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

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم قانون عام

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

التحري و التحقيق في الجرائم الالكترونية

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق

التخصص: قانون جنائي و العلوم الجنائية

من إعداد الطالب(ة):

بن عمارة فاتن نور الايمان

تحت إشراف الأستاذ(ة):

د.الوافي الحاجة

أعضاء لجنة المناقشة

الأستاذ(ة).....لطروش امينة .....رئيسا

الأستاذ(ة).....الوافي الحاجة.....مشرفا مقررا

الأستاذ(ة).....بلحنافي فاطمة .....مناقشا

السنة الجامعية: 2024/2023

نوقشت يوم:2024/06/09

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

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
لإنجاز البحث

أنا الممضي أدناه،

السيد: الآنسة بن عمارة فاتن نور الإيمان الصفة: طالبة

الحامل لبطاقة التعريف الوطنية رقم: 106992067 والصادرة بتاريخ: 12/09/2023

المسجل بكلية: الحقوق و العلوم السياسية قسم: علوم جنائية

والمكلف بإنجاز مذكرة ماستر بعنوان:

المتورطين والمتحقين في الجرائم الالكترونية

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

التاريخ: 12/06/2024

إمضاء المعني

المصادقة على شرعية الإمضاء
السيد/ بن عمارة فاتن نور الإيمان
106992067
2023-09-12
رئيس المجلس الشعبي البلدي
بالتفويض
إمضاء: عبد [illegible]
12 جوان 2024

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

الإهداء

إلى من علمتني أن الحب ليس له أسباب وأن العطاء ليس له حدود إلى من كانت لي الأمان ومهدت لي طريق العلم إلى حياتي "**أمي**"

إلى سندي ومصدر فخري وعزتي إلى ملجئي ومأمني "**أبي**" الغالي

إلى من لا تحلو الحياة إلا بوجودها أختي "**نور الهدى**"

إلى من نحن امتداد له "**جدي** " العزيز

إلى كل من أعانني على إنجاز هذا البحث

إلى.....أنا

أهدي كل نجاح

مقدمـــة

إن الحمد لله نحمده ونستعين به ونستغفره ونعوذ بالله من شرور أنفسنا ومن سيئات أعمالنا، من يهده الله فلا مظل له، ومن يظلل فلا هادي له، وبعد.

يشهد عالمنا اليوم تطور هائل في عالم التكنولوجيا والرقمنة، التي يشهد لها الجميع بأنها ساهمت في تسهيل حياة الإنسان في مختلف الميادين، وقد أصبحت جزءً لا يتجزأ من حياته اليومية ولها تأثير على مختلف الأصعدة سواء كانت على الصعيد الشخصي أو الاقتصادي أو الاجتماعي أو غيرها الكثير.

ومما لاشك فيه أن هذه التكنولوجيا كغيرها من الأشياء تحمل بين طياتها إيجابيات وسلبيات ولعل من أبرز سلبياتها ما نشهده اليوم من سوء استغلال لها في التعدي على الآخرين وسلبهم حقوقهم، وخاصة على مواقع الشبكة العنكبوتية، التي وإن ساهمت في تحسين العديد من الخدمات وتقريب المسافات إلا أنها كذلك أصبحت وسيلة في أيدي المجرمين تسهل لهم عملية ارتكاب جرائمهم بكل سلاسة وحتى دون عناء التنقل.

مما أدى إلى استحداث نوع جديد من الجرائم أطلق عليه مصطلح الجريمة الالكترونية أو الرقمية.

وكان هذا من أهم الأسباب التي دفعت بنا إلى اختيار هذا الموضوع كمادة لبحثنا المتواضع، بالإضافة إلى كون هذا النوع من الجرائم عرف انتشاراً واسعاً خصوصاً على مواقع التواصل الاجتماعي، والذي ذهب ضحيته العديد من الأبرياء جلهم من المراهقين.

وكذا جهل العديد منهم بوجود جهاز قانوني كامل يعمل على التحقيق والتحري لمكافحة هذا النوع من الجرائم.

وقد وقع اختيارنا لهذا الموضوع لما له من أهمية في توعية الأفراد حول طرق مواجهة والتصدي للجرائم الالكترونية، والعمل على مكافحتها بهدف التقليل من نتائجها عن طريق كشف الستار حول طرق مواجهتها وكيفية التبليغ عنها.

وانطلاقاً مما سبق فقد جاء موضوعنا لطرح الإشكالية التالية: **كيف يمكن مواجهة الجرائم الالكترونية؟ وما هي سبل التصدي لها؟**

وقد نتج عن هذه الإشكالية عدة تساؤلات نذكر منها: كيف يتم التحقيق في الجريمة الالكترونية؟ من هي الهيئات المختص بهذا النوع من الجرائم؟ وغير ذلك.

وللإجابة على هذه الإشكالية وما تفرع عنها من أسئلة، فقد قمنا بدراسة الموضوع وفق الخطة التالية: حيث قمنا بتقسيم بحثنا إلى فصلين وكل فصل إلى مبحثين، وقد تناولنا في الفصل الأول ماهية جهاز التحقيق للجرائم الالكترونية وعالجنا هذا في مبحثين لكل منها مطلبين، أما عن الفصل الثاني فقد تحدثنا فيه عن طرق التحري والتحقيق في الجرائم الالكترونية، وهو الآخر تم معالجته في مبحثين لكل منهما مطلبين، وقد اتبعنا في هذا المنهج التحليلي لكونه يتلاءم وطبيعة النصوص القانونية، إلى جانب اعتمادنا أيضاً على المنهج الوصفي لوصف موقف المشرع الجزائري من هذا الموضوع.

ومن خلال اطلاعنا لاحظنا أن هذا الموضوع كان محل اهتمام الدارسين والباحثين في الشؤون القانونية سواء كانوا طلبة مقبلين على التخرج أو مختصين، ونذكر من بين هذه الدراسات ما يلي: التحقيق في الجريمة المعلوماتية، بوبعاية ابتسام والتي تناولت في دراستها أهم جوانب التحقيق والتحري في هذا النوع من الجرائم، بالإضافة إلى البحث المعنون بإجراءات التحري والتحقيق في الجريمة الالكترونية لصاحبه مباركية رابح والذي أتى على ذكر الخطوات والإجراءات المعتمدة في التحقيق للجرائم الالكترونية.

وقد اعتمدنا في دراستنا على مجموعة من المصادر نذكر منها:إجراءات التحري وجمع أدلة التحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة) لصاحبه علي عدنان الفيل، إلى جانب كتاب الدليل الالكتروني في القانون الجزائي لصاحبه مناصرة يوسف.

وككل عمل أو بحث علمي قد تواجهه بعض الصعوبات ، التي لم نكن بمنأى عنها والتي كان من أبرزها عدم تمكننا من الحصول على المراجع من مكتبة الجامعة، وصعوبة التنقل إلى مدن أخرى من أجل البحث عنها.

وختاماً نحمد الله المعين الذي وفقنا إلى إنجاز هذا البحث، كما لا يفوتنا أن نتقدم بكلمة شكر إلى لجنة المناقشة التي شرفتنا بقراءة بحثنا هذا ومناقشته، كما نتوجه بالشكر إلى أستاذتنا الوافي الحاجة التي أشرفت على بحثنا هذا وعلى ما قدمته لنا من توجيهات.

الفصل الأول

تمهيد:

بعد أن غزت التكنولوجيا مختلف الميادين، وحتى الحياة اليومية للأفراد أصبح من السهل التعدي على خصوصية الآخرين، وتفشى نوع من الجرائم عرف بالجريمة الالكترونية، ويقصد بها تلك الأنشطة الإجرامية التي تتم عن طريق الأنترنيت، ولها عدة أشكال كالاحتيال الالكتروني والتجسس الالكتروني، والاختراقات السبريانية، والتشويش على الخدمات الرقمية وغيرها.

وقد كان لزاماً على الدولة وضع جهاز للتحقيق والتحري في هذا النوع من الجرائم، كي لا تفتح المجال أمام المجرمين للقيام بما يرغبون دون رادع لهم.

ومع عدم استقرار الفقهاء على تعريف واحد مشترك للجريمة الالكترونية، فقد ارتأينا تسليط الضوء على بعض المفاهيم التي جاء بها الفقهاء في المبحث الأول من هذا الفصل، وكيفية التحقيق فيها.

وقد خصصنا المبحث الثاني من هذا الفصل لذكر السلطات المعنية بالتحقيق والتحري في الجرائم الالكترونية.

المبحث الأول: الجريمة الالكترونية والتحقيق فيها:

لقد استعرضنا من خلال هذا المبحث، بعض التعريفات التي وضعت للجريمة الالكترونية بالإضافة إلى مفهوم التحقيق الجنائي في الجريمة الالكترونية.

المطلب الأول: مفهوم الجريمة الالكترونية:

كما سبق لنا وأن ذكرنا أنه لم يكن هناك اتفاق من قبل الفقه الجنائي على تسمية واحدة للجريمة الالكترونية، فمنهم من أطلق عليها اسم الجرائم المعلوماتية، وهناك من يسميها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال، ويطلق عليها البعض الآخر جرائم الكمبيوتر والانترنت، وهناك من يسميها الجرائم المستحدثة[1]

الفرع الأول: تعريف الجريمة الالكترونية:

إن التشريعات تتعامل مع جرائم المعلوماتية بطرق مختلفة حسب البلد والنظام القانوني المتبع فيها، وقد يتم تعريف هذه الجرائم بشكل مباشر أو غير مباشر، كما أنه يوجد في بعض الأنظمة القانونية تعريف صريح للجريمة الالكترونية، وفي البعض الآخر لا نجد مثل هذه التعريفات الصريحة حيث تم تركها للفقه.

1/ التعريف الفقهي:

لقد انقسم الفقهاء إلى عدة مذاهب واتجاهات من أجل وضع تعريف شامل للجريمة الالكترونية:

حيث هناك من عرفها على أنها الجرائم ذات الطابع المادي، وآخرون عرفوها بأنها الجرائم التي تتركب باستخدام الحواسيب والشبكات، بمعنى أنها ما كان فيه اختراق الكتروني.

1 الشكري عادل يوسف عبد النبي، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العراق، العدد 07، 2011، ص 112.

ومن بين هذه التعريفات " الجريمة الالكترونية نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزونة داخل الحاسوب أو التي تحول عن طريقه"[1]

من خلال هذا التعريف يمكننا القول أن الجريمة الالكترونية لا تقع بالضرورة عن طريق استخدام الحاسوب، بل قد تحدث داخل نظام الحاسوب عموماً.

وفي تعريف آخر لها والذي جاء فيه "أنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"[2]

وفي هذا التعريف نرى أن أصحابه قد أسندوا مفهوم الجريمة الالكترونية إلى الأداة المستخدمة في الجريمة وأضافوا إلى ذلك "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً".

وقد وضع تعريف الجريمة الالكترونية في المؤتمر العاشر للأمم المتحدة لمنع الجريمة الذي جاء فيه "أنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية".[3]

2/ التعريف القانوني:

لقد أطلق المشرع الجزائري على الجريمة الالكترونية، اسم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والذي نص عليها في القانون 04/09 والذي يعد أول قانون عرف الجريمة الالكترونية ونص على كل أنواع المعاملات والخدمات الالكترونية، حيث جاء فيه "جرائم

[1] بوضياف إسمهان الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية المسيلة، الجزائر، العدد11، سبتمبر 2018، ص 351.

2 المرجع نفسه، ص 351

3 – زبيدة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر،2011، ص 43.

المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية أو نظام الاتصالات الالكترونية"[1]

ومن خلال هذا التعريف نجد أن المشرع ألم بمختلف جوانب الجريمة الالكترونية، فقد ذكر الجانب الموضوعي والذي يمس أنظمة المعالجة والبيانات والجانب الفني والتقني، الذي ينظر إلى استخدام وسائل الاتصالات الالكترونية.

وقد كان هذا التعريف شاملاً حيث تدخل تحت مظلة الجريمة الالكترونية، كل ما يتولد عن التطور التكنولوجي ووسائل الاتصال المتقدمة، كما يعكس تحديات التكنولوجيا الحديثة في مجال الوقاية ومكافحة الجريمة وتطبيق القانون.

ونرى من خلال هذا التعريف أيضاً أن المشرع قد راع في ذلك الانتشار الواسع والتطور السريع لوسائل التواصل الاجتماعي، والتي تلعب دوراً كبيراً في انتشار الجريمة وتنوعها، فبالإضافة إلى وضع مواد قانونية تنص على العقوبات المترتبة عن الجرائم الالكترونية، نجد أن الجزائر وكذلك العديد من الدول قد انضمت إلى اتفاقيات دولية وإقليمية لمكافحة الجريمة الالكترونية، مثل اتفاقية مجلس أوروبا لمكافحة جرائم الحاسوب، ومعاهدة مجلس أوروبا للجرائم الالكترونية.

وفي الأخير يمكن أن نقول: أن الجريمة الالكترونية هي نشاط إجرامي بواسطة استخدام التكنولوجيا، انطلاقاً من استخدام الشبكة العنكبوتية، إلى الأنظمة الرقمية، وصولاً إلى استخدام الكمبيوتر كوسيلة وأداة للإجرام، والتي تسبب تهديداً على المستوى الشخصي والعام، وطنياً ودولياً.

[1] القانون 04/09 المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر 74، الصادرة في 2009/08/16.

الفرع الثاني: خصائص وأنواع الجرائم الالكترونية:

أ/ خصائص الجريمة الالكترونية:

إن الجرائم الالكترونية هي جرائم حديثة حداثة التكنولوجيا ووسائل الاتصال، مما جعلها تتميز بخصائص تجعلها مختلفة عن الجرائم التقليدية، والمتمثلة فيما يلي:

1- عابرة للدول والقارات:

إن الجريمة الالكترونية لا تحكمها الحدود الدولية، فهي غير خاضعة لسلطة المكان، بحيث تمتد عبر الحدود الوطنية حتى إنها تبلغ القارات المختلفة، مما يجعلها تحدياً كبيراً للسلطات القانونية والأمنية في جميع أنحاء العالم، حيث أتاحت للمجرمين ارتكاب جرائمهم دون الحاجة إلى التواجد في مكان الجريمة.[1]

وهذا ما يجعل من الصعب تتبعهم ومعاقبتهم،كون أن المجتمع المعلوماتي يعمل على محو الحواجز الجغرافية ويجعل ارتكاب هذه الجرائم سهل وهذا ما دفع بالدول إلى اللجوء إلى ما يسمى بالتعاون الدولي لمكافحة الجريمة الالكترونية.

2- سهلة الارتكاب:

إن خاصية السهولة التي تتميز بها الجريمة الالكترونية تعد سيفاً ذو حدين بالنسبة لها، فهي إن كانت سهلة الارتكاب لاستخدامها تقنيات التكنولوجيا وتوفر الأدوات لها، والتي يمكن استخدامها بسهولة، هي نفسها ماتسهل عملية القبض على المجرمين، فهي تختلف عن الجرائم التقليدية لحاجة هذه الأخيرة إلى الوقت والجهد العضلي والعقلي.

1 ميرفت محمد حبابية، مكافحة الجريمة الالكترونية، دار اليازوري العلمية، الجزائر، 2022،ص 40

3-ارتكاب الجريمة الالكترونية بواسطة جهاز الكتروني والتحكم بتقنية استخدامه:

إن الجريمة الالكترونية كغيرها من الجرائم لا تتم إلا بأداة للجريمة، وفي هذا النوع من الجرائم يعتبر الجهاز الالكتروني أهم وسيلة للجريمة.

فالجريمة الالكترونية تتطلب تكوين علمي، ودراية تامة بالجوانب التقنية التي تركز على استخدام وسائل الاتصالات الالكترونية. وكلما زادت الخبرة والتكوين في هذه المجالات كلها ازدادت صعوبة اكتشاف هذه الجرائم.[1]

4- صعوبة إثبات الجريمة:

إن التطور التكنولوجي جعل من عملية إثبات الجريمة الالكترونية عملية صعبة، ومعقدة في نفس الوقت، وهي بذلك تختلف عن الجرائم التقليدية التي غالباً ما تكون فيها الأدلة ملموسة على عكس الجرائم المعلوماتية فإثباتها يعد تحدياً بسب عدة عوامل منها:

- التقنيات المتقدمة.
- تشفير البيانات.
- تعدد الهوية الرقمية.
- عدم توفير الأدلة الرقمية.

بالإضافة إلى نقص الوسائل والأجهزة الحديثة التي تعطل عمليات البحث والتحقيق في الجرائم الالكترونية.[2]

[1] عبد الصديق شيخ، الوقاية من الجرائم الالكترونية في ظل القانون رقم 04/09، مجلة معالم الدراسات القانونية والسياسية، الجزائر، العدد 01، 2020، ص 194.

2 المرجع نفسه، ص196.

5- جرائم هادئة:

من أهم مميزات الجرائم الالكترونية أنها جرائم هادئة، حيث تتم الجريمة في صمت خالية من كل أشكال العنف، فهي تبدو هادئة من السياق الظاهري كون أن الجاني يعمل من خلف الكواليس، دون ترك أي أثر واضح، إلا أن هذا الهدوء يحمل بداخله مخاطر وأضرار كبيرة على الأفراد والمجتمعات من الناحية المالية، والخسائر الشخصية، إلى جانب انتهاك الخصوصية.

6- مهارة المجرمين التقنية:

يتميز المجرمين في الجرائم الالكترونية، بتكوين علمي على أعلى مستوى، إلى جانب معرفة واسعة بتقنيات الحماية، ومهارة عالية في إخفاء هوياتهم، كما يملكون المهارة في اختراق الأنظمة الأمنية، وسرقة المعلومات الحساسة، والاحتيال عبر الانترنت، وهذا ما يجعل من تتبعهم والكشف عن هويتهم أمراً صعباً.

ب/ أنواع الجريمة الالكترونية:

بعد ذكر الخصائص المميزة للجريمة الالكترونية، لابد لنا من ذكر الأنواع والأشكال التي تكون عليها الجريمة الالكترونية، وهي عديدة كون أنها تشمل مجموعة من الأنشطة غير القانونية التي تتعلق بالشبكة العنكبوتية أو التكنولوجيا الرقمية وتتمثل هذه الأنواع في:

1- الاحتيال عبر الانترنت:

وهذا النوع من الجرائم يتم فيه استخدام الوسائل الالكترونية، قصد الحصول على الأموال أو المعلومات، ويكون ذلك باستخدام تقنيات التلاعب لإقناع الضحية بتحقيق الهدف المراد.[1]

1رحموني محمد، خصائص الجريمة الالكترونية، دراسة استراتيجية، العدد11، 2018/01/10، أدرار، الجزائر،ص447.

2- الاختراق الالكتروني

ويتمثل في استخدام التكنولوجيا والمهارات التقنية، بهدف الوصول إلى معلومات بطريقة غير شرعية، وبدون إذن قصد سرقة البيانات أو تعطيل الخدمات الرقمية، وهذا النوع من الجرائم شائع في الوسط الإجرامي الالكتروني، والتي يعاقب عليها القانون في العديد من البلدان.

3- التجسس الالكتروني:

لقد عرف التجسس الالكتروني على أنه "أحد صور الإرهاب الالكتروني، يقوم باستخدام التكنولوجيا الضارة بشكل سلبي من أجل إحداث آثار مدمرة وأضرار بالغة لمحطات التحكم وأجهزة الكمبيوتر وشبكات الاتصال بدوافع سياسية أو عرقية أو دينية...الخ"[1]

من خلال هذا التعريف يمكننا القول أن التجسس الالكتروني، هو طريقة للحصول على معلومات سرية، أو حساسة بدون إذن وبطريقة غير مشروعة، والتي تمس بأمن الدولة.

4- التهديد والابتزاز الالكتروني:

يقصد بالتهديد "نشر وزرع الخوف في نفسية الشخص، بالضغط على إرادته وتخويفه من أن ضرراً ما سيلحق به أو سيلحق أشخاص أو أشياء له بها صلة"[2]

ويتضح لنا من خلال هذا التعريف أن المجرم يلجأ إلى استخدام الضغوطات على الضحية من أجل سلبه المال، أو معلومات أو خدمات، وقد عرف هذا النوع من الجرائم انتشاراً كبيراً على مستوى العالم، لكنه على عكس بقية أنواع الإجرام الالكتروني، سهل الكشف عن الجاني وتتبعه.

1 نجاري بن حاج علي فايزة، جريمة التجسس الالكتروني، دراسة استراتيجية، العدد11، السداسي الأول، 2019، ص66.
2 عراب مريم، حريمة التهديد والابتزاز الالكتروني، مجلة الدراسات القانونية المقارنة، المجلد07، العدد 01، 2021،ص1206

5- انتهاك حقوق الطبع والنشر:

ويقصد به استخدام أو نشر محتوى محمي بحقوق النشر، دون الحصول على إذن من صاحب هذه الحقوق، وتعتبر هذه العملية نوع من أنواع الجريمة الالكترونية لأنها عبارة عن التعدي على أملاك الآخرين الفكرية، فالتوزيع والنسخ دون إذن جريمة يعاقب عليه القانون.

6- الجرائم الالكترونية الأخلاقية:

وهي جرائم تمس بأخلاقيات وقيم المجتمع، كالتحرش عبر الانترنت، والشتم والقذف عبر مواقع التواصل الالكتروني، وانتهاك الخصوصيات وغيرها من الجرائم التي تعمل على أذية الضحية بشكل شخصي ومعنوي.

ومن خلال ما سبق ذكره، يمكننا أن نقول أن المشرع الجزائري اهتم بالجرائم الالكترونية، ويظهر ذلك من خلال وضعه لقوانين تجرم هذه الأفعال وتعاقب عليها، ولعل من أهم هذه المواد القانونية المتعلقة بالجرائم المعلوماتية، المادة 394 مكرر من قانون العقوبات الجزائري التي تنص على " يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة وبغرامة مالية من 50.000دج إلى 100.000دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريقة الغش المعطيات التي يتضمنها".[1]

تجرم هذه المادة كل أعمال الغش التي تتم في معطيات النظام المعلوماتي، كما أقر المشرع المادة 301 مكرر من قانون العقوبات، والتي تتعلق بجرائم إفشاء أو تسجيل أو نقل أو بث صور بطريقة غير قانونية وبدون إذن، ونلاحظ في هذه المادة أنها اهتمت بالأفعال غير القانونية التي تنتهك خصوصيات الأشخاص.

1 المادة 394 مكرر7 من القانون 15-04 المؤرخ في 2015/02/11، الجريدة الرسمية، العدد06، المؤرخة 02/10.

أما فيما يخص المادة 04/09 المتعلق بالقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية والتي تتضمن قواعد لحماية البريد ووسائل الاتصال المختلفة حفاظاً على الخصوصية وحماية للأسرار.

المطلب الثاني: التحقيق في الجريمة الالكترونية:

تعد مرحلة التحقيق في الجرائم عموماً وفي الجريمة الالكترونية خصوصاً، من أهم المراحل التي من خلالها تسهل عملية القبض على المتورطين، إلا أن التحقيق في الجريمة الالكترونية يختلف عن التحقيق في الجرائم العادية.

الفرع الأول: تعريف التحقيق الجنائي في الجريمة الالكترونية:

إن معظم التشريعات الجنائية لم تعرف التحقيق الجنائي في الجرائم الإلكترونية، وترك ذلك إلى الفقه، ويعتبر التحقيق الجنائي صراع بين المحقق والمجرم، ويعرف على أنه: "عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجرائم الالكترونية الرقمية من فاعل ودليل الكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل".[1]

أي أن عملية التحقيق تكون مبنية على أوامر من جهة قانونية، يقوم على تنفيذها ضابط مختص، وتكون الأدلة فيها بحسب نوعية الأدوات المستخدمة في الجريمة أي أن تكون رقمية ويشرف على هذه التحقيقات جهاز مختص في الجرائم الالكترونية.

وهناك من عرف هذا النوع من التحقيق على أنه: "الإجراءات التي يقوم بها مأموري الضبط القضائي أو المحققين عبر العالم الافتراضي لضبط الجريمة الالكترونية والتثبت من أدلتها ومعرفة فاعليها تمهيداً لإحالتهم للمحاكمة"[2]

وفي هذا التعريف نجد أن أصحابه قد حددوا أرضية البحث والمتمثلة في العالم الافتراضي ومحاولة الكشف عن ملابسات الجريمة لينتهي التحقيق بتسليم الجاني للقضاء.

1 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، 2009، ص166.

خالد علي نزار الشعار، التحقيق الجنائي في الجرائم الالكترونية، مذكرة دكتوراه، جامعة المنصورة، 2022، ص2.5

وفي تعريف آخر نجد أن هناك من اعتبره "علم يضم إجراءات نظرية وعلمية تحت إشراف مجموعة من المحققين لكشف الجريمة والإيقاع بالمتورطين"[1]

ومن خلال هذا التعريف يتضح لنا أن التحقيق هنا ليس مجرد تتبع لأثر الجريمة بل هو أكبر من ذلك فهو علم قائم بذاته يبحث في تقنيات وله نظريات وآراء علمية تعمل على تسهيل عملية الوصول إلى الجاني والاقتصاص منه وتحقيق العدالة.

يمكن لنا أن نستخلص مما سبق من تعريفات أن التحقيق في الجريمة الالكترونية هي مجموعة الإجراءات التي يقوم بها المحققين قصد جمع الأدلة المتعلقة بجرائم المعلوماتية، وذلك عن طريق استخدام مجموعة متنوعة من الأدوات والتقنيات المواكبة للتطور التكنولوجي بغية الوصول إلى معلومة دقيقة توصلنا إلى الحقيقة، وكذلك الاستعانة بشركات التكنولوجيا.

الفرع الثاني: مميزات التحقيق الجنائي:

إن للتحقيق الجنائي في الجرائم الالكترونية له عدة خصائص تميزه عن غيره من التحقيقات والمتمثلة في:

1-أول ميزة لهذا النوع من التحقيق هي الاستقلالية كونها تنتمي إلى بيئة الكترونية مما يجعل التحقيق يرتبط بمواقع التواصل الاجتماعي، وبيئة شبكة الانترنت.

2- من حيث الأدلة، فهي تختلف عن أدلة الجرائم العادية كونها عبارة عن بيانات ومعلومات يتم استخراجها من الأجهزة الالكترونية كالكمبيوتر، مما يجعلها أدلة يصعب التعامل معها إلا من قبل محققين مختصين وعلى مستوى عالي من التعليم المتخصص في هذه التقنيات.

1 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2010، ص18.

3- يتميز التحقيق الجنائي الالكتروني بكفاءة عالية للمحققين وذكائهم وقوة ملاحظتهم[1] ليتمكنوا من القيام بتحليل البيانات والمعلومات الرقمية، التي يحصلون عليها كأدلة للجريمة.وتتبع الأنشطة الالكترونية غير القانونية، كما يعتمد التحقيق على أدوات وتقنيات متقدمة.

4- يتميز التحقيق في الجرائم الالكترونية بالسرية "..عدم إطلاع الغير على مجريات التحقيق وفقاً لما نصت عليه المادة 11 من قانون الإجراءات الجزائية"[2]

بالإضافة إلى التدوين وكتابة جميع إجراءات التحقيق في محاضر مصادق عليها رسمياً، وأخيراً وضع خطة التحقيق.

1 محمد صلاح محمد عبد المنعم، الجرائم الالكترونية وتحدياتها دراسة مقارنة، رسالة دكتوراه، المنصورة،2005، ص225.

2 خلد ممدوح إبراهيم، المرجع السابق، ص19.

المبحث الثاني: السلطات المعنية بالتحقيق والتحري في الجرائم الالكترونية:

إن الهيئات المختصة في التحقيق في الجرائم الالكترونية، تختلف من دولة إلى أخرى، كما أن معظم الدول تكون لها جهة مختصة في مكافحة الجرائم الالكترونية كالوكالة الوطنية للأمن ،التابعة للولايات المتحدة الأمريكية، ومنظمة الشرطة الجنائية الدولية، وهي تابعة لهيئة التعاون الدولي لمكافحة الجرائم الالكترونية.

وسننطلق من هنا للحديث عن الهيئات المعنية في التحقيق في التشريع الجزائري، وعلى هذا الأساس قمنا بتقسيم هذا المبحث إلى مطلبين:

المطلب الأول: حول الهيئات الوطنية المختصة.

المطلب الثاني: حول الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

المطلب الأول: الهيئات القضائية المختصة:

سنتطرق في هذا المطلب إلى ذكر الجهات التي تملك سلطة التحقيق في الجرائم الالكترونية التي لها خصائص تميزها عن الجرائم التقليدية.

الفرع الأول: الضبطية القضائية:

يلجأ المشرع الجزائري إلى تخصيص ضبطية قضائية مختصة بالتحري والتحقيق في الجرائم الالكترونية، لكونها جرائم معقدة وصعبة الإثبات، حيث يكون عمل هذه الضبطية بعد وقوع الجريمة[1]

أي أن هذه الضبطية لا عمل لها إلا بعد وقوع الجريمة، على عكس الضبطية الإدارية والتي تكمن مهمتها في منع وقوع الجريمة[2]

وقد قسم المشرع الجزائري ضبطية القضاء إلى:

1- على مستوى جهاز الشرطة:

أنشأت المديرية العامة للأمن مخبر مركزي بمركز الشرطة شاطونان بالجزائر العاصمة ومخبرين بهوين بكل من قسنطينة ووهران وتحتوي على فروع تقنية من بينها خلية الإعلام الآلي وفرق متخصصة مهمتها التحقيق والكشف على جرائم الانترنت[3] بالإضافة إلى ثلاث مخابر على مستوى بشار، ورقلة، وتمنراست، قيد الإنجاز لنشر هذا الفرع في كافة أنحاء الوطن، كما أن هناك مخبر الذي جاء باسم الأدلة الرقمية والآثار التكنولوجية على مستوى مخبر الشرطة العلمية والتي تشمل ثلاث ولايات: الجزائر، وهران، قسنطينة، وهو عبارة عن

1 حازم حسن الجمل، الحماية الجنائية للأمن الالكتروني، دار الفكر والقانون، القاهرة، 2015، ص62.

2 المرجع نفسه، ص63.

3 فلاح عبد القادر، آيت عبد المالك نادية، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019، ص 1695.

مخبر خاص يتولى مهمة التحقيق في الجرائم الالكترونية، ويعمل على جمع الأدلة الرقمية وتحليلها للكشف عن التهديدات الأمنية التكنولوجية ومكافحتها، حيث تنقسم إلى 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 الالكترونية[1]

ويعتمد نجاح الضبطية القضائية كذلك على التعاون بين جهاز الشرطة والجهات القضائية بالإضافة إلى تكوين أفراد الشرطة لمكافحة الجرائم الالكترونية واستخدام التقنيات الحديثة لجمع الأدلة الرقمية.

إن الضبطية القضائية تشير إلى الإجراءات والتدابير التي يتخذها جهاز الشرطة في الجزائر للتصدي للجرائم المعلوماتية.

كما يوجد فرق متخصصة في الجرائم الالكترونية على مستوى أمن الولايات تابعة لمصالح الشرطة القضائية وتتكون من خبراء تقنيين متخصصين في مجال الحوسبة، وأمن المعلومات والتحقيق الرقمي، وغيرها من المجالات ذات الصلة.

2- على مستوى جهاز الدرك الوطني:

يعد الدرك الوطني من الأجهزة التي تعمل على مكافحة الجريمة الالكترونية، وذلك بواسطة المعهد الوطني للأدلة الجنائية وعلم الإجرام الكائن مقره ببوشاوي، وهو تابع لقيادة الدرك العامة قسم الإعلام والإلكترونيك الذي يختص بالتحقيق والكشف عن الجرائم الالكترونية.[2]

1 فلاح عبد القادر، آيت عبد المالك نادية، المرجع السابق، ص 1696.

2 المرجع نفسه، ص 1696.

ويعتبر هذا المعهد مؤسسة عمومية ذات طابع إداري، تم إنشاؤه بمرسوم رئاسي رقم 183-04 بتاريخ 2004/06/26، وهو عبارة أيضاً عن أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيا المناسبة، حيث يساعد في توجيه التحقيقات وكشف الحقائق باستخدام الأدلة العلمية والتحليلية، كما يقدم دعماً فنياً لوحدات التحقيق والشرطة القضائية، مما يسهم في تقديم خدمة العدالة بشكل أكثر فعالية ودقة.

الضبطية القضائية تتم بموجب إشراف وكيل الجمهورية المختص، الذي يعتبر ممثل النيابة العامة في المحكمة، ويتولى مسؤولية إشراف التحقيقات الجنائية واتخاذ القرارات القانونية المناسبة بناءً على الأدلة المقدمة، وهو المسؤول عن إعطاء صلاحية مباشرة التحقيق لمصالح الأمن.

كما أن للدرك الوطني وحدات متنوعة على مستوى القيادة العامة لتنفيذ مهامه والتحقيق في الجرائم الالكترونية وتقسم إلى:

- المصالح المركزية للتحريات الجنائية.
- المصالح والمراكز العلمية والتقنية.
- هياكل التكوين.
- المعهد الوطني لعلم الإجرام.

الفرع الثاني: صلاحية الضبطية القضائية:

إن الاختصاص النوعي في النظام القضائي يعني تحديد نوع معين من الجرائم التي يتم التحقيق فيها من قبل أعضاء الضبطية القضائية، مثل الجرائم الالكترونية ويساعد هذا

الاختصاص على تركيز الجهود والموارد القضائية في مجال المعلوماتي.[1] ونستخلص من هذا أن النظام القضائي قائم على وضع لكل نوع من التحقيقات جهاز خاص به لضمان الحصول على نتائج دقيقة وسريعة، ودون الخلط بين القضايا.

كما يوجد الاختصاص المحلي والذي يقصد به المجال الإقليمي الذي يباشر فيه ضابط الشرطة القضائية مهامه في التحري والتحقيق عن الجريمة الالكترونية.

وتتمثل صلاحية الضبطية القضائية في:

– مراقبة الانترنت ووسائل التواصل الاجتماعي: تملك الضبطية القضائية صلاحية مراقبة الانترنت للبحث عن أنشطة غير قانونية وغير مشروعة التي تهدد سلامة أمن الوطن.

– تتبع الجرائم الالكترونية: كما لها صلاحية التعاون مع وكالات أمنية دولية لتتبع الجرائم الإلكترونية التي تتجاوز الحدود الوطنية.

– إصدار أوامر الاعتقال وتقديم الدعم الفني للتحقيقات: يمكن أن تقوم الشرطة أو الدرك الوطني بالتحقيق الالكتروني وجمع الأدلة الرقمية وتحليلها إلى جانب إصدار أوامر الاعتقال وذلك تحت إشراف وكيل جمهورية مختص.

– التعاون مع مزودي الخدمات الالكترونية: تتعاون الضبطية القضائية مع شركات تقنية والمعلوماتية للحصول على معلومات تساعدها على حل القضايا.

– حظر الوصول: يمكن للشرطة الالكترونية منع الوصول إلى مواقع غير مشروعة.

– اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: لقد نصت المواد 65 مكرر5 إلى غاية 65 مكرر 10 من تعديل قانون الإجراءات الجزائية، بالسماح للضبطية القضائية اللجوء

[1] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، ص343.

في الجرائم المعلوماتية[1] بشرط الحصول على إذن وكيل الجمهورية المختص، أو قاضي التحقيق.

– تمديد الاختصاص المحلي للجهات القضائية:

وفقاً للمواد 40 مكرر 01 إلى غاية المادة 40 مكرر من قانون الإجراءات الجزائية المعدل والمتمم بموجب القانون 04-14 و06-22 حيث يجب على ضابط الشرطة القضائية في مرحلة البحث والتحري المتعلق بالجريمة المعلوماتية أن يخبر فوراً وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة ويقدم له أصل ملف الإجراءات، ومن ثم يتم تقرير الاختصاص أو عدم الاختصاص لأن الشرطة القضائية تتلقى تعليمات مباشرة من وكيل الجمهورية للمحكمة ذات الاختصاص الموسع[2].

– عملية التصدي للجريمة الالكترونية: يقوم جهاز الدرك الوطني بالتصدي للجرائم باستخدام التقنيات الرقمية الحديثة كما له صلاحية تقديم الدعم للمؤسسات الحكومية لتعزيز أمان أنظمتها الالكترونية وحماية بياناتها، كما يعمل أيضاً على تقوية التعاون الدولي في مجال مكافحة الجرائم الالكترونية.

المطلب الثاني: الهيئة غير القضائية للتحقيق في الجريمة الالكترونية:

بعد الحديث عن الجهات القضائية وأجهزة الدولة التي تعمل على مكافحة الجريمة الالكترونية سنمر في هذا المطلب للحديث عن الهيئات غير القضائية المكلفة بالتحقيق في الجرائم المعلوماتية، والمتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، التي لها دور هام في التحري عن هذا النوع من الجرائم.

---

[1] جباري عبد المجيد، دراسات قانونية عن المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، 2012،ص1.29

[2] قانون رقم 22/06 مؤرخ في 20 ديسمبر2006ن يعدل ويتمم الأمر رقم 155/66 المؤرخ في 08 يونيو1966، والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84، الصادر بتاريخ 24 ديسمبر2006.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

لقد حذا المشروع حذو باقي التشريعات المقارنة وقام بالبحث عن هيئات متخصصة تقوم بمساعدة الدولة وتنتهج منهج وقائي، وقد لجأ المشرع إلى فكرة السلطة الإدارية[1] وأنشئت الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال بموجب المادة 13 من القانون رقم 09-04 المؤرخ في 2009/08/05 حيث نصت على: "تنشأ الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم"[2] وقد صدر التنظيم في 2019 وجاء فيه تحديد مقر الهيئة بمدينة الجزائر مع إمكانية نقله إلى أي مكان آخر عبر التراب الوطني[3]، وذلك بقرار من وزير الدفاع الوطني، وتتمتع بالشخصية المعنوية والاستقلالية المادية تحت سلطة وزارة الدفاع الوطني[4]

وقد تأسست هذه الهيئة للعمل على مكافحة الجرائم التي ترتكب باستخدام تكنولوجيا المعلومات والاتصالات، كما تهدف إلى حماية المجتمع من جرائم الانترنت وتعمل أيضاً على توعية الناس بأخطار هذه الجرائم وكيفية الوقاية منها.

ولقد كانت سابقاً توضع تحت وصاية العدل سنة 2015 لتنتقل إلى وزارة الدفاع الوطني في 2019، ولها مجلس توجيهي ومديرية عامة يترأسها وزير الدفاع الوطني أو ممثله وهذا حسب ما نصت عليه المادة الخامسة والتي جاء فيها: "التنظير وتشكيل مجلس التوجيه والذي يتشكل من ممثلي الوزارات الآتية: وزارة الدفاع الوطني، الوزارة المكلفة بالمواصلات السلكية واللاسلكية"

إن مجلس التوجيه يعمل على تقييم حالة التهديد في هذه الجرائم، لتحديد مضامين عملية المراقبة الواجب القيام بها، كما يبدو واجب مجلس التوجيه أيضاً إعداد تقرير سنوي لنشاطات

---

[1] سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية، المجلة النقدية للقانون والعلوم السياسية، مجلد 17، عدد02، 2022،ص502.

2 المادة 13 من القانون 09-04، المؤرخ في 2009/08/05، الجريدة الرسمية عدد 47، الصادرة في 2009/08/16.

3 المادة الأولى من المرسوم الرئاسي رقم 19-172، المؤرخ في 2019/06/06، الجريدة الرسمية عدد2019،37

4.المادة الثانية من نفس المرسوم.

الهيئة والتي يجب أن يتم المصادقة عليها، حيث يجتمع مجلس التوجيه في السنة مرتين بناءً على استدعاء من رئيسه وهذا في دورة عادية، أما دورة غير عادية يمكن اجتماعه بطلب من الرئيس أو أحد أعضائه.

أما المديرية العامة للهيئة، والتي تتولى السهر على حسن سير الهيئة، وذلك لضمان فعاليات وسلامة عمل الهيئة وتحقيق أهدافها بنجاح، بالإضافة إلى إعداد مشروع الميزانية، وإعداد وتنفيذ برنامج عمل الهيئة، وتتولى أيضاً تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها، يعتبر جزء حيوي من الجهود المبذولة للحفاظ على الأمن الرقمي، وأيضاً تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتعرف عليهم.

كل هذه الصلاحيات منصوص عليها في المرسوم الرئاسي رقم 19-172 في المادة 09، وما نصت عليه أيضاً المادة 10 على أن: "تضم المديرية العامة: مديرية تقنية، مديرية الإدارة والوسائل، مصالح"[1]

يتضح لنا من خلال ما سبق أن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال هي مؤسسة عمومية ذات طابع إداري، تتميز باستقلاليتها وذات شخصية معنوية ومن أهم النتائج المترتبة عن الاعتراف بشخصية العمومية هي[2]:

ذمة مالية مستقلة: تتمتع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال باعتبارها شخصية معنوية بذمة مالية مستقلة.

الأهلية: يتم منح أهلية قانونية لشخص معنوي لممارسة الأنشطة القانونية للهيئة الوصية للوقاية من الجرائم الإعلام والاتصال فالشخص المعنوي يملك الحق في التقاعد وغيرها من السلطات الذي تخوله القوانين والأنظمة وقانونه الأساسي وسند إنشائه"

1 المادة 10 من المرسوم السابق.

2 سهيلة بوزبرة، المرجع السابق، ص564.

الموطن: وهو المكان لذي يوجد فيه والذي حدد من قبل المشرع والذي جعل مقرها بمدينة الجزائر.

تحمل مسؤولية التعويض عن الأضرار التي تسببها للغير: بما أن الهيئة الوطنية للوقاية من الجرائم المتصلة بالإعلام والاتصال تتمتع بشخصية معنوية فهي مسؤولة عن أي أضرار تسببها للغير سواء كان ضرر مادي أو معنوي.

الفرع الثاني: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بالإعلام والاتصال:

نصت المادة 14 من القانون 09-04 على أنه تتولى الهيئة مجموعة من المهام نذكر منها:

1- الوقاية من جرائم الإعلام والاتصال: وهي عملية التوعية لمستخدمي التكنولوجيا حول خطورة جرائم الاختراق والتجسس على الاتصالات والرسائل الالكترونية، ويعد هذا أمر بالغ الأهمية في عصرنا الرقمي الحالي.[1] وذلك باتخاذ عدة إجراءات لتحقيق هذه الغاية، مثل توفير موارد تثقيفية عبر الانترنت، وتشجيع المستخدمين على تحديث أنظمة التشغيل والتطبيقات الخاصة بهم بانتظام، وغيرها من الإجراءات.

2- مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: نصت المادة 14 من القانون 09-04 على طرق مكافحة الجريمة الالكترونية والمتمثلة في

أ- مساعدة السلطات القضائية الداخلية: من مهام الهيئة مساعدة السلطات القضائية ومصالح الشرطة في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، وعليه تتدخل الهيئة بطلب من الجهات القضائية المختصة، ولقد سحب المشرع في المرسوم الرئاسي رقم 19-172، والمرسوم الرئاسي

[1] بن عنصر سهام، التحقيق الجنائي في الجرائم الالكترونية، مذكرة لنيل الماستر، جامعة مولود معمري، تيزي وزو، 2005،ص54.

رقم 15-261، اختصاص المراقبة الالكترونية من جميع الهيئات الأخرى وخوله لهذه الهيئة بصفتها مساعد للجهة القضائية[1]

ب- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوحيا الإعلام والاتصال: وهي عبارة عن جهود مشتركة لجهات متعددة لمكافحة الجرائم المتعلقة بالتكنولوحيا والاتصال وهي جهود تقوم بها الهيئة لتعزيز الوعي والحماية من الجرائم الالكترونية. تقديم المساعدة لمصالح الأمن والدرك الوطنين ولجميع إدارات الدولة المركزية يعد جزءً أساسياً من دور الهيئة في مكافحة الجرائم الالكترونية، وذلك من خلال تبادل المعلومات والموارد والتعاون في التحقيقات والعمليات الأمنية.

ج- مساعدة السلطات القضائية الأجنبية: جاء في الفصل السادس من قانون 09-04 السالف الذكر وتحت عنوان التعاون والمساعدة القضائية الدولية، أنه يمكن اللجوء في إطار التعاون الدولي إلى إجراءين هما: تبادل المعلومات، وطلب إجراءات تحفظية.

- تبادل المعلومات: نصت المادة 17 من القانون 09-04 على أن: "تتم استجابة طلبات المساعدة الرامية لتبادل المعلومات"، وهذا يشمل تقديم المعلومات والوثائق التي تطلبها السلطة القضائية الجزائية، أو تلك التي تطلبها دولة أجنبية من الجزائر بشأن جريمة، كما أيضاً تساعد على تعرف الجهات القضائية على الماضي الجزائي (صحيفة السوابق القضائية) لشخص المتهم ويتضح ذلك بواسطة اتفاقات تبادل المعلومات بين الدولتين الطالبة والمطلوب منها.[2]

- طلب إجراءات تحفظية: وهو إجراء قضائي من إجراءات الدعوى الجزائية تتقدم به الدولة الطالبة إلى الدولة المطلوب منها وهو ما نصت عليه المادتين 16 و17 من القانون 09-04 السالف الذكر، ويمكن أن تشمل هذه الإجراءات إصدار أوامر مؤقتة من المحكمة مثل حظر

[1] حابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في مواجهة الجرائم المجلة الدولية للبحوث القانونية والسياسية، المجلد05،العدد03، ديسمبر 2021، ص474،473.

2 المرجع نفسه، ص 476.

السفر، تجميد الأموال وغيرها من الإجراءات وذلك وفقاً للاتفاقيات الدولية ذات الصلة، والاتفاقيات الثنائية، ومبدأ المعاملة بالمثل.

وتكون لطلبات المساعدة القضائية الدولية شروط منصوص عليها في المواد 18 و19 من القانون 09-04 من بينها:

- يمكن رفض المساعدة في حال المساس بالسيادة الوطنية، والنظام العام.

- استجابة طلب المساعدة بشرط المحافظة على السرية حول المعلومات المبلغ عنها وعد استعمالها في حالات أخرى غير معنية بالطلب.

د- ضمان المراقبة الوقاية للاتصالات الالكترونية للكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية، والمساس بأمن الدولة.

هـ- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.

و- تحديث المعايير القانونية في مجال الاختصاص يعتبر جزء مهم من عملية تطوير القوانين المتصلة بالإعلام والاتصال.

إن المشرع الجزائري أغفل الحديث عن دور الهيئة للوقاية من الجرائم المتصلة بالإعلام والاتصال، ومكافحتها في الحالات الاستعجالية والطارئة.[1]

1 حابت أمال، المرجع السابق، ص 478.

الفصل الثاني

طرق التحري والتحقيق في الجرائم الالكترونية:

يشهد عالمنا اليوم ثورة في عالم الرقمنة والتكنولوجيا التي أصبحت جزءاً مهماً في حياتنا اليومية لما توفره لنا من خدمات تسهل علينا أعمالنا، واهتماماتنا، كما أنها تعمل على فتح فرص عديدة لتطوير ذاتنا، إلا أن هذا الانفتاح على عالم التكنولوجيا والانترنت بخاصة كان بالنسبة للإنسان بمثابة السيف ذو حدين، وهذا ما ذكرناه في الفصل الأول من بحثنا هذا بحيث تمخض عن هذا التطور التكنولوجي نوع جديد من الجرائم والذي عرف باسم الجريمة الالكترونية، وقد سبق لنا تقديم تعريفات لها، الأمر الذي دفع بالسلطات القانونية والتنظيمية إلى التركيز على تطوير استراتيجيات جديدة لمكافحتها، ليأتي دور التحري والتحقيق في الجرائم الالكترونية، والمتمثل في عملية جمع الأدلة الرقمية والبيانات الالكترونية، لتحديد مرتكبي الجرائم إلى جانب توثيق الجرائم ووسائلها المتمثلة في أجهزة الكمبيوتر، والشبكات الالكترونية، كما يعتمد في عملية التحقيق استخدام تقنيات وأدوات التحليل الرقمي، من أجل تحليل البيانات واستخلاص الأدلة.

المبحث الأول: الدليل الالكتروني في الجرائم الالكترونية:

إن التطور التكنولوجي وخصائص أنظمة المعالجة الآلية سيغير حتماً العديد من المفاهيم الشائعة حول إجراءات وأساليب الحصول على الأدلة الرقمية، الأمر الذي يتطلب بالضرورة إعادة تقييم أساليب معينة لإدخال الإجراءات التقليدية والقواعد الإجرائية في قانون الإجراءات الجزائية ليتوافق مع طبيعة البيئة التقنية.

ولتوضيح ذلك بصورة مفصلة قمنا بتقسيم هذا البحث إلى مطلبين، أولهما سيكون حول "**مفهوم الدليل الالكتروني**"، أما فيما يخص المطلب الثاني فقد أدرجناه تحت عنوان "**حول شروط العمل بالدليل الالكتروني**".

المطلب الأول:مفهوم الدليل الالكتروني وخصائصه:

قد خصصنا هذا المطلب من أجل تحديد تعريف مفصل للدليل الالكتروني، مع ذكر الخصائص المميزة له:

الفرع الأول: تعريف الدليل الالكتروني:

1/ لغةً: الدليل المرشد، جمع أدلة، وأدلاء، ما يستدل به، الدليلة الواضح[1]، الكاشف عن الشيء[2].

2/ اصطلاحاً: "هو ما يوصل بصحيح النظر فيه بمطلوب خبري"[1]، والمقصود بهذا التعريف أن الدليل هو ما يلزم من العلم به العلم بشيء آخر، أي أن معرفة حقيقته توصلنا إلى معرفة حقيقة أخرى.

[1] مجموعة من العلماء في اللغة العربية، المعجم الوسيط في اللغة العربية، ج1، مطبعة مصر شركة مساهمة مصرية،

[2] الفيروز آبادي، القاموس المحيط،

وبعد تقديم تعريف مبسط حول مصطلح الدليل، ننتقل إلى تعريف الدليل الالكتروني بصفة مفصلة، والذي تعددت تعريفاته، وسنقوم بتقديم بعض منها:ذ

تعريف الدليل الالكتروني: ويعرف أيضاً بالدليل الرقمي وقد جاء في أحد تعريفاته على أنه: "المعلومات المخزنة أو المنقولة بصفة رقمية، ويعتمد عليها في التحقيقات وأمام المحكمة إما بالإدانة أو البراءة"[2]، ويتضح لنا من خلال هذا التعريف أن كل معلومة رقمية سواء كانت مخزنة أو منقولة ويمكن لها أن تثبت الجرم على المتهم أو تبرئه فهي بمثابة دليل الكتروني يمكن اعتماده أمام المحكمة.

وفي القانون المصري رقم 175 لسنة 2018، الخاص بمكافحة جرائم تقنية المعلومات فقد عرف الدليل الرقمي بأنه: "أي معلومة الكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة"[3].

ونجد هنا أن المشرع المصري استخدم مصطلح الدليل الرقمي بدل الدليل الالكتروني إلا أن هذا لم يغير في ماهية الدليل الالكتروني حيث نلمس في هذا التعريف تشابهاً كبيراً مع التعريف السابق، مع إضافة بعض التفاصيل والتي تتمثل في أن المعلومات مأخوذة من الحواسيب أو الشبكات المعلوماتية، بالإضافة إلى أن هذه المعلومة يجب أن تكون قابلة للتحليل باستخدام أجهزة أو برامج خاصة.

---

[1] محمد الحسن، شرح الورقات في أصول الفقه، دروس صوتية، موقع شبكة الإسلامية، www.islamweb.net، ص7.

[2] خالد ضو، حجية الدليل الالكتروني وشروط قبوله في الثبات الجنائي، مجلة الباحث الأكاديمية في العلوم القانونية والسياسية، المركز الجامعي، الأغواط، العدد 8، مارس 2022، ص 203.

[3] خالد ممدوح إبراهيم، الإثبات الالكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي، الإسكندرية، 2020، ص36.

كما عرفه البعض "بأنه يشمل جميع البيانات الرقمية التي يمكن أن تثبت بأن هناك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني، أو توجد علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة الرسومات، الخرائط، الصوت أو الصورة"[1]، أي أن الدليل الالكتروني هو كل معلومة رقمية يمكننا من خلالها إيجاد علاقة رابطة بين المجرم والجريمة أو الضحية بغض النظر عن شكل هذه المعلومة.

كما عرف أيضاً على أنه: " معلومات يقبلها المنطق والعقل ويعتمدها العلم، ويتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الكمبيوتر وملحقاتها، وشبكات الإتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة أو الجاني أو المجني عليه"[2]، ولعل هذا التعريف أشمل وأوضح مما سبقه من تعريفات لما ورد فيه من تفاصيل حول الدليل الالكتروني فهو وإن لم يخرج عن الإطار العام لتعريف الدليل الالكتروني كما ورد فيما سبق إلا أنه زاد عليها أن هذا الدليل يجب أن يكون خاضعاً لمنطق العقل بالإضافة إلى أنه لا يمكن الحصول عليه دون اللجوء إلى البرتكول القانوني الذي تفرضه مراحل التحقيق، كما يمكن أن يكون حاضر في مختلف مراحل التحقيق من بدايتها إلى غاية المحاكمة.

[1] وهيبة لعوارم، الدليل الرقمي في مجال الإثبات الجنائي وفقاً للتشريع الجزائري، المجلة الجنائية القومية، المجلد 57، العدد2 يوليو 2014، ص70.

[2] المرجع نفسه، ص 70.

ويمكن القول أن الدليل الالكتروني هو الدليل الذي يجد له أساساً في العالم الافتراضي ويقود إلى الجريمة، أو هو ذلك الدليل الذي ينشأ في العالم الرقمي، والذي يكون على شكل مستخرج مادي يتم قبوله في جلسة المحاكمة[1].

ومن التعريفات السابق ذكرها يمكننا أن نقول بأن الدليل الالكتروني هو كل معلومة مخزنة في العالم الرقمي على شكل معلومات أو بيانات رقمية يمكن من خلاله معرفة الحقائق وتوثيقها مع مراعاة الإجراءات القانونية للحصول عليه لضمان صحته وقبوله في المحكمة.

الفرع الثاني: خصائص الدليل الالكتروني:

تمتلك الأدلة الرقمية الجنائية العديد من المزايا التي تميزها عن جميع أشكال الأدلة الجنائية الأخرى، وتتمثل هذه المزايا في:

أ/ الدليل الرقمي دليل علمي: يعتبر الدليل الرقمي عادة دليل علمي، كونه يشير إلى موارد مثل المواقع الالكترونية أو التطبيقات التي تقدم معلومات أو خدمات عبر الأنترنت، وبشكل أوضح هو مجموعة البيانات والمعلومات ذات هيئة الكترونية غير ملموسة لا تدرك بالحواس العادية بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية، واستخدام نظم برامجية حاسوبية، فهو ينتمي إلى مجال تقني[2].

ب/ الدليل الرقمي ذو طبيعة تقنية: أصبح الوصول إلى الدليل الرقمي ممكنا من خلال الاستخدام المكثف للتكنولوجيا، ويشمل ذلك توظيف أنظمة الكمبيوتر والشبكات الالكترونية لتخزين وتنظيم البيانات، كما يعتمد على قواعد البيانات وتقنيات البحث والتحليل البياني، مما يجعله يسهل عملية المعرفة والمعلومات العلمية بشكل سريع وموثوق.

[1] محمد بن فردية، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي(دراسة مقارنة)، ص 278.

[2] وهيبة لعوارم، المرجع السابق، ص71.

ج/ الدليل الرقمي غير مرئي: يأتي الدليل الالكتروني في شكل غير مرئي كما عهدنا ذلك في الشكل التقليدي للدلائل الورقية، فهو عبارة عن مجموعة من البيانات والمعلومات المخزنة والمنظمة بشكل الكتروني، ويتم التعامل معها بواسطة استخدام الأجهزة ومعدات الحاسب الآلي ونظم برمجيات الحاسوب[1].

د/ صعوبة التخلص من الدليل الرقمي: تعتبر هذه الميزة من أهم مميزات الدليل الرقمي، والتي تميزها عن باقي الأدلة " حيث يقتضي الأمر مقارنة بين الدليل الرقمي والدليل الجيني، الذي يطلق عليه اسم الحمض النووي، وذلك لاتحاد كل منها في هذه الخاصية والمتمثلة في صعوبة التخلص منهما، وهذا ما يستوجب مقارنة الأدلة الرقمية بالأدلة التقليدية"[2]، وهذا القول يوضح لنا مدى تشابه كل من الدليل الالكتروني بالدليل الجيني لأنهما غير قابلان للإتلاف بسهولة كما هو حال الدليل المادي، الذي يكون عرضة للتدمير والإتلاف الكلي بكل يسر وسهولة، بحيث لو استخدمت طرق التخلص من الدليل الرقمي في الحاسب الآلي، فلن تكون هناك أي مشكلة في استعادته لوجود برامج حاسوبية يمكن من خلالها استرجاع البيانات التي تم التخلص منها وحذفها من قبل.

هـ/ الدليل الرقمي قابل للنسخ: تعمل هذه الميزة على التقليل أو إزالة مخاطر إتلاف الأدلة الأصلية، حيث تتطابق طريقة النسخ مع طريقة الإنشاء، مما يشكل ضمان لحفظ الدليل الرقمي ولا نجد هذه الخاصية في الأدلة التقليدية[3].

و/ الدليل الرقمي يسجل معلومات عن الجاني ورصدها وتحليلها: وعن هذه الخاصية يمكننا القول أن الدليل الرقمي يمنحنا فرصة كشف كل ما يخص الجاني لتمكنه من "تسجيل تحركات

---

[1] عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، ص61.

[2] وهيبة لعوارم، المرجع السابق، ص 72.

[3] محمد بن فردية، المرجع السابق، ص 278.

الأفراد وسلوكياتهم، مما يجعل من الدليل الالكتروني سهل الوصول إليه مقارنة مع الدليل المادي، كما يتميز بسعة تخزينية عالية"[1] أي أن الدليل الرقمي يمكننا من الوصول إلى مرتكب الجريمة بسهولة.

ز/ الدليل الالكتروني متنوع ومتطور: يشمل مصطلح الأدلة الالكترونية جميع البيانات والمعلومات الرقمية التي يمكن تداولها رقمياً بمختلف أشكالها وأنواعها، بغض النظر عما إذا كانت هذه الأدلة مضمنة في أجهزة الكمبيوتر أو غيرها من الأجهزة أو الأنترنت أو شبكات الاتصالات التي تعد غنية جداً بمعلومات متنوعة عن الوقائع التي قد تشكل وتصل إلى مستوى أدلة البراءة أو الإدانة، وهذا التنوع هو عبارة عن اتساع قاعدة الدليل الجنائي الرقمي[2].

ح/ التعامل مع الدليل الالكتروني يحتاج إلى خبراء ومحققين مختصين: إن طبيعة الدليل الالكتروني التقنية والفنية تحتم وجود محققين مختصين وعلى مستوى عالي من المعرفة بالمجال الرقمي والتكنولوجي للعناية بمسرح الجريمة واستخرج الأدلة الرقمية[3].

إن الحديث عن خصائص الدليل الالكتروني يقودنا إلى ضرورة الحديث عن أنواع الدليل الإلكتروني، بحيث يتميز بتعدد أنواعه، التي تختلف عن أنواع الدليل التقليدي، حيث يمكننا تقسيم الدليل الالكتروني إلى ثلاثة أنواع:

1/ السجلات المحفوظة في الكمبيوتر: وتتمثل في مجموعة الوثائق المكتوبة والمحفوظة مثل البريد الالكتروني، وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الانترنت[1]، أي

---

[1] وهيبة لعوارم، المرجع السابق، ص 73.

[2] خطوي مسعود، عكوش حنان، خصوصية الدليل الالكتروني، مجلة الفكر القانوني والسياسي، المجلد 7، العدد 1، 2023، ص1065.

[3] بندر عقاب حقين كميخ حطاب الدويش، خصائص وأنواع الدليل الالكتروني، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، مجلة علمية محكمة، الكويت ص 827.

أن كل ما يخزن على الكمبيوتر أو ما يتم القيام به من عمليات داخل الشبكة العنكبوتية ووسائل التواصل الاجتماعي هو بمثابة نوع من أنواع الدليل الرقمي الذي يمكن اللجوء إليه من أجل التحقيق في الجرائم الالكترونية.

2/ السجلات التي تم إنشاؤها بواسطة الكمبيوتر: كما سبق لنا وأن ذكرنا أن التكنولوجيا قد غزت جميع الميادين وبالأخص المصالح الإدارية لمختلف القطاعات، كونها تسهل وتسرع من عملية إنجاز المعاملات المختلفة، ويقودنا هذا إلى إنشاء سجلات كفواتير أجهزة السحب الآلي سجلات الهاتف، الكارت الالكتروني الذكي[2]، التي يمكن أن تستخدم كأدلة للإدانة أو البراءة في عملية التحقيق.

3/ السجلات التي تمت معالجتها عن طريق برامج الكمبيوتر: إن كل عملية لمعالجة البيانات والمعلومات من أجل حفظها أو إنشائها عن طريق برامج الانترنت والكمبيوتر تعد نوعاً من أنواع الدليل الالكتروني كأوراق المعاملات المالية التي تحتوي على مدخلات تتم معالجتها عن طريق برامج الكمبيوتر[3].

ونظراً للتطور الدائم لتكنولوجيا المعلومات، قد نجد أنواع أخرى للدليل الالكتروني، كما يجب علينا أن نشير إلى أن الدليل الالكتروني رغم أنه مستحدث وذو طبيعة صعبة ومعقدة، إلا أنه وبكل أنواعه يعتبر دليل مادي مهما كان شكله، سواء مخرجات ورقية أو غير ورقية.

---

[1] خالد ممدوح المرجع السابق، ص 37.

[2] يس حسن محمد عثمان، الدليل الرقمي وأثره على الدعوى الجنائية، مجلة العلوم القانونية والاجتماعية، المجلد 5، العدد3، سبتمبر 2020، ص 319.

[3] المرجع نفسه، ص 319.

على عكس الأدلة التقليدية التي قد تكون مادية كأن يمسك الجاني وبيده سلاح الجريمة، أو معنوية والتي تتميز بكونها غير ملموسة كاعتراف المتهم بجرمه وقد أطلق عليه اسم الأدلة الناطقة[1].

[1] بن الطيبي مبارك، رحموني محمد شروط قبول الدليل الرقمي كدليل الإثبات في الجريمة الالكترونية، مجلة القانون والعلوم السياسية، المجلد 5، العدد2، ص 24.

المطلب الثاني: شروط العمل بالدليل الالكتروني في الإثبات الجنائي:

إن الدليل الالكتروني هو المادة المستخرجة من أحد النظم المعلوماتية، أو من أحد الأجهزة الالكترونية، أو شبكات الاتصال لإثبات حق مدعي به أمام القضاء أو نفيه[1]، ومن خلال هذا نستطيع القول أن أي معلومة يكون مصدرها الكمبيوتر أو الانترنت ويمكن اعتمادها لإدانة شخص أو تبرئته فهي بمثابة دليل الكتروني، ولكن لنتمكن من اعتمادها كأدلة رسمية وكي تقبل من قبل القاضي لابد لها من الخضوع لشروط تضمن صحتها ومصداقيتها للأخذ بها في مراحل التحقيق وأثناء المحاكمة.

الفرع الأول: الشروط العامة لقبول الدليل الالكتروني:

1/ مشروعية الدليل الرقمي: والمقصود بهذا أن يتم استخراج الدليل الالكتروني وفق إجراءات قانونية كما هو منصوص عليه في ق. إ.ج، وأي مخالفة لما ورد فيه من قواعد يؤدي إلى بطلان الدليل المستخرج، لهذا ولكي تتأكد صحة الدليل الرقمي يجب أن يخضع للنظام العام الذي نص عليه الدستور[2]. وكمثال لذلك تسجيل المكالمات الهاتفية والتي يجب أن تكون بناءً على أمر قضائي، وأي تسجيل دون ذلك لا يمكن اعتماده كدليل، وهذا ما أوصى به المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في البرازيل ونص على "كل الأدلة التي يمكن الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة، ولا يمكن التمسك بها أو مراعاتها"[3] من خلال هذا نرى أن القانون حفظ حق المتهم

---

[1] طارق عفيفي صادق أحمد، نظرية الحق، المركز القومي للإصدارات القانونية، القاهرة،2016، ص 309.

[2] بن الطيبي مبارك، رحموني محمد، المرجع السابق، ص27.

[3] محمد سعيد عبد المولى، شروط قبول الدليل الالكتروني في الإثبات الجنائي، 2021/10/29، jordan-lauyer.com، تم الاطلاع عليه يوم 2024/05/07.

في حماية خصوصيته وأي تجاوز لهذا الحق يعد بمثابة تعدي عليه ولا يمكن قبول ما ينتج عن هذا التجاوز كأدلة أمام المحكمة.

كما صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 28/ 1981/01 على اتفاقية خاصة بحماية البيانات الشخصية للأفراد وعدم انتهاكها.

كما يجب أن يكون جمع الأدلة الرقمية من قبل السلطة المعنية والتي نص عليها المشرع الجزائري في المادة 12 من ق.إ.ج، والتي نصت على "يقوم بمهمة الضبط القضائي رجال القضاء والضباط والأعوان والموظفون"، ونصت أيضاً في الفقرة الثالثة "يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها مادام لم يبدأ فيها بتحقيق قضائي"[1]، نرى في هذه المواد إشارة إلى وجوب الحصول على الأدلة سواء مادية أو رقمية بواسطة الضبطية القضائية تحت إشراف وكيل الجمهورية.

2/ يقينية الدليل الرقمي: ويعني بهذا أن يكون الدليل الرقمي المستخرج من الحاسوب أو الانترنت غير قابلة للشك أو الطعن فيها، وأن تكون قريبة من الحقيقة بعيدة عن الظن لكي يتمكن من الحكم بها، ويمكن اعتبار اليقين حالة ذهنية وعقلية تؤكد وتدعم وجود الحقيقة، لتسهيل عملية إقناع القاضي بالدليل الرقمي[2].

3/ وجوب مناقشة الدليل الالكتروني: وهذا الشرط يكون خاص بالدليل الجنائي بصفة عامة حيث ينبغي لإعمال حق الإثبات وحق النفي في المادة الجزائية اتخاذ إجراءات الإثبات في مواجهة الخصوم وتمكينهم من مناقشة الأدلة المقدمة من طرف الجهات المختصة بالتحقيق

[1] الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق لـ8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم بالقانون 06-28 المؤرخ في 29 ذي القعدة 1427 الموافق ل 20 ديسمبر 2006، الجريدة الرسمية الجمهورية الجزائرية، العدد 84، الصادرة ب 04 ذو الحجة 1427 الموافق ل 24 ديسمبر 2006.

[2] بن الطيبي مبارك، رحموني محمد، المرجع السابق، ص 27.

كما يراد بهذه القاعدة (وجوب مناقشة الدليل في المواد الجزائية) أن القاضي لا يمكن أن يؤسس اقتناعاته إلا على أدلة الإثبات التي طرحت في جلسات المحاكمة أمامه وخضعت لما يسمى بحرية مناقشة أطراف الدعوى[1]، ومن خلال ما ذكر يمكننا القول أنه من أجل إثبات صحة الدليل وأخذه بعين الاعتبار لابد له من أن يخضع للمناقشة وأن يكون معلن عنه في جلسات المحاكمة.

حيث تعد هذه القاعدة من القواعد الأساسية المنصوص عليها في التشريع الجزائري، وهذا ما نصت عليه المادة 02/212 من قانون الإجراءات الجزائية وجاء فيها: "لا يسوغ للقاضي أن يبني قراره إلا من الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة حضورياً أمامه"[2]، وهذا ما يؤكد ما قلناه سابقاً حول عرض الدليل أثناء المحاكمة.

وقد أكدت عليه المحكمة العليا في قرارها المؤرخ 2010/01/07.

ويمكننا القول في الأخير أنه يجب على القاضي مناقشة الدليل أمام الخصوم كي يتيح لهم فرصة إبداء الرأي فيه وليكون على دراية بما قدم ضده من أدلة.وهذه القاعدة تنطبق على جميع الأدلة سواء كانت مستخرجة من الكمبيوتر أو شبكة الانترنت أو عبارة عن معطيات مخزنة في وسائل حفظ وتخزين البيانات أو على شكل أشرطة وأقراص، عند الأخذ بها كأدلة الإثبات أمام المحكمة، مما يحقق لنا مبدأ الوجاهية الذي يعد من بين أهم المبادئ التي تضمن محاكمة عادلة، وتمكين الخصوم من حق الدفاع بعد مناقشة الأدلة حضورياً.

[1] مناصرة يوسف، الدليل الالكتروني في القانون الجزائي، دار الخلدونية، الجزائر، 2021، ص 148،147,

[2] المادة 212 من قانون الإجراءات الجزائية الجزائري.

4/ أن تكون الأدلة الرقمية ذات صلة بالواقعة: من الضروري أن يكون هناك ترابط بين الدليل الرقمي وبين الواقعة، ليكون ذو قيمة وفعالية في إثبات الواقعة أو نفيها، وذلك وفقاً لقرار جهة التحقيق أو المحكمة المختصة[1].

الفرع الثاني: حجية الدليل الرقمي في الجريمة الالكترونية:

إن مرحلة الحكم تعتبر من أهم المراحل في الدعوى الجنائية، فهو أهم إجراءات الدعوى وذلك كونه يمثل غايتها، وعملية تقدير الأدلة تمثل جوهر الحكم وذلك بممارسة القاضي لسلطته التقديرية على الأدلة[2].

تعتبر الجزائر واحد من الدول التي تتبنى نظام إثبات الحر في مجال الإثبات الجنائي وهذا يعني أنها تسمح بإثبات الجرائم باستخدام أي طريقة من طرق الإثبات، باستثناء الحالات التي ينص فيها القانون على غير ذلك، وفقاً للمادة 212 من قانون الإجراءات الجزائية السابق الذكر، حيث يحق للقاضي أن يعتمد أي دليل يراه مناسب لإصدار قراره، ويجوز للقاضي أن يبني قراره على هذا الدليل حسب قناعاته الشخصية، وهذا ما يجعل مناقشة الأدلة أمام القاضي أثناء المرافعة أمراً مهماً،

كما قرر المشرع الجزائري ضمن إطار تعزيز قرينة البراءة، وتعزيز ممارسة الفرد لحق الدفاع بإتاحة حرية تقديم أدلة الإقناع في مواجهة القاضي، وهذا يعد قصور تشريعي واضح فلا يوجد أي ذكر في قانون الإجراءات الجزائية لحقيقة أن الأدلة الالكترونية هي نوع خاص

[1] عماد مفلح الحسان، عز الدين أحمد النعيمي، الجرائم المستحدثة، دار الخليج للنشر والتوزيع، ط1، الأردن، عمان،2024، ص128.

[2] بن الطيبي مبارك، رحموني محمد، المرجع السابق، ص28.

ويثير عدم وجود نص قانوني صريح في هذا الصدد المسائل التالية المتعلقة بطبيعة الأدلة الواجب تقديمها إلى السلطات القضائية[1].

إن الطبيعة العلمية للأدلة الالكترونية جعلت صلاحية القضاة في تقييم هذه الأدلة محل جدل فقهي، حيث هناك من يرى أن الدليل العلمي ومنه الدليل الالكتروني له قوة الثبوتية الملزمة حتى للقاضي، وهناك من يرى بأن مبدأ حرية القاضي في الرفض يمتد ليشمل جميع الأدلة، أي توسيع نطاق هذه السلطة دون استثناء حتى الأدلة الرقمية، فالمشرع الجزائري –كما ذكرنا سابقاً– أنه أجاز في طرق الإثبات استثناء الإثبات في جرائم معينة المنصوص عليها في القانون الإجرائي الجزائي.

كما نصت المادة 215 منه على أن: "لا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك" وفي هذه المادة نلاحظ تقرير مبدأ الاقتناع الشخصي للقاضي الجزائري.

مبدأ الاقتناع القضائي:

إن مبدأ الاقتناع القضائي من أهم المبادئ في نظام الإثبات الحر، وقد كرس المشرع الجزائري مبدأ الاقتناع القضائي في المادة 307 من قانون الإجراءات الجزائية التي نصت على: "إن القانون لا يطلب من القضاة حساباً عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما"[2]،

[1] بوبكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2012، ص 507، 508.

[2] قانون الإجراءات الجزائية code de procedure penale، مطبوعات الديوان الوطني للأشغال التربوية، ط4، 2005، ص102.

وهذا يدل على أن للقاضي أن يعتمد على اقتناعه الشخصي وتقديره للأدلة من أجل النطق بالحكم.

كما أصرت المحكمة العليا على احترام مبدأ الاقتناع القضائي، وأوصت بإجراءاتها أمام المحاكم الجزائية. وإن القاضي في تقديره للأدلة سواء كانت تقليدية أو رقمية، لا يكتفي بمحاضر التحقيق، بل يجب عليه الاستماع إلى الشهود الذين سبق لهم أن قدموا أقوالهم أثناء التحقيق الابتدائي، بالإضافة إلى اعترافات المتهم نفسه، وهذه الإجراءات التي يقوم بها القاضي بهدف أن لا يكون هناك وسيط بين الدليل والقاضي، ليساهم في تكوين قناعة القاضي بعد هذه المناقشات التي تجري أمامه في الجلسة[1].

نستخلص مما سبق أن القاضي يجب أن يقتنع بدليل الإدانة والأدلة الرقمية المقدمة أمامه شأنها شأن الأدلة التقليدية، وبهذا المبدأ يحمي حقوق المتهمين ويضمن تنفيذ العدالة.

ويلتزم القاضي ببعض القيود في الاقتناع بالدليل الالكتروني، أي أن القاضي لا يبني قناعاته على عواطفه وافتراضاته وتصوراته الشخصية، بل تحدد هذه القناعة بشروط وضمانات معينة تتمثل في:

- اقتناع القاضي يجب أن يكون قائماً على يقينية الدليل الالكتروني، وقد تم ذكر ذلك فيما سبق في شروط قبول الأدلة الالكترونية، كما ينبغي أن لا تكون الأدلة قابلة للجدل[2].

[1] يرمش مراد، القيود الواردة على الدليل الالكتروني كحجية في الإثبات الجنائي، المجلة الأكاديمية في البحوث القانونية والسياسية، المجلد 7، العدد 1، 2023، ص 1563.

[2] المرجع نفسه ص 1564.

- تسبيب الأحكام: إن القاضي غير مطالب بتبرير إدانته، إذ يكفي أن يعلن إدانته بصحة الأدلة أو عدم صدقها، كما يجب أن يتضمن حكم القاضي بالإدانة أو البراءة جميع الأسباب التي نبني عليها الحكم، وكذا العقوبة ونص القانون الذي حكم على ضوئه القاضي.

ونجد أن تسبيب الأحكام شرط نصت عليه المادة 379 من قانون الإجراءات الجزائية والتي جاء فيها "كل حكم يجب أن ينص على هوية الأطراف وحضورهم أو غيابهم في يوم النطق بالحكم ويجب أن يشتمل على أسباب ومنطوق وتكون الأسباب أساس الحكم. ويبين المنطوق الجرائم التي تقرر إدانة الأشخاص المذكورين أو مساءلتهم عنها، كما تذكر به العقوبة ونصوص القانون المطبقة[1]".

فالتسبيب الذي يبديه القاضي نجده في نقطتين:

أ/ يجب على القاضي في حكمه أن يقدم جميع الأسباب الواقعية والقانونية التي دفعته إلى إصدار حكمه.

ب/ أن تعبر هذه الأسباب عن العملية العقلية التي توصل القاضي من خلالها إلى نتيجة معينة[2].

[1] قانون الإجراءات الجزائية، مرجع سابق، ص 125.

[2] يرمش مراد، المرجع السابق، ص 1565.

المبحث الثاني: إجراءات التحري والتحقيق للحصول على الدليل الالكتروني

إن التحري والتحقيق في الجرائم الالكترونية مجال مهم، وهو في حالة تطور مستمر لمواكبة تطور التكنولوجيا، مما يجعل العمل فيه يتطلب مهارات متخصصة وتقنيات متعددة للكشف عن الجرائم ومعالجتها، وكون أن الأدلة في هذا النوع من الجرائم أدلة غير محسوسة تحتاج إلى خبرات فنية وتقنية عالية، فقد حاولنا في هذا المطلب ذكر أهم الإجراءات التي تساعد على الحصول عليها.

المطلب الأول: إجراءات التحري والتحقيق التقليدية

إن عملية الحصول على الدليل الالكتروني تمر بمراحل، ولها عدة إجراءات من بينها طرق التحري والتحقيق الابتدائية الكلاسيكية، بالإضافة إلى جميع الإجراءات التي يمكن إيجادها في الجرائم العادية، وسنأتي على ذكر هذا فيما يلي:

الفرع الأول: تلقي البلاغات والشكاوي:

يعتبر تلقي البلاغات والشكاوي أول خطوة في إجراءات التحري، حيث أنها جزء أساسي من العمل، والبلاغ بصورة عامة هو: "إخبار السلطات المختصة على وقوع الجريمة أو أنها على وشك الوقوع، أو أن هناك اتفاق جنائي على ارتكابها[1]"، لذلك يجب على من يتلقى البلاغ أن يكون ملماً بالجوانب الفنية لشبكات التكنولوجيا، وعلى معرفة واسعة بتقنياتها حتى يسهل عليه مناقشة المبلغ في الجوانب المتعلقة بالجريمة عند تلقي البلاغ، كما يجب على المحقق

[1] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دار الكتب والوثائق القومية، القاهرة، مصر، 2012، ص 11.

استفاء المعلومات من المبلغ لتسهيل عملية التحقيق، وتكون المعلومات عبارة عن أجوبة للأسئلة الآتية[1]:

- تاريخ ووقت تلقي البلاغ.
- المعلومات الخاصة بالمبلغ.
- المعلومات الخاصة بمتلقي البلاغ.
- طبيعة ونوع جريمة الحاسبة الالكترونية محل البلاغ.
- الأسئلة الستة المشهورة والمتعلقة بالجريمة: ماذا؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟
- المعلومات ذات العلاقة بالأنظمة الحاسوبية، كطبيعة العتاد ونوعية البرمجيات والمسؤولين عن الأنظمة، وطريقة الاتصال بهم وغيرها.

من خلال هذه المعلومات يتمكن المحقق من وضع تصور مبدئي لخطة العمل المناسبة للتحقيق في الحادث، وتعين فريق العمل اللازم، والمقصود بخطة العمل هو عملية التخطيط التي يقوم بها المحقق لتحديد الإجراء الأمثل في التعامل مع الجريمة الالكترونية الواقعة.

وبعد التحقيق تأتي مرحلة تشكيل فريق التحقيق، حيث يوجد هناك محققون جنائيين ذوو خبرة طويلة، وهناك أخصائيون في الحاسبة الالكترونية، كما أنه من الضروري أن يستعين المحقق بخبراء في هذا المجال، إلى جانب الاستعانة ببعض خبراء مسرح الجريمة التقليدية مثل خبير بصمات وخبير التصوير الشمسي اللذين يعتبران من الخبراء الأساسيين في كل أنواع الجرائم.

[1] علي عدنان الفيل، المرجع السابق، ص 12، 13.

ويتكون فريق العمل من قائد الفريق الذي يجب أن يمتلك خبرة في التحقيق الجنائي الالكتروني محقق جنائي الذي يجب أن تكون لديه خبرة بوسائل وأساليب التحقيق في هذا النوع من الجرائم خبير الحاسبة الالكترونية والشبكات، خبير مدقق حسابات، خبير بسمات وخبير رسم تخطيطي.

وبعد مرحلة جمع الفريق تأتي مرحلة الإجراءات التي يقوم بها هذا الفريق والتي تتمثل في المعاينة والتفتيش.

الفرع الثاني: الخبرة الفنية والمعاينة

أولا: الخبرة الفنية:

إن الاستعانة بالخبراء في مجال القضاء والتحقيقات، خاصةً فيما يتعلق بالجرائم الالكترونية هي خطوة ضرورة لضمان فهم دقيق وشامل للأدلة، والتحقيقات التقنية، فعندما يتعلق الأمر بالجرائم الالكترونية فإن التحقيق يتطلب فهماً عميقاً للتكنولوجيا والأنظمة الرقمية.

إن مساهمة الخبرة الفنية العاملة في مجال الجريمة الالكترونية، في الأمن العام له خبرة متوسطة في حفظ الأدلة الرقمية بطريقة خاصة كونها تختلف عن الأدلة المادية، وإن هذه الخبرة الفنية تساهم بمستوى متوسط في التعرف على أنواع الأدلة الرقمية وتحليلها بصورة علمية لكشف الجريمة، كما تساعد على تحويل الأدلة غير المرئية إلى أدلة مرئية لتسهيل عملية الكشف عن الجريمة[1].

إن الخبير الالكتروني هو الفني المتخصص وصاحب خبرة تقنية، كما له دراية بالتقنيات والشبكات الالكترونية، وله المقدرة على رؤية وسماع وإدراك المعلومات الهامة اللازمة للتحقيق

[1] فراس عقيل الدويري، البيانات الضخمة ودورها في الحد من الجرائم الالكترونية في ظل استيراتيجية الأمن، دار الخليج للنشر والتوزيع، ط1، عمان، الأردن، ص 141.

بحواسه، وهو قادر أيضاً على الدخول إلى أنظمة المعالجة الآلية للبيانات الرقمية إذا لزم الأمر من أجل التحقيق. وينقسم الخبراء الإلكترونيون إلى[1]:

- ✓ المبرمجون
- ✓ المحللون وهم الأشخاص الذين يضعون خطوات العمل ويقومون بتجميع بيانات نظام معين.
- ✓ مهندسو الصيانة والاتصالات.
- ✓ مشغلو الحاسوب الآلي.
- ✓ مدير النظام المعلوماتي.

إن على الخبير المعلوماتي أن يقوم بكل ما يمكنه في سبيل تحري الحقيقة والوصل إليها، وفي إطار ما يسمح به عمله، كما يجب عليه استخدام الأساليب العلمية التي يقوم عليها تخصصه والمتمثلة في[2]:

1/ القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في حد ذاتها: كجرائم التهديد أو النصب، أو جرائم النسخ، إذ يقوم بعملية التحليل الرقمي لها لمعرفة كيفية إعدادها، وتحديد عناصر حركتها وكيف تم الوصول إلى معرفتها، وبهذا يسهل معرفة برتوكول الانترنت الذي ينسب إلى جهاز الكمبيوتر الذي صدرت منه هذه الجرائم.

2/ القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته، وإنما حال تتبع موضوعها إلى الكشف عن قيام الأفراد بارتكاب الجرائم، كما هو الحال في المواقع

[1] بوبعاية ابتسام، التحقيق في الجريمة المعلوماتية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر، جامعة محمد البشير الإبراهيمي، برج بوعريرج، 2022/2021، ص 45.

[2] تابري مختار، الخبرة في الجريمة الالكترونية، الحوار المتوسطي، المجلد 11، العدد 3، ديسمبر 2020، الجزائر، ص 391.

التي تساعد الغير في التعرف على كيفية زراعة المخدرات بعيداً عن الأعين، وكذلك القيام بتحديد مسار الدخول على مواقع الدعارة من أماكن متفرقة.

قد اهتم المشرع الجزائري بتنظيم أعمال الخبرة وذلك في المواد 143 إلى 156 من قانون الإجراءات الجزائية، ونصت المادة 143 على أنه: "لجهات التحقيق أو الحكم عندما تتعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما من تلقاء نفسها أو بناءً على طلب النيابة العامة، وإما بطلب من الخصوم[1]"، ولها أهمية كبيرة في مجال التحقيق أو الحكم والتحري في الجرائم الالكترونية وتتمثل في[2]:

1. تساعد في الكشف عن الدليل الرقمي.
2. تحديد الخصائص الفريدة للدليل الرقمي.
3. إصلاح الدليل وإعادة تجميعه من المكونات المادية للكمبيوتر.
4. جمع الآثار المعلوماتية الرقمية التي قد تكون تبدلت خلال شبكة المعلوماتية.
5. تحريز الدليل الرقمي لإثبات أنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة في الدعوى.
6. عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.
7. استخدام الخورزميات للتأكد من أن الدليل لم يتم العبث به أو تعديله.

ثانياً: المعاينة

[1] القانون رقم 155/66، المؤرخ في 08 يونيو 1966، المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية، العدد 48، 2015.

[2] ثابري مختار، المرجع السابق، ص 392.

ويقصد بالمعاينة: "الانتقال إلى محل الجريمة وإثبات حالتها، وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها، وعليه فإن كل ما يترك في مكان الجريمة من أدوات وبصمات... وغير ذلك من الأدلة المادية، فهو في الحقيقة عبارة عن مساعدة لرجال الضبطية القضائية في معرفة المشتبه فيه[1]"، من خلال هذا القول نعرف أن المعاينة هو دراسة كل ما يوجد في مسرح الجريمة دون إهمال أي عنصر لاحتمال أن يكون دليل يوصلنا إلى الجاني.

إن المعاينة المعلوماتية هي عملية جمع وتحليل الأدلة الرقمية في التحقيقات الجنائية وتتضمن العملية استخراج البيانات من أجهزة الكمبيوتر والهواتف الذكية والأقراص الصلبة وغيرها من وسائط التخزين الرقمية وتحليل هذه البيانات لاستخراج المعلومات ذات الصلة بالتحقيق، كما تعد المعاينة الالكترونية جزءاً مهماً من عملية التحقيق الجنائي السيبرانية والرقمية حيث تساعد على جمع الأدلة وتحليلها بطريقة دقيقة ومنهجية مما يساهم في تحقيق العدالة وتنفيذ القانون.

فالمعاينة من إجراءات التحقيق الابتدائي، ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، ويخضع هذا الإجراء لمجموعة من الشروط تتمثل في:

1) **إذن أو أمر المعاينة المعلوماتية:** وهذا ما نصت عليه المادة 64 من قانون الإجراءات الجزائية: "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي سستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا

[1] قلات سمية، حاحا عبد العالي، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد 11، العدد 1، 2023، ص 523.

بتصريح مكتوب بخط يد صاحب الشأن..."[1]، جاء في هذه المادة أن من أهم شروط المعاينة أن يكون هناك بإذن المعني بالأمر.

2) **وقت إجراء المعاينة المعلوماتية:** بما أننا بصدد جريمة معلوماتية فإن إجرائها يكون في كل ساعة من ساعات النهار أو الليل، بناءً على إذن مسبق من وكيل الجمهورية حسب نص المادة 47 فقرة 3 قانون الإجراءات الجزائية، على عكس الجرائم التقليدية لها وقت محدد من الساعة الخامسة صباحاً إلى غاية الساعة الثامنة مساءً[2]. أي أن المعاينة في الجريمة الالكترونية ليست مقيدة بوقت معين على عكس الجريمة التقليدية.

3) **مكان إجراء المعاينة المعلوماتية:** ويجب أن تكون المعاينة في مكان وقوع الجريمة، مع مراعاة مبدأ الشخصية والعينية الذي نص عليها قانون الإجراءات الجزائية في نص المادة 582، والمادة 15 من القانون 04/09، وهناك حالات لا يجوز فيها معاينة المكان إلا بوجود إتفاقية.

4) **الأشخاص الذين يحق لهم حضور المعاينة المعلوماتية:** المتهم، والضحية ومحاميهم ووكيل الجمهورية وقاضي التحقيق، وضباط الشرطة القضائية.

5) **محضر المعاينة المعلوماتية:** ويعتبر المرحلة الأخيرة من المعاينة الالكترونية، إذ يجب على ضباط القضائية تحرير محاضر عن أعمالهم، وفق ما نصت عليه المادتين 18، و54، من القانون الإجرائي الجزائي.

تشمل المعاينة المعلوماتية عادة جمع البيانات، وتحليل البيانات، توثيق الأدلة، تقديم التقارير تقديم الشهادات، كما يجب مراعاة مجموعة من القواعد والإرشادات الفنية التي تشمل:

---

[1] الأمر رقم 155/66 المؤرخ 08 يونيو 1966، المعدل والمتمم لقانون رقم 06/ 22، المؤرخ 20 ديسمبر 2006، الجريدة الرسمية العدد 84.

[2] قلات سمية، حاحا عبد العالي، المرجع السابق، ص 528، 529.

1. تصوير الحاسبة الالكترونية والأجهزة الطرفية المتصلة به، المحتويات والأوضاع العامة بمكانه.
2. العناية البالغة بملاحظة الطريقة التي تم بها إعادة النظام والآثار الالكترونية الخاصة بالتسجيلات الالكترونية.
3. ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام.
4. إبعاد أي شخص عن أجهزة الحاسبة الالكترونية.
5. التحفظ عما قد يوجد في سلة المهملات.
6. عدم نقل أي معلومة من مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي.

الفرع الثالث: التفتيش الالكتروني

أولا: تعريف التفتيش في الجرائم الالكترونية:

يعرف التفتيش في الجرائم الالكترونية على أنه: "إجراء من إجراءات التحقيق تقوم به سلطة مختصة من أجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات، لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة، وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها[1]"

ويتضح لنا من خلال هذا التعريف أن التفتيش في الجرائم الالكترونية، هو التمكن من رؤية واستحضار البيانات المختلفة ومعالجتها وفق ما تقتضيه حيثيات التحقيق، وفي حدود ما يسمح به القانون.

[1] إبراهيم محمد بن حمود الزنداتي، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الالكترونية وأثرها على حجية أدلة الإثبات وأحكامها في القانون اليمني والكويتي، دراسة مقارنة، رسالة ماجستر ، جامعة غطاني، اليمن، 2018، ص 130.

كما عرفه البعض بأنه: "البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه، أو الإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه، أو الانترنت"[1]، ونجد في هذا التعريف أن التفتيش هو الإطلاع على خصوصيات المتهم التي تم عليها وضع اليد من قبل السلطة بغية الكشف عن أسرار قد تقودنا إلى معرفة الحقيقة، وإظهار أدلة تساهم في إثبات الجرم أو نفيه.

أما بالنسبة للمشرع الجزائري فإنه لم يضع تعريفاً للتفتيش عن الجرائم الالكترونية، وترك ذلك للفقه، لكن ورد في القانون الجزائري أحكام التفتيش الالكتروني وذلك في المادة الخامسة من القانون 04/09، والتي تستهدف تطوير ومجاراة التشريع الداخلي للتشريعات المقارنة، كما أن الهدف الأساسي من سن المادة 05 من القانون 04/09 هو إرساء وإيجاد السلطات في العالم الافتراضي خاصة بالمعطيات المكافئة للسلطات الموجودة في عالم الأشياء المادية في إطار التفتيش الكلاسيكي[2]، كما تهدف عملية التفتيش الالكتروني إلى جمع الأدلة الرقمية بطريقة تتوافق مع قانون الإجراءات الجزائية وتحليلها بشكل متسق ومنهجي، لدعم التحقيقات أو العمليات الإدارية المعنية.

ثانياً: خصائص التفتيش الالكتروني:

- ✓ إن التفتيش في المنظومات شأنه شأن التفتيش العادي حيث لا يتعرض الشخص للمساس بحريته الشخصية، أو حرية مسكنه، ونصت المادة 40 من الدستور الجزائري على: "فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه ولا تفتيش إلا

[1] محمد جمال مطلق الذنيبات، التفتيش في الجرائم الالكترونية ماهيته وشروطه الشكلية، مجلة الأردنية في القانون والعلوم السياسية، المجلد 13، العدد3، عمان، الأردن، 2021، ص 83.

[2] مناصرة يوسف، المرجع السابق، ص 348،349.

بأمر مكتوب صادر عن السلطة القضائية المختصة"، نجد في هذه المادة ضمان لعدم التعدي على حرية الأفراد إلا في إطار ما يسمح به القانون وتحت أمره.

- ✓ إن التفتيش أو البحث في الشبكات الالكترونية عن الجرائم المعلوماتية يكون باستخدام أساليب وطرق التحقيق الجنائي الفني المعروفة بتقنيات خاصة فهو عكس التفتيش الكلاسيكي.
- ✓ يتميز تفتيش المنظومات المعلوماتية بأن المحتوى المعلوماتي ذو طابع لا مادي ويتجاوز الحدود الوطنية، كما يتميز بأنه عرضة للإتلاف والمسح أو التغيير فهو تفتيش للفضاء الافتراضي، وتفتيش للبيانات الموجودة في جهاز الحاسوب[1].
- ✓ هو عملية معقدة، يجب أن تتم من طرف محقق ذو خبرة فنية وتقنية واسعة، وعلى دراية ومعرفة بتكنولوجيا المعلوماتية.

ثالثاً: شروط إجراء التفتيش الالكتروني:

وكغيره من إجراءات التحري والتحقيق، يخضع التفتيش الالكتروني إلى شروط تحكمه وتنقسم إلى شروط موضوعية، وشروط شكلية.

1/ الشروط الموضوعية لتفتيش نظم المعلوماتية: وتتمثل هذه الشروط في أسباب ومحل التفتيش المعلوماتي.

1. سبب التفتيش الالكتروني: لا يجب أن يخضع أي شخص للتفتيش دون أسباب، لهذا كان من أهم الشروط التي يقوم عليها التفتيش الالكتروني هو وجود سبب التفتيش والذي يتمثل في البحث عن الأدلة في تحقيق جار للوصول إلى حقيقة الحدث، كما يفترض أن

[1] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد 5، 2012، ص 100.

يكون للتفتيش مبررات توضح السبب والهدف منه، والتي تتمثل في وقوع الجريمة الالكترونية، وتوجيه التهمة لشخص ما أو مجموعة من الأشخاص.

2. محل التفتيش: والمقصود به في الجريمة الالكترونية كل مكونات الحاسوب سواء كانت مادية أو معنوية، بالإضافة إلى شبكات الاتصال الخاص به للتفتيش[1]، ويشمل كذلك البحث في البيانات والمعلومات والبرمجيات المخزنة في الحواسيب، فضلاً عن الأقراص والأشرطة، وغيرها من وسائل التكنولوجيا، كما يميز المشرع الجزائري في التفتيش الالكتروني بين ما إذا كانت المنظومة داخل التراب الوطني أو خارجه.

2/ الشروط الشكلية لتفتيش نظم المعلوماتية:

- ✓ إجراء التفتيش بحضور بعض الأشخاص المعينين من طرف القانون، إذ اشترط المشرع الجزائري لإجراء عملية التفتيش العمل بأحكام قاعدة الحضور تطبيقاً لنص المادة 5 من القانون 04/09، والتي نصت على وجوب حضور صاحب المسكن المشتبه به في ارتكاب جريمة أو حضور شاهدين في حال تعذر حضوره[2].
- ✓ محضر التحرير: وهو عبارة عن تقرير فني يلخص النتائج والاستنتاجات التي تم الوصول إليها خلال عملية التفتيش الالكتروني، كون أنه من إجراءات التحقيق ما يفرض عليه وجود هذا المحضر لإثبات ما أسفر عنه التفتيش من أدلة، ويجب أن يتضمن كافة الإجراءات المتبعة في عملية التفتيش[3].

يجب أن تتم عملية التفتيش من طرف خبراء وفنيين متخصصين بالحاسوب والأنظمة المعلوماتية، وعلى تكوين عال في هذا المجال.

---

[1] رضا هميسي، المرجع السابق، 166.

[2] المرجع نفسه، ص 169.

[3] ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد 16، 2017، ص 454.

المطلب الثاني: أدلة إلكترونية معتمدة على معدات تقنية

إن الأدلة الالكترونية المعتمدة على تقنيات تكنولوجيا المعلومات تشير إلى الأدلة التي تستند على استخدام الأجهزة والبرمجيات الرقمية لجمع البيانات وتحليلها وتقديمها كدليل في الإثبات الجنائي المعلوماتي، كما تكتسي الأدلة الرقمية أهمية في التحقيق والاستدلال لأنه يمكن استخدامها لتحديد ما إذا كانت الأنشطة الالكترونية قد حدثت أم لان وتحليلها لفهم خلفيتها ونواياها.

وتتمثل هذه الأدلة المعتمدة على معدات تقنية في المراقبة الالكترونية والتصنت، التسريب الالكتروني، اعتراض والتقاط المرسلات السلكية واللاسلكية.

الفرع الأول: المراقبة الالكترونية

أولاً: تعريف المراقبة الالكترونية:

نصت المادة 20 من الاتفاقية المتعلقة بمكافحة الجريمة المنظمة عبر الحدود الوطنية والتي سنتها منظمة الأمم المتحدة في إطار مكافحة الجريمة المنظمة على: "تقوم كل دولة طرف ضمن حدود إمكانياتها ووفقاً للشروط المنصوص عليها في القانون الداخلي، إذا كانت المبادئ الأساسية لنظامها القانوني الداخلي تسمح بذلك، باتخاذ ما يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب، وكذلك ما تراه مناسباً لاستخدام أساليب تحري خاصة أخرى مثل المراقبة الالكترونية، أو غيرها من أشكال المراقبة[1]" ونجد في نص هذه المادة دعوة لاعتماد أسلوب المراقبة ضمن ما يسمح به القانون، من أجل الحد من الجرائم.

[1] بن بادة عبد الحليم، المراقبة الالكترونية بين الحق في الخصوصية ومشروعية الدليل الالكتروني، المجلة الأكاديمية للبحث القانوني، المجلد 10، العدد 3، 2019، 390.

وقد تبنى المشرع الجزائري مصطلح المراقبة الالكترونية من هذه المادة، ولم يضبط تعريفاً له لا في مواد القانون الإجراءات الجزائية، ولا في مواد القانون 04/09، وترك ذلك للفقه.

وقد عرف على أنه: "عملية مراقبة سرية للمرسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو المشاركين في ارتكاب الجريمة[1]"، من خلال هذا التعريف يمكننا القول أن المراقبة الالكترونية هي تتبع لبيانات معينة من أجل معرفة الحقيقة، وإيجاد أدلة تساعد على حل قضية ما.

ونجد تعريفاً آخر للمراقبة الالكترونية والذي جاء فيه أنها: "إجراء تحقيق خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانوناً بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها، ويتضمن من ناحية استراق السمع ومن ناحية أخرى حفاظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض[2]" أي أن المراقبة الالكترونية هو تعدي على خصوصيات الفرد، والاستماع إلى محادثاته الخاصة بأمر من السلطات المختصة من أجل بلوغ الحقيقة وكشف ملابسات الجريمة الواقعة.

ويمكننا أن نستخلص من التعاريف السابقة أن المراقبة الالكترونية هي عملية استخدام تقنيات الرصد والتسجيل الالكتروني لجمع المعلومات والأدلة المتعلقة بجريمة ما.

ثانياً خصائص إجراء المراقبة الالكترونية

1/ سرية إجراء المراقبة الالكترونية: إن عملية المراقبة تتم في سرية تامة من أجل تحقيق نتائج جيدة، وبلوغ الهدف المراد الوصول إليه، بالإضافة إلى حماية خصوصية المحادثات والاتصالات، وضمان تنفيذ القانون بصورة جيدة، وحماية الخاصة للأفراد من جهة أخرى، ولكي

[1] بوبكر رشيدة، المرجع السابق، ص 442.

[2] بن بادة عبد الحليم، المرجع السابق، ص 391.

يتحقق ذلك، تم وضع عدد من الشروط المتمثلة في: الإذن القانوني في مراقبة المحادثات والاتصالات، وذكر هوية الشخص تتم مراقبته.

2/ الاعتماد على أجهزة خاصة في إجراء المراقبة الالكترونية:

لقد كان للتطور الذي شهده عالم التكنولوجيا والمعلوماتية، أثر كبير في تسهيل عملية المراقبة الالكترونية، حيث أدى إلى ظهور أجهزة ومعدات مراقبة إلكترونية حديثة ومتطورة تساهم بشكل كبير في تسهيل عملية مراقبة الاتصالات، حيث لا يمكن أن تكون مراقبة من دون هذه الأجهزة المتخصصة[1].

3/ هدف المراقبة الالكترونية هو الحصول على دليل غير مادي:

إن الهدف الرئيسي للمحققين الجنائيين الذين يتخذون هذا الإجراء هو الحصول على أدلة من شأنها أن تسهم في كشف غموض الجريمة الالكترونية، وتأكيد الأدلة التي يتم الحصول عليها من خلال التحقيقات والتحريات وبالتالي ضمان إسناد الجرائم المرتكبة في الفضاء الافتراضي إلى مرتكبيها[2].

4/ مساس إجراء المراقبة الالكترونية بحق الشخص في سرية المراسلات والاتصالات الالكترونية:

[1] كريم معروف، سعاد بن حليمة، الإجراءات المستحدثة في البحث والتحقيق للكشف عن الجرائم التي ترتكب في الفضاء الالكتروني، مجلة الدراسات الاستراتيجية والعسكرية، العدد 13، ص 7.

[2] بن بادة عبد الحليم، المرجع السابق، ص 394.

إن عملية المراقبة والتنصت على الاتصالات تؤدي بالضرورة إلى انتهاك حق الشخص في حماية خصوصياتها، لكنها من جهة أخرى تمكن المحققين من معرفة أفكار المشتبه به ونواياه والتعرف على مشاعره مما يمكنهم من معرفة الحقيقة والوصول إليها[1].

ثالثاً: شروط إجراء المراقبة الالكترونية:

تتمثل شروط إجراء المراقبة الالكترونية فيما يلي[2]:

– يجب أن يتضمن تصريح المراقبة المحادثات أو الاتصالات التي ستتم مراقبتها، وهوية الشخص الذي تتم مراقبته، لكي تكون المراقبة الالكترونية قانونية، يجب أن تكون بتصريح مكتوب من طرف السلطة القضائية.

– يجب تحديد ساعات المراقبة، وذلك لأن تمديد مدة المراقبة العلنية يشكل إفشاء أسرار المواطنين دون مبرر، وقد حدد المشرع الجزائري مدة المراقبة القابلة للتجديد ستة أشهر في المادة 4 من القانون 04/09.

– يجب على مشغلي المراقبة أن يسجلوا فقط ما هو مصرح به من قبل سلطة المراقبة، ويحضر عليهم تسجيل ومراقبة أي شيء يتجاوز ذلك.

– يجب أن تكون الأشرطة المسجلة عند تنفيذ أوامر المراقبة مختومة، لمنع التلاعب أو التغيير.

– يجب أن تتم عملية المراقبة بشكل شفاف ونزيه، كما يتعين على جهات التحقيق تقديم معلومات كافية حول أسباب وأساليب المراقبة المستخدمة.

[1] كريم معروف، سعاد بن حليمة، المرجع السابق، ص 6.

[2] المرجع نفسه، ص8.

– يجب أن يكون طرفي المراقبة هما المراقِب الالكتروني، والمتمثل في المحقق الجنائي أو قاض التحقيق أو ضابط الشرطة القضائية، أو أي جهاز مكلف بالتحقيق والتحري في الجرائم الالكترونية، والطرف الثاني وهو المراقَب الالكتروني ويتمثل في المشتبه به.

رابعاً: حالات اللجوء إلى إجراء المراقبة الالكترونية

نصت المادة 4 من القانون رقم 04/09 [1] على الحالات التي يتم فيها اللجوء إلى المراقبة الالكترونية، وتمثلت فيما يأتي:

- في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب، أو الجرائم التي تمس بأمن الدولة.
- في حال توفر معلومات عن احتمال وقوع اعتداء المنظومة المعلوماتية، التي تهدد الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- أن تكون المراقبة الالكترونية من مقتضيات التحري والتحقيق الجنائي، بحيث يستحيل الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء لها.
- في حالة تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما نصت الفقرة 05 من القانون 04/09 المادة 04، على أنه: "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة" أي أنه لا يحق إجراء المراقبة ما لم يكن هناك تصريح مكتوب من قبل السلطات المعنية.

[1] المادة 4 من القانون رقم 04/09.

كما نصت المادة 46 من التعديل الدستوري لسنة 2016 على أن: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، ولا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم.

حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حق أساسي يضمنه القانون ويعاقب على انتهاكه[1]"، ما جاء في هذه المادة يدل على أن المشرع الجزائري عمل على حماية خصوصية المواطنين وضمن لهم الحق في عدم انتهاكها، وفرض عقوبات على من يتعدى على هذا الحق.

الفرع الثاني: الاعتراض والالتقاط الالكتروني:

إن الاعتراض والتسجيل والالتقاط والتسريب هي عدة تسميات يمكن اختزالها في مصطلح واحد هو المراقبة، وهو لا يعني أكثر من المراقبة القانونية لشخص أو مكان أو محادثة أو وثيقة أو اتصال صوتي أو مرئي نتيجة الاشتباه في نشاط غير قانوني.

واختلف الفقه في تكييف هذا الإجراء، فهناك من ذهب إلى القول بأنها تعد تفتيشاً، وبالتالي فهي تخضع لقواعد وقيود التفتيش، في حين كان هناك من يقول بأنها من ضمن إجراءات المراقبة.

أولاً: اعتراض المراسلات

الاعتراض يعني الاستلاء، وقد نظم المشرع الجزائري في المادة 65 مكرر5 من قانون الإجراءات الجزائية الجزائرية الاتصالات عن طريق المواصلات السلكية واللاسلكية، دون الرسائل والخطابات والمطبوعات والطرود، لدى مكاتب البريد، ونظراً للتطور الذي عرفه مجال

[1] القانون رقم 01/16 المؤرخ في 06م03/2016، المتضمن التعديل الدستوري الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد 14، المؤرخ في 2016/03/07.

الاتصال فإن نص المادة 65 مكرر 5 السالف الذكر جاء موسعاً أي لم يقصر الاعتراض على المكالمات الهاتفية، بل وسعه لمختلف أنواع الاتصال السلكية واللاسلكية[1].

ثانياً: تسجيل الأصوات والتقاط الصور

يعتبر تسجيل الأصوات توثيقاً مهماً في العديد من السياقات القانونية، وهي عبارة عن عملية تسجيل المحادثات التي تجري بين المتهمين، رغم أن المشرع الجزائري أعطى للمتهم الحق في الصمت، إلا أنه بطريقة غير مباشرة أورد استثناءً عن هذا الحق في المادة 65 مكرر 5، أين أصبح من الممكن أخذ اعتراف الشخص ضد نفسه بشكل خفي دون رضاه وموافقته عن طريق تسجيل كل ما يتفوه به من كلام بصفة خاصة أو سرية[2].

ولقد اختلفت القوانين في المعيار الذي يجعلنا نميز بين ما يعد حديثاً خاصاً، وما هو حديث عام، فهناك من أخذ بطبيعة المكان الذي يدور فيه الحديث والبعض الآخر اعتمد على طبيعة الحديث ذاته[3].

ونرى أن المشرع الجزائري قد حدد موقفه من خلال المادة 65 مكرر 3/5 من قانون الإجراءات الجزائية، حيث اعتمد على المكان عام أو خاص، شرط أن يكون الحديث سري وخاص.

---

[1] المادة 65 مكرر 5، من قانون الإجراءات الجزائية.

[2] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، العدد 33، 2010، ص237.

[3] قيشاح نبيلة، ضمانات المراقبة الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، المجلد 10، العدد 2، 2022، ص1098.

التقاط الصور:

يعرف التقاط الصور بأنه: "حفظ الصورة على مادة معينة موجودة داخل أجهزة أو آلة التصوير، ليتم رؤيتها فيما بعد، بهدف التحقيق في جريمة أو أمر ما يتعلق بها[1]" أي أن عملية التصوير وحفظ الصور تكون بهدف كشف الحقائق وفي إطار ما يسمح به القانون.

ونجد أن المشرع الجزائري لم يكتفي بالسماح لقاضي التحقيق بتسجيل الأصوات بل مكنه أيضاً من إمكانية التقاط الصور، وهذا ما نصت عليه المادة 65 مكرر 5 وجاء فيها: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به، بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، أو التقاط الصور لشخص أو عدة أشخاص يتواجدون في مكان خاص"

وقد ذكرت هذه المادة أنه يمكن لوكيل الجمهورية السماح بالمراقبة الالكترونية بمختلف أشكالها حتى وإن لم يكن للمعني بالأمر علم بها من أجل السير الحسن لمجريات التحقيق، ولبلوغ الحقيقة.

ثالثاً: الشروط الموضوعية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

[1] المرجع نفسه، ص 1099.

1/ السلطة المختصة بإجراء هذه العمليات: من الطبيعي أن تكون هذه العمليات خاصة بجهاز معين في الدولة، للحفاظ على حق الفرد في حماية خصوصيته، ولهذا كان أمر اعتراض المراسلات وتسجيلها والتقاط الصور من تخصص قاضي التحقيق والذي وإن كان لا يقوم بالعملية بشكل مباشر، إلا أنها تتم تحت مراقبته، ويقوم بها من يملك الخبرة في التعامل معها[1]

ويقتصر دور القاضي على السهر على مدى تحقيق القواعد القانونية في هذه الإجراءات.

وبالرجوع إلى القانون رقم 06-22 من قانون الإجراءات الجزائية، نجد أن هذه الإجراءات تنفذ بموجب إذن من وكيل الجمهورية، وذلك أثناء مرحلة التحري بشرط أن تكون من دواعي التحري ضرورة اللجوء إلى هذا الإجراء[2].

أما بالنسبة للجهة المكلفة بالعملية تتمثل في ضابط الشرطة القضائية لإنجاز العمليات، أو لقاضي التحقيق، أو ضابط الشرطة القضائية الذي يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية لتكفل الجوانب التقنية وهذا ما جاء في نص المادة 65 مكرر 8 من قانون الإجراءات الجزائية.

2/ ميقات ومكان هذه العمليات: لم ينص قانون الإجراءات الجزائية الجزائري على قواعد الإجراءات من ناحية المكان والزمان.

حيث أجاز هذه الإجراءات في كل ساعة من ساعات النهار والليل، وفي كل مكان سواء كان خاص أو عام.

[1] فوزي عمارة، المرجع السابق، ص 238.

[2] مناصرة يوسف، المرجع السابق، ص 458.

3/ عدم مسؤولية القائم والمشرف على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: لقد سبق لنا أن ذكرنا أن المشرع الجزائري قد ضمن حق الفرد في حماية خصوصية وسرية اتصالاته، إلا أن ما يتعرض له الشخص من انتهاك لخصوصيته عن طريق تسجيل صوته أو التقاط صورة له خلسة ليلاً أو نهاراً كإجراء قانوني تفرضه خطورة الموقف، وضرورة من ضرورات التحقيق الجنائي لكشف جريمة ما، فهذا لا يترتب عليه أي مساءلة قانونية ولا يتحمل القائمون بها المسؤولية الجنائية، تحت مبدأ الضرورات تبيح المحظورات[1].

رابعاً: الشروط الشكلية لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

1/ صدور إذن مكتوب: إن ضابط الشرطة القضائية لا يمكنه القيام بإجراء الاعتراض إلا بالحصول على إذن من وكيل الجمهورية المختص أو قاضي التحقيق، وذلك طبقاً لأحكام المادة 65 مكرر من قانون الإجراءات الجزائية السالفة الذكر[2].

2/ تحرير محضر الاعتراض: نصت المادة 65 مكرر9 من قانون الإجراءات الجزائية على أن: "يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضراً عن كل عملية اعتراض تسجيل المراسلات، وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري.

ويذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها[3]"، أي أنه يجب أن تتبع كل عملية اعتراض أو تسجيل أو تصوير بمحضر كتابي تذكر فيه كل تفاصيل العملية.

---

[1] فوزي عمارة، المرجع السابق، ص 240.

[2] قيشاح نبيلة، المرجع السابق، ص 1010.

[3] المادة 65 مكرر9، من قانون الإجراءات الجزائية.

3/ تحديد مدة المراقبة: يجب تحديد المدة اللازمة لعملية الاعتراض، والتي حددها المشرع بمدة أربعة أشهر قابلة للتجديد[1]وهذا ما نصت عليه المادة 65 مكرر7 من قانون الإجراءات الجزائية.

وجميع العمليات السابقة يجب أن تنفذ تحت إشراف وكيل الجمهورية أو قاضي التحقيق حسب الحالة، وفي كل الأحوال يجب عدم المساس بالسر المهني[2]فإن اكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سبباً لبطلان الإجراءات العارضة.

الفرع الثالث: التسرب الالكتروني

أولاً تعريف التسرب الالكتروني

يتمثل معنى التسرب الالكتروني في: "قيام ضابط شرطة قضائية مختص باختراق والتوغل في منظومة معلوماتية أو نظام اتصالات إلكترونية أو منصة رقمية من أجل مراقبة مشتبه في تورطهم في ارتكاب جريمة المعلوماتية[3]"، أنه عملية الدخول إلى بيانات ونظم معلوماتية من أجل الكشف عن من يشتبه بهم في ارتكاب جريمة ما.

وقد اهتم المشرع بتعريف التسرب الالكتروني وذلك في المادة 65 مكرر12 في الفقرة الأولى من قانون الإجراءات الجزائية حيث نصت على: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص

[1] قيشاح نبيلة، المرجع السابق، ص 1102.

[2] مناصرة يوسف، المرجع السابق، ص459.

[3] فاطمة العرفي، تطبيق إجراء التسرب الالكتروني في القانون الجزائري، مجلة دراسات وأبحاث، مجلة العربية في العلوم الإنسانية والاجتماعية، المجلد 13، العدد 4، 2021، ص 215.

المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل مهم أو شريك لهم[1]" أي أن المشرع يعتبر هذا الإجراء أسلوب من أساليب التحريات الخاصة، فالتسريب هو عمل ضابط الشرطة القضائية على التوغل واختراق الجماعة الإجرامية، والعمل على كسب ثقتهم.

كما يعتبر التسرب الالكتروني عملية حساسة جداً تقتضي مجموعة من القواعد والشروط لتطبيقها، فالتسرب إجراء سري واختراق شبكة إجرامية عن طريق التنكر في شكل شريك يريد الحصول على الضحية، أو بتقمص شخصية مجرم يعرض خدماته ما يسمى بعملية التحريض على الجريمة دون وجود ضحية حقيقية. حيث يسمح القانون لضابط أو عون الشرطة القضائية باستخدام هوية مستعارة وأن يرتكب عند الضرورة الأعمال التالية: "اقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد وأموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم واستعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل والتخزين والاتصال"[2] ويتضح لنا من خلال هذا أنه لضمان نجاح عملية التسرب الالكتروني لابد للمعني بإنجاز المهم أن يتمكن من كسب ثقة الجماعة الإجرامية وقد سن له القانون ارتكاب بعض التجاوزات من أجل تحقيق ذلك.

ثانياً: شروط موضوعية لإتمام عملية التسرب الالكتروني

1/ دوافع اللجوء لعملية التسرب: إن من أهم الدوافع التي تدفع إلى اللجوء لهذا الإجراء هو الفائدة الكبرى المرجوة من ورائه في كشف الحقيقة، وهذا ما أكده المشرع في المادة 65 مكرر 11 في عبارة "عندما تقتضي ضرورات التحري أو التحقيق"[3] ويرجع ذلك الى السلطة التقديرية

[1] المادة 65 مكرر12، من القانون الإجرائي الجزائي.

[2] مناصرة يوسف، المرجع السابق، ص 478.

[3] شيخ ناجية، إجراء التسرب في القانون الجزائري وسيلة لمكافحة الجرائم المستحدثة، مجلة معارف، العدد25، 2018، ص10.

لكل من وكيل الجمهورية وقاضي التحقيق في تقييم مدى ضرورة اللجوء إلى التسرب الالكتروني.

2/ سرية عملية التسرب الالكتروني: إن نجاح عملية التسرب الالكتروني متوقف على شرط موضوعي وهو السرية، ولأهميته فقد نص عليه المشرع الجزائري في المادة 65 مكرر16 من قانون الإجراءات الجزائية وجاء فيها: "لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات"[1] كما نصت على جزاءات صارمة في حال الكشف عن الهوية الحقيقية لهم، حيث تتراوح العقوبة بالحبس من 5 سنوات إلى 10 سنوات.

3/ الجرائم المقصودة بعملية التسرب: ويقصد بها نوعية الجرائم التي تستدعي للكشف عن هذا النوع من الإجراءات وقد نصت المادة 65 مكرر5 من قانون الإجراءات الجزائية السالف الذكر على هذه الجرائم والمتمثلة في:

- جرائم المخدرات.
- الجريمة المنظمة العابرة للحدود الوطنية.
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- جرائم تبييض الأموال.
- جرائم الإرهاب.
- الجرائم المتعلقة بالتشريع الخاص وكذا جرائم الفساد.

[1] المادة 65 مكرر16، من قانون الإجراءات الجزائية.

ثالثاً: الشروط الشكلية لإتمام عملية التسرب الالكتروني:

1/ تحرير تقرير مسبق من طرف ضباط الشرطة القضائية: إذ يجب وضع تقرير مفصل حول عملية التسرب قبل الانطلاق في العملية، يوجه إلى وكيل الجمهورية، وذلك طبقاً للمبدأ العام المطبق على أعمال الشرطة القضائية التي نصت عليها المادة 18 من قانون الإجراءات الجزائية[1].

وقد ورد أيضاً في المادة 65 مكرر13 أنه: "يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقرير يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي تعرض للخطر أمن الضابط أو العون المتسرب وكذا الأشخاص المسخرين طبقاً للمادة 65 مكرر14 أدناه"[2]

أي أنه يجب على الضابط كتابة تقرير فيه كل تفاصيل العملية مع ذكر أكبر قدر ممكن من المعلومات حول الجريمة وتقديمه إلى وكيل الجمهورية أو قاضي التحقيق. مع طلب الإذن باتخاذ هذا الإجراء.

2/ صدور إذن قضائي بمباشرة الإجراء: ونظراً لخطورة هذا الإجراء، وضمانة للمشتبه به فإن المشرع الجزائري قيد ضابط الشرطة القضائية بإذن مكتوب سواء من وكيل الجمهورية أو قاضي التحقيق حسب الحالة، من أجل مباشرة هذا الإجراء وذلك تحت طائلة البطلان[3]، وحدد المشرع الجزائري في المادة 65 مكرر15 من قانون الإجراءات الجزائية مجموعة البيانات الواجب توفرها في الإذن والمتمثلة في: – الجريمة التي تبرر اللجوء إلى هذا الإجراء.

– هوية ضابط الشرطة القضائية الذي سيتولى هذا الإجراء.

– يجب أن يشتمل الإذن على الأسباب والدواعي لطلب هذا الإجراء.

---

[1] شيخ فاطمة، المرجع السابق، ص 5.

[2] المادة 65 مكرر13، من قانون الإجراءات الجزائية.

[3] مناصرة يوسف، المرجع السابق، ص 478، 479.

- يجب أن يكون الإذن مكتوباً.

3/ التسرب الالكتروني مكتوب محدد المدة: يجب أن يحدد في الإذن مدة عملية التسرب والتي حددها المشرع في المادة 65 مكرر15 من قانون الإجراءات الجزائية: "يحدد هذا الإذن مدة عملية التسرب التي يمكن أن تتجاوز 04 أشهر.

يمكن أن تحدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية"[1]أي أن مدة التسرب هي 4 أشهر وقد تزيد على ذلك إذا اقتضى التحقيق ذلك.

كما يمكن لوكيل الجمهورية أو قاضي التحقيق الذي أذن بعملية التسرب أن يأمر بوقفها في أي وقت حسب ظروف العملية.

4/ معاملة الضابط المتسرب كشاهد: نصت المادة 65 مكرر18 على أن: "يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب مسؤوليته دون سواه بوصفه شاهداً عن العملية"[2]أي أنه يجوز أثناء المحاكمة اعتبار ضابط الشرطة القضائية المسؤول عن العملية كشاهد في القضية.

5/ اشتراط الخبرة في ضابط الشرطة المتسرب: للحصول على الدليل الرقمي يقتضي ذلك وجود خبير يحسن التعامل مع المنظومات والمنصات والأنظمة الالكترونية، حيث يقوم بصنع شخصية مستعارة تسمح له باختراق مسرح الاشتباه[3]، فإن الخبرة في التعامل مع التقنيات الحديثة ضرورية من أجل نجاح عملية التسرب.

---

[1] المادة 65 مكرر 15، من قانون الإجراءات الجزائية.

[2] المادة 65 مكرر18، من قانون الإجراءات الجزائية.

[3] فاطمة العرفي، المرجع السابق، ص 218,

في الأخير يمكنا القول بأن إجراء التسرب يتميز عن باقي إجراءات التحري والتحقيق في الجرائم الالكترونية، ويظهر هذا التميز من خلال شروطه الموضوعية والشكلية التي تضمن نجاحه، فهو الإجراء الوحيد الذي يكون فيه التعامل مع الشبكة الإجرامية مباشر.

الخاتمة

من خلال هذه الدراسة حاولنا تسليط الضوء عن ماهية الجريمة الالكترونية، وكيفية التحقيق فيها، وكيف يمكن الحد منها.

وقد توصلنا من خلال هذا إلى مجموعة من النتائج يمكن تلخيصها فيما يلي:

- ✓ الجريمة الالكترونية هي استخدام تكنولوجيا المعلوماتية في القيام بأعمال غير قانونية والتعدي على الآخرين من خلال انتهاك خصوصياتهم، كما أنها تتميز بكونها سهلة الارتباك، هادئة خالية من كل أشكال العنف المادي.
- ✓ إن الجريمة الالكترونية تأتي بأشكال مختلفة، كالاحتيال عبر الانترنت، والتجسس، والتهديد والابتزاز.
- ✓ يختلف التحقيق في الجرائم الالكترونية عن التحقيق في الجرائم العدية كونه يتعامل مع تقنيات رقمية متطورة ويعتمد في تحرياتها على قاعدة من البيانات والمعلومات المخزنة ومسرح الجريمة فيها يكون شبكات الانترنت، ومواقع التواصل الاجتماعي.
- ✓ لقد تم تخصيص مخبر مركزية خاصة بمراكز الشرطة يتولى أمر التحقيق والتحري عن الجرائم الالكترونية، وكذلك يعمل جهاز الدرك الوطني على مكافحة هذا النوع من الجرائم.
- ✓ لم يقتصر العمل على مكافحة الجريمة الالكترونية على أجهزة الدولة الأمنية والقضائية فحسب، بل تم تكليف هيئات غير قضائية بهذه المهمة والمتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- ✓ إن عملية الكشف عن مرتكبي الجريمة الالكترونية يستدعي بالضرورة وجود دليل على ذلك، مما يجعل الدليل الالكتروني نقطة فاصلة في حيثيات التحقيق والتحري. والذي

لابد للباحثين عنه أن يكونوا على علم بماهيته وخصائصه، لكي يكون ذا فاعلية وتأثير في النطق بالحكم.

- ✓ إن أهمية الدليل الرقمي بالنسبة للتحقيق في الجرائم الالكترونية، يفرض عليه شروطاً لأجل الأخذ به، ولإثبات مشروعيته، ومدى حجيته، كما يجب أن يكون يقيناً غير قابل للشك.
- ✓ إن الحصول على الدليل الالكتروني يلزمه وجود إجراءات تسهل على المحققين الوصول إليه والكشف عنه، الأمر الذي يستدعي وجود خبرة فنية وتقنية للمحققين، وأن يكون لهم تكوين على مستوى عالي في مجال المعلوماتية.
- ✓ إن إجراء التفتيش الالكتروني من أنجع الطرق للوصول إلى الدليل الرقمين الذي به يمكن إدانة الشخص أو تبرئته، ولتحقيق هذا لابد من احترام شروط وقواعد التفتيش الالكتروني.
- ✓ تعمل المراقبة الالكترونية، على الوصول إلى أدلة قاطعة لها أثر في التحقيق، كما أن المراقبة تخضع هي الأخرى لشروط ولها خصائص تضمن مصداقية نتائجها.
- ✓ يعتبر الاعتراض والالتقاط والتسرب الالكتروني من مظاهر المراقبة الالكترونية فهي وإن تعددت مسمياتها إلا أنها تصب في قالب واحد وهو المراقبة الالكترونية بهدف بلوغ الحقيقة. ولكل منها خصائص تميزها عن الأخرى وشروط يجب أن تتوفر فيها.

قائمة

المصادر

و المراجع

المراجع باللغة العربية

1/ القوانين والمراسم:

- القانون 09م 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في 14 شعبان 1430 الموافق ل 05 أوت 2009. الجريدة الرسمية للجمهورية الجزائرية الديمقراطية، العدد 47، الصادر يوم 16 أوت 2009.
- القانون 22/06 المعدل والمتمم لأمر 66-155 المؤرخ في 18 صفر 1386 الموافق ل 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية المؤرخ في 20 ديسمبر 2006 الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 84 الصادر في 24 ديسمبر 2006.
- المرسوم الرئاسي رقم 172/19 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في 2019/06/06، الجريدة الرسمية.

2/ الكتب:

- زبيدة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011.
- ميرفت محمد حبابية، مكافحة الجريمة الالكترونية، دار اليازوري العلمية، الجزائر 2022.
- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، 2009.

- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2010.
- حازم حسن الجمل، الحماية الجنائية للأمن الالكتروني، دار الفكر والقانون، القاهرة، 2015.
- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، 2009.
- جباري عبد المجيد، الدراسات القانونية عن المادة الجزائية على ضوء أهم التعديلات الجديدة، دار الهومة، الجزائر، 2012.
- خالد ممدوح إبراهيم، الإثبات الالكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي الإسكندرية، 2020.
- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2010.
- طارق عفيفي صادق أحمد، نظرية الحق، المركز القومي للإصدارات القانونية، القاهرة 2016.
- مناصرة يوسف، الدليل الالكتروني في القانون الجزائي، دار الخلدونية، الجزائر، 2021.
- عماد مفلح الحسان، عز الدين أحمد النعيمي، الجرائم المستحدثة، دار الخليج للنشر والتوزيع، الأردن، 2024.
- بوبكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن منشورات الحلبي الحقوقية، الديوان الوطني للأشغال التربوية، الجزائر، 2005.
- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دار الكتب والوثائق القومية، القاهرة، 2012.

- فراس عقيل الدوبري، البيانات الضخمة ودورها في الحد من الجرائم الالكترونية في ظل استيراتيجية الأمن السبيراني، دار الخليج للنشر والتوزيع، الأردن، 2024.

3/ الرسائل والمذكرات:

- محمد صلاح محمد عبد المنعم، الجرائم الالكترونية وتحدياتها دراسة مقارنة، رسالة دكتوراه، 2005.
- خالد علي نزار الشمار، التحقيق الجنائي في الجرائم الالكترونية، رسالة دكتوراه، جامعة المنصورة، 2022.
- بن عنصر سهام، التحقيق الجنائي في الجرائم الالكترونية، مذكرة ماستر، جامعة مولود معمري، تيزي وزو، 2005.
- مباركية رابح، إجراءات التحرير والتحقيق في الجريمة الالكترونية، مذكرة ماستر، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021.

4/ المقالات والبحوث:

- الشكري عادل يوسف عبد النبي، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العراق، 2011.
- بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، الجزائر، 2018.
- عبد الصديق شيخ، الوقاية من الجرائم الالكترونية في ظل القانون رقم 04/09، مجلة معالم الدراسات القانونية والسياسية، الجزائر، 2020.
- رحموني محمد، خصائص الجريمة الالكترونيةن دراسة استراتيجيةن الجزائر، 2018.

- عراب مريم، جريمة التهديد والابتزاز الالكتروني، مجلة الدراسات القانونية المقارنة، 2021.
- فلاح عبد القادر، آيت عبد المالك نادية، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث في الدراسات القانونية والسياسية، الجزائر، 2019.
- وهيبة لعوارم، الدليل الرقمي في مجال الإثبات الجنائي وفقاً للتشريع الجزائري، المجلة الجنائية القومية، الجزائر، 2014.
- بن الطيبي مبارك، رحموني محمد، شروط قبول الدليل الرقمي كدليل الإثبات في الجريمة الالكترونية، مجلة القانون والعلوم السياسية، الجزائر، 2019.
- يؤمش مراد، القيود الواردة على الدليل الالكتروني لحجته في الإثبات الجنائي، المجلة الاكاديمية للبحوث القانونية والسياسية، الجزائر، 2023.

الفهرس

الفهرس

الملخص

الملخص

إن الموضوع الذي قمنا بدراسته والمعنون بالتحري والتحقيق في الجرائم الالكترونية له أهمية كبيرة في الدراسات القانونية والتي تتمثل في: تسليط الضوء على ماهية الجريمة الالكترونية وكيفية مواجهتها، وتوعية الأفراد بوجود سلطات قضائية تعمل على مكافحتها، وقد تمت مناقشة هذا البحث من زوايا متعددة انطلاقا من إشكالية محددة تتمثل في: كيف يمكن مواجهة الجريمة الالكترونية؟ وما هي سبل التصدي لها؟ وللإجابة عن هذه الإشكالية وضعت الخطة التالية: حيث قسمت البحث إلى فصلين حاولت من خلال الفصل الأول ذكر الأجهزة التي تعمل على التحقيق في الجرائم الالكترونية، وتم ذلك في مبحثين لكل منهما مطلبين. أما الفصل الثاني فقد تم فيه ذكر طرق التحري والتحقيق في الجرائم الالكترونية، وكذلك قسم هذا الفصل إلى مبحثين لكل منهما مطلبين حاولت من خلالهم الإجابة عن الإشكالية المطروحة، وبعد البحث وجمع المادة العلمية الخاصة بالموضوع خلصت إلى مجموعة من النتائج من أهمها: أن أي استخدام لتكنولوجيا المعلومات لأغراض غير قانونية، وبصورة سيئة يعد جريمة يعاقب عليها القانون,

وإن سهولة ارتكاب الجريمة الالكترونية لا يمنع من الوصول إلى مرتكبها ومعاقبته على ذلك وقد خصصت الدولة لذلك أجهزة قضائية وأمنية للحد من هذه الجرائم.

الكلمات المفتاحية: 1/ الجريمة الالكترونية 2/ أجهزة التحقيق في الجريمة الالكترونية

3/ التحري والتحقيق في الجرائم الالكترونية.

الملخص

The topic that we studied, entitled inquiry and investigation in cyber cimes, has a tremandous importance in legal studies which is to shed light on what cybercrime is and how to confront it, and to make individuals aware of the existence of judicial authorities working to combat it, This research was handled from multiple angles, based on a specific problematic wich is : How can cybercrime be confronted ? And what are the ways to address it ? and to solve this problematic i drew the following plan : where i divided the research into two chapters, through the first chapter, I tried to mention the services that work to investigate cyber crimes, this was done in two sections, each of which has two requirements. as for the second chapter, i mentioned the methods of inquiring and investigating in cyber crimes, ahis chapter was also divided into two sections, each with two requirements, through which I tried to answer problematic at hand .

After researching and collecting scientific material on the topic, I concluded a set of outcomes and results , the most important of wich are : that any use of information technology for illegal purposes, and in an inappropriate way is a crime punishable by law.

And the ease of committing a cybercrime does not prevent the perpetrator from being identified and punished for it,

And also the state has allocated judicial and security agencies and services to reduce these crimes.

Keywords :

1\ cybercrime 2\investigation services in cyber crimes 3\inquiry and investigation in cyber crimes .