، دار المطبوعات الجامعية، مصر، 2006 ص 622

[2] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2013، ص 143 .

[3] علي حسن محمد الطوالبة، التفتيش الجنائي في نظم الحاسوب والإنترنت، دراسة مقارنة، عالم الكتب الحديثة، الأردن 2004، ص28 .

إذا فالتفتيش ليس غاية في حد ذاته، وا ٍنما وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تسهم في كشف الحقيقة[1].

ثانيا: شروط التفتيش للتفتيش شروط موضوعية وأخرى شكلية، سنعرضها على النحو التالي :

أ-الشروط الموضوعية للتفتيش:

ويمكن تقسيمها إلى شرطين أساسيين هما السبب والمحل .

1-سبب التفتيش في البيئة المعلوماتية: وهو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث [2]، ويتمثل في :

- ✓وقوع جريمة من الجرائم الإلكترونية بالفعل سواء كانت جناية أو جنحة.
- ✓اتهام شخص أو أشخاص معينين بارتكاب جريمة أو المشاركة فيها .
- ✓توافر أمارات قوية أو قرائن على وجود بيانات أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره[3] .

2-محل التفتيش في البيئة المعلوماتية: ويتمثل محل التفتيش في الجريمة المعلوماتية في المكونات المادية والمعنوية للحاسوب وكذا شبكات الاتصال الخاصة به، ويستوي أن يكون محل التفتيش بحوزة شخص معين أو موجود في مكان ما كالمسكن أو المكتب[4]

ب-الشروط الشكلية للتفتيش:

أن يتم تفتيش النظم المعلوماتية بأسلوب إلكتروني من قبل الأجهزة القائمة بالتحقيق.

---

[1]أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015 ص 140.

[2]نبيلة هبة هروال،الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 229.

[3]عبد العال الديربي و محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، مصر 2012، ص 305 .خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، المرجع السابق، ص 154.

[4]أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، المرجع السابق، ص 151.

يجب أن يكون الإذن بالتفتيش مسببا حتى تتمكن الجهة القضائية من مراقبة مدى مشروعيتة . كما ينبغي في نهاية التفتيش تحرير محضر للتفتيش يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أيلة، ويشترط أن يكون المحضر مكتوبا باللغة الرسمية .

ثالثا: مدى قابلية مكونات و شبكات الحاسب الآلي للتفتيش:

كما أن له شبكات saftware ومكونات منطقية hardware يتكون النظام المعلوماتي من مكونات مادية اتصالات بعدية سلكية ولاسلكية سواء على المستوى المحلي أو على المستوى الدولي[1] .

تفتيش المكونات المادية للحاسوب :بخصوص تفتيش المكونات المادية للحاسوب لا توجد صعوبة في ذلك، لأنه يرد على عناصر مادية لا خلاف للقانون فيها، فتطبق بشأنه القواعد التقليدية للتفتيش، لكن مع الأخذ بعين الاعتبار القواعد الخاصة بضبط هذه الأجهزة لحساسيتها وا إمكانية تعريضها للتلف، كما تطبق على إجراء التفتيش الضمانات المقررة قانونا[2] .

تفتيش المكونات المنطقية للحاسوب ولما كان التفتيش وسيلة للإثبات المادي، لا غاية في حد ذاته، فهو إجراء يسعى إلى ضبط الأدلة المادية المتعلقة بالجريمة لتقديمها إلى المحكمة كدليل إدانة، فإن التساؤل يثور حول إمكانية اعتبار تفتيش المكونات المنطقية للحاسب الآلي نوعا من التفتيش باعتبار أن البيانات الإلكترونية أو البرامج في حد ذاتها ليس لها مظهر مادي محسوس في المحيط الخارجي، وقد انقسم الفقه في هذا الشأن إلى اتجاهين:

- **الاتجاه الأول:** تتجسد فكرة هذا الرأي في عدم إمكانية انسجام وتطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية. إذ أن التفتيش يقتصر مفهومه على أشياء ذات حيز مادي ملموس.

[1] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص 88.

[2] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و17 نوفمبر، 2015، كلية الحقوق، بسكرة، الجزائر، ص 3

- **الاتجاه الثاني:** يرى أنصار هذا الاتجاه أن برامج الحاسوب يمكن أن تطبق عليها خصائص وسمات المادة، وهو ما يجعلها تدخل في نطاق الأشياء المادية ويستوي في ذلك أن تكون برامجا أو تطبيقات حاسوبية، مستندين في ذلك إلى أن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ويمكن قياسه بمقياس معين مثل البايت (byte) و الميغابايت[1] MB .

وبخصوص موقف المشرع الجزائري فهو يتضح جليا من خلال القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حينما أجاز صراحة بموجب نص المادة 5 منه تفتيش المنظومات المعلوماتية [2].

إذا فالمشرع الجزائري قد حسم بذلك الجدل القائم حول مدى قابلية النظام المعلوماتي للتفتيش فيه.

الفقرة الثانية: ضبط الدليل الإلكتروني

إن الأدلة الرقمية المضبوطة أثناء عملية التفتيش لها أهمية كبيرة في إثبات الواقعة الجرمية ونسبتها لمرتكبها من عدمها و بالتالي الحكم عليه بالإدانة أو البراءة.

أولا: مفهوم ضبط الأدلة

سنتناول في هذا العصر تعريف ضبط الدليل وأنواع الأدلة القابلة للضبط .

أ-تعريف ضبط الأدلة

يعتبر ضبط الأشياء أثرا من آثار المعاينة والتفتيش باعتبارهما يؤديان إلى جمع الأدلة المادية وأدوات ارتكاب الجرائم، وبيان مدلولاتها من أجل الاستفادة منها في إثبات الوقائع الجنائية ونسبتها إلى مرتكبه، فضبط الأدلة إذا لا يخرج عن كونه وضع اليد على شئ يتصل بجريمة

[1] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 146.

[2] طبقا للمادة 5 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، الدخول بغرض التفتيش إلى منظمة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وقد يرد الضبط على منقولا أو عقارا ويستوي أن يكون الشئ المضبوط مملوكا للمتهم أو لغيره[1]

ب-الأدلة القابلة للضبط

توجد العديد من أدلة الإثبات القابلة للضبط في مجال الجرائم المعلوماتية، ومن أهم هذه الأكلة نذكر ما يلي :

- المخرجات الورقية والمستندات التي تفيد الكشف عن الجريمة .
- أجهزة الحاسوب الآلي وملحقاتها مثل وحدات المعالجة المركزية أجهزة لوحة المفاتيح وغيرها . الأقراص المرنة والشرائط الممغنطة والتي قد تحتوي معلومات تفيد في مجريات التحقيق .
- أجهزة المودم وهي الوسائل التي تمكن الحواسيب من الاتصال ببعضها .
- مختلف برامج الحاسوب حيث تعتبر الأدوات الرئيسية التي يستعملها الجاني في تنفيذ جرائمه
- البطائق الممغنطة وبطائق الائتمان والمواد المستعملة في إعدادها حيث تعتبر من قرائن الإثبات.

ثانيا: مدى قابلية جرائم الحاسوب لضبط أدلتها :

ونفرق في ذلك بين حالتين:

أ- ضبط الأدلة المادية للجريمة :لا يثار أي إشكال بشأن ضبط الأدلة المادية التي تفيد في كشف الحقيقية سواء كانت أجهزة حاسوب أو ملحقاته أو غيرها من الأشياء المنقولة، حيث أنه يمكن تحريزها، أما العقارات التي تحتوي على أجهزة الحاسوب وشبكاته فيتم التحفظ على ما تشتمل عليه من آثار الجريمة المعلوماتية أو أشياء يتعذر نقلها، عن طريق وضع الأختام على هذه الأماكن وتعيين السلطة المختصة حارسا عليها[2]

[1]عبد العال الدريبي، محمد صادق إسماعيل، الجرائم الإلكترونية، المرجع السابق، ص320

[2]علي حسن محمد طوالبة، روعية الدليل الإلكتروني المستمد من التفتيش الجنائي " دراسة مقارنة"، المرجع السابق، ص142

ب -ضبط المكونات المنطقية للحاسوب:

لقد سمح المشرع الجزائري للمحقق بحجز معطيات الحاسب الآلي، مع إمكانية نسخها إذا لم يكن هنالك داعي لحجز المنظومة المعلوماتية برمتها، بالإضافة إلى ذلك منحه سلطة استعمال الوسائل التقنية التشكيل أو إعادة تشكيل هذه المعطيات ثم حجزها ووضع الأختام عليها، طبقا لقانون الإجراءات الجزائية وفي حالة تعذر حجز هذه الأدلة لأسباب تقنية يتعين على السلطات المختصة بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات ومنع الإطلاع عليها، وذلك بتكليف أشخاص مؤهلين في هذا المجال[1] وهو الأمر الذي تناوله المشرع بالنص في المادة 6 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفرع الثالث: الشهادة الإلكترونية

في هذا الفرع سنعرف الشهادة بمختلف جوانبها في (الفقرة الأولى)، ثم نحدد مختلف فئات الشاهد المعلوماتي (الفقرة الثانية)، وفي الأخير نتطرق إلى التزام الشاهد المعلوماتي في (الفقرة الثالثة).

الفقرة الأولى: تعريف الشهادة

لم يتطرق المشرع الجزائري إلى تعريف الشهادة وترك ذلك للفقه والاجتهاد القضائي لكنه بالمقابل قام بتنظيمها وتحديد مجالها وشروط قبولها وحجيتها في الإثبات[2].

تعتبر الشهادة إجراء من إجراءات التحقيق، وهي الأقوال التي يدلي بها عبر الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء تعلقت تلك الأقوال بثبوت الجريمة وظروف ارتكابها

---

[1] أمال حابت، الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري، ورقة بحثية مقدمة الأعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر، ص17ء

[2] القسم الر ابع من الفصل الأول من الباب الثالث تحت عنوان: سماع الشهود، المواد 88،99 من قانون الإجراءات الجزائية الجزائري، والتي تتلخص حول استدعاء الشهود وحضورهم وكيفية تلقي إفاداتهم وحلف اليمين والحالات التي لا يجوز فيها سماع الشخص كشاهد ونصاب الشهادة...الخ. .

وا إسنادها إلى المتهم أو براعته منها[1]، ويختلف الشاهد في مجال الجرائم المعلوماتية عن الشاهد في سائر الجرائم.

أولا: الشاهد في الجرائم التقليدية:

"وهو كل شخص تاهت إلى علمه عن طريق حواسه معلومات عن واقعة إجرامية، وعليه الإدلاء للسلطات القضائية بكل ما يفيد في كشف الحقيقة عنها.

ثانيا: الشاهد في الجرائم المعلوماتية:

"وهو ذلك الفني صاحب الخبرة والتخصص في تقنية الحاسب وشبكات الاتصال والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذا النوع من الشهود مصطلح "الشاهد المعلوماتي وذلك تمييزا له عن الشاهد التقليدي[2]

الفقرة الثانية: فئات الشاهد المعلوماتي

يمكن القول أن الشهود في الجرائم المعلوماتية ينحصرون ضمن إحدى الطوائف التالية:

أ- **مشغل الحاسب الآلي:** وهو كل شخص مسؤول عن تشغيل الحاسوب والمعدات المتصلة به ولابد أن تكون لديه خبرة كبيرة وواسعة في هذا الميدان.

ب- **بالمبرمجون:** وهم الأشخاص المتخصصون في كتابة أوامر البرامج، وهم فئتين الأولى هم مخططوا برامج التطبيقات والثانية هم مخططوا برامج النظم[3].

ت- **المحللون:** فالمحلل هو ذلك الشخص الذي يقوم بتجميع البيانات الخاصة بنظام معين، ثم تقسيمها على وحدات منفصلة بغية استنتاج العلاقة الوظيفية بينها .

[1] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 461

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 263

[3] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، مرجع سابق، ص ص 612 - 613

ث- مهندسوا الصيانة والاتصالات: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

ج- مديروا النظم: الذين توكل لهم أعمال الغدارة في النظم المعلوماتية[1].

الفقرة الثالثة: التزام الشاهد الإلكتروني (المعلوماتي)

يتعين على الشاهد في حال حصوله على معلومات تفيد بارتكاب جريمة أن يعلم بها السلطات يدفعنا لتحديد المختصة على سبيل الإلزام، وهو ما يعبر عنه بالالتزام بالإعلام في الجريمة المعلوماتية، مما السمات الجوهرية لهذا الالتزام وشروطه، ولكن قبل التعرض لذلك سنحاول البحث في مدى إمكانية إجبار الشاهد على تقديم معلومات تتعلق بالجريمة[2] .

أولا: مدى التزام الشاهد بتقديم إفادته

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله لكن بالمقابل يثار التساؤل: هل أن الشاهد المعلوماتي ملزم بطبع ملفات البيانات المخزنة في ذاكرة الحاسب؟ أو هل يجوز له الإفصاح عن كلمات المرور السرية والشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج؟. في هذا الصدد برز هناك اتجاهان نتطرق إليهما كما يأتي:

أ- الاتجاه الأول: يرى القائلين بهذا الرأي أنه ليس من واجب الشاهد المعلوماتي أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة، ويميل إلى هذا الاتجاه الفقه الجنائي الألماني، على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب[3] .

[1] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص63.

[2] رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16، 7انوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر، 2015، ص 5

[3] على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 64،

ب- **الاتجاه الثاني:** على عكس الأول يرى أنصار الاتجاه الثاني، أن من بين الالتزامات التي يتحملها الشاهد القيام بطباعة ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة [1]، وقد أخذ المشرع الجزائري على غرار المشرع الفرنسي بهذا الاتجاه حيث ألزم كل شخص الله إطلاع ودراية بعمل المنظومات المعلوماتية، بمساعدة السلطات المختلفة وتزويدها بكافة المعلومات الضرورية لإنجاح مهامها[2].

ثانيا: التزام الشاهد بالإعلان في الجريمة المعلوماتية

ويعني ذلك باختصار أنه في الجرائم المعلوماتية ومتى كان الشاهد حائز المعلومات جوهرية لازمة الاختراق نظام المعالجة الآلية للبيانات بحثا عن أدلة للجريمة داخلها، فإنه يكون مطالبا بإعلام سلطات التحري والتحقيق على سبيل الإلزام ولا تعرض للعقوبات المقررة للامتناع عن الشهادة[3].

ثالثا: خصائص التزام الشاهد المعلوماتي:

مما سبق ذكره يتبين لنا أن هذا الالتزام له مجموعة من السمات الجوهرية هي:

- التزام الشاهد بالإعلام التزام قانوني.
- الالتزام بالإعلام التزام مستقل له ذاتيته الخاصة.
- يعتبر الالتزام بالإعلام التزام وقائى[4].

---

[1] رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، المرجع السابق، ص 06.

[2] أنظر: الفقرة 4 من المادة 5 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

[3] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية، المرجع السابق، ص ص 613 - 614 .

[4] رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، المرجع نفسه، ص 10.

رابعا: شروط التزام الشاهد المعلوماتي بالإعلام:

تتمثل هذه الشروط في ما يلي:

- ✓ وقوع جريمة معلوماتية بالفعل.
- ✓ علم الشاهد ومعرفته بالمعلومات المتعلقة بالجريمة
- ✓ أن تقتضي مصلحة التحقيق الحصول على معلومات من قبل الشاهد[1].

المطلب الثاني: الإجراءات الحديثة لجمع الدليل الإلكتروني

تطرقنا في المطلب السابق على الإجراءات التقليدية لجمع الدليل الإلكتروني وبالرجوع إلى الأنظمة القانونية الإجرائية الحالية، يلاحظ أن هناك قصورا بخصوص أساليب التحري التقليدية في استخلاص الدليل الإلكتروني. فالمشرع أجاز استخلاص الدليل عموما وفق ضوابط إجرائية معينة منها: الانتقال والمعاينة، الخبرة ، التفتيش وضبط الأدلة الشهادة... الخ، كما أن هذه الإجراءات تخص استخلاص الدليل من الجرائم سواء كانت تقليدية أم مستحدثة، والأكيد أن هذه الإجراءات غير كافية لاستيعاب كافة أشكال الجريمة الالكترونية، فهي تحتاج من المشرع تعديلها أو استحداث أخرى جديدة لمواكبة التطورات التقنية المتلاحقة في مجال مكافحة الجريمة الالكترونية، وهذا ما قام به المشرع الجزائري من خلال التعديلات المتتالية لأحكام قانون الإجراءات الجزائية، وذلك بإدراج قواعد إجرائية جزائية جديدة وفي الوقت نفسه أحاطها بجملة من الضمانات بهدف عدم المساس بحرمة الحياة الخاصة للأفراد[2]

وعليه ارتأينا تقسيم هذا المطلب إلى فرعين، نتناول الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب المادة (65 مكرر 5 إلى 65 مكرر 18 في (الفرع الأول) ثم نتطرق بعدها إلى الإجراءات الحديثة الجمع الدليل الإلكتروني بموجب القانون 09-04 في (الفرع الثاني).

[1] رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، المرجع السابق، ص ص 10- 11.

[2] يزيد بوحليط، أساليب التحري الخاصة في قانون الإجراءات الجزائية، المرجع السابق، ص 248.

الفرع الأول: الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب المادة (65 مكرر 5 إلى 65 مكرر 18) من قانون الإجراءات الجزائية.

قام المشرع الجزائري باستحداث أساليب جديدة في التحري ولو اعتبرها البعض بأنها تمس بالحياة الخاصة للأفراد وانتهاكا لحق كفله الدستور ولأن الضرورات تبيح المحظورات والمصلحة المحمية أولى جعل المشرع من اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب أهم الأساليب المستخدمة للكشف عن الجرائم الإلكترونية

ونظرا لأهمية هذه الوسائل ولما تشكله من مساس بحرية الأفراد وانتهاك لخصوصياتهم، ارتأينا إلى تقسيم هذا الفرع إلى ثلاث فقرات، تطرقنا إلى المقصود باعتراض المراسلات والتقاط الصور وتسجيل الأصوات في (الفقرة الأولى)، في حين تناولنا الضوابط التي تحكم اعتراض المراسلات والتقاط الصور وتسجيل الأصوات في (الفقرة الثانية)، وفي الأخير تطرقنا إلى التسرب في (الفقرة الثالثة).

الفقرة الأولى: المقصود باعتراض المراسلات والتقاط الصور وتسجيل الأصوات من خلال هذه الفقرة، سنتناول مفهوم مفصل لكل إجراء على حدة.

أولا: مفهوم اعتراض المراسلات:

يقصد باعتراض المراسلات على أنه إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث وتتم بواسطة الوسائل السلكية واللاسلكية[1].

من جانب آخر نجد المشرع الجزائري لم يعرف بإجراء اعتراض المراسلات، بل اكتفي بوضع بتنظيم لهذه العملية بموجب المادة (65 مكرر 5) من قانون الإجراءات الجزائية التي تنص على: "إذا اقتضت ضروريات التحري في الجريمة الملتبس بها أو التحقيق الابتدائي في

[1] سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماستر أكاديمي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، 2014، ص32

جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو بسرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص....
- باعتبار المشرع الجزائري لم يتطرق تحديد مفهوم اعتراض المراسلات فهل يقصد بها التنصت الهاتفي أم مجرد الاطلاع عليها؟ أو يمتد إلى أكثر من ذلك من خلال ضبط كل ما له علاقة بوسائل المواصلات السلكية واللاسلكية؟

باستقراء نصوص المواد (100-107) من قانون الإجراءات الجزائية الفرنسي[1] يتبين أن اعتراض المراسلات تتعلق بتلقي مراسلة مهما كان نوعها بغض النظر عن وسيلة إرسالها وتلقيها سلكية أو غير سلكية أو ورقية[2]كما عرفت لجنة الخبراء للبرلمان الأوروبي Support يتم تثبيتها وتسجيلها على دعامة إلكترونية المنعقدة بستراسبورغ بتاريخ 06-10-2006، حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية اعتراض المراسلات على أنها: "عملية مراقبة

[1] Article 100 du (cppf): “En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou superieur à deux ans d’emprisonnement, le juge d’instruction peut lorsque les necessités de l’information l’exigent, pre scrire l’interception l’enregistrement et la transcription de corespondance émises par la voix des télécommunications.
Ces operations sont éffectuées sous son autorité et son controle. La decision d’’interception est ecrite. Elle n’a pas de caractère juridictionnel et n’est susceptible d’’aucun recours.”

[2] عبد المجيد حجازي، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012، ص62

سرية المراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو مشاركتهم في ارتكاب الجريمة"[1].

ثانيا: مفهوم تسجيل الأصوات

يعرف التسجيل الصوتي بأنه: "النقل المباشر والألي للموجات الصوتية من مصادره بنبراتها ومميزاتها الفردية وخواصها الذاتية، بما تحمل من عيوب في النطق إلى شريط التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطسي بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه به[2].

كما تتم هذه العملية باستخدام وسائل تقنية خاصة لها صلة مباشرة بنوعيها السلكية واللاسلكية، والتي من خلالها يتم بث الكلام المتفوه وتثبيته واستغلاله في التحريات، وهو إجراء تحقيقي تأمره به السلطة القضائية خلسة وينتهك سرية الأحاديث الخاصة بغية الحصول على دليل غير مادي للجريمة[3].

إلا أن المشرع الجزائري لم ينص في قانون الإجراءات الجزائية على تعريف التسجيل الصوتي مثل ما لم ينص على تعريف اعتراض المراسلات كما رأينا سابقا، إنما أشار لها في نص المادة (65) مكرر في الفقرة المعنيين من أجل التقاط وتثبيت وبث تسجيل الكلام المتفوه به بصفة "وضع الترتيبات التقنية دون موافقة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية[4].

---

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2012، ص 442.

[2] سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، المرجع السابق، ص34.

[3] حافظ بن زلاط، التنصت الهاتفي في ظل قانون الإجراءات الجزائية، بحث متوفر على الموقع الرسمي لمجلة (القانون الأعمال) لسنة 2015 على الرابط الآتي/http://www.droitentreprise.org/web بتاريخ 10/04/2018، على الساعة 22.00 سا

[4] عباسي خولة، الوسائل الحديثة للإثبات الجنائي في القانون الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية حقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، 2013، ص 22.

وعليه فإن التسجيلات التي يقوم بها الأفراد فيما بينهم لا تعد من قبيل الإجراءات الجنائية نظرا لأنها لم تصدر في شأن دعوى جنائية حركتها السلطات القضائية قصد الوصول إلى الحقيقة، كما لا تعتبر أدلة، واستغلال التسجيل الذي لا يتضمن اعتداء على حق من تم تسجيل صوته أو حديثه، كما هو الشأن في حالة تسجيل الأحاديث الإذاعية أو التلفزيونية أو الصحفية.

ثالثا: مفهوم التقاط الصور:

تعتبر عملية التقاط الصور الفوتوغرافية من الإجراءات الجديدة التي جاء بها المشرع الجزائري لمكافحة الجرائم المستحدثة ومنها الجرائم الإلكترونية، غير أنه ومثل الإجراءات السابقة لم يتطرق إلى تعريف هذاالإجراء، وا ٍنما نص على مجال تطبيقه وتوضيح إجراءات القيام بذلك، يقوم هذا الإجراء أساسا على استخدام الكاميرات، أو أجهزة خاصة لالتقاط صورة للمشتبه فيه على الحالة التي كان عليها وقت التصوير بغرض استخدام هذه الصورة كدليل مادي، على اعتبار أن عدسة الكاميرا أصبحت من الأساليب العالمية والمطلوبة الإثبات الحالة بما تنقله من صور حية لحادثة معينة[1].

لقد شاع اليوم استخدام كاميرات رقمية بغرض المراقبة في الأماكن العامة والخاصة كالبنوك والمطارات وماكينات الصرف الآلي والمحلات والمستشفيات..إلخ قصد ضبط الجرائم وا ٍثباتها[2] ويكون الاطلاع على صور هذه الكاميرات في حالات وقوع الجرائم بأمر من المحكمة، ولاشك أن ذلك يثير قضايا تتعلق بالخصوصية الشخصية. لذا يرى جانب من الفقه أن تركيب هذه الكاميرات يكون في الأماكن العامة فقط و بترخيص قانوني[3].

وعليه يربط هذا الإجراء الشخص أو الأشخاص في مكان واحد وفي وقت واحد، خاصة في ظل التطور التكنولوجي الإلكتروني الذي يسمح بالتصوير ليلا وبجودة عالية من خلال الكاميرا ذات

---

[1] فوزيعمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط صور والتسرب كالإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة قسنطينة 1، الجزائر، العدد 33، جوان 2010

[2] سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، المرجع السابق، ص 39.

[3] عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص 782.

العدسات فائقة التكبير والتي تستخدم أيضا الأشعة تحت الحمراء بما يمكن ضابط الشرطة القضائية من التقاط الصور الثابتة أو المتحركة للمشتبه فيه خلال جميع مراحل البحث والتحري[1]"

الفقرة الثانية: الضوابط التي تحكم اعتراض المراسلات والتقاط الصور وتسجيل الأصوات

حدد المشرع الجزائري من خلال قانون الإجراءات الجزائية شروط للقيام بهذا الإجراءات كونها تشكل انتهاكا لحرمة الحياة الخاصة للأفراد، واعتداء على سرية مراسلاتهم واتصالاتهم.

أولا: الشروط الشكلية: تتعلق بالضوابط الشكلية بإجرائيين هما:

أ- الحصول على إذن من طرف وكيل الجمهورية:

لابد من ضابط الشرطة القضائية الذي يباشر هذا الإجراء في عملية التحري والبحث، أن يكون مستندا في ذلك على إذن من وكيل الجمهورية يخوله اللجوء إلى إجراء التقاط الصور واعتراض المراسلات وتسجيل الأصوات، وكذلك يمكن لضابط الشرطة القضائية أن يحصل على الإذن من طرف قاضي التحقيق المختص إذا كانت القضية معروضة عليه[2] ، وفي حالة قيام ضابط الشرطة القضائية بممارسة الإجراء دون إذن، فإن إجراءه الذي قام به يقع تحت طائلة البطلان.

ويشترط في الإذن أن يكون مكتوبا، ويتضمن عمل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط أو بث أو تسجيل أحاديثهم وكذا الأماكن المقصودة سواء كانت عامة أو خاصة وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، يسلم الإذن مكتوبا لمدة أقصاها 4 أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق.[3]

---

[1] نصر شومان، التكولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة للكتاب، طرابلس ليفان، طا، 2011، ص154.

[2] أنظر: المادة 65 مكرر 5 من القانون رقم 06-22 المؤرخ في 20-12-2006، المعدل والمتمم القانون الإجراءات الجزائية، الصادر بالجريدة الرسمية للجمهورية الجزائرية، عدد 84، المؤرخة في 24 ديسمبر 2006.

[3] أنظر: المادة 65 مكرر 5 من القانون رقم: 06-22، المعدل والمتمم لقانون الإجراءات الجزائية.

ب- بتحرير محضر عن العملية باعتبار محاضر الشرطة القضائية لها حجية في الإثبات، وجب على ضابط الشرطة القضائية الذي قام بإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات أن يقوم بتحرير محضر موقع عليه من طرفه، يسرد فيه بالتفصيل العمليات التي قام بها[1].

أما مضمون المراسلات المسجلة والصور الملتقطة، فيقوم ضابط الشرطة بنسخ محتواها في محضر يودع بملف الإجراءات، أما إذا كانت تلك المراسلات أو الاتصالات بلغة أجنبية فيتم تسخير مترجم لترجمتها[2] .

تتم عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65) مكرر 8[3].

ثانيا: الضوابط الموضوعية:

تتعلق هذه الضوابط بنشوء الحق في اللجوء إلى اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، وتتمثل هذه الضوابط في:

-أن يكون الإجراء من أجل التحري والكشف عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

-غاية المراقبة وضرورتها، عبر المشرع الجزائري عن المصطلح بلفظة: "إذا اقتضت ضرورة التحري في الجريمة الملتبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة

[1] أنظر: المادة 65 مكرر 9 من القانون رقم: 06-22 المعدل والمتمم لقانون الإجراءات الجزائية.

[2] أنظر: المادة 65 مكرر 10 من القانون رقم: 06-22 المعدل والمتمم لقانون الإجراءات الجزائية.

[3] حيث تنص المادة 65 مكرر 8 من قانون الإجراءات الجزائية على: يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينبيه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالعمليات المذكورة في المادة 65 مكرر 5 أعلاه."

العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد..."، وهذا حسب المادة 65 مكرر 05من قانون الإجراءات الجزائية الجزائري.

يتضح من خلال نص هذه المادة أن اللجوء لهذا الإجراء لا يتم إلا في حالة الضرورة التي تفرض استعمال تلك الوسائل الكشف الجريمة دون غيرها من الوسائل التقليدية.

ح -الجهة المكلفة بهذه العملية:

باعتبارها تمس بحرمة الحياة الخاصة، لا يقوم بها إلا ضابط الشرطة القضائية.

ثالثا: ضوابط التنفيذ:

تتعلق بكيفيات المراقبة ونتائجها والأدلة الناجمة عنها، لذا سمح المشرع من خلال نص المادة (65 مكرر 5)الفقرة 4، لضابط الشرطة القضائية الدخول إلى المكان المعني دون احترام الشروط الواردة في المادة 47 من قانون الإجراءات الجزائية وذلك باستخدام الترتيبات التقنية، حيث نصت الفقرة الثانية من المادة (65 مكرر 05) على أن النيابة العامة يمكنها منح الإذن لضابط الشرطة القضائية لوضع الترتيبات التقنية، التي يتم عن طريقها التصنت على المحادثات وتسجيلها والتقاط الصور دون الحاجة إلى موافقة المشتبه فيه[1] .

وتكمن تلك الترتيبات في وضع أجهزة التصنت وتسجيل الكلام الذي يتفوه به المشتبه فيه خاصة فيما يتعلق بموضوع الجريمة، إضافة إلى زرع وسائط التقاط الصور والغرض دائما من كل ذلك هو الحصول على أدلة تدين الأشخاص الذين يشتبه فيهم القيام بالجريمة.

وفي حالة اكتشاف جرائم أخرى غير تلك التي يتم التحقيق فيها والواردة في الإذن فيمكن التحري بشأنها ولا يكون ذلك سببا في بطلان الإجراءات وهذا حسب أحكام المادة (65 مكرر6)من قانون الإجراءات الجزائية الجزائري

[1]أنظر: المادة 65 مكرر 5من قانون الإجراءات الجزائية الجزائري.

الفقرة الثالثة: التسرب

استحدث المشرع الجزائري إجراء التسرب بموجب المادة (65 مكرر11) من قانون الإجراءات الجزائية الجزائري التي تنص على: "عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر 5) أعلاه، يجوز لوكيل الجمهورية أو القاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابة حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبنية في المواد أدناه.

وبخلاف إجراءات التحري السابقة الذكر التي لم يعرفها المشرع الجزائري، أورد تعريف التسرب بموجب نص المادة (65 مكرر 12)من قانون الإجراءات الجزائية الجزائري التي تنص على: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف، يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة (65 مكرر 14)أدناه، ولا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم". كما حدد المشرع نطاق تطبيق التسرب بموجب المادة(65 مكرر 5)سالفة الذكر والتي من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

يلاحظ من خلال التعريف السابق أن التسرب عملية تتسم بالتعقيد، فهو من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية، وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على أنه فاعل أو الشريك[1]، والتسرب كغيره من الإجراءات الحديثة، له ضوابط وشروط شكلية وأخرى موضوعية حتى يعتد به

[1]سارة قادري،أساليب التحري الخاصة في قانون الإجراءات الجزائية، المرجع السابق،ص42

أولا: الضوابط الشكلية: تتعلق بما يلي:

أ- تحرير التقرير:

يلزم ضابط الشرطة القضائية المكلف بعملية التنسيق بتحرير تقرير كتابي يتضمن بيان مفصل عن جميع العناصر المتعلقة بالعملية [1] ويجب أن يذكر في التقرير ووفق الترتيب الزمني جميع المعلومات ذات الصلة كالأفعال التي استدعت حدوث عملية التسرب، وكذا تحديد هوية العناصر المشتبه تورطهم في الجريمة (أسمائهم و ألقابهم)، تحديد الكيفيات التي تم بها مخادعة الجناة، فيجب ذكر جميع العمليات منذ بداية التسرب حتى نهايته.

ب-الحصول على إذن بالتسرب:

تنص المادة (65) مكرر11 من (ق.إ. ج) على: "عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65) مكرر 5 أعلاه، يجوز لوكيل الجمهورية أو القاضي التحقيق، بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة مباشرة عملية التسرب ضمن الشروط المبينة أدناه"، وعليه فالجهة القضائية المختصة بإصدار الإذن هو وكيل الجمهورية أو قاضي التحقيق، ومنه لا يجوز لضابط أو أعوان الشرطة القضائية القيام به حماية للحقوق المكرسة دستوريا.

كما يجب أن يكون الإذن مكتوبا، وهذا وفق نص المادة (65 مكرر 15) التي تنص على: "يجب أن يكون الإذن المسلم تطبيقا للمادة (65 مكرر 11) أعلاه، مكتوبا ... وذلك تحت طائلة البطلان" ذلك أن الأصل في العمل الإجرائي هو الكتابة وفقا لنص المادتين (138-139) من (ق.إ. ج) [2]، كما يشترط ذكر اسم الضابط المشرف، وهو ما نصت عليه

[1] أنظر المادة (65 مكرر 13)من قانون الإجراءات الجزائية الجزائري.

[2] حيث تنص المادة (138) من (ق... ج) على: يجوز لقاضي التحقيق أن يكلف بطريق الإثابة القضائية أي قاض من قضاة محكمته أو أي ضابط من ضباط الشرطة القضائية المختصة بالعمل في تلك الدائرة أو أي قاض من قضاة التحقيق بالقيام بما يراه لازما من إجراءات التحقيق في الأماكن الخاضعة للجهة القضائية التي يتبعها كل منهم، ويذكر في الإنابة القضائية نوع من الجريمة موضوع المتابعة وتؤرخ وتوقع من القاضي الذي أصدرها وتمهر بختمه..

المادة (65 مكرر 15) بقولها: "يجب أن يكون الإذن المسلم تطبيقا للمادة(65 مكرر11)أعلاه، مكتوبا ...وذلك تحت طائلة البطلان، تذكر في الإذن الجريمة التي تبرر اللجوء لهذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته...".

ج- مدة التسرب: حددتها المادة (65 مكرر 15/3) حيث تنص على:"... ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر..."، غير أنه ومراعاة لمقتضيات التحقيق الابتدائي يمكن تجديد هذه المدة ضمن نفس الشروط الشكلية والزمنية السابقة، وحفاظا على حياة العون المتسرب من الخطر إضافة إلى الأشخاص المسخرين، أجازا المشرع للقاضي الذي رخص بعملية التسرب أن يأمر في أي وقت بوقفها قبل انقضاء مدتها، وذلك إذا وصل إلى علمه أن معلومات تفيد باحتمال كشف العملية من طرف المجموعة الإجرامية.

د- إبقاء الإذن بالتسرب خارج ملف الإجراءات إلى غاية الانتهاء من العملية

وذلك للحفاظ على السرية المطلوبة لنجاح عملية التي التسرب والتي حصرها المشرع بين القاضي الأمر بها (وكيل الجمهورية أو قاضي التحقيق)، وضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرب.

بعد الانتهاء من عملية التسرب، يجب إيداع رخصة التسرب في ملف الإجراءات وهذا وفقا لنص المادة (65 مكرر 15/6) التي تنص على:"... تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب".

ثانيا: الضوابط الموضوعية:

تتمثل الضوابط الموضوعية لعملية التسرب في شرطين رئيسيين هما:

أ- التسبيب:

يعتبر التسبيب أساس العمل القضائي، وعليه يجب على وكيل الجمهورية أو قاضي التحقيق عند إصدار الإذن بالتسرب توضيح الأدلة القانونية والموضوعية بعد تقدير جميع

العناصر المعروضة عليه من طرف ضابط الشرطة القضائية[1]، وهذا طبقا لنص المادة (65 مكرر15/1) التي تنص على: يجب أن يكون الإذن المسلم تطبيقا للمادة (65 مكرر11) أعلاه مكتوبا ومسيبا وذلك تحت طائلة البطلان....

ب- **نوع الجريمة:**

وقد حصرتها المادة (65 مكرر 5) من (ق.إ.ج) في سبعة أنواع هي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، وجرائم الفساد[2].

وعليه يجب أن تكون الجريمة جناية أو جنحة.

المطلب الثالث : الإجراءات الحديثة بموجب القانون 09-04

تطرقنا سابقا إلى بعض الإجراءات التقليدية المتعلقة بجمع الدليل الإلكتروني وخلصنا إلى عدم كفايتها الاستيعاب كافة أشكال هذا النوع المستحدث من الجرائم، مما دفع بالمشرع الجزائري إلى استحداث أساليب بحث وتحري جديدة تتلائم وخطورة هذه الجرائم، ونظرا للطبيعة الخاصة للجرائم الإلكترونية، لم يكتف المشرع باستخدام هذه الأساليب حينما تقع الجريمة، ولكن أيضا قبل وقوعها. وعليه صدر القانون رقم: 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي جاء لتكريس إطار قانوني أكثر ملائمة وانسجاما مع خصوصية وخطورة الجريمة الإلكترونية.

نص هذا القانون على جملة من الإجراءات الهامة، وعليه سنتناول مراقبة الاتصالات الإلكترونية وحالات اللجوء إليها في (الفقرة الأولى)، ثم نتطرق إلى تفتيش المنظومة المعلوماتية في (الفقرة الثانية) ثم حجز المعطيات في (الفقرة الثالثة).

---

[1] سيدهم سيدي محمد، محاضرة حول التسرب حسب تعديل قانون الإجراءات الجزائية، محكمة فرندة، مجلس القضاء تيارت، في 03/20/ 2008، ص 03 .

[2] أحسن بوسقيعة، التحقيق القضائي، دار هومة، ط2، الجزائر ، 2009، ص 114.

الفقرة الأولى: مراقبة الاتصالات الإلكترونية وحالات اللجوء إليها

سنحاول التطرق من خلال هذه الفقرة إلى تعريف مراقبة الاتصالات الإلكترونية وحالات اللجوء إليها وشروطها.

أولا: المقصود بمراقبة الاتصالات الإلكترونية.

لم يتطرق المشرع الجزائري شأنه شأن أغلب التشريعات المقارنة إلى تعريف مراقبة الاتصالات الإلكترونية، لكنه بالمقابل أوضح لنا مفهوم الاتصالات الإلكترونية بموجب المادة 2 من القانون رقم: 09-04 [1] والتي تنص على: يقصد في مفهوم هذا القانون ما يأتي...:

- الاتصالات الإلكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية، وبذلك وسع المشرع الجزائري من مفهوم الاتصالات الإلكترونية والتي تتم بأي وسيلة إلكترونية حديثة كجهاز الفاكس والهاتف النقال...الخ" .

بالرجوع إلى المفهوم الفقهي لمراقبة الاتصالات الإلكترونية الذي يعني: العمل الذي يقوم به المراقب باستخدام الاتصالات الإلكترونية لجمع معطيات عن المشتبه فيه سواء أكان الخاضع للمراقبة شخصا أو مكانا، أو شيئا ومثال ذلك مراقبة أحد الأشخاص ممن قام باختراق الحاسب الآلي الخاص بالمجني عليه أو القيام بإعداد بريد إلكتروني مستنسخ في مراقبة المشتبه فيه عند إرساله أو استقبال لصور دعارة للأطفال عبرالانترنت، وإفراغ ما تسفر عنه المراقبة الإلكترونية في تقارير أمنه"[2]. أو هي "مراقبة شبكة الاتصالات" [3]

ثانيا: حالات اللجوء للمراقبة الإلكترونية.

مما لا شك فيه أن مراقبة الأحاديث والاتصالات الخاصة والتي تتم بالوسائل الإلكترونية، تمس بحق الإنسان في الخصوصية المكفول دستوريا في مختلف التشريعات الحديثة، وعليه لم يترك المشرع الجزائري الأمر على إطلاقه استجابة للمواثيق الدولية وحماية لحقوق الإنسان في

[1] يزيد بوحليط، أساليب التحري الخاصة في قانون الإجراءات الجزائية، المرجع السابق، ص ص303-304

[2] تاير نبيل عمر، مرجع سابق، ص 149، راجع أيضا: عفيفي كامل عفيفي، مرجع سابق، ص ص 474 475

[3] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، المرجع السابق، ص 183.

هذا المجال، حيث نصت المادة (04) من القانون 09-04 سالف الذكر على الحالات التي يجوز فيها مراقبة الاتصالات الالكترونية حيث تنص على: يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 من القانون 09-04 في الحالات الآتية:

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

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

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

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية. لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة المختصة.

ثالثا: شروط مراقبة الاتصالات الالكترونية

كما رأينا سلفا، وحفاظا على الحق في سرية المراسلات بكافة أنواعها والمكفولة دستوريا، أحاط المشرع الجزائري إجراء المراقبة الالكترونية تحت طائلة البطلان بشروط قانونيا، تتمثل في النقاط الآتية:

أ- وجود إذن قضائي: أوجب المشرع الجزائري وجود الإذن القضائي الصادر عن السلطة القضائية المختصة وذلك بموجب المادة (04/05) من القانون 09-04 سالف الذكر التي تنص على:"...لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية، عندما يتعلق الأمر بالحالات المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه إننا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها"[1].

[1]تجيز بعض التشريعات الوطنية كالقانون الأمريكي وضع أجهزة التسجيل الاتصالات الالكترونية في حالة الضرورة دون إذن من النيابة العامة، إذا توفر خطر على الحياة أو خطر جسيم على السلامة الجسمية، خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص 351.

بوجود ضرورة: يتم اللجوء إلى إجراء مراقبة الاتصالات الالكترونية في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو المقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية

الفقرة الثانية: تفتيش المنظومة المعلوماتية.

عرفت المادة (02/2) من القانون رقم: 09-04 سالف الذكر المنظومة المعلوماتية "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، كما عرف أيضا النظام المعلوماتي على أنه: "جهاز يتكون من مكونات مادية ومكونات منطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية، وهو يشتمل على وسائل الإدخال والإخراج وتخزين البيانات، وهذا قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة".

جعل المشرع الجزائري من إجراء التفتيش مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة الإلكترونية، وذلك من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة (3) من القانون رقم: 09-04 السالف الذكر، التي تنص على:"مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن المقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

من جهة أخرى بهدف التفتيش المنصب على المنظومة المعلوماتية إلى استخلاص الدليل الإلكتروني، قبل قيام المجرم المعلوماتي بتدميره أو إخفائه للإفلات من العقوبة. لكن ما هي الجهة القضائية المختصة بمنح الإذن بالتفتيش؟ هذا ما سنجيب عنه.

الجهة القضائية المختصة بذلك:

بالرجوع إلى المادة (04/أ) [1] من القانون رقم: 09-04 السالف الذكر، يبين لنا المشرع الجهة القضائية المختصة بهذه الحالة في المادة نفسها الفقرة الأخيرة إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنصوص عليها بموجب المادة (13) من القانون نفسه، إذنا لمدة ستة أشهر قابلة للتجديد، وذلك على أساس طبيعة ونوعية الترتيبات التقنية المراد أخذها بخصوص الحالات التي تسمح باللجوء إلى المراقبة الالكترونية .

الفقرة الثالثة: حجز المعطيات المعلوماتية

يظل الهدف الأساس لعملية تفتيش المنظومة المعلوماتية، هو وضع اليد على الأدلة الرقمية لإدانة المجرم الإلكتروني، فإذا كان حجز الأشياء المادية كالمعدات المكونات المادية للحاسوب) والأوراق والمستندات... الخ، لا يعد مشكلة ويتم وفق القواعد الإجرائية التقليدية، غير أن الأمر يختلف تماما، إذ ليس من السهل توقيع الحجز على المنظومة المعلوماتية التي هي في الأصل شيء معنوي غير ملموس.

وطبقا لنص المادة (06) من القانون رقم : 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تنص على: 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 اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية".

[1] أنظر: المادة (4) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي يجري بها العملية. غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشغيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

أولا: الحجز عن طريق منع الوصول إلى المعطيات.

نص المشرع الجزائري في المادة (7) من القانون رقم: 09-04 السالف الذكر إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (6) أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها...".

والملاحظ أن المشرع لم يحدد الأسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه، لذلك نص على ضرورة إجراء تدابير احترازية من طرف المختصين باستعمال الوسائل التقنية المناسبة القصد منه عدم تمكين المجرم من الوصول للمعطيات المخزنة في المنظومة المعلوماتية .

ثانيا: حدود استعمال المعطيات

تطرقنا فيما سبق إلى أن إجراء مراقبة الاتصالات الالكترونية يمس بحق الأشخاص في سرية مراسلاتهم ومنها المراسلات الالكترونية، وهو حق مكفول دستوريا، لذا نص المشرع الجزائري تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة، إلا فيما تتطلبه التحريات والتحقيقات القضائية، وهذا بموجب نص المادة (09) من القانون رقم: 09-04 السالف الذكر التي تنص على: تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية."

المبحث الثاني: حجية الدليل الإلكتروني في الإثبات

يخضع الدليل الإلكتروني لمبدأ عام في الإثبات الجنائي بالاقتناع، وتعاظم دور الإثبات العلمي مع بروز الدليل الإلكتروني الإثبات الجرائم الالكترونية كأفضل دليل إثبات، ولهذا سنتعرض في هذا المبحث إلى سلطة القاضي الجنائي في تقدير الدليل الرقمي، وتأثير الدليل الإلكتروني على قناعة القاضي في المطلب الثاني كالتالي:

المطلب الأول: سلطة القاضي الجنائي في تقدير الدليل الالكتروني

يعتبر مبدأ حرية الاقتناع الشخصي للقاضي الجزائي ، من أهم عناصر الإثبات في الدعوى الجنائية ، فالقاضي حر بأن يأخذ بالأدلة التي يراها مناسبة للكشف عن الحقيقة و له أن يحتوي بنفسه صدق الأدلة الرقمية ، و له الحق في أن يستمد اقتناعه و عقيدته من أي مصدر يطمئن إليه ، و حرية الاقتناع هي حرية خاصة بالقاضي من خلالها يعمل السلطة التقديرية و ببسطها على الأدلة الجنائية ، فبالرغم من أن النيابة العامة عليها أن تقيم الدليل على الإدانة و المتهم عليه أن ينفي هذا الدليل ، إلا أن التزام القاضي بإدراك الحقيقة الواقعة أما المادية استجابة لمقتضيات التجريم ، جعلت له دورا إيجابيا يدرك بمقتضاه الحقيقة و تختلف عن دور القاضي المدني الذي يقتصر على الموازنة بين الأدلة التي يقدمها الأطراف دون البحث عن حجج أخرى من تلقاء نفسه[1].

[1] باطلي غنية، الجريمة الإلكترونية، أطروحة لنيل شهادة دكتورة، جامعة باجي مختار، عنابة، 2015، ص 286
يتميز الإقناع الشخصي للقاضي الجزائى بخاصيتين .
الخاصية الأولى : تعتبر عن حالة ذهنية معينة على الإحتمال و أن العبرة ليست بكثرة الأدلة و إنما مما تركه من أثر في نفسية القاضي الذي سيحدد مصير الدعوى الجزائية إما البراءة أو الإدانة _
الخاصية الثانية : تتمثل في أن القاضي حر في أن يأخذ عقيدته أو إقناعه من أي دليل يراه مناسبا لأظهار الحقيقة ، نعيم سعيداني ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستر ، كلية الحقوق و العلوم السياسية ، قسم الحقوق ، جامعة الحاج لخضر باتنة ، 2013 ، ص 226.

ومنه سنتناول في مطلبنا هذا مضمون الاقتناع الشخصي للقاضي الجنائي في (الفرع الأول) ثم تتطرق إلى الضوابط التي تحكم الاقتناع القاضي الجنائي بالدليل الإلكتروني في (الفرع الثاني) وفي الأخير نتطرق إلى موقف المشرع الجزائري في (الفرع الثالث).

الفرع الأول: ماهية اقتناع القاضي الجزائي بالدليل الالكتروني

إن الأدلة الرقمية سواء تلك المتواجدة على هيئة ورقة يتم إنتاجها عن طريق الطباعات أو الراسم، أو كانت شكل مخرجات رقمية كالأشرطة و الأقراص الممغنطة أو الضوئية و أسطوانات الفيديو أو المصغرات الفيلمية و غيرها من الأشكال غير التقليدية ، و إما أن تكون مخرجات مرئية يتم عرضها على شاشة الحاسوب تخضع جميعها النظام الأدلة المعنوية الذي تأخذ به أغلب التشريعات المقارنة حديثا و الذي يقوم على مبدأ الاقتناع الشخصي للقاضي الجنائي[1].

أولا: تعريف الاقتناع الشخصي للقاضي الجزائي

هو الإيمان العميق والركون إلى صحة الوقائع التي يقدمها الأطراف المتنازعة والتي اعتمدها القاضي وتنتج عنها أثرا عميقة في نفسية القاضي الجزائي، تتركه يصدر حكمه عن قناعة وحرية وا ٍحساس كبير بإصابته في حكمه[2].

[1]بن فريدة محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)، مجلة سداسية متخصصة محكمة، السنة الخامسة، المجلد 09، عدد 01، بجاية 201، ص. 297 289.

- الأقراص المغناطيسية: تعد من أفضل الوسائط التي يمكن استخدامها للتخزين المباشر ومن أهم أنواعها القرص المرن، FloppyDisk، القرص الصلب. المصغرات الفلمية : أو ما يسمى بالمايكرو و فيلم و هي عبارة أفلام فوتوغرافية ، يتم استخدامها في تصوير صفحات البيانات مع تصغيرها لدرجة متناهية عن طريق جهاز تحويل البيانات المسجلة على الأشرطة، و الأقراص المغنطة.

[2]سامي جلال فقي حسين ، الأدلة المتحصلة من الحاسوب و حجيتها في الإثبات الجنانى ، دار الكتب القانونية ، مصر ,2014 ، ص. 280. د هلال أمنة ، الإثبات الجنائي بالدليل الإلكتروني، مذكرة محكمة من مقتضيات نيل شهادة الماستر في الحقوق، تخصص القانون الجنائي، جامعة محمد خيضر، بسكر، 2014-2015، ص.28.

ولقد أشار المشرع الجزائري إلى هذه المسألة بنصه على مبدأ الاقتناع القضائي الجزائي في المادة 307 قانون الإجراءات الجزائي الجزائري ، و التي هي مستوحاة من المادة 353 من قانون الإجراءات الجزائية الفرنسي[1].

وكما تطرق المشرع الجزائري إلى مبدأ الاقتناع القضائي في نص المادة 212 من قانون الإجراءات الجزائية الجزائري على:" يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عاد الأحوال الشخصية التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ..." ويطبق المبدأ أمام جهات الحكم القضائية [2].

ثانيا: أساس مبدأ الاقتناع القضائي

تناولت أغلب التشريعات المقارنة موضوع الاقتناع الشخصي للقاضي الجزائي ، وجسدته في قوانينها الإجرائية ، كما تم الأخذ به في أحكام محاكمها و سيتم تناول أهم الأنظمة القانونية و أهم الأحكام القضائية التي طبقت المبدأ دون أن ننسى موقف كل من التشريع و القضاء الجزائر ي في هذا الصدد سيتم دراسة الأساس القانوني لمبدأ الاقتناع ، ثم الأساس القضائي لمبدأ الاقتناع القضائي.

أ_ الأساس القانوني لمبدأ الاقتناع القضائي

حرصت الكثير من التشريعات على جعل مبدأ الاقتناع القضائي عنوانا للإثبات الجزائي حيث يستند إليها القاضي في حكمه، فقد أقر المشرع الجزائري ذلك في قانون الإجراءات الجزائية على مبدأ الإقتناع الشخصي للقاضي الجزائي و جسده بنصوص واضحة و هذا ما أوردته المادة 307 من ق.إ ج. ج :" يتلو الرئيس قبل مغادرة قاعة الجنايات التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة ..."

[1] هلال أمنة، نفس المرجع، ص.28.

[2] القانون رقم 66/155، يتضمن الإجراءات الجزائية، مرجع سابق.

كما أوردته المادة 1/212 من نفس القانون الذي يتضمن توجيه القسم من الرئيس إلى المحلفين فيما يخص إجراءات انعقاد محكمة الجنايات[1].

ومن بين التشريعات التي أخذت بهذا المبدأ نجد القانون الفرنسي الذي يقر على مبدأ الاقتناع الشخصي للقاضي الجزائي لأول مرة وذلك ما جسده في المادة 343 من قانون الإجراءات الجزائية[2]. في شأن التعليمات التي تلقى على محكمة الجنايات ثن ألغي هذا الأخير بموجب القانون الصادر في 25 نوفمبر إلا أن مضمون المادة السالفة الذكر أعاد القانون الجديد التأكيد عليها في نص المادة 353 قانون الإجراءات الجزائية.

و تقر المادة 304 ق. إ. ج الفرنسي أنه على المحلفين أن يحلفوا يمينا بأن يحكموا بالعدل الأدلة الإتهام ووسائل الدفاع على ضمائرهم و اقتناعهم الداخلي مع النزاهة و التي يتمتع بها الإنسان حر مستقيم " و أيضا كما خول المشرع لرئيس محكمة الجنايات سلطة تفويضية بمقتضاها يمكنه أن يتخذ كافة الإجراءات التي يعتقد أنها مفيدة للكشف عن الحقيقة ، حيث لا يقدم عليه سوى ضميره و شرفه حسب نص المادة 310 قانون الإجراءات الجزائية الفرنسي.

---

[1] محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي، د، ط، ديوان المطبوعات الجامعية،الجزائر،1999، ص427.

_ أما القانون البلجيكي : قد تناولت المواد 189،154،242 ، من قانون الإجراءات الجزائية مسألة الاقتناع القضائي ، في حين نصت المادة 249 من قانون السويد الاتحادي الصادر في 1934 على أنه :" تقدر السلطة المنوطة بها الحكم الأدلة بحرية ن و لا تتقيد بالقواعد المتعلقة بالأدلة القانونية أن كما نصت المادة 169/3 من قانون الإجراءات الجنائية الاتحادي :" يقدر القضاء بحرية مدى صدق الشهود و القوة الإقتناعية للأدلة المقدمة

_ أيضا القانون الإيطالي : فإن الإجراءات الجنائية منه و الصادر في 16 فبراير 1988 حين خضض الكتاب الثالث ، و جعل له عنوان و هي الأدلة الجنائية ، كما تتقسم في حيث تناول الباب الثاني أنواع الأدلة ، أما الباب الثالث فجاء بعنوان وسائل البحث عن الدليل أما فيما يخص الاقتناع القضائي بالدليل الجنائي فقد تناولته عدة مواد منها المادة 189 التي تناولت حرية القاضي في الأخذ بالدليل وجاء فيها " القاضي عند طلب دليل لا ينظمه القانون الأخذ به إذا تبين أنه ملائم لضمان التحقيق من الوقائع و لا يؤثر على حرية الإرادة..."

[2] بن فريدة محمد ، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)، مرجع سابق ص. 308.

كما نصت المادة 1/427 من قانون الإجراءات الجزائية الفرنسي " فيما عدا الحالات التي ينص عليها القانون خلاف ذلك تثبت الجرائم بكل وسائل الإثبات و يقضي القاضي بمقتضى اقتناعه الشخصي.

أما التشريعات العربية أخذت بهذا المبدأ فقد تناول القانون المصري مسألة الإقتناع في المواد 1/291 ، 300، 1/302 ق.ا.ج المصري.

وتنص المادة 1/302 ق.ا.ج المصري. " يحكم القاضي في الدعوى حسب العقيدة التي تكونت الديه بكامل حرياته[1].

ونستخلص مما سبق أن أغلب التشريعات المعاصرة تأخذ بمبدأ الإقتناع القضائي مع إختلاف في الصياغة بين التشريعات اللاتينية و التشريعات النجلو أمركية ، و لكن العبرة ليس النص بل هو التعبير في جانبه العملي الذي يقره القاضي في حكمه خاضعا بذلك لضميره دون تقييده ، بأي قيد عاد القيود و الضوابط التي وضعها و صاغها القانون.

ب- الأساس القضائي لمبدأ الاقتناع القضائي

قضت المحكمة العليا الجزائرية في الشق الجزائي بهذا المبدأ و جاء في عدة أحكام منها ما يلي: من المقرر قانونا أنه لا يطالب من القضاة المشكلين لمحكمة الجنايات ، أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم الشخصي ، و لا يرسم لهم بها قواعد يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما ، و من ثم النعي على الحكم المطعون فيه بحر القانون غير سديد مما يستوجب رفضه ، و لما كان الثابت في قضية الحال أن الحكم الصادر من محكمة الجنايات بالبراءة كان بأغلبية الأصوات و أن الأسئلة قد

[1]ابن فريدة محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)، مرجع سابق، ص .310.

بخصوص الشريعة الأنجوسكسونية فيلاحظ أن هذه الطائفة من القوانين لا تعرف تعبير الاقتناع القضائي بهذه العبارة ، و إنما تشير إلى معناه بتعبيرات مشابهة ، فمثلا : القانون الأمريكي نجده يستخدم تعبير " إثبات الإدانة بعدا عن أي شك معقول كما أن الفقه الإنجليزي يرفضان تفسير ماهية الشك المعقول و يلقون إلزاما على المحلفين يتمثل في العبارة التالية : لابد قبل إدانة المتهم أن تكونوا مقتنعين بصورة أكيدة بأنه مذنب .

طرحت بصفة قانونية و أن الأجوبة المعطاة كانت حسب الاقتناع الشخصي للقضاة الذي لا يخضع لرقابة المحكمة العليا و متى كانت كذلك استوجب رفض الطعن[1].

و جاءت بذات المبدأ في قرار آخر ما يلي : من المقرر قانونا أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك و من ثم فإن القضاة بما يخالف هذا المبدأ يعد خرقا القانون ، ولما كان الثابت في قضية الحال أن القضاة الاستئناف ناقشوا الأدلة الإثبات و أوجه دفاع المتهم واقتنعوا بعدم صحة دفاعه فيما يخص النكران للتهمة المنسوبة إليه علما أن الجريمة لم تكن من الجرائم التي ينص فيها القانون على إثباتها بنص خاص يكونوا قد طبقوا القانون تطبيقا سليما ، و متى كانت الأمر كذلك استوجب رخص الطعن.[2]

و كما جاء في قرار آخر أنه :" يمكن للقاصي تأسيس اقتناعه على أية حجة حصلت مناقشتها حضوريا أمامه [3]

كذا لا يمكن القضاة الموضوع أن يؤسسوا قرارهم إلا على الأدلة المقدمة لهم أثناء المرافعات و التي تم مناقشتها حضوريا [4].

و لم يكن القضاء الجزائري الوحيد الذي انتهج هذا المبدأ حيث نجد من بين هذه التشريعات القضاء الفرنسي بإدراجه هذا الأخير لمبدأ الاقتناع القضائي، الذي يشمل قبول الدليل و تقديره ، وفقا لحرية القاضي الجزائي في تكوين اقتناعه و ذلك ما جاء به في المادة 427 من قانون الإجراءات الجنائية الفرنسية[5].

---

[1]- المحكمة العليا الجزائرية قرار صادر بتاريخ 30/06/1987 الملف رقم 50971 المجلة القضائية العدد الثالث لسنة 1991 ، ص 199.

[2]المحكمة العليا قرار صادر بتاريخ 29/01/1991 الملف رقم رقم 70690 المجلة القضائية العدد الثالث لسنة 1991 ، ص 199.

[3]-ر.ع. ج 9 جويلية 1990 _مجموعة قرارات ع ج ، ص 153 على المجلة القضائية 1993_3، 282.

[4]- رغ . ج م 28 . 03_ 1989 ملف 647_56، المجلة القضائية 1993 _3 ص 291.

[5]بنفريدة محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)، مرجع سابق ، ص.313.

أما القضاء المصري ، فقد أكدت محكمة النقض المصرية في العديد من أحكامها على حرية القاضي الجنائي في تكون إقناعه من أي دليل برامج إليه مالم تفرض عليه القانون الأخذ بديل معين[1].

وسنستخلص من ما سبق من أحكام محاكم النقض في مختلف الأنظمة القضائية أن الاتجاه القضائي في عملية الإثبات يقوم أساسا على مبدأ الاقتناع الشخصي للقاضي الجزائي ، و للقاضي السلطة التقديرية في الأخذ بالدليل بغض النظر سواء كان هذا الأخير رقميا أو دليلا ماديا دون تفاضل في الأدلة ، فالعبرة في النهاية تعود إلى قناعته الشخصي.

ثالثا : ممارسة القاضي الجزائي لمبدأ الاقتناع الشخصي بالدليل الرقمي

إن ممارسة القاضي الجنائي لمبدأ الاقتناع الشخصي فيما يخص الدليل الإلكتروني تتجسد هذه مظاهر في الممارسة من جهة ، ثم تطبيقات هذه الممارسة فيما يخص الدليل من جهة أخرى ، و عليه تجدر الإشارة إلى أن القاضي الجزائي في أغلب التشريعات القضائية لا سيما تشريعات النول اللاتنية لم يتناول مسألة الدليل الإلكتروني كمسألة مستقلة في الإثبات ، و إنما يخضعها للمبادئ العامة في الإثبات ، فمثلها مثل أي دليل أخر فالأدلة الرقمية ليست إستثناءا من الأدلة الأخرى فهي تخضع للقواعد العامة و على ما استقرت عليه الأحكام القضائية ، وعليه سيتم تناول هذه الجزئية كالتالي :

- مظاهر ممارسة القاضي الجنائي لمبدأ الاقتناع بالنسبة للدليل الإلكتروني

أوضحت محكمة النقض المصرية مظاهرة لمبدأ الاقتناع القضائي في حكمها الصادرة في 1939/04/12 ، كما نصت عليها المادة 302 من قانون الإجراءات الجزائية المصرية سالفة الذكر و هو أيضا ما قضت به بمحكمة التمييز الكويتية في أحد أحكامها حيث تقضي بأن

[1] نقض جلسة 06/03/1939 مجموعة القواعد القانونية 31 رقم 62 ص 328 وكذا ورد في الطعن رقم 29020 جلسة 1998/02/08 لسنة 59 ق. رقم 28 ، ص.193.

القاضي الجزائي يعتمد على تكوين قناعته الشخصية اعتمادا منه على الأدلة التي تعرض عليه ، و تتسع سلطة التقديرية للأخذ أو رفض أي دليل أو قرينة يرتاح إليها[1] .

أ- سلطة القاضي الجنائي في تقدير الأدلة الالكترونية بذاتها

يظهر من أحكام محاكم النقض أن القاضي الجنائي أن يستعد الدليل و يطرحه إن لم يطمئن إليه و أن يأخذ به كاملا أو يأخذ بالجزء الذي يطمئن إليه و يقتنع بصحته[2] ، وهو الأمر الذي ينطبق على الأدلة الإلكترونية سواء أكانت في بيئتها الرقمية أما على شكل مخرجات طباعة أو اتخذت شكل صور أو مقاطع فيديو.

1-حرية القاضي الجنائي في استبعاد الأدلة

للقاضي الجنائي أن يستبعد في مجال تقديره الدليل ما لم يطمئن إليه عندما يمارس سلطته في الدعوى موضوعيا و يعود عدم الاطمئنان القاضي القيمة الدليل الذي يطرحه تكمن في ضعف الدليل المستبعد في الدلالة على الحقيقة التي يسعى الحكم في جعلها عنوانا له بذلك القضاء ، أو لأن هنالك أدلة أخرى تدحض الدليل المستبعد ، أو لأن هناك أدلة أقوى منه في الإثبات و كافية في تكوين قناعة المحكمة ، كما قضت به محكمة تمييز دبي[3] .

2-حرية القاضي الجنائي بالأخذ بالدليل هذه الحرية لها صور عديدة فالقاضي ينجم الأخذ بمبدأ الاقتناع القضائي ما يتعلق بالدليل فللقاضي أن يأخذ به كاملا أو يأخذ بجزء منه دون

---

[1] محكمة التمييز الكويتية 1976/06/30 ، المجلة الفضائية العربية ، الأمانة العربية لمجلس وزراء العمل العرب ، العدد الأول ، السنة الأولى ، نسيان 1984 ، ص 326- 327

[2] شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة ، الإسكندرية ، 2007 ، ص، 85. إجباري عبد المجيد درلمة قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة ، دون طبعة ، دار هومة ، الجزائر، الجزائر 2012 ، ص، 122،

[3] محكمة تمييز دبي : "وزن أقوال الشهود و تقديرها من حق محكمة الموضوع المنزلة التي تراها و تقدره التقدير الذي تطمئن إليه و للمحكمة أن تعود على ما قاله شهود الإثبات وتعرض عما قاله شهود النفى فقضاؤها بالإدانة استنادا إلى أدلة الثبوت يفيد دلالة أنها طرحت شهادتهم ولم تر الأخذ بها .'

الجزء الآخر ، و أن يأخذ به المتهم دون شريكه ، و أن يأخذ بالدليل في حالة تعدد التهم دون التهم الأخرى [1]، وهذا كما قضت عليه محكمة دبي في قرارها[2] .

ب- سلطة القاضي الجنائي في تقدير الأدلة الرقمية من حيث مصدرها :

إن سيادة مبدأ الاقتناع القضائي في مجال الاثبات الجنائي ، منحت للقاضي الجزائي الحرية في تقدير الأدلة بغض النظر عن المصدر الذي استمدت منه المهم أن يكون مشروعا[3] دون النظر عن أي مرحلة من مراحل الدعوى تحصل على هذا الأخير ، كما له أن يعتد بمحاضر جمع الاستدلالات التي يحررها ضباط الشرطة المختصون وله أيضا سلطة عدم الاعتداد بها[4] ، كما له أن يرفض تقرير خبرة أجريت في مرحلة التحقيقات بتعيين من قاضي التحقيق ، إذا فالقاضي يقر الدليل بحسب اقتناعه لا حسب الدليل ذاته ، على أنه وجب عليه تسبيب الحكم إثر رفضه لهذا النوع من المحاضر أو التقارير كي لا يتعسف القاضي في استعمال حقه[5].

الفرع الثاني الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الرقمي

إن الأصل العام أن القاضي الجنائي حر في تقدير الأدلة المطروحة عليه في الدعوى عملا بمبدأ الاقتناع الشخصي ، فهو غير ملزم بإصدار حكم الإدانة أو البراءة لتوافر دليل معيب طالما أنه لم يقتنع به ،و هذا الأمر وضعت له ضوابط حيث لا تعطي لهذا القاضي الجنائي مطلق الحرية التي يتمتع بها لغاية ير اها المشرع ضرورية[6].

---

[1] محمد على العريان ، الجرائم المعلوماتية، دار الجامعة الجديدة ، الإسكندرية ، 2011 ، ص45

[2] محمد تميز دبي : "أنه من المقرر أن المحكمة أن تأخذ بأقوال الشاهد في مرحلة من مراحل التحقيق و المحاكمة ، فلها أن تأخذ بأقواله في محضر الجلسة وا ن خالفت قولا أخر أثناء تحقيقات النيابة العامة

[3] شيماء عبد الغنى، الحماية الجنائية للتعاملات الإلكترونية، مرجع سابق، ص. 94

[4] المرجع نفسه، ص 95.

[5] محمد علي العريان، الجرائم المعلوماتية، مرجع سابق، ص. 52

[6] بلوهلي مراد، لحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، ماجستير، منشورة، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، باتنة، الجزائر ، ص 2011، ص، 189.

و على ذلك فإن دراستنا للضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني سنتطرق فيها في البدء إلى الضوابط التي تتعلق بمصدر الإقتناع (أولا) ، ثم سوف نتكلم عن الضوابط المتعلقة بالاقتناع في حد ذاته (ثانيا).

أولا: الضوابط المتعلقة بمصدر الاقتناع

إن الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني ، و التي تتعلق بهذا الأخير تكون هي الضوابط المشتقات منه في حد ذاته و تتمثل في :

ضابط أن يكون الدليل الإلكتروني مشروعا و هذا الضابط مكمل لقيد مشروعية الدليل الإلكتروني ، فعلى القاضي أن يستمد إقتناعه من أدلة مقبولة و مشروعة[1] . فإن مسألة قبول هذا الدليل لا بد أن تحضي بالأهمية ، لاعتبارها ركيزة في مبدأ حرية القاضي الجنائي في تقدير الدليل الإلكتروني ، و يستبعد في المقابل جميع الأدلة الإلكترونية غير المقبولة ، لأنه من غير المعقول أن تكون عنصرا من عناصر اقتناعه و تقديره[2] .

فمشروعية و مقبولية الدليل الإلكتروني تعد ضمانا للحرية الفردية و العدالة، و أيضا تجبر القائمين على جمع و تحصيل الأدلة المتعلقة بالإدانة أن يقوموا بعملهم على أكمل وجه، وذلك

حتى لا يتم هر أهم مبدأ و هي قرينة البراءة، و لهذا فعلى القاضي الجنائي أن يستمد اقتناعه الذاتي في مجال الإثبات المتعلق بالجرائم الالكترونية، من دليل رقمي مشروع و مقبول.[3]

أما بالنسبة لضابط الضرورية طرح الدليل الإلكتروني في الجلسة للمناقشة بصفة عامة يجب على القاضي أن يستمد اقتناعه من أدلة طرحت في الجلسة أو خضعت للمناقشة من

---

[1] بلوهلي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، المرجع السابق، ص 190

[2] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، مرجع سابق، ص. 268.

[3] المرجع نفسه، ص. 269.

طرف الخصوم الذين يتواجهون بهذه الأخيرة، واستناد القاضي إلى أدلة لم تطرق للمناقشة موجب للبطلان[1].

فهذه القاعدة تعني أن القاضي لا يجوز أن يؤسس اقتناعه إلا على عناصر الإثبات التي طرحت في جلسات المحكمة ، و خصصت لحرية مناقشة أطراف الدعوى إعمالا لمبدئ المحاكمة الجزائية ، المتمثلة في الشفوية بحسب المواد 300،304،353 من قانون الإجراءات الجزائية الجزائري ، و مبدأ العقلية بحسب المواد 285،342،355،399، من قانون الإجراءات الجزائية الجزائري ، و كذا مبدأ المواجهة بحسب المادة 2/212 من نفس القانون و هذه المناقشة عليها أن تأخذ في عين الإعتبار ضرورة احترام حقوق الدفاع بإعطاء فرصة للمتهم للاستفسار حول كل وسيلة من وسائل الإثبات المقدمة أمام القاضي الجنائي هذا من جهة ، من جهة ثانية يتعين توافر المناقشة الحضورية لأنها تعتبر مطلبا منطقيا ، و تنطوي على فحص شامل و جماعى لكل وسيلة إثبات[2].وضابط وضعية الدليل الإلكتروني يقوم على عنصرين أساسيين، حيث يتمثل العنصر الأول في إتاحة الفرصة للخصوم للإطلاع على الدليل الإلكتروني والرد عليه، أما العنصر الثاني فهو يتمثل في أن يكون للدليل الإلكتروني أصل في أوراق الدعوى[3].

ثانيا: الضوابط المتعلقة بالاقتناع ذاته

إن مبدأ الاقتناع القضائي الذي تبناه المشرع الجزائري كغيره من التشريعات ، يتيح للقاضي الجنائي حرية كبيرة في تقدير عناصر الإثبات بما في ذلك الدليل الإلكتروني ، و الذي يعتبر من أهم النتائج التي تترتب عن هذا المبدأ و السبب في الأخذ بهذا الدليل المستحدث ، لذلك فإن تقدير كفاية الدليل الإلكتروني أو عدم كفايته في إثبات الجريمة الإلكترونية و نسبتها إلى

[1] العربي شحط عبد القادر، قبيل صقر، الإثبات في المواد الجنائية، دار الهدى للطباعة والنشر والتوزيع، الجزائر، دام، ن، ص. 26.

[2] أنظر المواد 300,304 353 ، 285,356,399و2 / 212 من قانون الإجراءات الجزائية قانون رقم 17_07 مؤرخ في 28 جمادى الثاني عام 1438 الموافق 27 مارس سنة 2017 ، المعدل و المتمم

[3] باطلي غنيمة، الجريمة الإلكترونية، مرجع سابق، ص. 289.

فاعلها ، أمر تختص به محكمة الموضوع المعروض عليها هذا الأخير ، و لا تخضع في ذلك لرقابة المحكمة العليا و التي يقتصر دورها على مراقبة المنطق القضائي لمحكمة الموضوع عن طريق مراقبتها صحة تسبيب الحكم[1].

إن القاضي في تكوين اقتناعه و إن كان حرا في اختياره للأدلة التي يطمئن إليها ، إلا أن هذا الأمر مشروط بأن يكون إستنتاج القاضي الحقيقة الواقعة و ما كشف عنها من أدلة لا يخرج عن مقتضيات العقل و المنطق[2] .

و بهذا يكون القاضي قد توصل إلى اقتناع تام و تأكده بالحقيقة و ذلك ما يعتبر يقين و يتم التوصل إلى هذا الأخير عن طريق ما تستخلصه وسائل الإدراك المختلفة من خلال ما سبق و تقدم إليه من وقائع في الدعوى[3]

وهذا يعني أنه في حالة ما انتاب القاضي شك حول براءة أو إدانة المتهم لا يسعه إلا الحكم بالبراءة وذلك تقيدا بقاعدة الشك يفسر لصالح المتهم و هو الأمر الذي حرص عليه المشرع الجزائري في أخر تعديل لقانون الإجراءات الجزائية لسنة 2017 في المادة الأولى منه التي جاءت كالتالي: «... أن يفسر الشك في كل الأحوال لصالح المتهم

وفي كل الحالات يجب تسبيب الحكم الذي يقوم به القاضي الجزائي من وقت سريان الدعوى إلى غاية صدور الحكم فيها ، كما أن القاضي يثبت فهمه للواقع فهما كافيا ، و تكفيه لكل الأدلة و القرائن الواردة و أنه قد قدرها تقديرا سليما و إضافة إلى أنه يثبت جدارته في تطبيق القانون تطبيق سليما[4] .

و مدلول التسبيب في التشريع و القضاء الجزائري أن التشريع لم يضع مدلولا للتسبيب إلا أنه أشار إلى ضرورة بيان الأسباب الواقعة و القانونية ،و أسباب الرد على طلبات الهامة و

---

[1] المرجع نفسه، ص. 114.

[2] هلال آمنة، الإثبات الجنائي بالدليل الإلكتروني، مرجع سابق ص.112

[3] هلال آمنة، الإثبات الجنائي بالدليل الإلكتروني، مرجع سابق، ص114.

[4] شرفة وليد، فركان كنزة ، تسبيب الحكم الجزائي ، مذكرة الماستر ، جامعة ، بجاية ،2016،ص ص، 07-08.

الدفوع الجوهرية ، و لكن من ناحية أخرى نجد أن القضاء قد وضع الضوابط الصحيحة لتسبيب الأحكام و استقرار على مدلول محدد للتسبب لا يصح إلا به كما نراه في نص المادة 309 من الجريدة الرسمية العدد 20 على الحكم بالبراءة و استبعاده عن محكمة الجنايات[1] .

المطلب الثاني: تأثير الدليل الإلكتروني على قناعة القاضي

نظرا لتطور العلمي الذي عرفه المجال الجنائي و مع بروز ادلة علمية حديثة، من بينها نجد الدليل الإلكتروني الذي يعد كأفضل دليل الإثبات الجرائم الالكترونية و ذلك يعود إلى نقص الثقافة العلمية، و الأخذ به يجب توافر شروط مصداقيته، و كذا الاستعانة باهل الخبرة و الفصل في النزاعات في حالة ما استعصى عليه الأمر، ولهذا سنتطرق في هذا المطلب إلى مصداقية الدليل الرقمي، كذا القيمة العلمية لدليل الإلكتروني و تأثيره على قناعة القاضي .

الفرع الأول: مصداقية الدليل الإلكتروني في الإثبات

إذا كان لدليل الإلكتروني في الإثبات قيمة الإثبات من الناحية العلمية، يجب توافر شروط مصداقيته، و لكن هذا لا يمكن أن يستبعد عن موضوع الشك من حيث سلامة العبث به من جهة، و كذا صحة الإجراءات المتبعة في الحصول عليه من جهة أخرى.

أولا :يقينية الدليل الإلكتروني

اليقين هو عبارة عن حالة ذهنية أو عقلية تؤكد وجود الحقيقة، ويتم الوصول إلى ذلك عن طريق ما نستخلصه من وسائل الإدراك المختلفة للقاضي ما يقدم إليه من وقائع الدعوى، و ما ينطبع في ذهنه من تخيلات ذات درجة عالية، لذلك عندما يصل القاضي إلى اليقين فإنه يصبح في المرحلة مقتنعا بالحقيقة[2].

[1]أنظر نص المادة 309 من الأمر، رقم 66 /155يتضمن قانون الإجراءات الجزائية مرجع سابق.

[2]رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص 517

و يصل القاضي إلى يقينية المخرجات المقدمة ذكرها عن طريق المعرفة الحسية التي تدركها الحواس من خلال معاينتها لهذه المخرجات، و عن طريق المعرفة العقلية التي يتم كمن خلالها استخلاص و استقراء الحقيقة التي تهدف إليها، و يجب أن يصدر حكمه استنادا إليها[1].

ونظرا لطبيعة التقنية التي يتميز بها الدليل الإلكتروني إلا انه هناك قواعد محددة، تم وضعها من طرف المختصين التي تحكم يقينيتها و من بينها استعمال الوسائل الفنية، تكون من طبيعة هذا الدليل، تكمن في فحص سلامة و صحة الإجراءات المتبعة للحصول عليه.

أ-تقييم الدليل من حيث سلامة العبث به

للتأكد من سلامة العبث بالدليل الإلكتروني يجب أن نتبع عدة طرق منها:

-علم الكمبيوتر يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون الدليل الرقمي، و هذا النوع من العلوم تتم الإستعانة به في الكشف عن مدى تلاعب بمضمون هذا الدليل، و فكرة التحليل التناظري الإلكتروني تبدوا من الوسائل المهمة للكشف عن مدى مصداقية الدليل، و من خلالها يتم التأكد من مدى إمكانية حصول العبث في النسخة المستخرجة أم لا.

-و هناك نوع من الأدلة الالكترونية و التي تسمى بالأدلة المحايدة، وهو من الأدلة التي لا علاقة بموضوع الجريمة، إلا أنه يساعد من التأكد من سلامة الدليل الرقمي، يجعله يقيني و لا مجال للشك فيه حتى تتم مراجعة المتهم به هذا ناحية، و من ناحية أخرى ضمان حقوق المتهم المعلوماتي.

-في حالة عدم حصول الدليل على نسخة الأصلية، أو أن الدليل وقع في حالة عبث، وقد وقع على النسخة الأصلية، فيمكن التأكد من سلامة الدليل الإلكتروني من العبث و ذلك من خلال استخدام عمليات حسابية خاصة بالخوارزميات[2].

---

[1] خالد ممدوح إبراهيم، التقاضي الإلكتروني، مرجع سابق، ص.88.

[2] كحيل خير الدين ، إثبات الجريمة الالكترونية، مذكرة الماستر تخصص قانون جنائي، مسيلة، 2015، ص.136.

ب-تقيم الدليل الإلكتروني من حيث القيمة الفنية

من بين الإجراءات الفنية التي يمكن الاعتماد عليها لتأكد من سلامة الدليل الإلكتروني في الإثبات.

1- التأكد من و دقة الأدوات المستخدمة في استخلاص الدليل الجنائي الإلكتروني

يتم التأكد من صحة الأدوات المستخدمة في استخلاص الدليل الإلكتروني بالتحقيق من مدى قدرة هذه الأدوات على عرض كافة البيانات المتعلقة بالدليل الرقمي، و كذلك خضوعها لأدوات الاختيار، فمن خلاله يمكن أن تتأكد من أن الأدلة لا تعرض بيانات إضافية جديدة[1].

و من خلال هذا الاختبارين نتأكد من الأدلة المستخدمة عرضت على البيانات المتعلقة بالدليل الرقمي، و بالتالي لم يضف اليه أي بيان جديد و يعطي نتائج مقدمة عن طريق جهاز الكمبيوتر مصداقية في التدليل على الواقع[2].

2-الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفائتها في تقديم أفضل

لقد بينت الدراسات العلمية في مجال تقنية المعلومات على الطريقة الواجب إتباعها في الحصول على الدليل الإلكتروني و في المقابل أوضحت الدراسات الأدوات المشكوك في كفائتها و هذا ساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات.

ثانيا: مناقشة الدليل

تتم مناقشة الدليل بناء على مبدأ شفوية المرافعات، وهذا طبقا لنص المادة 212 ق.إ.ج التي تنص على أنه لا يسوغ القاضي أن يبني قراره إلا على الأدلة المقدمة له في المرافعات و التي حصلت المناقشة فيها حضوريا أمامه[3] .

[1] أحمري سميرة، عاشور رزيقة ، المرجع نفسه، ص.87.

[2] كحيل خير الدين، إتيات الجريمة الالكترونية، مرجع سابق ص 136.

[3] كحيل خير الدين، المرجع نفسه، ص.137.

من خلال هذه نجد أن القاضي يعتمد في الحكم على الاجتهاد ، و لا يعتمد على رأي الغير إلا إذا كان ذلك من الخبراء المتخصصين، هذا قد تطرقنا إليه في المطلب الأول من هذا المبحث[1].

الفرع الثاني: القيمة العلمية للدليل الإلكتروني و تأثيرها على قناعة القاضي

يعرف الدليل العلمي بأنه ذلك الدليل الذي تقام عليه تجارب علمية لإثبات أو نفي واقعة تثار فيها الشك، و فهمه يتطلب دراية خاصة لا يملكها القاضي في حكمه، و تكوينه القانوني المحضي، و الدليل الإلكتروني باعتباره تطبيقا من تطبيقات الدليل العلمي لا يمكن للقاضي أن ينازع في قيمته الاثباتية و ذلك لامتيازه بقوة الاستدلالية من الناحية العلمية

فالتقدير القاضي برأي الخبير ، فنجد أن الدليل الإلكتروني يعتبر ما الأدلة العلمية التي لا يمكن للقاضي إن ينازع في القيمة و ذلك لتمتعه بقوة استدلالية ، و هنالك بحجية قاطعة في الدلالة عن الوقائع التي الوضعية التي تتضمنه الأدلة ، و كما يمكن التقلب من مشكلة الشك في المصداقية الدليل من خلال إخضاعه لتجارب تمكن منه التأكد من صحته ، و أنه لا يمكن الخلط بين الشك الذي يشوب الدليل بسبب إمكانية العبث به ، و كذا لوجود خطأ في الحصول عليه ، و كذلك القيمة الاقتناعية به ، و القاضي لا يمكن أن يفصل فيها باعتبارها مسألة فنية و رأي هنا يعود إلى الخبير ، فإذا سلم الدليل من العبث و توافره فيه كل الشروط ، فإن على القاضي القبول بهذا الدليل، لذلك ير ى هذا الاتجاه أن رفض القاضي الرأي الخبير فيكون تعارض مع رأيه و نفسه ، و عليه فإن الدليل العلمي و منه الدليل الإلكتروني أصبح يقيد حرية القاضي في تقدير الأدلة ، و يلزمه على الحكم حتى و لو لم مقتنعا بصحة الواقعة المطروحة أمامه[2] .

[1] سنور محمودي، حجية الدليل الإلكتروني في إثبات الجريمة المعلوماتية، مجلة الباحث الدراسات الأكاديمية، العدد 11، جامعة باتنة، 2017 ،ص 919.

[2] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص.218

و هناك من يناقد أنصار هذه النظرية و يكاد أن الأدلة العلمية ليست دليلا مستقلا ، بل هي عبارة عن قرائن إما أن يتخذ شكل قرينة قضائية يعتمد عليه وحده في الإثبات ، و إما يتخذ بشكل دلائل (قرينة تكميلية) لا تصلح كدليل وحيد في الإثبات ، بل على القاضي الاستعانة بأهل الخبرة ، إلا أن القاضي لا يمكن أو إن هناك مجالات لا يمكن لهذا الأخير ، فمثلا إذا كان الدليل الإلكتروني لا يوافق ظروف وملابسات التي وجد فيها ، و كذلك لا يمكن للقاضي أن يباشر حكمه بالإدانة أو البراءة إذ توفر الدليل الإلكتروني ، فالدليل ليس آلية معدة لتقرير اقتناع القاضي على مسألة غير مؤكدة ، فرأي هذا الاتجاه أن الدليل العلمي و الإلكتروني مهما علا شأنهم في الإثبات الجنائي إلا أن سلطة القاضي الجنائي محددة و مسيطرة في الحقيقة و خلالها يمكن للقاضي أن يفسر الشك لصالح المتهم و أن يستبعد الأدلة التي يتم الحصول عليها بطريقة غير مشروعة و هو أمر ضروري و هذا ما جعل الحقيقة العلمية قضائية[1] .

وتكمن مهمة القاضي في تقرير الفني في الرقابة القانونية على هذا التقرير وهو ما ورد في نص المادة 212 ق.إ. ج كما أن المادة 215 ق.إ. ج تؤكد على أن: لا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك." وهو الأمر الذي أخذ به المشرع الجزائري حيث بموجبه يقرر مبدأ الشخصي للقاضي الجزائي يجعله يبسط سلطاته على جميع الأدلة بدون استثناء بما فيها تقرير الخبير[2].

بحيث قضت المحكمة العليا هذا الاتجاه في أحد أحكامها: "إن تقرير الخبرة ليس إلا عنصر من عناصر الاقتناع يخضع لمناقشة الأطراف و التقدير قضاة الموضوع."

و كما أكدت في حكم آخر لها : " إن تقرير الخبرة لا يقيد لزوما قضاة الموضوع إنما هو كغيره من أدلة الإثبات قابل للمناقشة و التمحيص ، و متروك لتقديرهم و قناعتهم ." و كما يلزم القاضي بالحقائق العلمية لا يسلب منه سلطة الرقابة القانونية على عناصر الدعوى بما فيها

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق ، ص 223.

[2] الأمر رقم 155/66 يتضمن قانون الإجراءات الجزائية ، مرجع سابق

طرق الحصول على الليل و الظروف التي وجد فيها، فهي تدخل ضمن الاختصاصات الأصلية للقاضي ، كما إنها تخضع أيضا لمبدأ تكافي الأدلة بحيث يمكن للقاضي استبعاد أي دليل علمي لا يتناسب مع ظروف الواقعة أو الجريمة.

و كما يمكن الاستعانة بمعطيات التطور العلمي في إطار الكشف عن الجريمة و يبقى للقاضي حرية مطلقة في تقرير الدليل المعروض أمامه، و الأخذ بما هو مناسب بالواقع[1].

[1]عباسي خولة، الوسائل الحديثة للإثبات الجنائي في القانون الجزائري، مذكرة الماجستر في الحقوق جامعة محمد خيضر ، بسكرة، 2014 ص، 57.

خلاصة الفصل :

اعتبار الدليل الرقمي ليس كغيره من الأدلة المادية كونه مزيج من المعلومات و الأرقام التي تتواجد في الحواسيب و شبكات الانترنت ، و بالتالي الإشكال يظهر جليا في كيفية التعامل مع الدليل الرقمي كونه ذو طبيعة تقنية تستوجب الدقة التقنية القانونية و الإجرائية الواجب انتهاجها للحصول على الدليل الرقمي وكذا مدى إضفاء صفة المشروعية و مدى قبوليته و اعتباره وسيلة من وسائل الإثبات أمام القاضي خصوصا في ظل غياب النصوص القانونية التي تنظمه.

الخاتمة

من خلال الدراسة التي قمنا بها والتي هدفها الرئيسي هو الوصول إلى تحديد مدى حجية الدليل الالكتروني في الإثبات الجنائي .

نظرا للطبيعة الخاصة للجريمة الالكترونية، لا يوجد اتفاق على وضع تعريف موحد لها، تتم في فضاء افتراضي يتسم بالتغيير والانتشار الجغرافي العابر للحدود.

لقد اعتمد المشرع الجزائري مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها بموجب أحكام المادة (2/أ) من القانون رقم :09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها .

كما تتميز الجرائم الالكترونية بخصائص متفردة من باقي الجرائم، فهي جرائم عابرة للحدود . تتنوع الجرائم الالكترونية، فهي لم تأتي في صوره واحده بل تعددت إلى الجرائم التي تمس بالنظم المعلوماتية والجرائم الواقعة على الأموال، والجرائم الماسة بالأشخاص.

اعتراف المشرع الجزائري بحجية الدليل الالكتروني في الإثبات الجنائي

إن الدليل الرقمي مثله مثل باقي الأدلة في إثبات الجريمة، فهو يخضع لسلطه التقديرية للقاضي الجنائي أي يخضع لقناعة القاضي .

مع هذا ينبغي الاعتراف بحقيقة وهي أنه رغم جهود الجبار ة التي بدلها المشرع الجزائري في سبيل التصدي لظاهره الإجرام المعلوماتي، إلا إنها غير كافيه لي بلوغ الهدف الذي يتطلع إليه، نظرا لتطورات السريعة والمستمرة التيعرفها لهذه الظاهر ة، من جهة أخرى الطابع العالمي والعابر للحدود.

الملخص

مـلخص مذكرة الماستر

لا تترك الجرائم المعلوماتية آثارا مادية يمكن إدراكها بالحواس على عكس الجرائم التقليدية الأمر الذي أضحى يشكل تحديا كبيرا من الناحية التقنية والقانونية لإثباتها، وعليه بعد الدليل الإلكتروني الوسيلة المناسبة لذلك، حيث تدخل المشرع الجزائري بنصوص قانونية إجرائية تساعد على استنباط الدليل الذي يتوافق مع الطبيعة الخاصة لهذه الجرائم، فبدأ المشرع بتعديل قانون الإجراءات الجزائية بموجب القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006، أين نص على أساليب خاصة للبحث والتحري تتلائم وطبيعة هذه الجرائم المستحدثة وذلك بموجب المواد: (65 مكرر5 65 -مكرر 18) كاعتراض المراسلات وتسجيل الأصوات ...الخ. بالإضافة إلى إصداره للقانون 09 04-المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على جملة من الإجراءات الوقائية كمراقبة الاتصالات الإلكترونية حيث كان هدف المشرع الوقاية من الجريمة قبل حدوثها، وعليه اعترف المشرع الجزائري بحجية الدليل الإلكتروني في الإثبات الجنائي بصفة عامة بموجب المادة (323 مكررا من القانون المدني) وأعطاه نفس درجة الدليل التقليدي، وذلك بإتباع إجراءات حديثة تتوافق وتكنولوجيات الإعلام والاتصال لاستخلاص الدليل الإلكتروني، من هذه البيئة الافتراضية والتي تشكل صعوبات بالغة لأجهزة البحث والتحري.

الكلمات المفتاحية:

1/.الدليل الالكتروني 2/الجريمة الالكترونية 3/المشرع الجزائري 4/الإجراءات الجزائية 5/الاتصالات الالكترونية 6/الإثبات الجنائي

Abstract of The master thesis

Information crimes do not leave material effects that can be perceived by the senses unlike traditional crimes, which has become a major technical and legal challenge to prove it, and after this electronic guide has the appropriate means for that, as the Algerian legislator has entered into procedural legal texts that help in devising evidence that is compatible with the special nature of this Crimes, so the legislator began to amend the Code of Criminal Procedure under Law No.: 06-22 of December 20, 2006, where provided for special methods of

research and investigation appropriate to the nature of these crimes introduced According to the articles: (65 bis5 - 65 bis 18), such as intercepting correspondence, recording of votes, etc. In addition to issuing Law 09-4 including the special rules for the prevention and control of crimes related to information and communication technologies, a set of preventive measures, such as monitoring electronic communications, where the goal of the legislator was to prevent crime before it occurred, and accordingly the Algerian legislator recognized the authority of the electronic evidence in criminal proof in general under the article (323 bis of the Civil Law) and gave him the same degree of traditional evidence, by following modern procedures that are compatible with information and communication technologies to extract electronic evidence from this virtual environment that poses great difficulties for research and investigation devices.

keywords:

1/ Electronic Manual **2** Electronic crime **3/** Algerian legislator

4/ Penal procedures **5/** Electronic communication **6/** Evidence Criminal