الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد –الطارف
كليّة الحقوق والعلوم السياسية
قسم الحقوق

الرقم التسلسلي:.....

مذكرة بعنوان:

إجراءات البحث والتحري عن الجريمة الإلكترونية

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون أعمال

إعداد الطالبة:
كوثر عزالدين
بشرى آية عبد المومن

إشراف الأستاذ: نصرالدين العايب

لجنة المناقشة

نذير قورية	أستاذ مساعد قسم –أ–	الشاذلي بن جديد –الطارف	رئيسا
نصرالدين العايب	أستاذ مساعد قسم –أ–	الشاذلي بن جديد –الطارف	مشرفاً ومقرراً
فارس مازوزي	أستاذ محاضر قسم –ب–	الشاذلي بن جديد –الطارف	ممتحنا

السنة الجامعية: 2022/2021

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد

UNIVERSITE CHADLI BENDJEDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحته .

تصريح شرفي

خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة) : ...كوثر عز الدين.....

الحامل لبطاقة التعريف الوطنية رقم: ..119990841068320008.....

الصادرة بتاريخ: ...2022.01.24.....

عن دائرة: ....البيساسرع.....

المسجل بكلية : ..الحقوق والعلوم السياسية.. قسم: ..الحقوق.....

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

...إجراءات التحري عن الجريمة الإلكترونية.....

.....

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

التاريخ: 2022/04/25

إمضاء المعني

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد

UNIVERSITE CHADLI BENDJEDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحته .

تصريح شرفي

خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة) : عبد الرحمان بشرى آية

الحامل لبطاقة التعريف الوطنية رقم: 103157491

الصادرة بتاريخ: 2017/01/31

عن دائرة: القالة

المسجل بكلية : الحقوق والعلوم السياسية قسم: الحقوق

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

إجراءات المحقق الحر عن الجريمة الإلكترونية

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

التاريخ: 2022/06/25

إمضاء المعني

بسم الله الرحمن الرحيم

صدق الله العظيم

شكر

قال تعالى ‘ولئن شكرتم لأزيدنكم’

الحمد لله المعين الذي الذي أعاننا ووفقنا على إنجاز هذه المذكرة فله الحمد و الشكر و الثناء.

نتقدم بالشكر في هذا المقام أولا إلى الدكتور القدير و الأستاذ المحترم **نصر الدين العايب** لقبوله مهمة الإشراف على مكرة تخرجنا هذه و هو الذي لم يبخل علينا بنصائحه القيمة النابعة عن خبرته في ميدان البحث العلمي ومتابعته المتواصلة لأطوار إنجاز هذا البحث وصبره علينا فلك منا أستاذنا الفاضل أزكى عبارات الشكر و الإمتنان.

كما نتقدم بالشكر إلى كل أعضاء لجنة المناقشة المحترمين الأستاذين نذير قورية وفارس مازوي الذين و بالإضافة إلى إنشغالاتهم المتعلقة بأداء مهام تبليغ الرسالة العلمية غير أنهم أبوا إلا أن يشاركوا في مناقشة هذا العمل بدافع هدف نبيل وهو تطوير مجالات المعرفة العلمية.

إهداء

أولا وقبل كل شيء نحمد الله ونشكره على نعمته

التي لا تعد ولا تحصى وبفضله وعظيم سلطانه وأعانني على إنجاز هذا العمل

وإتمامه والذي نرجو أن يكون في المستوى ولقوله تعالى "لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ"

اللهم نور الكتاب بصري واشرح به صدري وسع به فهمي وقوي

به عزمي بحولك وقوتك فإنه لا حول ولا قوة إلا بك.

ما أثقل قلمي في يدي وأثقل قلبي في صدري حيث أكثر إهدائي إلى اللذين لا تكفيهم كل

الكلمات والتقدير والعرفان إلى من زينت حياتي بأزهار الحنان ، إلى التاج الذي وضع فوق

رأسي إلى أوفى خلقي الله وأحبهم إلى قلبي أمي الغالية "صباح"

إلى أعز كنز في حياتنا إلى تاج رأسي واعتزازي إلى قدوتي في الحياة أبي الغالي "ناصر"

إلى قرة العين ونبض القلب إخوتي الأعزاء :قطر الندى ،محمد إسلام،عبد الرؤوف.

إلى جدتي"حورية" وإلى روح جدتي "فتيحة " رحمها الله .

إلى صديقاتي ورفيقات دربي: بشرى، ملاك، ريمة، فريال، مهى، سميرة، زينب.

وفي آخر كلامي إهدائي إلى أساتذتي وجميع دفعة 2022 السلام عليكم ورحمة الله تعالى

وبركاته.

عز الدين كوثر

إهداء

"قل اعملوا فسير الله عملكم و رسوله و المؤمنين"

صدق الله العظيم

الحمد لله الذي أنعم علينا بنور العلم و أعاننا على إتمام هذا العمل المتواضع.

إلى من بلغ الرسالة ... و أدى الأمانة ... و نصح الأمة

سيدنا محمد صلى الله عليه و سلم

إلى من كلله الله بالهيبة و الوقار... إلى من أحمل إسمه بكل إفتخار ...أرجو من الله أن يمد في عمرك

والدي العزيز منصف

إلى سبب سعادتي منبع الحنان...إلى من قرأت في عينيها مستقبلي...إلى من كان دعاؤها سر نجاحي

أمي الغالية نورة أطال الله في عمرها

إلى مصدر فرحي

إخوتي الأعزاء : سارة ، رؤوف ، هاجر، محمد ، مريم ، و بسمة الأخت التي لم تلدها أمي

إلى كل أهلي و أقاربي

إلى من صادقتهن فصدقن :كوثر، إيناس ، سارة

إلى كل إنسان عزيز على قلبي

إلى جميع زملاء الدراسة، و إلى كل أساتذة كلية الحقوق، إلى كل هؤلاء أهدي ثمرة جهدي المتواضع.

عبد المومن بشرى أية

مقدّمة

مقدمة

قدم الحاسب الآلي والإنترنت للبشرية الرقي في جميع مناحي الحياة، غير أن هذا التقدم المذهل واكبه من جهة أخرى تطور الفكر والعقل البشري الاجرامي، مما أدى الى إفراز أنواع جديدة من السلوك الإجرامي تمثل في ظهور ما يسمى بالجريمة الإلكترونية، حيث أدت إلى حدوث خسائر فادحة غير مسبوقة، لضحايا هذا النوع من الجرائم وقد تعددت مظاهر الإعتداءات حيث قد تتمثل في امكانية الولوج الى الحاسب وتدمير برامجها أو إتلافها أو تزويرها، كما قد تكون في شكل الاستغلال غير المشروع لبطاقات الائتمان، أو حتى الاعتداء على الاشخاص عبر الانترنت بالقذف والسب، وإفساد الاخلاق والاستغلال الجنسي للاطفال، وكذلك الاعتداء على الأموال عبر الانترنت، عن طريق التحويل الإلكتروني غير المشروع للأموال، و إتلاف نظم المعلومات، بل أكثر من ذلك ساهمت هذه النوع من الجرائم في تطوير سبل ارتكاب الجرائم التقليدية كالقتل والسرقة والتجارة بالاعضاء البشرية و الارهاب و التجسس.

وقد وضعت الجرائم الإلكترونية نظرا لطبيعتها لخاصة كونها غير مادية وترتكب من طرف أشخاص غير عاديين، ومن ثم يصعب على القائمين على التحريات والتحقيقات الجنائية الكشف عن تلك الجرائم و إثباتها نظرا للسرعة والدقة العالية في تنفيدها وكذا إمكانية محوها و تمويه آثارها وإخفاء الأدلة المتحصلة منها عقب تنفيذها، الأمر الذي استلزم على على التشريعات في مختلف الدول مواكبة هذا التطور بتعديل قانون الاجاءات الجزائية أو استحداث قانون خاص يضمن توفير القواعد الاجرائية تختلف عن تلك المتبعة في الجرائم التقليدية، التي يمكن من خلالها لجهات البحث والتحري الوصول إلى الدليل المناسب لاثبات الجريمة الالكترونية.

في هذا السياق ورغبة من المشرع الجزائري في مكافحة فعالة للجريمة الإلكترونية، تبنى أساليب جديدة للتحري، من خلال: تعديل قانون العقوبات بموجب القانون رقم 06-22 بتاريخ 20 ديسمبر 2006 عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وفي سنة 2009 أصدر المشرع الجزائري القانون رقم 09-04 المؤرخ في 05 أوت سنة

2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، في هذا القانون خلق المشرع آليات جديدة خاصة للتحري من أجل مكافحة الجريمة الإلكترونية.

أهمية موضوع الدراسة:

يعد موضوع البحث من الموضوعات الجديدة والمهمة في إطار القسم الإجرائي من القانون الجزائي وهو من موضوعات التي لا تزال حديثة ولم تنل حظها من البحث والتمحيص على مستوى الفقه الجزائي، إذ أن أغلب الدراسات المنشورة في مجال الجريمة الالكترونية، اقتصرت على البحث في الجوانب الموضوعية لها دون محاولة الغوص في مسالة إثباتها و التحرى فيها.

كذلك إذا كانت الجرائم الالكترونية تعد من الأنماط الاجرامية التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات عن بعد، فهي تعتبر أيضا من المستجدات التي لم تكن معروفة للقانون الجزائي سواء الموضوعي أو الاجرائي، فمن دون شك أن أي محاولة للتعامل إجرائيا معى هذا النمط الاجرامي في إطار عملية البحث والتحري سوف يخلق اشكالات إجرائية للاجهزة المكلفة بهذه العملية وعليه ينبغي أن تأتي الدراسات القانونية عليها بالشرح والتحليل، ومن هنا تأتي أهمية الموضوع الذي حاولنا من خلاله مناقشة المفاهيم القانوينة المتعلقة بالجرائم الالكترونية.

كذلك تم اختيار هذا الموضوع لأهميته فى الوقت الحالى، حيث ترجع الأهمية لإنتشار الجرائم الإلكترونية وشدة تأثيرها على الأفراد والمؤسسات والدولة وصعوبة تطبيق القواعد الإجرائية فى الجرائم التقليدية على هذه الجرائم المستحدثه.

أسباب اختيار الدراسة:

بالنسبة للأسباب الذاتية فقد وقع اختيارنا لهذا الموضوع لعدة اسباب ذاتية تتمثل في:

– الرغبة الشخصية الملحة في دراسة جوانب الموضوع وتبيان أهم الخصوصيات التي يمتاز بها اجراء التحري في الجرائم الالكترونية، خاصة وأن هذا الموضوع يدخل في صميم القانون الجنائي في شقه الاجرائي والذي أحببناه مند دراستنا له في السنة الثانية ليسانس مع الأستاذ المشرف.

– قناعتنا الخاصة كطالبتين في القانون بضرورة وجود دراسة كثيرة لتوضيح خصوصيات التحري في مواجهة الجرائم الالكترونية باعتبار هذه الاخيرة جرائم مستحدثة تستدعي دراستها، و التطرق للموضوع بصيغة متخصصة في كل وقت مواكبة لتطور هذه الجريمة الذي لا يتوقف ويستمر باستمرار تطور الوسائل التكنلوجية المستعملة.

– الرغبة الخاصة في نشر الوعي و إثراء المكتبة ببحث جديد متخصص قد يساعد باحثين آخرين في المستقبل في دراساتهم.

أما الدوافع والأسباب الموضوعية: فلم تكن وليدة الصدفة بل لحداثة الموضوع، كونه يصب حول ما أحدثته التكنولوجيا الحديثة من تطور وتغير في المنظومة القانونية الأمر الذي يحتم الدراسة وتعميق المعرفة في مجال التحري في مجال في الجرائم الالكترونية، من خلال إبراز أهم خصوصياته لمواجهة هذا النوع من الاجرام، من حيث التطرق لاهم عناصر الجريمة الالكترونية وأساليب التحري فيها ودور الاجهزة المختصة في حسن سيره وأهم الآليات الإجرائية في مجال التحقيق والتحري في هذه الجرائم.

أهداف الدراسة:

يتمثل الهدف الأساسي من الدراسة من محاولة المساهمة في التعرف على طرق التحري و التحقيق في هذا النوع من الجرائم، ذلك أن جدة وحداثة الجرائم الالكترونية وما تسسم به من خصائص سوف يجد معه المحقق نفسه في حيرة امامها وكيفية التعامل مها وأسلوب التحقيق فيها، إذ لاشك أن إجراءات التحقيق وجمع الأدلة بخصوص هذه الجرائم يختلف عما هو الحال عليه الجرائم التقليدية.

إشكالية الدراسة:

تعتبر الجريمة الإلكترونية من الجرائم المستحدثة في عالمنا المعاصر، وبتطور الجريمة كان لزاما على التشريعات الإجرائية ومنها المشرع الجزائري تطوير إمكانيات رجال البحث والتحري لمكافحة هذا النوع من الجرائم.

والإشكالية التي نطرحها هنا هل استجاب المشرع الجزائري لهذه المبررات واستحدث في سبيل ذلك تشريعات جديدة لمعالجة آثار وانعكاسات التقنية المعلوماتية على اجراءات البحث والتحري ؟ وإلى أي مدى وفق المشرع في استحداث طرق إجرائية في سبيل البحث والتحري عن الجريمة الالكترونية ؟.

ويتفرع عن هذه الإشكالية الرئيسية مجموعة من التساؤلات الفرعية تتمثل في ما يلي:

- ما المقصود بالجريمة الالكترونية ؟.
- بما تتميز الجريمة الإلكترونية عن غيرها من الجرائم ؟.
- ما هي الأجهزة الخاصة بالتحري عن الجريمة الإلكترونية ؟.
- ماهي أهم الإجراءات التقليدية والمستحدثة الخاصة بالتحري عن الجريمة الإلكترونية ؟.

منهج الدراسة:

تطلب منا البحث في موضوع الدراسة الاعتماد على مجموعة من المناهج منها ما هو أصلي ومنها ما هو ثانوي كلما استوجب منا البحث ذلك، لإثراء جوانب الدراسة.

حيث اعتمدنا على المنهج الوصفي كأساس من خلال قيامنا بوصف ظاهرة الجريمة الالكترونية وتحديد بعض المفاهيم التي تقوم عليها، وكذا قيامنا بوصف المفاهيم الخاصة بالاجراءات المستعملة في استخلاص الدليل.

كذلك اعتمدنا على المنهج التحليلي حيث حاولنا في هذا البحث تحليل بعض المفاهيم والغوص في جزئياتها وطرحها بشكل من التفصيل لما بدا لنا من اهميتها.

كذلك اعتمدنا على المنهج المقارن من خلال التطرق إلى المعالجة التشريعية سواء الموضوعية أو الاجرائية على مستوى التشريعات المقارنة، كذلك مقارنة بعض المفاهيم التي اعتمدها المشرع الجزائري مع بعض التشريعات الاخرى كلما كان ذلك ممكنا.

تقسيم الدراسة:

للاجابة على إشكالية الدراسة ارتاينا اعتماد خطة ثنائية متوازنة تنقسم الى فصلين تسبقهما مقدمة وينتهي بخاتمة:

بحيث خصصنا الفصل الأول لدراسة الإطار النظري للتحري عن الجرائم الالكترونية، الذي يحتوي على مبحثين، حيث تناولنا في المبحث الأول ماهية الجريمة الالكترونية، أما المبحث الثاني فتناولنا الاختصاص بالتحري عن الجريمة الالكترونية.

أما الفصل الثاني من الدراسة خصصناه لدراسة إجراءات التحري في مكافحة الجريمة الالكترونية الذي يحتوي بدوره على مبحثين، تناولنا في المبحث الأول الاجراءات التقليدية للتحري عن الجريمة الالكترونية، أما المبحث الثاني تناولنا الاجراءات المستحدثة للتحري عن الجريمة الالكترونية.

الفصل الأول

الإطار النظري للتحري عن الجرائم الإلكترونية

الفصل الأول

الإطار النظري للتحري عن الجرائم الإلكترونية

تعتبر الجريمة الالكترونية من الجرائم المستحدثة في عالمنا المعاصر نظرا لارتباطها بالتكنولوجيا الحديثة، وبتطور الجريمة كان لزاما على التشريعات إيجاد آليات للتصدي لها ومن بينها تطوير إمكانيات رجال البحث والتحري لمكافحة هذا النوع من الجرائم.

ونظرا لحداثة الجريمة الإلكترونية وكذلك إجراءات التحري عنها وتطورها بشكل مستر لارتباطها بوسائل التكنولوجية الحديثة ما سبق القول؛ فمن الضروري أن تكون مختلفة عن غيرها من الجرائم التقليدية، مما جعل تحديد المقصود بها وكذلك إجراءات التحري عنها يكتنفه الغموض ومثار للجدل والبحث المستمر، لأجل ذلك فضلنا البحث في ماهية الجريمة الإلكترونية كظاهرة مستحدثة، ثم التطرق إلى المقصود التحري عن هذه الجريمة، والتعرف على السلطات أو الأجهزة المختصة التي تتولى التحري والتحقيق في هذه الجريمة وعليه سوف نقسم دراستنا لهذا الفصل إلى مبحثين على النحو التالي:

المبحث الأول: ماهية الجريمة الالكترونية.

المبحث الثاني: الاختصاص بالتحري عن الجريمة الالكترونية.

المبحث الأول

ماهية الجريمة الالكترونية

بالرغم من الايجابيات التي جاءت بها الثورة التكنولوجية الحديثة في مختلف المجالات إلا أنه صاحبها مجموعة من السلبيات المتمثلة أساسا في الاستغلال السيئ للأنظمة المعلوماتية ما أدى إلى ظهور نمط جديد من الجرائم يسمى الجرائم الالكترونية التي يعتمد فيها الجاني على الوسائل الالكترونية، ونظرا لحداثة هذا النوع من الإجرام لا يزال يكتنفه الغموض في العديد من جوانبه القانونية.

وعليه لمعرفة ماهية الجريمة الالكترونية سوف نقسم دراستنا في هذا المبحث إلى مطلبين، نتناول في المطلب الأول مفهوم الجريمة الإلكترونية، أما في المطلب الثاني أركان الجريمة الإلكترونية.

المطلب الأول

مفهوم الجريمة الالكترونية

الجريمة الالكترونية بوصفها ظاهرة إجرامية ذات طبيعة خاصة صعبت من جهود الفقه وكذلك على رجال القانون الجنائي من التوصل إلى اتفاق حول مصطلح دقيق يعبر عن هذه الظاهرة حيث ظهرت تعابير كثيرة حول تعريف الجريمة الالكترونية ما بين مضيق لمفهومها وموسع كما تعددت المصطلحات المستخدمة للدلالة عليها وفيما يلي تفصيل لمفهوم هذه الجريمة حيث سوف نقسم دراستنا لهذا المطلب إلى فرعين، نتطرق في الفرع الأول إلى تعريف الجريمة الإلكترونية، أما الفرع الثاني نتناول فيه خصائص الجريمة الالكترونية.

الفرع الأول

تعريف الجريمة الالكترونية

لقي البحث عن تعريف الجريمة الالكترونية اهتمام الفقهاء والمختصين في مجال القانون من أجل وضع تعريف لها، وسوف نتطرق إلى التعريف الفقهي أولا، ثم التعريف التشريعي للجريمة الإلكترونية ثانيا، وذلك على النحو التالي:

أولا: التعريف الفقهي للجريمة الإلكترونية

وجدت عدة اتجاهات لتعريف الجريمة الالكترونية، عرف الاتجاه الأول بالاتجاه الموسع، أما الاتجاه الثاني عرف بالاتجاه الضيق، بالإضافة إلى اتجاهات أخرى عرفت الجريمة الالكترونية بالاعتماد على معايير متعددة وسوف نتناول التعريف حسب كل اتجاه من الاتجاهات السابقة وذلك على النحو التالي:

1: الاتجاه المضيق لتعريف الجريمة الإلكترونية

يذهب أنصار هذا الاتجاه إلى حصر الجريمة الكترونية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، وأن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة تعد جرائم عادية تتكفل بها النصوص التقليدية للقوانين العقابية، وذلك على خلاف الجرائم التي يتوافر لها هذه المعرفة فهي التي تكون بحاجة إلى نصوص خاصة تتلاءم مع طبيعتها التي تختلف عن غيرها من الجرائم التقليدية[1].

ومن التعريفات التي وضعها أنصار هذا الاتجاه أن الجريمة الكترونية هي "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية ب قدر كبير لازما لارتكابه من ناحية ولملاحقته وتحقيقه من

[1] نائلة عادل محمد فريد قورة، "جرائم الحاسب الآلي الاقتصادية" ، ط 01، منشورات الحلبي، بيروت، 2005، ص 30.

ناحية أخرى"[1]، وفي هذا الاتجاه أيضا عرفها الفقيه **دافيد تومسون** أنها: "أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"[2].

وفي هذا الاتجاه أيضا عرفها جانب من الفقه بالنظر إلى معيار نتيجة الاعتداء، إذ يرى الأستاذ **ماس** أن المقصود بالجريمة الكترونية هي: " الاعتداءات التي ترتكب بواسطة المعلوماتية بغرض تحقيق"، كما عرف الأستاذ" **باركر**" الجريمة الكترونية بأنها: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنها خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل"[3].

2: الاتجاه الموسع لتعريف الجريمة الالكترونية

على عكس الاتجاه السابق فإن أنصار هذا الاتجاه يذهبون إلى التوسيع من مفهوم الجريمة الالكترونية باعتبار أن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يصبغ عليه وصف الجريمة الالكترونية.

فيذهب فريق من الفقهاء إلى تعريف الجريمة الالكترونية بأنها كل سلوك إجرامي يتم بمساعدة الحاسب الآلي، وفريق آخر يعتبرها أنها كل جريمة تتم في محيط الحاسبات الآلية، ومن هذه التعريفات ما جاء به الفقيه" **ميروي**" الذي يرى أن الجريمة الكترونية تتمثل في الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي[4].

---

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص 28.

2 رشيدة بوكر، "جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري والمقارن"، ط 01، منشورات الحلبي الحقوقية، لبنان، 2012 ، ص 40.

3 نهلة عبد القادر المومني ، "الجرائم المعلوماتية"، دار الثقافة للنشر والتوزيع ، ط 02، عمان، 2010، ص48.

4 محمد أمين الشوابكة، "جرائم الحاسوب والانترنت (الجريمة المعلوماتية)"، ط 01، دار الثقافة للنشر والتوزيع،عمان، الاردن، 2009، ص8.

وفي ذات الاتجاه يرى كل من الفقيهين **"كريدو"** و**"ميشال"** أن الجريمة الالكترونية هي التي تسهل استخدام الحاسب كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته، كما تمتد لتشمل الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به[1].

وفي هذا الاتجاه أيضا عرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها الجريمة التي تلعب فيها بيانات الكومبيوتر والبرامج المعلوماتية دورا رئيسيا[2].

وهناك اتجاه فقهي آخر عرفها بالقول أن الجريمة الكترونية كل سلوك غير مشروع وغير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها[3].

كما عرفها الفقيهين **"ريشارد توتي"** و **"أنطوني هاردكاستل"** وعلى أنها الجرائم التي يكون للحاسب فيها دورا إيجابيا أكثر منه سلبيا[4].

3: اتجاهات أخرى لتعريف الجريمة الالكترونية

بالإضافة إلى الاتجاهين السابقين هناك اتجاهات عرفت الجريمة الإلكترونية حيث اعتمدت على معايير أخرى نذكر منها ما يلي:

أ: تعريفات تسند إلى موضوع الجريمة

[1] هلالي عبد الإله أحمد، "التزام الشاهد بالإعلام في الجرائم المعلوماتية (دراسة مقارنة)" ط 01، دار النهضة العربية، القاهرة، 2000، ص 14.

[2] خالد عياد الحلبي، "اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت"، ط 01 ، دار الثقافة، الاردن، 2001، ص 30.

[3] وضع هذا التعريف من طرف مجموعة من خبراء منظمة التعاون والتنمية في اجتماعها في باريس عام 1983 ضمن حلقة الإجرام المرتبط بتقنية المعلومات.

[4] محمد سامي الشواء، "ثورة المعلومات وانعكاساتها على قانون العقوبات"، ط 01، دار النهضة العربية ، القاهرة، 1994، ص 06.

يرى أصحاب هذا الاتجاه أن الجريمة الالكترونية ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع على النظام أو داخل نطاقه، ومن أنصار ذلك التعريف **"روزن بلات"** الذي عرف الجريمة الالكترونية بأنها "شاط غير مشروع موجه لنسخ أو تغير أو حدف أو الوصول للمعلومات المخزنة داخل النظام أو التي تحول عن طريقه"[1].

وهي حسب تعريف **"أرتور سوبك"**، " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات"[2].

ب: تعريفات تستند إلى وجوب إلمام الفاعل بتقنية المعلومات

يستند أصحاب هذا الاتجاه إلى معيار شخصي، يستوجب أن يكون الفاعل ملما بتقنية المعلومات واستخدام الحاسب الآلي، حيث عرفها **"ستريت سكتوبر"** أنها "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية عند المرتكب"[3].

كما عرفها **"دافيد تونيسون"** بأنها: "جريمة تتطلب لاقترافها توافر المعرفة بتقنية النظام المعلوماتي لدى فاعلها"[4].

كما عرفتها منظمة الأمم المتحدة في مؤتمرها العام لمنع الجريمة ومعاقبة المجرمين المنعقد بفينا سنة 2000 بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية[5].

[1] أحمد خليفة الملط، "الجرائم المعلوماتية"،ط 02 ، دار الفكر الجامعي، الاسكندرية، 2006، ص 85-86.

[2] خالد عياد الحلبي، المرجع السابق ، ص28.

[3] سميرة معاشي، "ماهية الجريمة الالكترونية"، مجلة المنتدى القانوني،كلية الحقوق و العلوم السياسية ،جامعة محمد خيضر، بسكرة، العدد07،مارس 2018 ،ص277.

[4] أحمد خليفة الملط، المرجع السابق، ص86.

[5] محمد أمين الشوابكة، جرائم ، المرجع السابق، ص10.

ثانيا: تعريف التشريع الجزائري للجريمة الالكترونية

لم يشر المشرع الجزائري إلى المصطلح الجريمة الالكترونية، غير أنه عالج بعض أنماط هذه الجرائم وأطلق عليها تسمية "الجرائم الماسة بأنظمة المعالجة الآلية المعطيات" وذلك سنة 2004 أين أضاف قسما جديدا تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات ضمن قانون العقوبات، ليقوم بتعديلات فيما بعد سنة 2006، على كل من قانون العقوبات والإجراءات الجزائية، وسدا منه للفراغات القانونية وضع مجموعة ترتيبات في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، وأطلق على الجرائم الالكترونية "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال" حيث عرفها بموجب المادة الثانية منه على أنها "جرائم المساس بأنظمة المعالجة لآلية المعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية"، ثم وضع في الفقرة الموالية من نفس المادة المقصود بمنظومة معلوماتية المعطيات المعلوماتية والاتصالات الالكترونية.

الفرع الثاني

خصائص الجريمة الالكترونية

تشترك الجريمة الالكترونية مع غيرها من الجرائم التقليدية، كما تختص بمجموعة من الصفات وتنفرد بها عن الجرائم العادية، وعليه نتناول الخصائص المشتركة أولا، ثم الخصائص التي تنفرد بها الجريمة الإلكترونية ثانيا، وذلك على النحو التالي:

أولا: الخصائص المشتركة للجريمة الالكترونية مع الجرائم التقليدية

[1] قانون رقم 09-04 ،المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، الجريدة الرسمية للجمهورية الجزائرية، عدد 47، الصادرة بتاريخ 16 أوت 2009.

تشترك الجريمة الالكترونية مع الجرائم العادية في كونها خطيرة، وذات أضرار جسيمة، وفيما يلي تفصيل لذلك:

1: خطورة الجريمة الالكترونية

تتسم الجريمة الإلكترونية بخطورتها، وذلك لمساسها بالإنسان في فكره وحياته الخاصة كما تمس المؤسسات في اقتصادها، والبلاد في أمنها القومي والسياسي والاقتصادي، ومن شأن ذلك أن يضفي أبعادا خطيرة غير مسبوقة على حجم الأضرار والخسائر التي تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات، وقد بينت إحصائيات وفقا لتقديرات المركز الوطني جرائم الحاسب الآلي في الولايات المتحدة الأمريكية بأن الخسائر حوالي 500 مليون دولار أمريكي بينما قدرتها مصادر أخرى بـ 3 و5 بليون دولار في السنة[1].

2: الجريمة الإلكترونية جريمة ذات أضرار جسيمة

فالخسائر تتسبب فيها الجريمة الإلكترونية كبيرة، سواء تعلق الأمر بالخسائر المعنوية المرتبطة بالحياة الشخصية للأفراد والمتعلقة بعامل الثقة بين الأفراد والشركات، كما أن الأضرار المادية التي تنجم عن الجريمة الإلكترونية غالبا ما تكون مرتفعة جدا كتلك التي تلحق بالمؤسسات المالية والاقتصادية بل وحتى المؤسسات العسكرية والمؤسسات الصحية كالمستشفيات والمؤسسات الإعلامية كالقنوات التلفزيونية، فالتجسس الإلكتروني وسرقة التكنولوجيا المعلوماتية وإذاعة الأسرار يكلف الدول والمؤسسات وحتى الأفراد أضرارا بليغة على المستوى المادي والمعنوي[2].

ثانيا: الخصائص التي تنفرد بها الجريمة الالكترونية عن الجرائم التقليدية

[1] سميرة معاشي، المرجع السابق، ص 281.

2 محمود أحمد عبابنة ، "جرائم الحاسوب وأبعادها الدولية"، ط 02، دار الثقافة للنشر والتوزيع ، عمان الاردن، 2009، ص 34

نظرا لارتباط الجريمة الالكترونية بجهاز الحاسوب، وشبكة الانترنت بصفة عامة، ووسائل التواصل الاجتماعي بصفة خاصة، فقد أصفى عليها ذلك مجموعة من الخصائص المميزة لها عن الجريمة التقليدية التقليدية، ومن هذه الخصائص ما يلي:

1- الحاسب الآلي هو أداة ارتكابها: فغالبا ما يكون الحاسب الآلي هو الأداة التي تمكن الشخص من الدخول إلى شبكة الانترنيت وقيامه بتنفيذ جريمته أيا كان نوعها[1].

2- ترتكب هذه الجرائم عبر شبكة الانترنيت أو عليها: تعد شبكة الانترنيت الحقل الذي تقع فيه الجريمة الإلكترونية، وذلك لأنها تمثل حلقة الوصل بين كافة الأهداف المحتملة لتلك الجريمة كالبنوك والشركات الصناعية وغيرها من الأهداف التي تكون غالبا الضحية لها[2].

3- الجريمة الكترونية عابرة للحدود: إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة وعمل على إزالة الحدود السياسة والجغرافية، والقدرة التي تتمتع بها أجهزة الكمبيوتر في نقل وتبادل كميات كبيرة من المعلومات وتخزينها ومعالجتها في وسط أنظمة معلوماتية بفضل منها آلاف الأميال قد أدت إلى إمكانية ارتكاب جرائم في دول معينة وتقع نتائجها في دولة أخرى[3].

4- الجريمة الإلكترونية صعبة الاكتشاف: فهي جريمة يصعب اكتشافها وإثباتها كونها تفتقر الدليل المادي الملموس، فغالبا ما ترتكب هذه الجريمة من قبل مجرم متميز عن المجرم التقليدي نظرا لما تمتاز به

1 محمد منير الجنيبهي وممدوح محمد، "الجوانب الإجرائية لجرائم الانترنيت والحاسب الآلي ووسائل مكافحهما"، ط 01، دار الفكر الجامعي، الإسكندرية، 2005، ص14.

2 نبيلة هبة هروال، "الجوانب الإجرائية لجرائم الانترنت"، ط 01 ، دار الفكر الجامعي، الاسكندرية، 2007 ، ص37.

3 أبو شامة عبد المحمود عباس، "عولمة الحرية الاقتصادية"،د ط ، غزة –المكتبة المركزية–قاعة عامة طالبات، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2007، ص 52.

من تقدم وتطور في مجال استخدام التقنيات الحديثة، فضلا عن إمكانية تدمير المعلومات التي يمكن استخدامها كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة[1].

5- الجريمة الإلكترونية جريمة ناعمة: الجريمة الكترونية من الجرائم الناعمة التي لا يتطلب ارتكابها استخدام الأدوات والعنف كما في غيرها من جرائم الإرهاب والسرقة والسطو المسلح، فمثلا نقل بيانات من حساب إلى حساب آخر أو السطو الالكتروني على أرصدة بنك ما لا يطلب المواجهة المباشرة مع موظفي وحراس البنك وإنما التواجد أمام الكمبيوتر واستخدام الذكاء البالغ من المخترق[2].

6- سرعة التنفيذ والتخلص من الدليل: الجريمة الالكترونية هي إحدى تلك الجرام التي يمكن أن تحدث في أجزاء من الثانية، لكن نتيجتها قد تكون أكبر من النتائج الناتجة عن التقليدية التي تقوم بها عدد أكبر من الأشخاص و بأدوات أكبر، ولن يكون من الممكن ضبطها والسيطرة عليها بشكل كامل ونهائي لأنها أسرع تطور من التشريعات ويرجع ذلك إلى التطور الرهيب لتكنولوجيا المعلومات[3].

المطلب الثاني

أركان الجريمة الإلكترونية

الجريمة الالكترونية كغيرها من الجرائم تقوم على مجموعة من الأركان العامة المتعارف عليها و يتعلق الأمر بالركن الشرعي و الركن المادي ، و أخيرا الركن المعنوي ، غير أن خصوصية هذه الجريمة جعلت تلك الأركان تتميز عن باقي أركان الجرائم التقليدية، كما أن خصوصية هذه الجريمة و المتمثلة في ظروف وقوعها على نظام المعالجة الآلية للمعطيات جعلت الفقه يشترط لقيامها إضافة إلى الأركان العامة سالفة الذكر ركنا مفترضا يتعلق بضرورة وقوعها على نظام المعالجة الآلية للمعطيات.و عليه

[1] رفعي سمير، "البحث والتحري عن الجريمة الالكترونية"، ط 01، دار المثقف للنشر والتوزيع، الجزائر، 2019، ص 24.

[2] محمد خليفة، "خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها"، مجلة دراسات وأبحاث،كلية الحقوق و الاداب و العلوم الاجتماعية ، جامعة 08 ماي 45 قالمة ، العدد 01، سبتمبر 2009، ص 375.

[3] رفعي سمير، المرجع السابق، ص25.

سوف نتناول في هذا المطلب الركن المفترض للجريمة الالكترونية في الفرع الأول، أما في الفرع الثاني نتناول الأركان العامة لهذه الجريمة

الفرع الأول

الركن المفترض للجريمة الإلكترونية

يتمثل الركن المفترض لقيام هذه الجريمة في تواجد نظام معالجة آلية للمعطيات وهو ما سنتعرض إليه أولا، إضافة إلى ضرورة توافر حماية للمعطيات و هو ما سنتطرق إليه ثانيا.

أولا: وجود نظام معالجة آلية للمعطيات

هو عبارة عن مجموعة من الوحدات والأجهزة والبرامج التي تعمل مجتمعة بغية التوصل إلى معالجة المعطيات آليا وإخراجها أو تخزينها واسترجاعها عند الحاجة[1].

وقد قامت الاتفاقية الدولية للإجرام المعلوماتي بتعريف النظام المعلوماتي على أنه[2]: "يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات صلة بذلك، ويقوم إحداهما أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات".

ويقصد بـ "بيانات الكمبيوتر" أية عملية عرض للوقائع، أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر، بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها.

فنظام المعالجة الآلية للمعطيات هي عبارة عن مجموعة العمليات التي تتم آليا –أي باستخدام الحاسب الآلي– وتتعلق بالتجميع والتسجيل والإعداد والتعديل والاسترجاع والاحتفاظ ومحو

[1] بلال أمين زين الدين، "الجريمة المعلوماتية في التشريع المقارن والشريعة الإسلامية"،د ط، دار الفكر الجامعي، مصر، 2014، ص 264.
[2] أمال قارة، "الحماية الجزائية للمعلوماتية في التشريع الجزائري" ، ط01، دار هومة للطباعة والنشر، الجزائر، 2006، ص 102.

المعلومات الاسمية، ومجموعة العمليات التي تتم آليا بغرض استغلال المعلومات وخصوصا عمليات الربط والتقريب وانتقال المعلومات الاسمية ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومات ذات دلالة خاصة[1].

ويكون نظام المعالجة الآلية للمعطيات في طور التشغيل عند إرسال إشارة كهربائية نحو وحدة المعالجة المركزية، والتي تقوم بدورها بإرسال البرنامج المسؤول عن تشغيل ذاكرة القراءة، هذه الأخيرة تقوم بالبحث عن المعطيات التي تسمح بتشغيل النظام المسؤول عن البحث، ثم تقوم بتسجيلها في ذاكرة القراءة والكتابة التي تقوم بمتابعة المراحل اللاحقة[2].

ثانيا: ضرورة خضوع النظام للحماية.

يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية المعطيات المتنقلة عبر الشبكات، وبالأخص حاليا شبكة الانترنت فهم يسعون لتأمين سرية الرسائل الإلكترونية وسرية المعطيات المتناقلة وخاصة بأعمال التجارة الرقمية، ويمثل التشفير أفضل وسيلة للحفاظ على سرية المعطيات المتناقلة، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الإطلاع على الرسائل الإلكترونية[3].

ويستوي في ذلك النظام أن يكون محميا بأسلوب معين –مثل كلمة السر– أو غير محمي[4].

ولقد انتقد هذا الرأي من جانب آخر من الفقه على أساس أن النظام الأمني للنظم المعلوماتية هو في الأهمية بالنسبة إلى شركات التأمين، والتي تضع حدا أدنى من الحماية الذي لا يمكن النزول عنه من قبل مستخدمي النظام المعلوماتي، حيث يؤدي التقصير في ذلك إلى تحمل شركات التأمين خسائر

[1] محمد أحمد عبابنة، المرجع السابق، ص 83.

[2] نائلة عادل محمد فريد قورة، المرجع السابق، ص331.

[3] أمال قارة، المرجع السابق، ص 103.

[4] شيماء عبد الغني محمد عطا الله، "الحماية الجنائية للتعاملات الالكترونية"، د ط، دار الجامعة الجديدة، مصر، 2007، ص 101 .

فادحة، وتعويضات جمة نتيجة المطالبات القضائية التي تتعلق بتعويض الخسائر الناشئة عن الاعتداء على الأنظمة المعلوماتية.

وبالتالي كان من الأولى يعطي القانون الجنائي حماية أكثر من تلك التي توليها شركات التأمين للأنظمة المعلوماتية، ولا يتسنى ذلك إلا باشتراط أن تكون هذه النظم مشمولة بالحماية من قبل أصحابها ضد التسلل إليها، أو الولوج والبقاء في محتوياتها أو ارتكاب أي من الأفعال الإجرامية المعلوماتية الأخرى، ولهذا كان على القانون الجنائي أن يلزم مستخدمي أو مالكي النظم المعلوماتية بوضع أي من الأطر الحمائية لأنظمة المعالجة الآلية للمعطيات الخاصة بهم، والتي تتناسب مع قدر وأهمية ما تحتويه من معلومات وأسرار[1].

الفرع الثاني

الأركان الأساسية للجريمة الالكترونية

الجريمة الالكترونية لا تختلف عن غيرها من الجرائم، إذ تتطلب لتحققها الأركان المتفق على ضرورة توافرها في أية جريمة لكي تتواجد على أرض الواقع، وهي الركن الشرعي ، الركن المادي ، والركن المعنوي، وهو ما سوف نتناوله تباعا كما يلي:

أولا: الركن الشرعي

[1] بلال أمين زين الدين، المرجع السابق، ص ص 256-266.

الركن الشرعي هو نص التجريم الذي يجرم الفعل ويعاقب عليه[1]، وذلك تأسيسا على أول مبدأ في قانون العقوبات وهو مبدأ الشرعية الذي يقضي بأن "لا جريمة ولا عقوبة أو تدابير أمن بغير قانون."

ولقد خصص المشرع الجزائري منذ تعديل 2004 وتبعته تعديلات 2006 القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات والذي يندرج ضمن الباب الثاني الجنايات والجنح ضد الأفراد، الفصل الثالث الجنايات والجنح ضد الأموال وذلك في المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري.

بالنسبة إلى التشريع الفرنسي، تناول المشرع الفرنسي جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في الباب الثالث من القسم الثاني من قانون العقوبات الفرنسي وهي تضم المواد 1/323 إلى 7/323[2].

ثانيا: الركن المادي

إن تحديد الركن المادي في الجرائم المرتكبة عبر الانترنت يثير جملة من الصعوبات التي تفرضها طبيعة الوسط الذي تتم فيه الجريمة والمتمثل في الجانب التقني، وهذا ما يميز ركنها المادي، الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي أو الشبكة العالمية للانترنت، ومن هنا تبدأ التساؤلات التي تتعلق بداية النشاط التقي أو الشروع فيه ومكان البداية واكتمال الركن المادي، وأجزاء السلوك

[1] عبد الرحمان خلفي، "محاضرات في القانون الجنائي العام (دراسة مقارنة)"، موجهة لطلبة السنة الثانية حقوق ل م د، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2016-2017، ص 44.

2 علي عبد القادر القهوجي، "الحماية الجنائية لبرامج الحاسب الآلي"، د ط ، دار الجامعية للطباعة و النشر، مصر 1999، ص117.

الإجرامي المرتكب في العالم المادي، أو العالم الافتراضي وغيرها من التساؤلات التي تتعلق بطبيعة الجريمة حيث يعتبر الركن المادي للجريمة المظهر الخارجي لها فالقاعدة انه "لا جريمة دون ركن مادي"[1].

1- السلوك الإجرامي في الجرائم الإلكترونية: يتمثل النشاط أو السلوك العادي في جرائم الانترنت وجود بيئة رقمية واتصال بالانترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته ليس كل جريمة تستلزم وجود أعمال تحضيرية، إلا أنه يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الانترنت حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية[2].

ففي مجال التكنولوجيا المعلومات الأمر يختلف بعض الشيء فشراء برنامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

مجمل القول أن السلوك الإجرامي في الجريمة المرتكبة عبر الانترنت بربط بالمعلومة السرية داخل الحاسب الآلي أو انتهاك حرمة الأشخاص، والسلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب الآلي فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك[3].

2- النتيجة الإجرامية في الجرائم الإلكترونية: تثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة، فهل تقتصر على العالم الافتراضي، أم أن لها في العالم المادي؟، وهل تقتصر النتيجة على مكان واحد أو تمتد لتشمل دولا وأقاليم عدة؟

1 حمزة خضري و عشاش حمزة ، "خصوصية اركان الجريمة المعلوماتية" ، مجلة الدراسات القانونية و السياسية ، كلية الحقوق و العلوم السياسية ،قسم الحقوق، جامعة محمد بوضياف ، المسيلة ، المجلد 06 العدد 02، 2020، ص 174.

2 منصور بن صالح السلمي، "المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي"، رسالة ماجستير في العدالة الجنائية، كلية الدراسات العليا ،جامعة نايف العربية للعلوم الأمنية، ، الرياض، 2010، ص 74.

3 منصور بن صالح السلمي، المرجع نفسه، ص 76.

فعلى سبيل المثال إذا قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم أحد البنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة؟ هل هو توقيت بلد المجرم؟، أم توقيت بلد البنك المسروق؟، أم توقيت الجهاز الخادم في الصين؟.

إن تحديد رابطة السببية في مجال أضرار الانترنت يعد من المسائل الصعبة والمعقدة بالنظر إلى تعقيدات صناعة الحاسوب والانترنت متطور إمكانياتها وتسارع هذا التطور إضافة إلى تعدد وتنوع أساليب الاتصال بين الأجهزة الإلكترونية وتعدد المراحل التي تمر بها الأوامر المدخلة حتى تخرج وتنفد النتيجة المراد الحصول عليها كل ذلك سيؤدي حتما إلى صعوبة تحديد السبب أو الأسباب الحقيقية للإيماءات المرتكبة في هذه المسؤولية[1].

ثالثا: الركن المعنوي

يقوم الركن المعنوي الجريمة المرتكبة عبر الانترنت على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون كانتحال شخصية المزود غير الإنترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن توفر النتيجة الجريمة المترتبة على الأفعال السابقة، فكتب إرادة الحالي الصفة العربية من العمل المشروع التي يدين الشبه في ارتكابه وهو عالم بالآثار الصدارة الناشئة عنه[2].

يختلف الركن المعنوي في الجرائم الالكترونية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة اي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى

[1] منصور بن صالح السلمي، المرجع السابق، ص 68.

[2] خالد عياد الحلبي، المرجع السابق، ص ص 73- 74.

نظام الحاسب الآلي خطا أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي[1].

وفي جريمة الاحتيال الإلكتروني التي بدورها جريمة عمدية، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بتوعية العام والخاص، والمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه بينه إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع[2].

المبحث الثاني

الاختصاص بالتحري عن الجرائم الإلكترونية

الجريمة الالكترونية يرتكبها جناة ذوي صفات معينة أهمها الدراية الفنية بعمل الحاسب الآلي، وكلما تقدم الجاني في فهم تقنيات العمل في الحاسبات الآلية، وكيفية تصميم البرامج كلما استطاع أن يرتكب جريمته دون ترك أي آثار يمكن أن يستدل عليه من خلالها، هذا ما يصعب على المحققين و أجهزة التحري الكشف عن هاته الجرائم والقبض على مرتكبيها، وهذا الأمر جعل البحث والتحري عن هذا النوع من الجرائم يتميز بخصوصية كذلك بالنسبة للجهات المكلفة بالتحري عنها.

وعليه سوف نقسم دراستنا لهذا المبحث إلى مطلبين، حيث نتناول في المطلب الأول مفهوم التحري عن الجرائم الالكترونية، أما المطلب الثاني نتناول فيه السلطات المختصة بالتحري عن الجريمة الالكترونية.

المطلب الأول

[1] حنان ريحان مبارك المضحكي، "الجرائم المعلوماتية(دراسة مقارنة)" ،ط 01، منشورات الحلبي الحقوقية، بيروت، 2014، ص 107.
[2] أحمد خليفة الملط، المرجع السابق، ص 113-121.

مفهوم التحري عن الجرائم الإلكترونية

إن مسالة البحث والتحري في جرائم الكمبيوتر مسالة في غاية الاهمية و الصعوبة ولاسيما لاعتبارات التكوين العلمي و التدريبي والخبرات المكتسبة لرجال القانون والعدالة الجنائية، وحداثة هذه الجرائم وتقنياتها العالية التي تتطلب من القائمين بالبحث والتحري المام كاف بها ومنه سوف نتطرق لمفهوم التحري عن الجرائم الالكترونية من خلال فرعين، حيث نتناول في الفرع الأول تعريف التحري الجرائم الإلكترونية، أما الفرع الثاني خصائص الجرائم الإلكترونية.

الفرع الأول

تعريف التحري عن الجرائم الالكترونية

التحري لغة هو "من الفعل تحرى فيقال تحرى المكان أو الشيء أي عانيه وهو عمل أصيل لضباط الشرطة القضائية يعملون عليه بواسطة حواسهم والوسائل التقنية والمعلوماتية الحديثة التي تكوين تحت تصرفهم من أجل معاينة ومعرفة ملابسات الأشياء"[1].

أما اصطلاحا، فهو الإجراءات المتبعة وفقا للقانون والعمل المنظم الذي تقوم به أجهزة البحث والتحري الجنائي، وتكون هذه الإجراءات مشروعة، والهدف من ورائها جمع المعلومات والاستدلالات الصحيحة لاستقصاء ومعرفة الحقيقة، وأن يكون القصد منها كشف النشاط الإجرامي ومعرفة حقيقة الأشخاص وجوانب الفعل وآلية ارتكابه[2] باستخدام الوسائل التكنولوجية أو المعالجة للمعطيات للوصول إلى إدانة المتهم عن عدمه بعد جمع الأدلة القائمة على الجريمة[3].

[1] رفعي سمير، المرجع السابق، ص 21.

[2] الصبحي داوود سليمان، "إجراءات التحري والبحث الجنائي"، مجلة الدراسات الاسلامية ،كلية التدريب –قسم البرامج التدريبية– جامعة نايف العربية للعلوم الأمنية، الرياض، افريل 2009، ص 4.

[3] رفعي سمير، المرجع السابق، ص21.

كما يمكن تعريف التحري أو التحقيق الابتدائي في الجرائم المعلوماتية بأنه عمل قانوني يقوم به رجال الضبط القضائي المختصين في ضبط الجرائم المعلوماتية الرقمية للتحقيق في مدى صحة الاتهام الموجه بشأن واقعة جنائية معروضة عليها[1].

والثابت أن الدعوى الجزائية تمر بثلاث مراحل، كل مرحلة يتولاها جهاز محدد، أول مرحلة هي مرحلة البحث والتحري وجمع الاستدلالات وتسمى أيضا مرحلة التحقيق الأولي، ويتولاها جهاز الضبطية القضائية، والمرحلة الثانية في مرحلة التحقيق القضائي، ويكون من اختصاص قضاء التحقيق ممثلا في قاضي التحقيق وغرفة الاتهام، أما المرحلة الثالثة وهي مرحلة التحقيق النهائي ويكون عن طريق المحاكمة من طرف قضاة الحكم.

وما يهمنا في بحثنا في المرحلة الأولى مرحلة البحث والتحري التي نظمتها المادة 12 من قانون الإجراءات الجزائية الجزائري الواردة في الباب الأول من هذا القانون تحت عنوان "في البحث والتحري عن الجرائم" حيث نصت على أنه: "يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات..."[2].

الفرع الثاني

خصائص التحري عن الجرائم الكترونية

إن التحري عن الجرائم باعتباره يهدف إلى التنقيب عن الأدلة وكشف الحقيقة كان لزاما أن تحاط إجراءاته بسياج من الضمانات تكفل له السير الحسن، واهم هذه الضمانات السرية والتدوين،

[1] أوهابية عبد الله، "شرح قانون الإجراءات الجزائية (التحري والتحقيق)"، الجزء الثامن، ط 02 ، دار هومة، بوزريعة، الجزائر، 2004، ص308 وما بعدها.

[2] الأمر رقم 66- 155 المؤرخ في 18 صفر 1386 الموافق 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

كما تختص الجرائم الإلكترونية ببعض الخصائص عند التحري فيها وتتمثل في ضرورة وضع خطة للتحقيق، وكذلك تشكيل فريق للتحقيق، وهو ما نتناوله في ما يلي:

أولا: السرية

السرية والتي هي نقيض العلانية، والمقصود بها عدم السماح للجمهور بالدخول للمكان الذي يسري به التحقيق[1]، ولا يمكنهم الإطلاع على محاضر ومجريات التحقيق كما لا يسمح لوسائل الإعلام والاتصال بنشر مضمون محاضر التحقيق الذي قد ينتهي بإصدار قرار ألا وجه لإقامة الدعوى ولحماية الأدلة من العبث[2].

إلا أن هذه السرية نسبية، ذلك أنها لا تشمل أطراف الدعوى ولا محاميهم أو وكلائهم ويجد مبدأ السرية ما يبرره من خلال ضرورة حماية حقوق المتهم وصيانة سمعته ومنع التشهير به، كذلك من خلال الإبقاء على جهة التحقيق في منأى عن الضغط ومحاولات التأثير على سير التحقيق.

وقد اختلف في مسألة علانية التحقيق أو سريته فظهر اتجاهان:

1- الاتجاه المؤيد للعلانية: قرر هذا للاتجاه علانية التحقيق بالنسبة لعامة الناس ولأطراف الخصومة الجزائية ووكلائهم، ومثال ذلك قانون التحقيق الجنايات المصري السابق، فجعل الأصل علانية التحقيق والسرية هي الإستثناء لإحقاق الحق، كما أخذ به القانون البحريني 1966 والقانون السوداني 1984.[3]

[1] أوهابية عبد الله، المرجع السابق، ص 336.

[2] عمر بن إبراهيم بن حماد العمر، "إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي"، مذكرة ماجستير، كلية الملك فهد الامنية-مركز البحوث و الداسات-،جامعة نايف العربية للعلوم الأمنية، السعودية، 2009 ، ص22.

[3] الجو خدار حسن، "التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، دار الثقافة للنشر و التوزيع" ، دار الثقافة للنشر و التوزيع ، عمان، ط 01 ، 2011، ص11.

2- الاتجاه المؤيد للسرية: خلافا للرأي الأول جعل هذا الاتجاه التحقيق سري بالنسبة للعامة والخصوم على حد سواء، بمن فيهم المدعي عليه، وقد اعتمد هذا الاتجاه القانون الفرنسي القديم والحالي الذي أخذ بسرية إجراءات التحقيق كأصل وعلانيته كاستثناء بالنسبة للخصوم[1]، نفس الشيء بالنسبة للمشروع الجزائري الذي نص في المادة 11 من قانون الإجراءات الجزائية على "تكون إجراءات التحري والتحقيق سرية، ما لم ينص القانون على خلاف ذلك ودون إضرار بحق الدفاع..."

ثانيا: التدوين

ويقصد به قيام الجهة المختصة بالتحري بإثبات كل الإجراءات المتخذة خلال التحقيق، وذلك بكتابتها في محاضر رسمية وفق الشكل الذي حدده القانون[2].

للتدوين أهمية بالغة من خلال مساهمته في الحفاظ على كل تلك الإجراءات التي قام بها القائمين على التحقيق مع كافة الأطراف، سواء كانوا متهمين أو ضحايا أو شهود، فالتدوين حجة لكل الأطراف، لهم وعليهم وتتجلى أهميته كذلك في كونه يعد بمثابة ضمان لحقوق المتهم، ذلك أن القيام بكتابة كل ما صرح به المتهم من أقوال أثناء التحقيق وتثبيتهما كتابيا في محاضر دون زيادة أو نقصان يكرس نزاهة التحقيق.

وعلاوة على شرط الكتابة، نجد أن مختلف التشريعات أوجبت أن يتم التدوين بواسطة كاتب مختص وذلك تحت طائلة البطلان[3]، والعلة من ذلك هي تمكين قاضي التحقيق من التفرغ للقيام بعمله الفني المتمثل في التفكير واستعمال قدراته الذهنية، لذلك كان من غير اللائق إنقال كاهل قاضي التحقيق من خلال إلزامه بكتابة وتدوين التحقيق.

[1] الجو خدار حسن، المرجع نفسه، ص34-35.

[2] محمد علي سالم عياد الحلبي، "الوجيز في أصول المحاكمات الجزائية"، دار الثقافة، عمان، ط 01 ، 2009، ص147.

[3] محمد علي سالم عياد الحلبي، المرجع السابق، ص147.

كما أن وجود كاتب مختص من أجل كتابة المحاضر يبعد الشبهة عن قاضي التحقيق ويضفي صفة الصحة على الإجراء، وإلا نتج عن ذلك بطلان المحاضر أو اعتبارها محاضر استدلال فقط وليست محاضر تحقيق.

ثالثا: وضع خطة للتحقيق

يبدأ المحقق عليه عند تجميع الاستدلالات المتعلقة بالجريمة الإلكترونية بوضع خطة العمل اللازمة على ضوء المعلومات المتوافرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق[1]، وذلك على النحو الآتي:

- وضع الخطة المناسبة والتي لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الحظر ووضع التصورات الكفيلة للتصدي للجريمة.
- التخطيط الفني للتحقيق وذلك للوصول إلى أفضل الطرق والأساليب للتعامل مع هذه الجرائم بالتفصيل والوضوح.
- عمل دراسة واقية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في التحقيق.
- تنسيق جهود الفريق القائم بالتحقيق لتسهيل صفتهم وغلهم وتقليل الآثار السلبية والإسراع في إنجاز العمل وهو ما يؤدي إلى ضمان مستوى جيد من الأداء.
- تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطاء الفردية التي قد تنتج، قلة الخبرة أو نقص المعرفة.[2]

[1] محمد بن نصير محمد السرحاني، "مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت"، مذكرة ماجستير، كلية الدراسات العليا ،قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 72.

[2] محمد بن نصير محمد السابق، المرجع السابق، ص 72.

رابعا: تشكيل فريق التحقيق

إن التحقيق الابتدائي في الجرائم الكترونية غالبا ما يكون أكبر من أن يتولاه شخص واحد بمفرده، حتى ولو كانت المضبوطات هي مجرد حاسب شخصي واحد، ولذلك يفضل التعاون بين عدة محققين في إنجاز التحقيق والعثور على الأدلة.

ويجب أن يتشكل فريق التحقيق من فنين وأخصائيين ذوي خبرة في مجال الحاسوب والانترنت، ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الالكتروني بشكل خاص[1].

وإن كان استخدام أسلوب عمل الفريق موجود في العديد من الجرائم، إلا أنه له أهمية خاصة في الجرائم المعلوماتية نظرا لما تتطلبه هذه الأخيرة من خبرات ومهارات فنية، وغالبا ما يتكون فريق التحقيق في هذا النوع من الجرائم من:

- التحقق الرئيسي يكون له خبرة في التحقيق الجنائي
- خبراء الحاسوب وشبكات الإنترنت من يعرفون حيثيات الحادث وطريقة التعامل مع هذه الجرائم.
- خبراء ضبط وتحرير الأدلة الرقمية.
- خبراء أنظمة الحاسوب الذين يعاملون مع الأنظمة البرمجية.
- خبراء التصوير والبصمات والرسم التخطيطي[2].

[1] عبد الله حسين علي محمود، "إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات"، المؤتمر العلمي الاول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، اكاديمية شرطة دبي ، دبي، 2003، ص612.

[2] عبد الله حسين علي محمود، المرجع السابق، ص 613.

أشار المشرع الجزائري إلى هذه المسألة حول إمكانية إستعانة الجهات المختصة بالتحري بالمختصين في مجال الحاسوب والنظم المعلوماتية، وذلك بهدف المساعدة في إنجاز المهمة والتزويد بالمعلومات الضرورية لذلك[1].

المطلب الثاني

السلطات المختصة بالتحري عن الجرائم الإلكترونية

نظرا لانتشار الجريمة الالكترونية بشكل ملفت للانتباه، ولأن أجهزة التحقيق في الجرائم التقليدية لم تكن كافية للتصدي لهذا النوع من الإجرام، وعليه فالمحقق التقليدي لم يعد يمكنه التعامل مع هذه الجرائم لما تنقصه من مهارات تقنية وكفاءة لمواجهته خصوصا أنها عابرة للقارات وقد يمتد أثرها إلى الأجهزة المعلوماتية الأخرى في إقليم آخر لذا تم التفكير في إنشاء أجهزة مخصصة لمثل هذا النوع من الجرائم سواء على المستوى الوطني أو الدولي، و هو ما سنتطرق اليه في هذا المطلب، لكن قبل التطرق لاقسام هذه الاجهزة كفرع ثاني ،سنتناول في الفرع الاول تعريف جهاز التحري عن الجريمة الالكترونية .

الفرع الأول

تعريف جهاز التحري عن الجريمة الالكترونية

إن أجهزة التحقيق في الجرائم الكترونية عبارة عن إدارة متخصصة يحكم وظائفها مبدأ التخصص والتميز الذي يكون فيه المعرفة الالكترونية وتطبيقا بسرعة وسرية عنصر أساسي لفاعلية التحقيق في الجرائم الالكترونية، ويكون لهذه الأجهزة تركية بشرية يتصل أفرادها وفقا لقواعد أمن

[1] أنظر المادة 5 الفقرة الأخيرة من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

المنشأة (أمن الأفراد، المعلومات وسائل الاتصال والتنقل) وذلك بهدف الحد من الجريمة وضبطها وضبط الأدلة الالكترونية[1].

ويلعب المحقق دورا هاما في حسن سير إجراءات التحقيق، من خلال إتسامه بالمعرفة الإلكترونية وتجاوزه للأخطاء المعلقة بتدوين الإجراءات أو بعدم الدقة أو إغفال إجراءات جوهرية في التحري، حيث يلتزم المتحري أو المحقق الابتدائي بالمحافظة على سرية التحقيق والسرعة في إجراءات جمع الأدلة والتعامل معها بدقة واحترافية[2].

الفرع الثاني

أقسام الأجهزة المختصة بالتحري عن الجرائم الالكترونية

لقد كان للتزايد المسمر للجرائم الالكترونية الأثر البالغ في ضرورة تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال الجريمة، ونتيجة لهذا التحدي قامت معظم الدول بإحداث أجهزة متخصصة بمكافحة هذا النوع من الإجرام المستحدث، تتولى مهمة التحري عن هذا النوع من الجرائم وكشف النقاب عنها، وقد حملت هذه الأجهزة تسميات مختلفة منها مثلا شرطة الانترنت أو فرقة التحري عن جرائم المعلوماتية إلى غير ذلك من التسميات، ولا يقتصر دور هذه الأجهزة على المستوى الوطني فقط، بل هناك أجهزة متخصصة على المستوى الدولي أيضا، وسوف نستعرض أهم هذه الأجهزة سواء على المستوى الداخلي أو الدولي وذلك كما يلي:

أولا: الأجهزة المختصة بالتحري عن الجرائم الالكترونية على المستوى الوطني

1 مصطفى محمد موسى، "التحقيق الجنائي في الجرائم الالكترونية"، ط 01، مطابع الشرطة، القاهرة، 2008، ص287.

2 ربيعي حسين،" اليات البحث و التحقيق في الجرائم المعلوماتية" ،اطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات و العلوم الجنائية ،كلية الحقوق و العلوم السياسية، جامعة باتنة 1 ، 2015-2016 ص 232

لقد أولت الجزائر أهمية وعناية بتطوير أجهزة التحقيق والتحري عن الجرائم الالكترونية لديها من أجل مواجهة هذه الأخيرة، لذا فقد أنشأت هيئات غير قضائية إضافة إلى الوحدات التابعة للأمن والدرك الوطني.

1: الهيئات غير القضائية المختصة بالتحري عم الجرائم الكترونية: وتمثل الهيئات غير القضائية المكلفة بالتحقيق في الجرائم المعلوماتية في:

أ: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

مواكبة مع التطورات التي عرفتها الجزائر في مجال تطور التقنية والتكنولوجيا، ولأنها ليست بمنأى عن الإجرام الالكتروني، باشر المشرع الجزائري إجراءات جديدة للمواجهة تضمنت إصدار القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وفي سبيل ضمان فاعلية التحري والتحقيق أنشأ المشرع الجزائري بموجب المادة 13 من هذا القانون الهيئة الوطنية للوقاية من الجرائم المتنقلة بتكنولوجيا الإعلام والاتصال، وترك تحديد تشكيلتها وتنظيمها وكيفيات سيرها عن طريق التنظيم، حيث نظمت هذه الهيئة وفقا لعدة مراسم، آخرها المرسوم الرئاسي 20-183 المؤرخ في 13 يوليو 2020[1]، حيث عرفت الهيئة بأنها: "سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة رئيس الجمهورية".

كان مقر الهيئة مقتصر في مدينة الجزائر في المرسوم الرئاسي لسنة2015، ثم أضيفت إمكانية تمديد مقر الهيئة إلى أي مكان آخر من التراب الوطني بموجب المرسوم الرئاسي لسنة 2019، وأبقى المرسوم الرئاسي لسنة 2020 على أن مقر الهيئة كأصل عام يحدد بمدينة الجزائر مع إمكانية نقل المقر

[1] مرسوم رئاسي رقم 20-183 مؤرخ في 13 جويلية 2020 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها جريدة رسمية عدد 40، الصادرة بتاريخ 18 جويلية 2020، ص5.

إلى أي مكان آخر من التراب الوطني، ويمكن الاختلاف بين المادة 03 في المرسومين الآخرين أن نقل مقر الهيئة في مرسوم 2019 كان بموجب قرار من وزير الدفاع الوطني وأصبح نقل مقر الهيئة إلى كامل التراب الوطني بموجب المرسوم الرئاسي الأخير يتم بموجب مرسوم رئاسي.

أ-1- مهام الهيئة: أبقى المرسوم الرئاسي لسنة 2020 على مهام الهيئة تحت رقابة السلطة القضائية، والمتمثلة في:[1]

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

- مساعدة السلطات القضائية المختصة ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

- تجميع وتسجيل وفقط المعطيات الرقمية للأنظمة المعلوماتية.

- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجريمة المتصلة بتكنولوجيا الإعلام والاتصال.

[1] أنظر المادة 04 من المرسوم 20-183 سالف الذكر.

- المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تحيين المعايير القانونية في مجال اختصاص الهيئة.

أ-2- تنظيم الهيئة: تتكون الهيئة من مجلس توجيه ومديرية عامة، وضعتا تحت السلطة المباشرة لرئيس الجمهورية:[1]

أ-2-1- مجلس التوجيه: أبقى المرسوم الرئاسي الجديد على نفس الصلاحيات الممنوحة لمجلس التوجيه بموجب المرسوم الرئاسي لسنة 2019، غير أنه عدل التشكيلة برئاسة رئيس الجمهورية، ويمكنه أن يفوض ممثله، حيث يتشكل مجلس التوجيه من الوزير المكلف بالعدل، الوزير المكلف بالداخلية، الوزير المكلف بالمواصلات السلكية واللاسلكية، وقام المرسوم بإضافة كل من المدير العام للأمن الوطني الداخلي ، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية وممثل من وزارة الدفاع الوطني. ويعين رئيس الجمهورية ممثلي رئاسة الجمهورية ووزارة الدفاع الوطني، هذا حسب ما جاء في المادة 06 من المرسوم 20-183 ، وأضافت المادة 8 من نفس المرسوم أن اجتماع مجلس التوجيه يكون في دورة عادية مرتين في السنة، بناءا على استدعاء من رئيسه، ويمكن أن يجتمع في دورة غير عادية في حالة الضرورة، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

أ-2-2- المديرية العامة: ويديرها مدير عام، تعينه أو إنهاء مهامه تكون بموجب مرسوم رئاسي، أسندت للمديرية العامة نفس الصلاحيات المنصوص عليها في مرسوم 2019، غير أن الاختلاف يكمن في أن المرسوم الجديد جعل من صلاحياتها مقيدة بوجوب موافقة مجلس التوجيه على مشروع ميزانية الهيئة وإعداد وتنفيذ برنامج عمل ا الهيئة، ووجوب رفع التقرير السنوي لنشاطات الهيئة لمصادقة

[1] أنظر المادة 05 من المرسوم الرئاسي رقم 20-183، سالف الذكر.

مجلس التوجيه، وتضم المديرية العامة:[1] مديرية المراقبة واليقظة الالكترونية، مديرية الإدارة والوسائل، مصلحة للدراسات والتلخيص، وأخيرا مصلحة للتعاون واليقظة التكنولوجية.

أ-3- سير الهيئة: أضاف المرسوم الرئاسي الأخير المواد من 21 إلى 30 والتي تنظم كيفيات سير الهيئة، وأهم ما جاء في هذه المواد:

- إضافة صلاحية مهمة للهيئة حيث تكلف حصريا بمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في الحين، والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.
- إمكانية طلب أي وثيقة أو معلومة ضرورية لإنجاز مهامها في أي جهاز أو مؤسسة أو مصلحة.
- إمكانية طلب المساعدة من الوزارات المعنية للأعوان العموميين المختصين في مجال تكنولوجيا الإعلام والاتصال.
- وجوب المحافظة على السر المهني.
- استعمال الوسائل والتجهيزات الالكترونية أو استيراد أو اقتناء أو حيازة لا يكون إلا من طرف الهيئة في حدود اختصاصها، أو عند الاقتصاد سلطة ضبط الاتصالات السلكية واللاسلكية، والمؤسسة العمومية المكلفة بشكات الاتصالات.
- تفتيش أي مكان أو هيكل أو جهاز بلغ إلى علم الجهات المختصة بأنه يجوز أو يستهل وسائل وتوجيهات موجهة لمراقبة الانتقالات الالكترونية.

ب: السلطة الوطنية لحماية المعطيات ذات الطابع شخصي

[1] أنظر المادة 11 من المرسوم الرئاسي رقم 20-183، سالف الذكر.

استحدث المشرع الجزائري بموجب القانون 18- 07[1] سلطة وطنية تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي، وهي عبارة عن سلطة إدارية مستقلة تتمتع بالشخصية المعنوية وبالاستقلال المالي والإداري تضمن عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة توضع لدى رئيس الجمهورية وذلك بهدف حماية المعطيات[2].

ب-1- مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: تتمثل مهامها فيما يلي:

- تلقى التصريحات المسبقة المتعلقة بمعالجة المعطيات ذات الطابع الشخصي: حيث تضمنت المواد من 13 إلى 16 من القانون 18-07 كل ما يخص إجراء التصريح الذي يجب أن يودع مسبقا لدى السلطة الوطنية، كما أن تقديم التصريح المسبق يكون بأي شكل من الأشكال، حيث يمكن تقديمه الكترونيا، وسيتم وصل إيداع أو يرسل فورا بالطرق الإلكترونية في أجل أقصاه 48سا.

- إخضاع المعالجة لنظام الترخيص: وقد تضمنت المواد من 17 إلى 21 من نفس القانون كل ما يخص نظام الترخيص، حيث لابد للسلطة الوطنية إذا بتين لها أن المعالجة محل التصريح تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص.

وبالرجوع إلى المادة 25/ 2 من القانون 18-07 فتتمثل بقية مهام هذه السلطة الوطنية في:

---

[1] قانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، عدد 34.

[2] إن إقرار إنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي إحدى أهم الآليات للحد من الفوضى التي سادت مجال استغلال المعطيات الشخصية للأشخاص الطبيعيين وضمانة أساسية لحماية البيانات الشخصية كما تضمن عدم المساس بالحياة الخاصة. أنظر غزال نسرين، حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 56، العدد 1، 2019، ص 106-138.

– **الإعلام وتقديم الاستشارات والاقتراحات اللازمة:** حيث تسهر السلطة على سلام الأشخاص المعنيين والمسؤولين من المعالجة بحقوقهم وواجباتهم، وتسهر على تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي، كذلك تقديم الاقتراحات.

– **تطوير علاقات التعاون مع السلطات الأجنبية المماثلة:** بشرط مراعاة مبدأ المعاملة بالمثل.

– **إصدار الأوامر:** حيث تأمر بالتغيرات اللازمة من أجل حماية المعطيات ذات الطابع الشخصي للمعالجة.

– **وضع معايير وقواعد السلوك والأخلاقيات:** التي تخضع لها معالجة المعطيات، إضافة إلى إصدار عقوبات إدارية وفقا لأحكام المادة 46 من نفس القانون.

– **تختص بالإعلام الفوري للنائب العام المختص:** في حالة معاينة وقائع تحتمل الوصف الجزائي

– **إعداد تقرير سنوي:** حيث تقوم السلطة الوطنية بإعداد تقرير سنوي حول نشاطاتها وترفعه إلى رئيس الجمهورية.

ج : وكالة أمن الأنظمة المعلوماتية

استحدثت منظومة وطنية لأمن الأنظمة المعلوماتية توضع لدى وزارة الدفاع، والتي تضمنها القانون 20-05[1]، وتتكون من المجلس الوطني لأمن الأنظمة المعلوماتية، والوكالة الوطنية لأمن الأنظمة المعلوماتية التي من بين مهامها إجراء التحقيقات الرقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية.

[1] مرسوم رئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية، عدد 04، الصادرة في 26 جانفي 2020.

وتعتبر وكالة أمن الأنظمة المعلوماتية مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلال المالي، يقع مقرها في مدينة الجزائر.

وتدير الوكالة لجنة توجيه وتزود بلجنة علمية، تتوفر على مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطة المدير العام الذي يسير بدوره الوكالة وسرعة تنسيق وتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنفيذ المخططات والبرامج المسطرة من قبل لجنة التوجيه[1].

2- الوحدات التابعة للأمن والدرك الوطني المختصة بالتحري عم الجرائم الالكترونية

إن الأجهزة التابعة للأمن والدرك الوطني تسهر على المواجهة التنظيمية للجرائم المعلوماتية والحفاظ على الأمن والنظام العام من خلال تنفيذ مهامهم كل في مجال اختصاصه.

أ: وحدات الأمن الوطني

تتولى المديرية العامة للأمن الوطني التحقيق في الجرائم الالكترونية عن طريق قسمين، يشمل القسم الأول المخابر ويشمل القسم الثاني الفرق، وهذا في إطار تجسيد سياسة أمنية فعالة، حيث تضع كافة الإمكانيات البشرية والتقنية المتاحة لديها للتصدي لكل أنواع الجرائم وبالخصوص تلك المستحدثة منها الجرائم الإلكترونية[2].

أ-1- المخابر: يوجد مخبر مركزي للشرطة العلمية في الجزائر العاصمة، ومخبر جهوي في قسنطينة و وهران[3]، وقد استحدثت أقسام متخصصة في تتبع الأدلة الرقمية من خلال استغلال أجهزة الكترونية

[1] أومدور رجاء، "خصوصية التحقيق في مواجهة الجرائم المعلوماتية"، أطروحة دكتوراه تخصص قانون خاص، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد البشير الابراهيمي، برج بوعريريج ، 2020-2021، ص 99.

[2] ربيعي حسين، المرجع السابق، ص 176.

[3] تجدر الإشارة أن هناك مخابر أخرى قيد الانجاز في ورقلة، بشار وتمنراست.

قصد استخراج ما من شأنه إفادة التحقيق ومساعدة العدالة في تقرير الأحكام في القضايا التي تكون من هذا النوع، وهي ثلاث أقسام:

- قسم استغلال الرقمية الناتجة عن الحواسيب والشبكات.
- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات.

وذلك بالاستعانة بأجهزة مادية للكشف عن الجرائم الإلكترونية[1]، أهمها:

- أدوات التخزين الرقمية، كأجهزة التصوير، بطاقات الذاكرة والأقراص الصلبة.
- أجهزة الكمبيوتر ولواحقها[2].

وحسب إحصائيات دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لحيز الأدلة الجنائية بقسنطينة، فقد شهد سنة 2004 ما يقارب 250 قضية محل تحقيق أبرزها تمس بأنظمة المعالجة الآلية للمعطيات، وسجلت في الثماني أشهر الأولى من سنة 2016[3] حوالي 570 قضية قيد التحقيق أغلبها تتعلق بسوء استخدام مواقع التواصل الاجتماعي من خلال قضايا المساس بالأشخاص عبر الانترنت بالصورة والابتزاز، القذف، والتشهير..[4]

أ-2- وجود فرقة على مستوى أمن كل ولاية: في سبيل ضمان نجاعة التحقيق في مواجهة الجرائم الالكترونية تم إنشاء ما يعرف بالمصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال،

[1] ربيعي حسين، المرجع السابق، ص177.

[2] حملاوي عبد الرحمن، "دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية"،مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق و العلوم السياسية ،قسم الحقوق، جامعة محمد خيضر بسكرة ، الموسوم بعنوان الجريمة الالكترونية بين الوقاية و المكافحة ،يومي 16-17 نوفمبر 2015، بسكرة ، الجزائر، ص08.

[3] موقع المديرية العامة للامن الوطني http:www.dgsn.dz : تاريخ الإطلاع: 2022/02/12، الساعة 20:00.

[4] ربيعي حسين، المرجع السابق، ص 181.

وهي مصلحة تابعة لمديرية الشرطة القضائية مقرها على مستوى الجزائر العاصمة، ثم أنشأت خلايا تابعة للفرق الاقتصادية والمالية على مستوى أمن الولايات، تشمل خلية مكافحة الجرائم المعلوماتية، ثم مع تطور الجرائم واعتماد Modem و3g، تم ترقية الخلية لتصبح فرقة في حد ذاتها، حيث أصبحت مستقلة وتابعة للفرق الولائية للشرطة القضائية، وتوجد فرق على مستوى كل ولاية، مهمتها التحقيق في الجرائم الكترونية وتعمل بالتنسيق مع هذه المخابر السالف ذكرها[1].

أ-3- دور المديرية العامة للأمن الوطني في مواجهة الجرائم الالكترونية

للمديرية العامة للأمن الوطني دور أساسي في مواجهة الجرائم الالكترونية وذلك من خلال دورها الوقائي والتحسيسي والردعي.

يتحلى الدور الوقائي من خلال عقد دورات افتراضية على مستوى شبكات المعلومات عموما مواقع التواصل الاجتماعي خصوصا، أما دورها التحسيسي يكون مثلا بالتنقل لمختلف المؤسسات التربوية، وتنظيم النشاطات و التحسيس حول سوء استعمال شبكات التواصل الاجتماعي أو سوء استخدام الانترنت.

وأخيرا دورها الردعي والذي يعتبر امتداد لدورها الوقائي في حالة الإخلال بالنظام العام، أو في حالة منشورات تمس النظام العام، حيث يتم التدخل وتحديد هوية صاحب الحساب واتخاذ الإجراءات القانونية، مع إنجاز ملف قضائي ضده.

ب: وحدات الدرك الوطني

[1] سعيد علي نعيم، "آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري"، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر باتنة، 2012-2013، ص107.

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العالم ومحاربة الجريمة بكافة أنواعها وبصفة خاصة الجريمة الالكترونية وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية، نذكر منها:[1]

ب-1- المعهد الوطني للأدلة الجنائية وعلم الإجرام: وهو جهاز تابع للدرك الوطني، أنشأ سنة 2004 بموجب المرسوم الرئاسي رقم 04-183[2]، يتكون من 11 دائرة متخصصة في عدة مجالات تضمن الخبرة والتكوين والتعليم وتقديم المساعدات التقنية والبحوث والدراسات والتحاليل في علم الجريمة.

حيث تختلف دارة الإعلام الآلي والالكترونيك بمعالجة تحليل وتقديم كل دليل إلكتروني وتماثلي للعدالة، كما تقدم مساعدة تقنية العامة للتحقيق في التحقيقات المعقدة.

يسهر أفراد الدائرة على تأمين اليقظة التكنولوجية من أجل تحيين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية لإنجاز المهام المنوطة بها تنقسم الدائرة إلى ثلاثة مخابر وكل مخير مزود بفصيلة مهمتها اقتناء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل :

- **مخبر الإعلام الآلي:** يختص بتحليل ومعالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش) ، كما يقوم بتحديد التزوير الرقمي للبطاقات البنكية.
- **مختبر الفيديو:** يختص بإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد، كما يعمل على تحيين توعية الصورة (فيديو، صورة) مختلف التقنيات، ومقارنة الأوجه وشرعية الصور والفيديو.

[1] ربيعي حسين، المرجع السابق، ص182-183.

[2] مرسوم رئاسي رقم 04 - 183 مؤرخ في 8 جمادى الأولى عام 1425 الموافق 26 يونيو 2004، يتضمن أحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطن وتحديد قانون الأساسي، الجريدة الرسمية للجمهورية الجزائرية، عدد 44، الصادر في 27 جوان 2004.

- **مخبر الصوت:** يختص بمعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية، ويعمل على تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة[1].

ب-2- مركز الوقاية من جرائم المعلوماتية ومكافحتها: وهو مركز تابع لأجهزة الدرك الوطني بدأ عمله منذ سنة 2004، والذي يكلف لمهمتين رئيسيتين:

- قبلية تتعلق بالتدقيق والوقاية.

- بعدية تتعلق بردع الجرائم الالكترونية بالتعاون مع مختلف مصالح الأمن والهيئات الوطنية[2].

عالج هذا المركز في الـ10 أشهر الأولى من سنة 2015 ما يقارب 240 قضية متعلقة بالجرائم الالكترونية، منها جرائم التهديد، المساس بالنظام العام، جرائم الاختراق، التحرش الجنسي بالقصر، إهانة هيئات ورموز وطنية...[3]

ب-3- المصلحة المركزية للتحريات الجنائية : تعد مصلحة تابعة لأجهزة الدرك الوطني، تقوم بالتحقيق التقني والعلمي، وهي هيئة ذات اختصاص وطني مهمتها التصدي للجريمة الالكترونية[4]، المرتبطة بتكنولوجيا الإعلام والاتصال.

إضافة إلى كل فصائل الأبحاث التابعة للدرك الوطني والمكلفة بالتحقيق في الجرائم الالكترونية.

---

[1] هواري عياش ،" المعهد الوطني الأدلة الجنائية مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية بين الوقاية والمكافحة" مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق و العلوم السياسية ،قسم الحقوق، جامعة محمد خيضر بسكرة ،يومي 16-17 نوفمبر 2015، بسكرة ، الجزائر، ص08.

[2] موقع وزارة الدفاع الوطني https://www.mdn.dz. تاريخ الإطلاع: 2022/02/12، الساعة 20:30.

[3] عز الدين عز الدين، "قيادة الدرك الوطني الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها"، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة الذي نظمته كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة بسكرة، يومي16-17 نوفمبر 2015، الجزائر، ص 29.

[4] ربيعي حسين، المرجع السابق، ص182.

ثانيا: الأجهزة المختصة بالتحري عن الجرائم الالكترونية على المستوى الإقليمي والدولي

تماشيا مع طبيعة الجريمة الالكترونية، فهناك مجموعة أخرى من الدول لم تكتف بتقوية السلطات الداخلية لها وإنما قامت كذلك بتوحيد جهودها من خلال إنشاء أجهزة إقليمية ودولية لإدراكها مخاطر الجريمة الالكترونية بوصفها جريمة عابرة للحدود تتعدى النطاق المكاني، ومن أهم هذه الأجهزة:

1- منظمة الشرطة الجنائية الدولية (الأنتربول): وهي أكبر منظمة شرطية دولية، أنشأت عام 1923، مكونة من قوات الشرطة، تضم 195 دولة[1] مقرها الرئيسي "ليون" فرسا وبها أربع لغات رسمية هي العربية الفرنسية الانجليزية والاسبانية، حيث يتبادل أعضاء الشرطة الدولية المعلومات من المجرمين الدوليين ويتعاونون فيما بينهم لمكافحة الجرائم المنظمة، كما تزود هذه المنظمة أعضاء الشرطة الدولية بالدعم الفني والميداني مختلف أشكاله، بفضل بنية تحتية دولية متطورة لمساعدتها على مواجهة التحديات المتنامية في مجال مكافحة أشكال الجريمة النامية كالجريمة الالكترونية.

يقوم برنامج الأنتربول بمكافحة الجرائم الالكترونية من خلال تحقيق مجموعة من الأهداف أبرزها:[2]

- تعزيز تبادل المعلومات بين الدول الأعضاء عن طريق الفرق العاملة والمؤتمرات الإقليمية.
- توفير دورت تدريبية لتنسيق العملية الدولية.
- توفير الدعم لأجهزة الشرطة على مدار الساعة.
- تقديم المساعدة للبلدان الاعضاء على تقديم الاشخاص الفارين و كشف المجرمين و تحديد مكان تواجدهم و توقيفهم.

ثانيا: مكتب الشرطة الأوربية (الأوروبول)

[1] إنتسبت الجزائر إلى منظمة الشرطة الجنائية الدولية الأنتربول عام 1963.
[2] ربيعي حسين، المرجع السابق، ص148.

هو جهاز على مستوى الاتحاد الأوروبي، أنشأ أول مرة من قبل ألمانيا أمام المجلس الأوربي سنة 1991، وتجسد فعليا سنة 1995 ومقرها في مدينة "لاهاي" بولندا. يعتبر الأوروبول أكبر الهيئات الاستشارية حول العالم في مجال الجرائم الالكترونية من خلال دعمه للحكومات والأجهزة الأمنية والمؤسسات في مسارها ضد أخطار الجرائم الالكترونية عن طريق تبادل المعلومات بتزويد المحققين بتحاليل علمية وإستراتيجية ودعمهم بالخبرات والمساعدات التقنية.

ويختص الأوروبول بالتحري عن الجرائم الكترونية خصوصا تلك المتعلقة بالاستغلال الجنسي للأطفال والإرهاب الالكتروني، ويهدف من خلال نشاطه إلى تسهيل الإجراءات أمام أجهزة الشرطة للدول الأعضاء للتحري بشأن الجرائم المتعلقة ببلدانهم، من خلال مدهم لمختلف النشرات الأمنية والتقارير حول المتهمين والأدلة المحصلة خارج الحدود الإقليمية لمجال اختصاصاتهم، لذلك تسهيل تبادل وتجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم التي في مجال الأوروبول ومنها الجريمة الالكترونية[1].

ثالثا: منظمة التعاون القضاء للاتحاد الأوربي (الأوروجست):

هو جهاز يعمل على المستوى الأوربي إلى جانب الأوروبول ويمهد له عمله، أنشأ سنة 2002 من قبل مجلس الإتحاد الأوربي، ويعد الأورجست وحدة التعاون القضائي، مهمتها الأساسية التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيقات ومباشرة متابعات جزائية، كما يعمل على تطوير آليات مكافحة الجريمة الكترونية من خلال تبادل المعلومات بصفة دورية مع محاكم الاتحاد الأوربي[2].

رابعا: رابطة رؤساء أجهزة الشرطة التابعة لرابطة أمم جنوب شرق آسيا (الأسيانابول):

[1] نبيلة هبة هروال، مرجع سابق، ص 158.

[2] سعيداني علي نعيم، مرجع سابق، ص 108.

تأسست بتاريخ 08-08-1967 رابطة دول جنوب شرق آسيا والتي تسمى اختصار بالأسيان أو ASEANA بالعاصمة التايلندية بانكوك، ويطلق عليه كذلك تسمية إعلان "بانكون" حيث ضم آنداك الدول الخمسة المنظمة له: تايلند، أندونيسيا، الفليبين، ماليزيا ،سنغفورة، ثم انقسمت لاحقا من بروناي سنة 1984، الفيتنام سنة 1995، لاوس وميانمار سنة 1997، وأخيرا الحمبوديا سنة 1999.

وسعيا منها لتكثيف التعاون الإقليمي فيما بينها وتطوير قدراتها من أجل مكافحة الجريمة الالكترونية، عمدت رابطة دول جنوب شرق آسيا لتقسيم قدرات كل دولة طرف فيها على كشف الجريمة الالكترونية والتحقيق فيها، ليتم فيما بعد التركيز على تقديم تدريب متخصص يتعلق بشبكة الانترنت وتحليل البرمجيات الخبيثة لما له من أهمية في موضوع التحقيق في الجرائم الكترونية.

خامسا: آلية الإتحاد الإفريقي للتعاون الشرطي (أفريبول):

تسمى أيضا منظمة الشرطة الجنائية الإفريقية، وهي منظمة تسهل تبادل المعلومات بين قوات الشرطة الوطنية بخصوص الجريمة الدولية والإرهاب والمخدرات والاتجار بالأسلحة في إفريقيا، وهي أكبر منظمة شرطة في القارة الإفريقية أنشأت في 13 ديسمبر 2015 في الجزائر خلال المؤتمر الإقليمي الإفريقي مكونة من قوات الشرطة بـ 41 دولة مقرها الرئيسي في أعالي بن عكنون بالعاصمة الجزائرية، لها خمس لغات أساسية هي: العربية، الانجليزية، الفرنسية، الإسبانية والبرتغالية.

وتهدف هذه الهيئة الإقليمية في المقام الأول إلى تعزيز وترقية التعاون بين أجهزة الشرطة للدول الأعضاء بالإتحاد الإفريقي، وذلك من أجل مكافحة الجريمة بكافة أشكالها بما فيها الجريمة الالكترونية[1].

[1] لزعر عزيز، زياني رشيد، آلية الإتحاد الإفريقي للتعاون الشرطي (الأفريبول) ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، كلية الحقو، جامعة مولاي الطاهر، سعيدة، المجلد 14، العدد 03، 2021، ص 254-256.

الفصل الثاني

إجراءات التحري في مجال مكافحة الجريمة الالكترونية

الفصل الثاني

إجراءات التحري في مجال مكافحة الجريمة الالكترونية

نتيجة التطورات المستمرة الحاصلة في مجال التكنولوجيا الحديثة وما صاحبها من عصرنة القطاعات والمؤسسات، و عصرنة الاتصالات والمواصلات، استدعى مواكبة التشريعات الداخلية لهذه التطورات لتجنب الجرائم المعاصرة ومن بينها الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، وأصبح على كل دولة اتخاذ التدابير التشريعية والإجراءات الضرورية لغرض التحري والبحث عن في الجرائم الإلكترونية.

وهو ما يؤدي بنا إلى التساؤل حول ما يتماشى مع طبيعة العالم الافتراضي خاصة وأن استخلاص الأدلة يحكمها قواعد إجرائية معينة كالمعاينة والتفتيش والخبرة والشهادة والتي تعد قواعد ذات نطاق عام صالحة لكل الجرائم، إلا أن تنظيمها للجرائم الالكترونية لابد أن يتناسب مع طبيعتها وخصوصيتها ، ومع طبيعة الدليل الذي يصلح لإثباتها وهو ما استدعى البحث عن درجة ملائمة القواعد الإجرائية التقليدية للتحقيق في الجريمة الإلكترونية ، مع كل الصعوبات التي تكتنف التوصل إلى الجرائم الالكنرونية ومرتكبيها خاصة مع سهولة محو آثار الجريمة وسرعة تدمير الأدلة الناجمة عنها لم تبق القوانين الإجرائية مكتوفة الأيدي وبقيت المحاولات مستمرة في سبيل في تخطي شبح الجرائم المعلوماتية وهو ما استدعى تدعيمها بإجراءات خاصة استحدثت لتتماشي مع خصوصية هذا النوع من الجرائم ومنه سوف نقسم دراستنا لهذا الفصل إلى مبحثين على النحو التالي:

المبحث الأول : الإجراءات التقليدية للتحري عن الجريمة الالكترونية.

المبحث الثاني : الإجراءات المستحدثة للتحري عن الجريمة الالكترونية.

المبحث الأول

الإجراءات التقليدية للتحري عن الجريمة الالكترونية

على الرغم من وجود اختلاف بين إجراءات التحقيق في الجرائم المعلوماتية وإجراءات التحقيق في الجرائم الأخرى، فهي جميعا تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش كما تشترك في كونها تسعى للإجابة على الأسئلة المشهورة لدى المحقق بهدف كشف الحقيقة بمساعدة الخبرة والشهادة التي تقود المحقق لضبط الدليل الرقمي، وتعتبر مرحلة ضبط الدليل النتيجة التي تعقب إجراءات البحث والتفتيش عن الدليل وكل هذه الإجراءات، سوف نتناولها من خلال مطلبين، نتطرق في المطلب الاول لاجرائي المعاينة و التفتيش لمسرح الجريمة، اما في المطلب الثاني الى اجرائي الخيرة و الشهادة في مجال الجريمة الالكترونية .

المطلب الأول

المعاينة والتفتيش لمسرح الجريمة

دفعت خصوصية الجريمة الالكترونية الى ابراز مكافحة اجرائية خاصة من الناحية القانونية والتطبيقية، كتلك التي تمس بالحياة الخاصة و من بين هذه الاجراءات التي سوف نسلط عليها الضوء في هذا المطلب ، اجراء المعاينة في الجريمة الالكترونية التي سنتطرق لها في الفرع الاول، أما في الفرع الثاني فسنتطرق الى اجراء التفتيش لمسرح الجريمة .

الفرع الأول

المعاينة في الجريمة الالكترونية.

أولا: تعريف المعانية

المعاينة بصفة عامة إجراء يتضمن وصف مكان بما فيه من أشياء[1]، مع الفحص الدقيق لكافة المحتويات بهدف كشف مخلفات وآثار الجاني بالمكان، والتي تشير إلى شخصيته وشركائه، وما يفيد في إثبات ارتكاب الجريمة وتوضح قدرا من الاستنتاجات التي تشكل في حد ذاتها الأساس الذي يقوم عليه التحقيق[2].

ويقصد بمعاينة مسرح الجريمة الالكترونية معاينة الآثار والبصمات الالكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت، وتشمل الرسائل المرسلة منه، أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسب الآلي والشبكة العالمية، أو التي من الممكن أن يطلق عليها البصمات المعلوماتية، وذلك مع ضرورة مراعاة مبدأ الشرعية والخصوصية المعلوماتية للأفراد ودون البحث في المحتوى إلا في حدود السلطات القصرية الممنوحة لجهات التحقيق[3].

ثانيا: مدى صلاحية مسرح الجريمة المعلوماتية للمعاينة

إذا كانت المعاينة في الجرائم التقليدية تتم في مسرح الجريمة العادي فإن الجريمة المعلوماتية تتم المعاينة فيها على مستويين.

---

[1] حازم محمد حنفي، "الدليل الالكتروني ودوره في المجال الجنائي"، ط 01، دار النهضة العربية، القاهرة، 2017، ص 55.

[2] فالمقصود من هذا الاجراء إثبات حالة الأمكنة والأشياء والاشخاص ووجود الجريمة، بمعنى آخر مشاهدة المكان الذي ارتكبت فيه الجريمة، وعمل وصف شامل له سواء بالكتابة أم التخطيط أم التصوير الشمسي أم الفيديو لاثبات حالته بالكيفية التي تركها بها الجاني، كما يشمل فصح جسم المجني عليه والمتهم، وبيان ما يوجد بهما من آثار وسماع أقوال الحاضرين أو كل ما يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبها، عليه فقد تسفر المعاينة–كالتفتيش–عن ضبط أدلة مادية تفيد في كشف الحقيقة، ولكن المعاينة إجراء لا يتضمن إكراها أو اعتداء على حرمة الأشياء أو الأشخاص(الحق في الخصوصية) ، كما أن التفتيش يستلزم الانتقال إلى المكان للبحث عن الأدلة، أما المعاينة فقد لا تتطلب ذلك أحيانا عندما يكتفي المحقق وهو في مقره بمعاينة الأشياء التي تم ضبطها، علاوة على ما تقدم ليس في النصوص ما يوجب حضور المتهم عند إجراء المعاينة، أما التفتيش فينبغي إجراؤه بحضور المتهم أو من ينيبه إن أمكن، كما أن التفتيش غايته ضبط الأدلة بالبحث في محتويات المكان، أما المعاينة فهي الاطلاع على شيء معين، أو وصف لحالة المكان أو الأشياء أو الأشخاص بالكيفية التي تركها عليها الجاني ، ولذلك فهي تحتاج في معظم الحالات إلى الاستعانة بخبير فني. أنظر إدوار غالي الذهبي، "الإجراءات الجنائية في التشريع المصري"، ط2، مكتبة غريب، القاهرة، 1992، ص 416.

[3] محمد كمال شاهين، "الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)"، ط 01، دار الجامعة الجديدة، الإسكندرية، 2018، ص 259.

1- المسرح التقليدي

المسرح التقليدي هو المسرح الذي يقع عادة خارج بيئة الحاسوب، ويتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة، وهو قريب من مسرح الجريمة التقليدية، ومن أمثلة هذه الجرائم تلك الواقعة على أشرطة الحاسب والكابلات الخاصة به وشاشة العرض الملحق به ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب الآلي ذات الطابع المادي المحسوس[1].

وليس هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل ضباط الشرطة القضائية والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل الأدوات والوسائل التي استخدمت في ارتكاب الجريمة مع وجوب إخطار النيابة العامة بذلك[2].

وفي هذه الحالة تتميز المعاينة بالسهولة، باعتبار أنها تتم على عناصر ملموسة كانت محلا الجريمة أو تخلفت عنها.

2- المسرح الافتراضي

المسرح الافتراضي يقع عادة داخل البيئة الالكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله، وفي مقدمة هذه الجرائم الواقعة على برامج الحاسب الآلي أو بياناته أو تتم بواسطتها، وكذلك الجرائم التي تتم بطريق الانترنت ومنها جرائم التزوير المعلوماتي والتخريب[3]. وتتميز المعاينة في العالم الافتراضي بالصعوبة التي تتمثل في:

---

[1] أنظر المادة 42 فقرة 3 من قانون الإجراءات الجزائية جزائري .

[2] عبد الفتاح بيومي حجازي، "مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت"، ط 01، دار الكتب القانونية، القاهرة، 2007 ، ص 162.

[3] عبد الفتاح بيومي حجازي، المرجع نفسه، ص164.

- ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلومات.
- الأعداد الهائلة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة زمنية[1] وحتى يمكن لضابط الشرطة القضائية القيام بالمعاينة في العالم الافتراضي لابد عليه أن ينتقل إلى العالم الافتراضي لمعاينة من مكتبه أو اللجوء إلى مقهى الانترنت أو إلى الخبراء وغيرها من الأماكن التي تساعده في إظهار الحقيقة.

ثالثا: إجراءات المعاينة التقنية

لابد على الضابط الشرطة القضائية تباع بعض القواعد والإرشادات الفنية عند معاينة مسرح الجريمة المعلوماتية، تتمثل هذه الإجراءات[2] في:

- عند العثور على حاسبات آلية أو أجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها، تدوين الحالة التي هي عليها إذا كانت منطفئة لو في حالة تشغيل موصولة بالكهرباء أو بجهاز لاحق آخر، كما ينبغي ترقيم لواحقها بشكل متسلسل.
- يجب تحرير الأوراق المطبوعة على الحاسب الآلي والتي عثر عليها في مسرح الجريمة ووضعها في أكياس حسب حالتها، ويمكن إعادة الطباعة إذا كان الجهاز في حالة تشغيل

وتحرير الأوراق التي تمت طباعتها، بالإضافة إلى تفقد الجهاز وتسجيل ما إذا كانت هناك برامج تم استخدامها لحظة دخول مسرح الجريمة.[3]

[1] نظرا لكون الجريمة المعلوماتية صعبة الإثبات واكتشاف من قام بها خاصة في مقاهي الانترنت لتوافد عدد كبير جدا من على مسرح الجريمة.

[2] رزيق محمد، "اجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتية "،مذكرة لنيل شهادة الماستر في القانون العام، تخصص القانون الجنائي و العلوم الجنائية، كلية الحقوق و العلوم السياسية، قسم الحقوق، جامعة اكلي محند اولحاج، البويرة، 2018-2019 ،ص 18

[3] محمد أمين الشوابكة، مرجع سابق ، ص 122.

- عند العثور على دعائم التخزين (أسطوانات، أقراص، حوامل مغناطيسية) يجب ترقيمها وتسجيل الحالة التي هي عليها والمكان الذي وجدت فيها (داخل الحاسب الآلي أو خارجه)[1].
- عند الانتهاء من الترقيم يجب تصوير ونسج الأجهزة وملحقاتها في الحالة التي هي عليها.
- يجب تحرير جميع العينات التي عثر عليها من أجهزة ودعائم داخل أكياس خاصة (بلاستيكية أو ورقية) كما ينبغي حمايتها من الكسر وتأثير العوامل الجوية وأبعادها عن أي مجال مغناطيسي لتفادي فقدان المعلومات وإرسالها إلى المخبر لإجراء الخبرة.

تقتضى القاعدة العامة بأن تكون هناك استعانة بالخبراء في المسائل العلمية والتقنية التي تحتاج إلى خبرة خاصة ،كخبرة الطبيب الشرعي لمعرفة سبب الوفاة فالخبرة في الجريمة المعلوماتية، لها أهمية بالغة التطور السريع والمتلاحق في مجال صناعة الحاسبات والبرمجيات شبكات الاتصال ما قد يصعب على المحقق لا تتبعها واستيعابها[2].

يحتاج خبراء الأدلة الجنائية الرقمية لتأدية أعمالهم التقنية إلى الأدلة الرقمية واكتشاف المعلومات التي يحتويها كل دليل ومن هذه الأجهزة والأنظمة والبرمجيات ما يلي:

- أجهزة بقدرة عالية على التحليل وتخزين المعطيات.

- نسخ من مختلف أنظمة التشغيل المستعملة أدى الأفراد والمؤسسات

- نسخ من برامج حذف وكسر كلمات المرور المختلف الحاسبات، برامج نسخ الأقراص المدمجة والمحمولة، برامج الضغط وفك الضغط برامج التشفير وفك التشفير، برامج حماية الأنظمة والشبكات

[1] وهي أهم إجراء من إجراءات المعاينة من أجل ضبط الدليل الرقمي وأيضا كافة الأدلة التي تساعد في الكشف عن المجرم.

[2] ويقصد بها بعث جميع الأدلة التي تم ضبطها في مجال الجريمة المعلوماتية آلي خبراء تقنيين من أجل فحصها وكشف الغموض والقبض على مرتكبيها.

من الاختراق، برامج كشف الأجهزة المخفيةمن الأقراص الصلبة، برامج استعادة الملفات المحذوفة وبرامج البحث عن الانترنت.[1]

الفرع الثاني

التفتيش لمسرح الجريمة الالكترونية

التفتيش بوجه عام هو إجراء قضائي يهدف إلى الحصول على أدلة تساعد في كشف الحقيقة، ويتميز بخاصيتي الجبر والإكراه، أي أن الإنسان يخضع له مجبرا، إذا لم يوافق على إجرائه برضاه، ويتضمن هذا الإجراء مساسا بمستودع سر الإنسان، سواء كان مسكنا أو في جسمه، وهو إجراء يهدف إلى جمع الأدلة التي تساهم في كشف الحقيقة[2].

أولا: تعريف التفتيش

يمكن تعريف التفتيش بصفة عامة أنه: ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي، ولا يمكن أن يقوم به سوى النيابة العامة وقاضي التحقيق، عن طريق أمر ندب أحد ضباط الشرطة القضائية المختص بإجرائه، والغرض منه هو البحث عن أدلة الإثبات للجريمة المرتكبة، وكل ما يفيد للوصول إلى الحقيقة في متابعة أي شخص يشتبه أنه مرتكب الجريمة[3].

ثانيا: إجراءات التفتيش في المنظومة المعلوماتية

[1] كل هذه الإجراءات تكون إجراءات عند الوصول إلى مسرح الجريمة، بالإضافة إلى الخطوات أو الإجراءات التي تكون قبل التحرك والانتقال إلى مسرح الجريمة كتوفير معلومات مسبقة عن الجريمة، إعداد خريطة للموقع الذي تتم عليه الهجوم على المكان الجريمة وغيرها.

[2] سامي جلال ففي حسين، "التفتيش في الجرائم المعلوماتية (دراسة مقارنة)"، ط01، دار الكتب القانونية، القاهرة مصر، 2011، ص55.

[3] بلعليات إبراهيم،" أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري"، ط 01، دار الخلدونية، الجزائر، 2012،ص 214.

عند التطرق لإجراءات التفتيش عن الجريمة الإلكترونية، إضافة إلى القواعد الإجرائية، وجب الوقوف عند الضمانات التي يجب على المحقق احترامها والتقيد بها عند قيامه بعملية التفتيش، كذلك الوقوف عند الآثار المترتبة عن التفتيش.

1- تفتيش الحاسب الآلي:

يشتمل الحاسب الآلي على مجموعة من المكونات المادية المتمثلة في الوحدات المختلفة (وحدات الإدخال كلوحة المفاتيح والماسح الضوئي والميكروفون، وحدات الإخراج كالشاشة والطابعة والسماعات)، كما يشتمل على مجموعة من المكونات المعنوية المتمثلة في المعلومات والبيانات المعالجة آليا، غير أن التساؤل يثور حول مدى قابلية هذه المكونات للتفتيش؟

أ- بالنسبة لتفتيش مكونات الحاسب الآلي المادية:

لا يوجد إشكال حول إمكانية خضوعها للتفتيش غير أن ذلك يتوقف على طبيعة المكان: فإذا كان المكان خاصا؛ لا يجوز تفتيشه إلا بنفس الضمانات المقررة قانونا في التفتيش التقليدي، أما إذا كان المكان عاما؛ لا يجوز التفتيش إلا بنفس الضمانات والقيود المرتبطة بتفتيش الأشخاص[1]، وهناك بعض التشريعات تبين ضوابط التفتيش لمكونات الحاسب الآلي، ومنها قانون المنافسة الكندي، حيث يتيح للقائم بالتفتيش إمكانية استخدام أي نظام لأجهزة الحاسب الآلي لتفتيش أي بيانات، وبإمكانه أن يعمل على تسجيل تلك البيانات في شكل مطبوعات أو مخرجات أخرى.[2]

ب- بالنسبة لتفتيش مكونات الحاسب الآلي المعنوية

[1] خالد عياد الحلبي، مرجع سابق، ص 159.

[2] يوسف بن سعيد الكلباني، "الحماية الجزائية للبيانات الالكترونية في التشريعين العماني والمصري (دراسة مقارنة)"، ط 01، دار النهضة العربية، القاهرة، 2017، ص 341.

يقصد بالمكونات المعنوية للحاسب الآلي تلك البرمجيات التي تقوم بعملية التحكم في المكوّنات المعنوية للحاسوب وهي محل خلاف فقهي، حيث يرى جانب من الفقه أن المكونات المعنوية لا تصلح بطبيعتها لأن تكون محلا للتفتيش والضبط باعتبار أن التفتيش يهدف إلى ضبط أدلة مادية، وهذا يقتضي أحكاما خاصة تكون أكثر ملائمة لتفتيش وضبط تلك البيانات غير المحسوسة، واقترح بعض الفقهاء أن تضاف للنصوص التقليدية عبارة المواد المعالجة عن طريق الحاسب الآلي أو بياناته، ويرى بعض الفقهاء في فرنسا أن النبضات والإشارات الالكترونية الممغنطة، لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تأخذ حكم الأشياء المادية عند التفتيش[1].

وهناك من يرى أن المكونات المعنوية تخضع للتفتيش مثلها مثل المكونات المادية، وعلة ذلك أن القوانين الإجرائية عندما تمنح سلطات التحقيق إمكانية ضبط أي شيء يكون ضروريا لجمع الأدلة فان ذلك يجب تفسيره ليشمل ضبط البيانات المخزنة أو المعالجة الكترونيا، كما يشمل بيانات الحاسب الآلي غير المحسوسة[2].

أما عن موقف المشرع الجزائري يمكن اعتباره جعل التفتيش يمتد ليشمل جميع المكونات المادية والمعنوية، وتبرير ذلك نص المادة 81 من قانون الإجراءات الجزائية" يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة" حيث استعمل في نص المادة مصطلح "أشياء"

كما تناول المشرع من خلال المادة 05 من القانون 04/09 القواعد الإجرائية لتفتيش المنظومات المعلوماتية من خلال إجازته للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى كل منظومة معلوماتية أو جزء منها، وكذا المعطيات

[1] محمد كمال شاهين، مرجع سابق، ص 281.

[2] يوسف بن سعيد الكلياني، مرجع سابق، ص 342.

المعلوماتية المخزنة فيها أو الدخول بغرض التفتيش ولو عن بعد إلى منظومة تخزين معلوماتية[1]، وهو ما يؤكد صراحة أن المشرع جعل من المكونات المعنوية للحاسب الآلي محل تفتيش.

2- تفتيش شبكات الحاسب الآلي:

قد تمتد شبكات الحاسب الآلي في الدولة نفسها أو إلى عدة دول:

أ- في حالة اتصال حاسب المتهم بحاسب آخر في نفس الدولة:

يرى الفقه والقانون حلا للصعوبات التي تثيرها القواعد التقليدية، حيث أن الفقه الألماني يرى إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجنائية الألماني، كما ذهبت بعض التشريعات إلى جواز امتداد التفتيش إلى نظام معلوماتي آخر غير النظام محل التفتيش ومن بينها: قانون تحقيق الجنايات البلجيكي الصادر في 23 نوفمبر سنة 2000 حيث جاء في المادة 88 منه على أن يتم الامتداد إذا كان الولوج ضروريا لكشف الحقيقة بشأن الجريمة محل البحث، وإذا وجدت مخاطر تتعلق بضياع الأدلة نظرا لسهولة محو أو إتلاف أو نقل البيانات محل البحث[2].

وقد تطرق المشرع الجزائري لتوسيع الصلاحيات في تفتيش الجرائم المعلوماتية إلى كامل امتداد التراب الوطني، حيث يجوز إجراؤه في كل محل سكني أو غير سكني، وفي أي وقت، بناء على إذن مسبق من وكيل الجمهورية المختص، كما يمكن لقاضي التحقيق أن يقوم بأي عملية تفتيش ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو ياسر ضباط الشرطة القضائية المختصين بذلك، مع

[1] أنظر المادة 05 من قانون رقم 09-04 المؤرخ في 5-04-2009 سالف الذكر.

[2] محمد كمال شاهين، مرجع سابق، ص 284.

إمكانية اتخاذ تدابير أخرى أو الأمر باتخاذ تدابير أخرى أو الأمر باتخاذ تدابير تحفظية بناء على تسخير النيابة العامة أو طلب من ضباط الشرطة القضائية[1].

ب- في حالة اتصال حاسب المتهم بحاسب آخر خارج حدود الدولة

امتداد التفتيش لخارج الأقاليم الوطني أو ما يعرف بالتفتيش العابر للحدود الوطنية يتعارض مع مبدأ سيادة الدولة على إقليمها، لهذا لابد أن يتم بموجب اتفاقيات ثنائية أو دولية تجيز هذا الامتداد أو على الأقل الحصول على إذن الدولة الأخرى بذلك، وقد اعتبر الفقه الألماني السماح باسترجاع بيانات ثم تخزينها بالخارج أمر مشكوك فيه، خاصة في ظل غياب اتفاق متبادل بين الدول والذي يعد خرقا لحقوق السيادة الدولة أخرى، ونفس الرأي أيده القضاء الألماني عندما عرضت عليه واقعة تتعلق بالعش المعلوماتي، حيث كانت طرفية أحد الحواسيب الموجودة في ألمانيا، سويسرا وعندما حاولت سلطات التحقيق الألمانية ضبط هذه البيانات لم تتمكن من ذلك إلا من خلال التماس المساعدة المتبادلة[2].

وقد انتهج المشرع الجزائري إمكانية امتداد النفسي إلى خارج الإقليم الوطني وذلك وفقا لمبدأ المعاملة بالمثل وبمساعدة السلطات الأجنبية المخلصة طبقا للاتفاقيات ذات الصلة، وهذا في حالة اتصال حاسب المتهم بحاسب آخر خارج الدولة[3].

وفي نفس الساق والرجوع إلى الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية (بودابست 2001) نجد أنها أجازت النفاذ (التفتيش) العابر للحدود إلى بيانات الكمبيوتر المخزنة دون ترخيص من الدولة الطرف، وذلك في حالة تفتيش بيانات مخزنة ومتاحة للجمهور بغض النظر عن مكان

[1] انظر الفترة 03 و 04 من المادة 47 من قانون الإجراءات الجزائية.

[2] المادة 32 من اتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، مجلس اوروبا، مجموعة المعاهدات الاوربية، رقم185، بودابست،2001، ص 18.

[3] انظر المادة 45 فقرة الأخيرة قانون إجراءات الجزائية جزائري.

تواجد البيانات جغرافيا، كما أجازت الدخول بغرض التفتيش إلى بيانات مخزنة في دولة طرف، من خلال موافقة قانونية وطوعية للشخص الحائز على المعلومات أو البيانات اللازمة في إجراء التفتيش.

غير أننا نرى أنه بالنظر إلى الأبعاد الدولية فلا يمكن مواجهة الجرائم المعلوماتية خارج الإقليم إلا بتعزيز آليات التعاون الدولي على المستوى الأمني والقضائي والفني، بشرط عدم إتاحة فرصة التحكم والتجسس من قبل الدول الرائدة في المجال المعلوماتي على الأنظمة المعلوماتية للدول الأخرى.

ثالثا: ضمانات التفتيش في البيئة الإلكترونية

رغم اعتبار التفتيش من الإجراءات الجوهرية في عملية التحقيق البحث عن حقيقة الجرائم إلا أن معظم القوانين الإجرائية حرصت على إحاطته بجملة من الضمانات القانونية، وذلك تفاديا لتعسف سلطات البحث والاستدلال وما يمكن أن يحدثه من اعتداء على حقوق وحريات الأفراد وحرمة مساكنهم وحياتهم الخاصة من جهة، وإحقاقا لحق الدولة ممثلة المجتمع في كشف غموض الجرائم ومتابعة مرتكبيها وتوقيع العقاب عليهم من جهة أخرى، ويمكن تقسيم هذه الضمانات إلى ضمانات موضوعية وأخرى شكلية أو إجرائية نذكرها على النحو التالي:

1- الضمانات الشكلية:

وهي شروط شكلية لصحة التفتيش تتمثل فيما يلي:

- الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في العالم الافتراضي وهي من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، وذلك لضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط والأصل أن الشخص الذي يستجوب الحضور هو المتهم أو أحد أقاربه وهو الشرط الذي استثناه المشرع الجزائري، إذ اشترط المشرع الجزائري أنه لا يجوز تفتيش مسكن المتهم إلا بالضوابط والضمانات المقررة في نص المادة 45 و 64 ق ا ج ج، وهو ما استثناء المشرع لتطبيق

هذه الضمانات بالنسبة لبعض الجرائم ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بموجب الفقرة 03 من المادة 47 ق ا ج ج[1].

– أن يتم التفتيش بأسلوب آلي أي أن يكون التفتيش على دعامة الكترونية وهو بالضرورة الحاسب الآلي.

– أن يتم التفتيش من طرف فريق يتكون من خبراء.

– إذن التفتيش لابد أن يكون مسببا.

– الميعاد الزمني لإجراء التفتيش حيث اختلفت التشريعات الإجرائية في وقت تنفيذ التفتيش، ومن بينهم المشرع الجزائري ذهب إلى حضر التفتيش للمساكن وما في حكمها في أوقات معينة[2]، وهناك حالات استثنائية خرج فيها عن هذه القاعدة الأصل أن يكون التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساء وإلا كان التفتيش باطلا؛ غير أنه في بعض الجرائم خرج المشرع الجزائري عن القاعدة العامة لميعاد التفتيش وأجاز التفتيش في جميع الأوقات 24 ساعة في بعض الجرائم مذكورة على سبيل الحصر ومن بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات[3].

2– الضمانات الموضوعية:

بالإضافة للضمانات الشكلية السابقة يجب توافر ضمانات موضوعية تتمثل أساسا فيما يلي:

أ: يجب الحصول على إذن بالتفتيش

[1] انظر المادة 47 فقرة 03 من قانون الإجراءات الجزائية الجزائري .

[2] انظر المادة 47 فقرة 01 من قانون الإجراءات الجزائية الجزائري .

[3] أحمد شوقي الشلقاني، "مبادئ الإجراءات الجزائية في التشريع الجزائري"، الجزء2،د ط، دار الفكر العربي ، الجزائر،1999،ص 45 .

تنص المادة 44 من ق إ ج ج نجدها تنص على أنه: "لا يجوز إجراء التفتيش إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة "، ويشترط المشرع الجزائري في هذا الإذن وجوب استظهاره قبل الدخول إلى مسكن المشتبه فيه والشروع في تفتيشه وأن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل وعنوان لأماكن التي سيتم زيارتها وتفتيشها وإجراء الحجز عليها وذلك تحت طائلة البطلان.

وبالرجوع إلى القانون رقم 04/09 والبحث في مدى التقيد بهذا الضابط من عدمه عند القيام بإجراء التفتيش الالكتروني فإننا نجد أن المادة 05 من ذات القانون المنظمة لهذا النوع من التفتيش لا تنص صراحة على وجوب استصدار إذن بتفتيش المنظومات المعلوماتية من طرف ضباط الشرطة القضائية كما هو الشأن بالنسبة لمراقبة الاتصالات الالكترونية، إلا أن هذا لا يعني أن التفتيش الالكتروني يتم دون وجوب إذن بمباشرته خاصة وأن المادة 05 جاء في مطلع نصها القانوني " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه، الدخول بغرض التفتيش ولو عن بعد إلى .....، وبالتالي فإنه يفهم ضمنيا من هذا النص القانوني أن التفتيش في الجرائم المعلوماتية لا يختلف عن الجرائم الأخرى إذ يشترط لمباشرته هو الآخر ضرورة الحصول على إذن من الجهات المختصة[1].

وهذا الإذن يجوز أن يشمل البحث عن معلومات في الكمبيوتر عن الأدلة التي تتعلق بجريمة من الجرائم، ويسوي أن تكون هذه المعلومات في أي شكل كان سواء كان الكترونيا أو مغناطيسيا، في صورة ديسك أو أسطوانة أو مسجلة على الهارد ديسك، أو في شكل ورقي تم طباعته بناء على ذلك. [2]

ب: تحرير محضر التفتيش الالكتروني

[1] عربوز فاطمة الزهراء، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم الإلكترونية، مجلة جيل الأبحاث القانونية المعمقة، العدد 34، 2019، ص 134.

[2] فهد عبد الله العازمي، "الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة"، د.ط ،دار الجامعة الجديدة، الاسكندرية، 2016، ص686.

لما كان التفتيش عملا من أعمال التحقيق فإنه يجب تحرير محضر يثبت فيه كل ما تم من إجراءات وما أسفر عن التفتيش من أدلة، ولا يتطلب القانون شكلا معينا يعني لا يشترط لصحته سوى ما تستوجبه أو تفرضه الأسس العامة في تحرير المحاضر بشكل عام، وهي ضرورة أن يكون مكتوب باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع الشخص أو الجهة التي قامت بتحريره وأن يتضمن كافة البيانات المتعلقة بالتفتيش[1].

رابعا: آثار التفتيش الإلكتروني

يعد ضبط الأدلة الإلكترونية الأثر المباشر للتفتيش عن الجرائم المعلوماتية، كما قد يترتب عن هذا التفتيش حجز المنظومة المعلوماتية، وقد تتعارض هذه الإجراءات مع الحق في الخصوصية أو قد تتنافى مع الشروط المقررة قانونا مما يتطلب الدفع ببطلان إجراءات التحقيق.

1- ضبط الدليل الإلكتروني

يترتب عن التفتيش إما عدم ضبط أي دليل معلوماتي بعد تفتيش الحاسوب والشبكة المرتبطة به، أو نشوء الحق في ضبط الأشياء التي تفيد في الكشف عن الجريمة.

غير أن التساؤل يثور حول نوع الأشياء محل الضبط في الجرائم المعلوماتية، خاصة لطبيعة هذه الجرائم وأن محلها (البيانات والبرامج) تتسم بصورة معنوية غير محسوسة؟

وإجابة على ذلك الأشياء في نطاق التفتيش في وسائل التقنية الحديثة قد تكون أشياء مادية (منقولات كالأجهزة، أو عقارات كالأماكن الكائن بها منقولات معنوية)، وقد تكون أشياء معنوية (كالمراسلات والاتصالات الالكترونية والمعلومات المعالجة الكترونيا وغيرها من الأشياء المعنوية)[2].

[1] عربوز فاطمة الزهراء، المرجع السابق، ص 136.

[2] بكري يوسف بكري، "التفتيش عن المعلومات في وسائل التقنية الحديثة"، ط 01،دار الفكر الجامعي، الإسكندرية، 2011، ص157.

فالأصل أن الأشياء المادية التي يحوزها المتهم تكون محلا للضبط أما الأشياء المعنوية كالبيانات والبرامج فهي محل إشكال فقهي، غير أنه باعتبارها تسجل وتحفظ على وسائط المادية فقد تكون محلا للضبط أيضا، ففي حالة العثور على الدليل المعلوماتي، وكون الأدلة عبارة عن نبضات مغناطيسية يجب تفريغها على دعامة مادية المغناطيسية وغيرها من وسائط التخزين، أو تفريغها على الورق، ويتم تثبيت تفاصيل الأدلة المعلوماتية في محضر ضبط.[1]

ويثير إجراء ضبط البيانات المعالجة الكترونيا عدة صعوبات من بينها : كبر حجم الشبكات التي تحتوي على المعلومات المطلوب ضبطها، كالبحث في نظام الشركة متعددة الجنسيات، إضافة إلى مشكلة وجود البيانات في شبكات أو أجهزة تابعة لدول أجنبية، مما يتطلب التعاون مع أجهزة العدالة التابعة لهذه الدول.[2]

2- حجز المنظومة المعلوماتية

قد يترتب عن التفتيش حجز المنظومة المعلوماتية في حالة اكتشاف السلطة التي تباشر إجراء التفتيش عن وجود معطيات مخزنة تفيد في الكشف عن الجريمة ومرتكبيها، ففي هذه الحالة من الممكن أن تحجز المنظومة برمتها، كما يمكن أن يحجز جزء منها فقط، ذلك باعتماد مجموعة من الإجراءات حسب ما يفهم من نص المادة 06 من القانون 09-04 سالف الذكر، وتتمثل في:

- نسخ المعطيات على دعامة تخزين الكترونية تكون قابلة للحجز (سواء المعطيات محل البحث أو المعطيات اللازمة لفهم المعطيات محل البحث) الوضع في إحراز وفقا لما هو مقرر في قانون الإجراءات الجزائية

[1] رامي متولي القاضي، "مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية"، ط 01،دار النهضة العربية، مصر، 2011، ص 344.

[2] سامي جلال فقي حسين، مرجع سابق، ص 120.

– السهر على سلامة المعطيات في المنظومة المعلوماتية.

– إمكانية استعمال وسائل تقنية لتشكيل أو إعادة تشكيل المعطيات لتكون قابلة للاستغلال لأغراض التحقيق بشرط عدم المساس بمحتوى المعطيات، وتجدر الإشارة أنه في حالة تعذر إجراء الحجز لأسباب تقنية، يتعين على السلطة التي تباشر إجراء التفتيش أن تستخدم تقنيات مناسبة لمنع نسخ أو الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال المنظومة[1]، والهدف من هذا الإجراء الاحترازي هو الحفاظ على الأدلة في محيطها الالكتروني، لمنع أي محاولة لطمسها أو إخفاء معالمها، مما يساهم في نجاح إجراء التفتيش والحجز باعتباره أثر للتفتيش.[2]

المطلب الثاني

الخبرة والشهادة في مجال الجرائم الالكترونية

يهدف التحري عن الجريمة الالكترونية إلى كشف الحقيقة، وذلك بمساعدة إجرائي الخبرة والشهادة التي تقود المحقق لضبط الأدلة والقرائن و هو ما سنفصل فيه من خلال فرعين، الفرع الاول الذي سوف نتناول فيه اجراء الخبرة ، اما الفرع الثاني نتناول فيه اجراء الشهادة في مجال الجريمة الالكترونية.

الفرع الأول

الخبرة في مجال الجريمة الالكترونية

[1] وهذا حسب ما جاء في المادة 07 من القانون 09-04 سالف الذكر.

[2] همیسي رضا، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، كلية الحقوق و العلوم السياسية ، جامعة الشهيد حقه لخضر بالوادي، الجزائر، ع 03، جوان 2012، ص 174 .

الخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية والعلمية والتي لا تتوافر لدى رجال القضاء من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع الجريمة ونسبتها إلى المتهم أو تحديد ملامح شخصيته الإجرامية[1]، ولهذا فإن للخبرة التقنية في مجال الجريمة المعلوماتية أهمية بالغة حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية وخبرة في مجال الشبكات.

ونظرا لأن الجريمة المعلوماتية لها خصوصيتها فإن الخبير المعلوماتي لابد أن توافر لديهم المقدرة الفنية والإمكانيات العلمية والفنية في المسألة موضوع الخبرة، ولا يكفي في ذلك حصول الخبير على شهادة علمية[2]، بل يجب مراعاة الخبرة العملية لأنها هي التي تحقق الكفاءة الفنية من أجل كشف الغموض عن الجريمة أو تجميع دلالتها والتحفظ عليها ومساعدة المحقق في إيجاد جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق[3].

أولا: دور الخبرة في مجال الجرائم المعلوماتية

للخبير التقني دور وقائي وهو حماية وتأمين النظام محل الاعتداء من استمرار التهديد المعلوماتي ضده، كالحد من استمرار انتشار الفيروسات التي يمكن أن تنتقل وتسجل أوتوماتيكيا على الحاسبات والتي يمكن أن تدمر ما تبقى من النظام المعلوماتي، أو أن يساعد على وقف التجسس المعلوماتي بنسخ الملفات أو بمنع سرقة وقت الآلة[4].

كما تساعد الخبرة في مجال الجرائم المعلوماتية في الكشف عن الدليل الالكتروني وتحديد خصائصه المميزة وخصائص كل جزء منه كالمستند الرقمي، البرامج، التطبيقات، الاتصالات، الصور،

[1] أحمد شوقي الشلقاني، مرجع سابق، ص259.

[2] صغير يوسف، "الجريمة المرتكبة عبر الانترنت"، مذكرة تخرج لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013، ص 88-89.

[3] عبد الفتاح بيومي حجازي، "الإثبات في جرائم الكمبيوتر والانترنت"،د ط ، دار الكتب القانونية، مصر، 2007، ص 137.

[4] محمد كمال شاهين، مرجع سابق، ص 335.

الأصوات وغيرها، ويقوم الخبير بعمل نسخة أصلية منه للتأكد من عدم وجود معلومات مفقودة أثناء استخلاصه، ويمكن إجراء اختبارات عليه للتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنفاذ القانون، كما تساعد الخبرة في إصلاح الدليل وإعادة تجميعه من المكونات المادية للحساب الآلي، وفي جمع الآثار المعلوماتية الرقمية، واستخدام خوارزميات للتأكد من أن الدليل لم يتم العبث به أو تعديله.[1]

يكون عمل الخبير بحضور وتحت إشراف المحقق، ويرى الفقه أن حضور المحقق هو بمثابة رقابة إجرائية لتسهيل مهمة الخبير ومساعدته في تعيين مكان البحث وتوفير الظروف الموضوعية، غير أنه لا يجوز للمحقق التدخل في الأعمال الفنية التي يجريها الخبير، وينحصر دور الخبير في إبداء رأيه في المسائل الفنية التي حددها له المحقق، وله أن يستعين بغيره من الخبراء نظرا لعدم وجود خبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرمجياتها، ولا خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع بواسطة أو على الحاسب الآلي.[2]

وبالإسقاط على ما جاء في قانون الإجراءات الجزائية الجزائري فقاضي التحقيق أو القاضي الذي تعينه الجهة القضائية له أن يراقب أعمال الخبرة، وإذا ظهر للخبير مسألة تقنية خارجة عن اختصاصه فيجوز للقاضي أن يصرح لهم بضم فنيين متخصصين، ويؤدي الفنيون المعينون على هذا الوجه نفس يمين الخبراء ويرفق تقريرهم بكامله بتقرير الخبراء[3].

ثانيا: ضوابط الخبرة

تخضع الخبرة لمجموعة من الضوابط القانونية والفنية:

[1] خالد ممدوح إبراهيم، "فن التحقيق الجنائي في الجرائم الالكترونية"،ط 01 ،دار الفكر الجامعي، الإسكندرية، 2009، ص 302.

[2] محمد كمال شاهين، مرجع سابق، 338.

[3] انظر المادة 149 من قانون الإجراءات الجزائية الجزائري.

أ-الضوابط القانونية:

وتنحصر في تلك الضوابط القانونية المنصوص عليها في قانون الإجراءات الجزائية كاختيار الخبراء واجبات والتزامات الخبير (الحلف اليمين، وخضوعه للرقابة القضائية)[1] القيام بمهامه بنفسه واستجابته لطلبات الخصوم إيداعه التقارير خلال المدة المحددة.[2]

ب-الضوابط الفنية:

تشمل خطوات اشتقاق الدليل الالكتروني والتي تتمثل في خطوات ما قبل التشغيل والفحص وخطوات التشغيل[3]، وتحديد مدن الترابط بين الدليل المادي والالكتروني ومرحلة تدوين النتائج وإعداد التقارير وتتمثل هذه الضوابط في:

- جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع ومن جهاز المعتدي بعد التوصل إلى تحديد[4].

- تحليل رقمي لمعرفة كيفية إعداد الأدلة الرقمية ونسبتها وتحديد عناصر حركتها، ثم التوصل في النهاية إلى معرفة بروتوكول الانترنت (IP) للحاسوب الذي صدرت منه الرسائل والهجمات الالكترونية.

ويرى بعض المتخصصين أن عمل الخبير المعلوماتي في اشتقاق وتجميع الأدلة الرقمية يتم عبر 03 مراحل:

المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الحاسبات الخادمة التي دخل فيها المجرم المعلوماتي[1].

[1] أنظر المواد 144، 145، 143، 148، 153 قانون الإجراءات الجزائية الجزائري،

[2] المادة 5 فقرة أخيرة من القانون 04/09 السالف الذكر.

[3] عبد الفتاح بيومي حجازي، "الإثبات في جرائم الكمبيوتر والانترنت" ، المرجع السابق، ص187.

[4] خالد ممدوح إبراهيم، مرجع سابق، ص 300.

المرحلة الثانية: مرحلة المراقبة ويتم بطرق مختلفة، كبرامج مراقبة يمكن تحميلها البحث عن المشتبه فيه وتسجيل بيانات الدخول وخروج الموقع.

المرحلة الثالثة: فحص النظام المعلوماتي المشتبه فيه بعد ضبطه من طرف السلطات المختصة بمكوناته المادية والمعنوية لاشتقاق الدليل وتقديمه للعدالة[2].

الفرع الثاني

الشهادة في مجال الجريمة الإلكترونية

تعرف الشهادة بصفة عامة بأنها الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت ،سواء تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته فيها[3]، ولا تقل أهمية الشهادة في مجال المعلوماتية عن نظيرتها في مجال الجرائم الأخرى، غير أن ما يمكن الإشارة إليه في موضوع الدراسة أن الشاهد المعلوماتي يختلف عن غيره من الشهود فهو صاحب معرفة علمية وتقنية بمجال المعلوماتية، وهو ما يفرض عليه التزامات من نوع خاص أمام جهة التحقيق.

أولا: تعريف الشاهد الإلكتروني

الشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي لديه خبرة جوهرية لازمة للدخول إلى نظام المعالجة الآلية للمعطيات[4].

---

[1] خالد ممدوح إبراهيم، المرجع نفسه، ص 306.

[2] سعيداني علي نعيم، مرجع ، سابق ص 171.

[4] عبد العالي الديري ومحمد صادق اسماعيل ،"الجرائم الالكترونية"،ط 01، المركز القومي للاصدارات القانونية، القاهرة،2012 ، ص 70.

[4] عبد الفتاح بيومي حجازي، "الإثبات في جرائم الكمبيوتر والانترنت"، المرجع السابق، ص 339.

متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات داخله، ولذلك يطلق على الشخص اسم الشاهد المعلوماتي تمييزا عن الشاهد التقليدي.

ثانيا: فئات الشاهد الإلكتروني

الشاهد المعلوماتي عدة أصناف يجوز لقاضي التحقيق استدعاء من شاء منهم لسماعه وهم:

1- **القائم على تشغيل الحاسوب:** وهو المسؤول عن تشغيل الحاسوب والمعدات المتصلة به وهو شخص تتوفر فيه الخبرة الكافية في مجال تشغيل الجهاز واستخدامه.

2- **المبرمجون:** وهم الأشخاص المختصمون في كتابة البرامج المعلوماتية وهم فئتان[1]:

أ- **مخطط برامج التطبيقات:** يقوم هؤلاء بالحصول على خصائص ومواصفات النظام المعلوماتي المطلوب من محلل النقد تم تحويلها إلى برامج دقيقة لتحقق هذه المواصفات.

ب- **مخطط برامج النظم:** يقوم هؤلاء بتصحيح واختبار وتعديل برامج نظم الحاسوب الداخلية في تلك الخاصة بالوظائف المتعلقة بتجهيز الحاسوب بالبرامج و الأجزاء الداخلية منه.

3- **المحللون:** هم قلة من الأشخاص مهمتهم تحليل الخطوات وجمع ببيانات النظام المعلوماتي ثم تحليلها، أي تقيمه الوحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات.

4- **مهندسو الصيانة والاتصالات:** هم فئة المسؤولين عن أعمال الصيانة الخاصة بالحاسوب الشبكات المتصلة به.

5- **مديرو النظم:** وهم من توكل لهم إدارة النظم المعلوماتية[1].

[1] هلالي عبد الاله أحمد ، "التزام الشاهد بالاعلام في الجرائم المعلوماتية"، ط 02 ، دار النهضة العربية، القاهرة، 2008، ص 23.

ويبقى قاضي التحقيق الشخص الوحيد الذي له حرية استدعاء أيا كان منهم.

ثالثا: التزامات الشاهد الالكتروني

ويتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن البحث عن أدلة الجريمة بداخله، والسؤال الذي طرح من قبل الباحثين هنا: هل يلتزم الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟ وفي الإجابة عن ذلك هناك اتجاهان:

الاتجاه الأول: يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسبة على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب.[2]

الاتجاه الثاني: يرى أنصاره أن من بين الالتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة، ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهاداتهم والإفصاح عن كلمات المرور السرية ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة[3].

المبحث الثاني

الإجراءات المستحدثة المتعلقة بالتحري عن الجريمة الالكترونية

[1] همیسي رضا، "أحكام الشاهد في الجريمة المعلومائية"، بحث مقدم إلى أعمال الملتقى الوطني الذي نظمته كلية الحقوق و العلوم السياسية ،قسم الحقوق، جامعة محمد خيضر بسكرة ،الموسوم بعنوان الجريمة المعلوماتية بين الوقاية والمكافحة ،يومي 16 و17 نوفمبر 2015 ، ص4-5.

[2] علي عدنان الفيل، "اجراءات التحري و جمع الادلة و التحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)"، ط 01 ، المكتب الجامعي الحديث ،الاسكندرية ، 2012 ص 63 وما بعدها.

[3] عوض محمد عوض، "المباديء العامة في قانون الاجراءات الجنائية"،ط 01 ،دار المطبوعات الجامعية،الاسكندرية، 2012 ، ص 404

مع التعقيدات والصعوبات التي تواجه السلطات المختصة أثناء استخلاص الأدلة الالكترونية، كان من اللازم مواكبة التطورات التكنولوجية واستحداث إجراءات خاصة تتناسب مع خصوصية التعامل مع البيئة التقنية، وذلك بغية تسهيل التوصل إلى مرتكبي الجرائم المعلوماتية وجمع الأدلة ضدهم.

وفي سياق ذلك اتجهت غالبية التشريعات إلى استحداث هذه الإجراءات الخاصة والمشرع الجزائري من ضمن المقومات التشريعية التي أرساها المشرع الجزائري كغيره من التشريعات المقارنة استحدث إجرائين ضمن خطته في مكافحة الجريمة المعلوماتية، يتعلق الأمر بالتسرب الالكتروني ومراقبة الاتصالات الالكترونية اللذان سنفصل فيهما من خلال مطلبين، حيث نتناول في المطلب الاول اجراء التسرب الالكتروني، أما في المطلب الثاني اجراء مراقبة الاتصالات الالكترونية.

المطلب الأول

التسرب الالكتروني

نظر للغموض الذي انتاب نص المادة 56 من القانون 01/06 المتعلق بالوقاية من الفساد ومكافحته[1]، بخصوص المقصود بالاختراق أو التسرب وشروطه وآليات مباشرته، بقي هذا الإجراء جامدا وبدون مفعول إلى أن تم تعديل قانون الإجراءات الجزائية بموجب قانون 22/06 المؤرخ في 20/ 12/ 2006، أين تم تحديد معالم إجراء التسرب من خلال تعريفه وتحديد شروط، وعليه سوف نتناول تعريف التسرب الالكتروني في الفرع الأول، أما الفرع الثاني نتناول شروطه.

الفرع الأول

تعريف التسرب الالكتروني

[1] القانون رقم 06-01 مؤرخ في20 فيفري 2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 14.

تعرف المادة 65 مكرر12 من القانون الإجراءات الجزائية الجزائري التسرب على أنه: "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 أو خاف....".

انطلاقا من هذا التعريف الذي جاء به المشرع الجزائري، يتبين أن التسرب عملية معقدة جدا تتطلب أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية[1]، بل أحيانا يكون القيام بتلك الأفعال ضرورة لقبوله في الخلية، لذلك اعتبار لهذه الضرورة تفطن المشرع الجزائري وجرد الضابط أو العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد يقدم على ارتكابها أثناء عملية التسرب[2].

ليس هذا فحسب، بل أحاط المشرع المتسرب كذلك بعدة ضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرب وبعد انقضائها، منها ما ورد في المادة 65 مكرر 16 من قانون الإجراءات الجزائية بأنه: "لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أية مرحلة من مراحل الإجراء[3]، وما تضمنته كذلك المادة (65 مكرر 17) من القانون نفسه بأنه: "إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة 65 مكرر 14 أعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسئولا جزائيا، على أن لا يتجاوز ذلك 4 أشهر"

[1] أنظر المادة 65 مكرر 14 من القانون الإجراءات الجزائية الجزائري.

[2] أنظر المادة 65 مكرر 14 فقرتها الأخيرة من القانون الإجراءات الجزائية الجزائري.

[3] وقد فرض المشرع الجزائري في الفقرات 1، 2 و3 من المادة 65 مكرر 16 من قانون الإجراءات الجزائية على من يكشف هوية المتسرب عقوبات صارمة تتفاوت درجتها حسب الضرر الذي برتبه الكشف على المشرب أو على الم أفراد أسرته قد تصل إلى 20 سنة حبسا وغرامة مليون دينار.

وعلى ذلك لا يجوز اللجوء لعملية التسرب إلا في بعض الجرائم البالغة الخطورة والتي حددها المشرع الجزائري على سبيل الحصر في المادة (65 مكرر) وهي: جرائم المخدرات، الجريمة المنظمة، جرائم تبييض الأموال والإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1].

ويمكن تصور عملية التسرب في الجرائم الالكترونية في ولوج ضابط أو عون الشرطة القضائية إلى العالم الافتراضي ومشاركته في محادثات غرف الدردشة أو حلقات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو اختراقه في مجموعات أو نوادي الهاكر، مستخدما في ذلك أسماء وصفات مستعارة وهمية ظاهرا فيها بمظهر طبيعي كما لو كان واحد مثلهم قصد استدراجهم والكشف عنهم وعن أعمالهم الإجرامية.

الفرع الثاني

شروط التسرب الالكتروني

نظرا للخطورة التي يشكلها إجراء التسرب على حرمة الحياة الخاصة للمشتبه فيه، فقد قيده المشرع بجملة من الشروط والضوابط الواجب مراعاتها قبل وأثناء مباشرته وهي كالتالي:

أولا : **صدور إذن قضائي بالتسرب:** نصت على هذا الشرط المادة 65 مكرر 11 من قانون الإجراءات الجزائية ومفاده أنه لا يجوز لضابط الشرطة القضائية اللجوء إلى التسرب إلا بناءا على إذن مكتوب، صادر من وكيل الجمهورية المختص أو قاضي التحقيق بعد إخطار وكيل الجمهورية، على أن يذكر فيه اسم الضابط المشرف على العملية وهويته الكاملة، وتاريخ بداية التسرب[2].

[1] أنظر المادة 65 مكرر من القانون الإجراءات الجزائية الجزائري.

[2] تجدر الإشارة إلى أن الكتابة شرط جوهري لصحة الإذن بالتسرب وهو ما نصت عليه المادة 65 مكرر 15 بأنه: "يجب أن يكن الإذن أن المسلم طبقا للمادة 65 مكرر 11 أعلاه مكتوبا... تحت طائلة البطلان.

ثانيا : احترام المدة المقررة للتسرب: حددت الفقرة الثالثة من المادة 65 كرر 15 من قانون الإجراءات الجزائية مدة التسرب بأربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق بنفس الشروط، ويجوز للقاضي الذي رخص بإجراء التسرب أن يأمر في أي وقت بوقفه قبل انقضاء المدة القانونية، وفي هذه الحالة وتحسبا للظروف الأمنية للضابط المتسرب أجازت المادة 65 مكرر 17 من نفس القانون لهذا الأخير مواصلة نشاطه لمدة لا تتجاوز أربعة أشهر دون أن يكون مسئولا جزائيا على ذلك، بشرط أن يخطر السلطة مصدرة الإذن في اقرب أجل".[1]

ثالثا : تسبيب عملية التسرب: يعتبر التسبيب شرط جوهري لمشروعية عملية التسرب، لذلك اشترط القانون على إصدار الإذن بالتقرب من السلطات المختصة ذكر السبب أو الدافع الحقيقي الجاد الذي يبرر اللجوء إلى هذا الإجراء تحت طائلة البطلان[2].

رابعا : محل التسرب: بمعنى أن عملية التسرب، يجب أن تنصب على إحدى الجرائم السبعة المنصوص عليها في المادة 65 مكرر 5، وهي: جرائم المخدرات، الجريمة المنظمة، الجرائم العامة بأنظمة المعالجة الآلية المعطيات، جرائم تبييض الأموال و الإرهاب، و جرائم المتعلقة بالتشريع الخاص بالصرف، وفيما على ذلك يعتبر التسرب إجراء باطلا.

الجدير بالذكر في الأخير هو أن المشرع الجزائري سمح لسلطات الضبطية القضائية إذا اقتضت ضرورة التحري والتحقيق ممارسة عملية اعتراض المراسلات وتسجيلها والتقاط الأصوات والتسرب، وكذا باقي إجراءات التحقيق التي تدخل في اختصاصاتها، عبر كافة الإقليم الوطني إذا تعلق الأمر ببحث ومعاينة جرائم العامة والمعالجة الآلية المعطيات، المتمثل في تمديد الاختصاص المحلي لضباط الشرطة القضائية إلى كامل الإقليم الوطني هو من ضمن التدابير غير المألوفة في السابق والتي

[1] أنظر الفقرة الثالثة من المادة 65 مكرر 15 ونص المادة 65 مكرر 17 قانون الإجراءات الجزائية الجزائري.

[2] أنظر المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري.

استحدثها المشرع في المادة 16 الفقرة 7 و 8[1] والمادة 16 مكرر[2] من قانون الإجراءات الجزائية من اجل حسن المواجهة الفعالة لظاهرة الإجرام الالكتروني.

المطلب الثاني

مراقبة الاتصالات الالكترونية

إن الإقدام الهائل للأفراد والمؤسسات على وسائل الاتصال الحديثة والاستخدام المفرط لشبكات المعلوماتية في الآونة الأخيرة، جعل المشرع في العديد من الدول يدرك الصعوبات الكثيرة التي تنيرها محاولة من نطاق إجراءات الاعتراض والمراقبة وفق النصوص التقليدية لتشمل المراسلات والاتصالات عبر الشبكات المعلوماتية، لذلك عمدت العديد من هذه الدول إلى مراجعة قوانينها الإجرائية، بوضع نصوص صريحة تنظم هذه العملية.

ولم يتخلف المشرع الجزائري عن غيره من الدول، بل تدخل بموجب التعديل رقم 22/06 المؤرخ في 20/09/2006 لقانون الإجراءات الجزائية الجزائري، حيث استحدث هذا الإجراء حيث أضاف الفصل الرابع كاملا تحت عنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط صور"، ثم عززه بالقانون رقم 04/09 المؤرخ 5 أوت 2009[3]، وعليه نتعرض في الفرع الأول إلى تعريف مراقبة

[1] تنص المادة 16 فقرة 7و 8 من قانون الاجراءات الجزائية الجزائري على أنه:"...غير انه فيما يتعلق ببحث و معاينة جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بانظمة المعالجة الالية للمعطيات و جرائم تبييض الاموال و الارهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد اختصاص ضباط الشرطة القضائية الى كامل الاقليم الوطني.

و يعمل هؤلاء تحت اشراف النائب العام لدى المجلس القضائي المختص اقليميا و يعلم وكيل الجمهورية المختص اقليميا بذلك في جميع الحالات."

[2] تنص المادة 16 مكرر من قانون الإجراءات الجزائية الجزائري على أنه :"يمكن ضباط الشرطة القضائية، و تحت سلطتهم اعوان الشرطة القضائية ، ما لم يعترض على ذلك وكيل الجمهورية المختص بعد اخباره ، ان يمددوا عبر كامل الاقليم الوطني عمليات مراقبة الاشخاص الذين يوجد ضدهم مبرر مقبول او اكثر يحمل عللى الاشتباه فيهم بارتكاب الجرائم المبينة في المادة 16 اعلاه او مراقبة وجهة او نقل اشياء او اموال او متحصلات من ارتكاب هذه الجرائم او قد تستعمل في ارتكابها.

[3] القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

الاتصالات الالكترونية، أما في الفرع الثاني نتعرض إلى الضوابط المتعلقة بمراقبة الاتصالات الالكترونية.

الفرع الأول

المقصود بمراقبة الاتصالات الالكترونية

المشرع الجزائري لم يضع تعريفا للمراقبة الالكترونية لا في مواد قانون الإجراءات الجزائية ولا في مواد القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ونشير في هذا المقام إلى تصدي بعض التشريعات لتعريف إجراء المراقبة الالكترونية مثل التشريع الأمريكي الذي عرفها في المادة 2510-04 من قانون الاتصالات الفدرالي الأمريكي لسنة 1968 بأنها: عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز إلكتروني أو أي جهاز آخر"، وطبقاً لقانون الاتصالات الالكترونية الأمريكي لسنة 1986 أصبح التعريف المذكور يشمل الاتصالات الالكترونية الأخرى[1].

كما قامت لجنة خبراء البرلمان الأوروبي بمناسبة اجتماعها المنعقد بستراسبورغ في 06 أكتوبر 2006، لدراسة أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية، بتعريف إجراء المراقبة الالكترونية بأنها: " عملية مراقبة سرية المراسلات السلكية واللاسلكية وذلك في إطار البحث

[1] ياسر الأمير فاروق،" مراقبة الأحاديث الخاصة في الإجراءات الجزائية "، ط 01، دار المطبوعات الجامعية، الإسكندرية، مصر، 2009، ص 138

والتحري عن الجريمة وجمع الأدلة، والمعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب جريمة"[1].

أما بالنسبة للفقه اختلف هو الآخر في وضع تعريف دقيق وموحد لإجراء المراقبة الالكترونية، حيث عرفها بعض الفقه بأنها: "إجراء يتعمد فيه الإنصات والتسجيل ومحلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة أي سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية واللاسلكية"[2].

كما تعرف كذلك بأنها: "مراقبة شبكة الاتصالات أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع المعطيات والمعلومات عن المشتبه فيه سواء كان شخصاً أو مكاناً أو شيئاً حسب طبيعته، مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر".[3]

من خلال التعريفات السابقة يتضح لنا أن مفهوم المراقبة الإلكترونية يعني التنصت ومن ناحية أخرى التسجيل، بالإضافة إلى إشارة تلك التعريفات إلى محل المراقبة الإلكترونية، وهي الأحاديث الشخصية والمحادثات السلكية واللاسلكية، فضلا عن تبيان التعريفات السابقة ضرورة حصول التنصت أو التسجيل خلسة دون علم صاحب الحديث وبواسطة إحدى الوسائل أو الأدوات العلمية الحديثة، كما أكدت أغلب التعريفات على ضرورة أن تتم عملية المراقبة الإلكترونية من طرف جهات مختصة وبإذن من الجهات القضائية ذات الصلة[4].

[1] بوكر رشيدة، "جرائم الاعتداء على نظم المعالجة الالية للمعطيات في التشريع الجزائري و المقارن "،ط 01 ،منشورات الحلبي الحقوقية ، ، لبنان، 2012 ، ص 370.

[2] عوض محمد عوض، المرجع السابق، ص404.

[3] بوكر رشيدة، المرجع السابق، ص 370 .

[4] أحمد مسعود مريم، "آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04"، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية،قسم الحقوق، جامعة قاصدي مرباح ورقلة، 2012/2013، ص 80.

ويذكر هنا أن المشرع الجزائري لم يحدد وسائل المراقبة الإلكترونية ما عدا ذكره أنه يتوجب وضع الترتيبات التقنية الخاصة بالمراقبة، وبالرجوع إلى الفقه المقارن فقد ذهب البعض إلى تحديد أشكال المراقبة الإلكترونية تتمثل في:

1- استخدام وسائل فنية من خلال ما يسمى بالفخ والمتابعة، في هذه الحالة يتم تسجيل أسماء المتراسلين مع متهم معين أي مع بريده الإلكتروني أو من يقوم بالمحادثة الفورية معه.

2- استخدام وسائل التصنت على محتوى الرسالة الإلكترونية أو المحادثة الفورية الإلكترونية بوسائل للإعتراض والتضنت[1].

الفرع الثاني

الضوابط المتعلقة بمراقبة الاتصالات الالكترونية

نظرا لخطورة إجراءات المراقبة الالكترونية على حقوق وحريات الأفراد فقد أورد المشرع العديد من الضمانات والإجراءات التي تعتبر بمثابة قيود، ترد على السلطة التي تأمر بإجراء المراقبة وتحول دون تعسفها سواء كانت هي أو السلطات التي تتولى تنفيذها، وبقدر ما تكون هذه الأحكام القانونية محددة وواضحة بقدر ما تكون مباشرة المراقبة مقيدة وفقا للهدف منها، وعلى العكس من ذلك فإن عدم تحديد هذه الأحكام أو قصورها يفسح المجال لوجود سلطة تقديرية واسعة في اللجوء إلى المراقبة تختلف ممارستها من سلطة إلى أخرى مما يمثل خطرا كبيرا على حرمة الحياة الخاصة[2]، وهذه الضمانات يمكن أن نلخصها في ما يلي:

[1] ثابت دنيازاد، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الإجتماعية والإنسانية، المجلد 05، العدد 06، 2012، ص 207-208.

[2] ركاب أمينة، "أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري"، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبي بكر بلقايد، تلمسان، 2014/2015، ص 69.

أولا : الإذن

يعد الإذن من بين الضمانات التي وضعها المشرع الجزائري لمراقبة الاتصالات الالكترونية، حفاظا على خصوصية الأفراد بما فيها الخصوصية المعلوماتية، وبذلك نصت الفقرة 2 من المادة 14 من القانون رقم 09-04 السابق الذكر علي أنه لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب صادر عن السلطات القضائية المختصة دون تحديد فيما تتمثل هذه السلطة، إلا أنه بالرجوع إلى المادة 3 من نفس القانون نجد أنها نصت على... " :مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات... ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية ."
ويتبين أن المشرع الجزائري أحال بصفة صريحة إلى قانون الإجراءات الجزائية بخصوص ما يتعلق بمحتوى المادتين 3 ،4 من hgقانون 09-04، وعليه تتمثل إذن السلطة القضائية المختصة في منح الإذن بمراقبة الاتصالات الالكترونية نية في وكيل الجمهورية قبل فتح التحقيق أو قاضي التحقيق في حالة فتح تحقيق قضائي هذا كقاعدة عامة[1].

ثانيا : تحرير محضر

حيث يشترط تحرير محضر من ضابط الشرطة القضائية المأذون له أو المناب، مع ذكر تاريخ وساعة بداية العملية وانتهائها.

يذكر هنا أنه يتم تحرير محضرين حيث يتعلق المحضر الأول بالجانب التقني وبتاريخ وساعة بداية العملية وانتهائها، ويوجد محضر ثاني يدرج فيه مضمون اعتراض المراسلات أو الصور أو المحادثات، والتي تفيد في تقصي الحقائق، مع الاحتفاظ بالتسجيل برمته وجعله في حرز مختوم يضمن سلامته ولم يمنع القانون من أخذ نسخ احتياطية لذلك التسجيل، وما يلاحظ أن المشرع الجزائري لم يتطرق لمصير

[1] مرزوقي كريمة، مراقبة الاتصالات الإلكترونية وحق الفرد في الخصوصية المعلوماتية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 05، العدد 02، 2020، ص 1372.

السند المادي للتسجيل، خلافا للمشرع الفرنسي الذي نص على تحطيمه بعد انقضاء الدعوى العمومية نهائيا، بينما المحاضر تبقى مدرجة في ملف الدعوى[1].

ثالثا: الالتزام بكتمان السر المهني

حيث يشترط عدم الإخلال بالسر المهني واتخاذ جميع التدابير اللازمة لضمان احترام ذلك السر، وذلك تأسيسا على نص المادة 65 مكرر 6 التي تقضي بأن تتم العمليات المحددة في المادة 65 مكرر 5، دون المساس بالسر المهني المنصوص عليه في المادة 45 من القانون 06-22.

اشترطت املادة 10 من قانون رقم 09-04 على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذا املعلومات المحصلة منها، لذا يعاقب كل من يتجه نحو استغلال هذا الإجراء لأغراض شخصية، أو كل تجاوز لحدود المراقبة االلكترونية نحو انتهاك حرمة الحياة الخاصة للألفراد، و هذا ما أقرته املادة 4 من القانون أعلاه[2].

[1] جمال نجيمي، "قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي"، الجزء الأول، ط 04 ،دار هومة، الجزائر، 2018، ص161.

[2] مرزوقي كريمة، مرجع سابق، ص 1373.

الخاتمة

الخاتمة

إن ما أحدثته تكنولوجيا المعلومات من توفير خدمات نوعية وسريعة تلبي حاجيات الأفراد والمجتمعات والدول، يستدعى تحديث المنظومة القانونية لمواجهة أي استخدام سلبي لذلك، مما استوجب على المشرع الجزائري ملائمة النصوص القانونية للتطورات الحديثة والأخذ في الحسبان خصوصية التحقيق لضمان فاعليته بهدف الوصول إلى الحقيقة، وقد توصلنا إلى مجموعة من النتائج والتوصيات التي نوردها على النحو التالي:

النتائج :

- إن مفهوم الجرائم الالكترونية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات، وكنتيجة فلم يتفق على تحديد مفهوم جامع مانع لهذه الجرائم، و يمكن تعريفها بأنها الأفعال المخالفة للقانون التي ترتكب بواسطة الكمبيوتر عن طريق شبكة الانترنت.

- إن من أهم خصائص الجريمة الالكترونية، أنها تنصب على محل من نوع خاص يختلف تماما عن محل الجرائم التقليدية، فهذه الجرائم تستهدف المساس بالمعلومات الالكترونية المتواجدة في البيئة الرقمية على هيئة إشارات و نبضات غير مرئية تنساب عبر أجزاء النظام المعلوماتي و شبكات الاتصال العالمية.

- أما فيما يخص أجهزة التحري عن الجريمة الالكترونية ، فقد استحدث المشرع الجزائري هيئات غير قضائية لتدعم الهيئات القضائية المتخصصة و الوحدات الخاصة بالأمن و الدرك الوطني ،لمواكبة التطورات التكنولوجية الحديثة و تطويق نطاق الجريمة الالكترونية حيث تم إنشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الاتصال و مكافحتها بموجب القانون 09-04 ،كما تم إنشاء سلطة وطنية لمعالجة المعطيات ذات طابع شخصي بموجب القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، و تم استحداث وكالة خاصة

بأمن الأنظمة المعلوماتية بموجب مرسوم رئاسي سنة 2020 ، وكل ذلك في سبيل توفير حماية اكبر للأفراد والمجتمعات وضبط الجرائم الالكترونية والحصول على الأدلة التي تفيد في إثبات هذه الجرائم.

– توصلنا كذلك في هذا البحث إلى أن الطبيعة الخاصة للجريمة الالكترونية دعت المشرع إلى إعادة

تقييم بعض القواعد الإجرائية المتاحة في استخلاص الدليل كالمعاينة ، التفتيش ، الخبرة و الشهادة و جعلها ممكنة الاستعمال في مجال البيئة الرقمية ، وهو ما كان فعلا بموجب القانون 09-04 السالف الذكر ،فضلا عن استحداث نوع من القواعد الإجرائية الأخرى تتلاءم مع الطبيعة الرقمية التي يكون عليها الدليل المناسب في إثبات هذا النوع من الجرائم كالتسرب الالكتروني و المراقبة الالكترونية.

التوصيات:

بناءا على النتائج نالسابقة يمكم أن نقترح التوصيات التالية :

– ضرورة العمل على التحسيس بخطورة الجريمة الإلكترونية على الأمن العام وأمن الأفراد من خلال تدريسها في كلية الحقوق، فمثلا بإدراجها في محاور مقياس القانون الجنائي للسنة الثانية ليسانس.

– تفعيل دور المجتمع المدني ووسائل الإعلام في التحسيس بخطورة الجرائم الإلكترونية و ضرورة التبليغ عنها .

– الإستفادة من التجارب الدولية في المجال الالكتروني لكسب المهارات الازمة لمكافحتها.

– إنشاء دورات تكوينية بشكل دائم للمحققين والقضاة في مجال المعلوماتية والحواسيب، وتأهيلهم على كيفية التعامل مع هذا النوع من الجرائم.

– تدعيم الأجهزة المكلفة بالتحري عن الجرائم الإلكترونية في كل مرة بآليات وتقنيات ووسائل وأساليب جديدة تضمن المواجهة الفعالة.

- سن قوانين جزائية موضوعية وإجرائية خاصة بالجرائم الإلكترونية، وكذا الإسراع إلى تعديل وترشيد قوانينها القائمة بما يجعلها تسري وتطبق على مثل هذه الجرائم، تفاديا لإي قصور تشريعي وتخطيا للثغرات القانونية الحاصلة في هذا المجال، و التي قد يستفيد منها المجرم الإلكتروني لإفلات من المتابعة الجزائية و العقاب.

- ضرورة تكثيف التعاون والتنسيق الدولي في مجال مكافحة الجريمة الإلكترونية، عن طريق إبرام إتفاقيات دولية و إقليمية في هذا المجال، أو الإنضمام إلى الإتفاقيات المبرمة في هذا الخصوص.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا : النصوص القانونية

1- الأمر رقم 66- 155 المؤرخ في 18 صفر 1386 الموافق 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

2- القانون رقم (06-01) ، المؤرخ في20 فيفري 2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية ، العدد 14.

3- قانون رقم 09-04 ،المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 47.

4- قانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، عدد 34.

5- القانون رقم 06-01 مؤرخ في20 فيفري 2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 14.

ثانيا: المراسيم والقرارات

1- مرسوم رئاسي رقم 04 - 183، مؤرخ في 8 جمادى الأولى عام 1425 الموافق 26 يونيو 2004، يتضمن أحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطن وتحديد قانونه الأساسي، الجريدة الرسمية للجمهورية الجزائرية، عدد 44.

2- مرسوم رئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية، عدد 04.

3- مرسوم رئاسي رقم 20-183 مؤرخ في 13 جويلية 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 40.

ثالثا : الكتب

1-أبو شامة عبد المحمود عباس، عولمة الجريمة الاقتصادية، د ط ، غزة –المكتبة المركزية-قاعة عامة طالبات، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2007.

2-إدوار غالي الذهبي، الإجراءات الجنائية في التشريع المصري، ط2، مكتبة غريب، القاهرة، 1992.

3- أحمد خليفة الملط، الجرائم المعلوماتية، ط 02 ، دار الفكر الجامعي، الاسكندرية، 2006.

4- أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء2،د ط، دار الفكر العربي ، الجزائر،1999 .

5-أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، ط01، دار هومة للطباعة والنشر، الجزائر، 2006.

6-أوهابية عبد الله، شرح قانون الإجراءات الجزائية (التحري والتحقيق)، الجزء الثامن، ط 02 ، دار هومة، بوزريعة، الجزائر، 2004.

7- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، ط 01، دار الفكر الجامعي، الإسكندرية، 2011.

8-بلال أمين زين الدين، الجريمة المعلوماتية في التشريع المقارن والشريعة الإسلامية،د ط ، دار الفكر الجامعي، مصر، 2014.

9- بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، ط 01،دار الخلدونية، الجزائر، 2012.

10- بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الالية للمعطيات في التشريع الجزائري و المقارن،ط 01 ،منشورات الحلبي الحقوقية ، لبنان، 2012.

11- جمال نجيمي، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، ط 04 ،دار هومة، الجزائر، 2018.

12- الجو خدار حسن، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، دار الثقافة للنشر و التوزيع ، دار الثقافة للنشر و التوزيع ، عمان، ط 01 ، 2011.

13- حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، ط 01، دار النهضة العربية، القاهرة، 2017.

14- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية(دراسة مقارنة) ،ط 01 ،منشورات الحلبي الحقوقية، بيروت، 2014.

15- خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، ط 01 ،دار الثقافة، الاردن ، 2001.

16- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط 01 ،دار الفكر الجامعي، الإسكندرية،2009.

17- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط 01، دار النهضة العربية، مصر، 2011.

18- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري والمقارن، ط 01، منشورات الحلبي الحقوقية ،لبنان، 2012 .

19- رفعي سمير، البحث والتحري عن الجريمة الالكترونية، ط01، دار المثقف للنشر والتوزيع، الجزائر، 2019.

20- سامي جلال ففي حسين، التفتيش في الجرائم المعلوماتية (دراسة مقارنة)، ط01، دار الكتب القانونية، القاهرة مصر،2011.

21- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، د ط، دار الجامعة الجديدة، مصر،2007.

22- عبد العالي الديري ومحمد صادق اسماعيل ،الجرائم الالكترونية،ط ،01 المركز القومي للاصدارات القانونية، القاهرة،2012.

23- عبد الفتاح بيومي حجازي، الإثبات في جرائم الكمبيوتر والانترنت،د ط ، دار الكتب القانونية، مصر، 2007.

24- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، ط 01، دار الكتب القانونية، القاهرة، 2007.

25- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي،د ط ، دار الجامعية للطباعة و النشر، مصر 1999.

26- علي عدنان الفيل، اجراءات التحري و جمع الادلة و التحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، ط 01 ، المكتب الجامعي الحديث ،الاسكندرية ، 2012.

27- عوض محمد عوض، المباديء العامة في قانون الاجراءات الجنائية،ط 01 ،دار المطبوعات الجامعية،الاسكندرية، 2012.

28- فهد عبد الله العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، د.ط ،دار الجامعة الجديدة، الاسكندرية، 2016.

29- محمد أمين الشوابكة ، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)،ط 01،دار الثقافة للنشر والتوزيع، عمان، الاردن، 2009.

30- محمد سامي الشواء، ثورة المعلومات وانعكاساتها على قانون العقوبات،ط 01 ، دار النهضة العربية، القاهرة، 1994.

31- محمد علي سالم عياد الحلبي، الوجيز في أصول المحاكمات الجزائية، دار الثقافة، عمان، الطبعة الأولى،2009.

32- محمد كمال شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، ط 01، دار الجامعة الجديدة، الإسكندرية، 2018.

33- محمد منير الجنيبهي وممدوح محمد، الجوانب الإجرائية لجرائم الانترنيت والحاسب الآلي ووسائل مكافحهما، ط 01 ، دار الفكر الجامعي، الإسكندرية، 2005.

34- محمود أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية،ط 02 ، دار الثقافة للنشر والتوزيع ، عمان الاردن ، 2009.

35- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، ط 01، مطابع الشرطة، القاهرة، 2008.

36- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية ، ط 01 ،منشورات الحلبي ، بيروت ،2005

37- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، ط 01، دار الفكر الجامعي، الاسكندرية، 2007 .

38- نهلة عبد القادر المومني ، الجرائم المعلوماتية ،ط 02 ،دار الثقافة للنشر والتوزيع ،عمان،2010 .

39- هلالي عبد الاله احمد ، التزام الشاهد بالاعلام في الجرائم المعلوماتية، ط 02 ، دار النهضة العربية، القاهرة، 2008.

40- هلالي عبد الإله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية (دراسة مقارنة) ، الطبعة الأولى، دار النهضة العربية،القاهرة، 2000.

41- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، ط 01، دار المطبوعات الجامعية، الإسكندرية، مصر، 2009.

42- يوسف بن سعيد الكلباني، الحماية الجزائية للبيانات الالكترونية في التشريعين العماني والمصري (دراسة مقارنة)، ط 01، دار النهضة العربية، القاهرة، 2017.

رابعا : المقالات العلمية

1- ثابت دنيازاد، مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الإجتماعية والإنسانية، المجلد 05، العدد 06، 2012.

2- حمزة خضري وعشاش حمزة، خصوصية اركان الجريمة المعلوماتية ، مجلة الدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد بوضياف ، المسيلة، المجلد 06، العدد 02، 2020.

3- سميرة معاشي، ماهية الجريمة الالكترونية، مجلة المنتدى القانوني،كلية الحقوق والعلوم السياسية ،جامعة محمد خيضر، بسكرة، العدد07، مارس 2018.

4- الصبحي داوود سليمان، إجراءات التحري والبحث الجنائي،مجلة الدراسات الاسلامية ،كلية التدريب – قسم البرامج التدريبية- جامعة نايف العربية للعلوم الأمنية، الرياض، افريل 2009.

5-عربوز فاطمة الزهراء، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم الإلكترونية، مجلة جيل الأبحاث القانونية المعمقة، العدد 34، 2019

6- غزال نسرين، حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 56، العدد 1، 2019.

7- لزعر عزيز، زياني رشيد، آلية الإتحاد الإفريقي للتعاون الشرطي (الأفريبول) ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، كلية الحقو، جامعة مةلاي الطاهر، سعيدة، المجلد 14، العدد 03، 2021.

8- محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث،كلية الحقوق والاداب والعلوم الاجتماعية، جامعة 08 ماي 45 قالمة، العدد 01، سبتمبر 2009.

9-مرزوقي كريمة، مراقبة الاتصالات الإلكترونية وحق الفرد في الخصوصية المعلوماتية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 05، العدد 02، 2020.

10- هميسي رضا، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حقه لخضر بالوادي، الجزائر، ع 03، جوان 2012.

خامسا: الرسائل و المذكرات

أ: رسائل الدكتوراه

1- أومدور رجاء ،خصوصية التحقيق في مواجهة الجرائم المعلوماتية، اطروحة دكتوراه تخصص قانون خاص،كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد البشير الابراهيمي، برج بوعريريج ، 2020-2021.

2-ربيعي حسين، اليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015-2016 .

ب: مذكرات الماجستير

1- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة قاصدي مرباح ورقلة، 2012/2013.

2-ركاب أمينة، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبي بكر بلقايد، تلمسان،2014-2015.

3-سعيد علي نعيم، آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير ، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر باتنة، 2012-2013.

4- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة تخرج لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013.

5- عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، كلية الملك فهد الامنية-مركز البحوث و الداسات-،جامعة نايف العربية للعلوم الأمنية، السعودية، 2009 .

6-محمد بن نصير محمد السرحاني ، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، مذكرة ماجستير ، كلية الدراسات العليا ،قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

7- منصور بن صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، رسالة ماجستير في العدالة الجنائية، كلية الدراسات العليا ،جامعة نايف العربية للعلوم الأمنية، ، الرياض، 2010.

ج: مذكرات الماستر

1- رزيق محمد ،"إجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتية "،مذكرة لنيل شهادة الماستر في القانون العام، تخصص القانون الجنائي و العلوم الجنائية، كلية الحقوق و العلوم السياسية،قسم الحقوق ، جامعة اكلي محند اولحاج، البويرة،2018-2019.

سادسا: المداخلات العلمية

1- حملاوي عبد الرحمن، دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية ،قسم الحقوق، جامعة محمد خيضر بسكرة ، الموسوم بعنوان: الجريمة الالكترونية بين الوقاية و المكافحة ،يومي 16-17 نوفمبر 2015.

2- عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات"، المؤتمر العلمي الاول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، اكاديمية شرطة دبي، دبي، 2003.

3-عز الدين عز الدين، قيادة الدرك الوطني الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة الذي نظمته كلية الحقوق و العلوم السياسية ،قسم الحقوق، جامعة بسكرة ،يومي16-17 نوفمبر 2015.

4-هميسي رضا، أحكام الشاهد في الجريمة المعلومائية، بحث مقدم إلى أعمال الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الموسوم بعنوان الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و17 نوفمبر 2015.

5-هواري عياش ، المعهد الوطني الأدلة الجنائية مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية بين الوقاية والمكافحة ، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق و العلوم السياسية ،قسم الحقوق، جامعة محمد خيضر بسكرة ،يومي 16-17 نوفمبر 2015.

سابعا: مطبوعات علمية

1- خلفي عبد الرحمان، محاضرات في القانون الجنائي العام، محاضرات موجهة لطلبة السنة الثانية حقوق ل م د، كلية الحقوق و العلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2016-2017.

ثامنا: المواقع الالكترونية

1- المديرية العامة للامن الوطني: https://www.dgsn.dz.

2- وزارة الدفاع الوطني: https://www.mdn.dz.

فهرس الموضوعات

فهرس الموضوعات

الموضوع	الصفحة
مقدمة	2
الفصل الاول :الاطار النظري للتحري في جرائم الكترونية	8
المبحث الاول :ماهية الجريمة الالكترونية	9
المطلب الاول :مفهوم الجريمة الاكترونية	9
الفرع الاول : جريمة تعريف الالكترونية	10
اولا: التعريف الفقهي للجريمة الالكترونية	10
ثانيا: تعريف التشريع الجزائري للجريمة الالكترونية	13
الفرع الثاني: خصائص الجريمة الالكترونية	14
اولا: الخصائص المشتركة للجريمة الالكترونية مع الجرائم التقليدية	14
ثانيا: الخصائص التي تنفرد بها الجريمة الالكترونية عن الجرائم التقليدية	15
المطلب الثاني :اركان الجريمة الالكترونية	17
الفرع الاول :الركن المفترض	17
اولا: وجود نظام معالجة الية للمعطيات	18
ثانيا: ضرورة خضوع النظام للحماية	18
الفرع الثاني :الاركان الاساسية	20
اولا: الركن الشرعي	21
ثانيا: الركن المادي	22

ثالثا: الركن المعنوي	23
المبحث الثاني :الاختصاص بالتحري في الجرائم الالكترونية	24
المطلب الاول :مفهوم التحري في الجرائم الالكترونية	25
الفرع الاول :تعريف التحري عن الجرائم الالكترونية	26
الفرع الثاني :خصائص التحري عن جرائم الكترونية	27
اولا: السرية	28
ثانيا: التدوين	29
ثالثا: وضع خطة للتحقيق	30
المطلب الثاني:السلطات المختصة بالجرائم الالكترونية	31
الفرع الاول :تعريف جهاز التحري عن الجرائم الالكترونية	32
اولا: أجهزة مختصة بالتحري عن الجرائم الالكترونية على المستوى الوطني	32
ثانيا: الأجهزة المختصة بالتحري عن الجرائم الاكترونية عن المستوى الاقليمي و الدولي	43
ثالثا: منظمة التعاون القضاء الاتحاد الاوروبي الاوروجست	44
رابعا: رابطة رؤساء أجهزة الشرطة التابعة لرابطة أمم جنوب شرق اسيا	45
خامسا: الية الاتحاد الافريقي للتعاون الشرطي	45
الفرع الثاني :اقسام الاجهزة المختصة بالتحري في الجرائم الالكترونية	45
الفصل الثاني :اجراءات التحري في الجرائم الالكترونية	49
المبحث الاول :الاجراءات التقليدية للتحري في مجال مكافحة الجريمة	50
المطلب الاول :معاينة و تفتيش لمسرح الجريمة	50

الفرع الاول :المعاينة	51
اولا: تعريف المعاينة	53
ثانيا: مدى صلاحية مسرح الجريمة المعلوماتية للمعاينة	55
الفرع الثاني: تفتيش لمسرح الجريمة الالكترونية	55
اولا: تعريف التفتيش	56
ثانيا: اجراءات التفتيش في المنظومة المعلوماتية	60
ثالثا: ضمانات التفتيش في البيئة الالكترونية	63
رابعا: اثار التفتيش الالكتروني	65
المطلب الثاني :الخبرة و الشهادة في مجال الجرائم الالكترونة	66
الفرع الاول:الخبرة في مجال الجريمة الالكترونية	66
اولا: دور الخبرة في مجال الجرائم الاكترونية	67
ثانيا:ضرورة الخبرة	69
الفرع الثاني :الشهادة في مجال الجريمة الالكترونية	69
اولا: الشاهد الاكتروني	70
ثانيا : فئات الشاهد الالكتروني	71
ثالثا: التزامات الشاهد الالكتروني	72
المبحث الثاني :الاجراءات المستحدثة المتعلقة بالتحري عن جريمة الكترونية	72
المطلب الاول :التسرب الالكتروني	73
الفرع الاول: تعريف التسرب الالكتروني	74

اولا :صدور اذن قضائي بالتسرب	74
ثانيا:احترام المدة المقررة للتسرب	75
ثالثا:تسبب عملية التسرب	75
رابعا:محل التسرب	75
الفرع الثاني: شروط التسرب الالكتروني	76
المطلب الثاني: مراقبة الاتصالات الالكترونية	77
الفرع الاول: المقصود بمراقبة الاتصالات الاكترونية	79
الفرع الثاني: الضوابط المتعلقة بمراقبة الاتصالات الالكترونية	79
اولا :تحرير محضر	80
ثانيا :تحرير محضر	81
خاتمة	83
المصادر و المراجع	87
فهرس الموضوعات	97
الملخص	100

ملخص البحث:

تعتبر الجريمة الإلكترونية من الجرائم المستحدثة في عالمنا المعاصر، وبتطور الجريمة كان لزاما على الأجهزة المكلفة بالبحث والتحري تطوير امكانياتهم لمكافحة هذا النوع من الجرائم، وقد تناولنا من خلال هذه الدراسة، الإجراءات المتبعة من قبل تلك الأجهزة المكلفة ببابحث والتحري عن الجريمة الإلكترونية من أجل الحصول على الدليل المناسب لإثبات هذا النوع من الجرائم، حيث تناولنا في الفصل الأول الجانب النظري للجريمة الإلكترونية من خلال البحث في ماهية هذا النوع المستحدث من الجرائم، كما تناولنا السلطات المختصة بالتحري عنها، أما الفصل الثاني من هذه الدراسة فقد تناولنا فيه آليات البحث والتحري عن الجريمة الإلكترونية، وذلك من خلال البحث في الآليات التقليدية والمستحدثة منها.

الكلمات المفتاحية:

جريمة إلكترونية، مجرم إلكتروني، شهادة إلكترونية، تفتيش إلكتروني، تسرب إلكتروني.

The summary of study:

Cybercrime is considered one of the newest crimes in our contemporary world, and with the increase and development of technology, it was necessary for the agencies charged with investigation and research to develop their capabilities facing this type of crime. We discussed in this study the procedure adopted by the agencies to get the appropriate evidence to prove this type of crime. In the first chapter, we dealt with the theoretical aspect of cybercrime by researching what this new type of crime is, and we also dealt with the concerned authorities to investigate it. As for the second chapter of this study, we dealt with the mechanisms of research and investigation of cybercrime, by researching and discussing the traditional and the new mechanisms.